Bitdefender ANTIVIRUS PLUS

GHIDUL UTILIZATORULUI

Bitdefender Antivirus Plus

Ghidul utilizatorului

Data publicării 19.07.2023

Aviz juridic

Avertisment și declinare a răspunderii. Acest produs și documentația acestuia sunt protejate prin drepturi de autor. Informațiile din acest document sunt furnizate „ca atare”, fără garanție. Deși au fost luate toate măsurile de precauție la pregătirea acestui document, autorii nu vor avea nicio răspundere față de nicio persoană sau entitate cu privire la orice pierdere sau daune cauzate sau presupuse a fi cauzate direct sau indirect de informațiile conținute în această lucrare.

Această carte conține link-uri către site-uri web ale terților care nu se află sub controlul Bitdefender, prin urmare Bitdefender nu este responsabil pentru conținutul niciunui site legat. Dacă accesați un site web al unei terțe părți enumerate în acest document, veți face acest lucru pe propriul risc. Bitdefender furnizează aceste link-uri doar pentru comoditate, iar includerea link-ului nu implică faptul că Bitdefender aprobă sau acceptă orice responsabilitate pentru conținutul site-ului terță parte.

Mărci comerciale. Numele mărcilor comerciale pot apărea în această carte. Toate mărcile înregistrate și neînregistrate din acest document sunt proprietatea exclusivă a proprietarilor respectivi și sunt recunoscute cu respect.

Bitdefender®

Cuprins

DESPRE ACEST GHID

Scopul și publicul vizat

Acest ghid este destinat tuturor utilizatorilor Windows care au ales Bitdefender Antivirus Plus ca soluție de securitate pentru computerele lor. Informațiile prezentate în această carte sunt potrivite nu numai pentru cunoștințele de calculator, ci sunt accesibile tuturor celor care sunt capabili să lucreze cu un PC Windows.

Veți afla cum să configurați și să utilizați Bitdefender Antivirus Plus pentru a vă proteja împotriva amenințărilor și a altor programe rău intenționate. Veți învăța cum să obțineți tot ce este mai bun din dvs Bitdefender.

Vă dorim o prelegere plăcută și utilă.

Cum să utilizați acest ghid

Acest ghid este organizat în jurul mai multor subiecte majore:

Introducere (pagina 14)

Începeți cu Bitdefender Antivirus Plus și cu interfața sa de utilizator.

Gestionarea securității (pagina 47)

Aflați cum să utilizați Bitdefender Antivirus Plus pentru a vă proteja împotriva software-ului rău intenționat.

Cum să (pagina 102)

Aflați mai multe despre Bitdefender Antivirus Plus.

Obține ajutor (pagina 149)

Unde să cauți și unde să ceri ajutor dacă apare ceva neașteptat.

Convenții utilizate în acest ghid

Convenții tipografice

Manualul conține diferite stiluri de text, pentru o lectură cât mai ușoară. Aspectul și semnificația acestora sunt prezentate în tabelul de mai jos.

Aspect	Descriere
`sample syntax`	Exemplele de sintaxă sunt imprimate cu caractere `monospaced`.
https://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
documentation@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.
Despre acest Ghid (pagina 1)	Acesta este un link intern, care vă direcționează către o locație din document.
`filename`	Fișierul și directoarele sunt tipărite folosind `monospaced` font.
opțiune	Toate opțiunile de produs sunt imprimate folosind caractere **îngroșate**.
cuvânt cheie	Cuvintele cheie sau expresiile importante sunt evidențiate folosind caractere **îngroșate**.

Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

Nota

Nota este o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect relevant.

Important

Segmentele marcate astfel necesită atenția ta și nu este recomandat să le omiți. De obicei, aici sunt furnizate informații importante, dar nu esențiale.

Avertizare

Acestea sunt informații esențiale, care trebuie tratate cu o atenție deosebită. Dacă urmezi indicațiile, nu se va întâmpla nimic rău. Este recomandat să citești și să înțelegi despre ce este vorba, deoarece aici se descrie ceva extrem de riscant.

Comentarii

Te invităm să participi la procesul de îmbunătățire al manualului. Toate informațiile prezentate au fost testate și verificate în mod riguros. Te rugăm să ne scrii despre orice inexactități pe care le vei găsi în acest manual, precum și să propui moduri prin care îl putem îmbunătăți, astfel încât să îți putem furniza o documentație ireproșabilă.

Anunțați-ne trimițând un e-mail la documentation@bitdefender.com. Scrieți toate e-mailurile dvs. legate de documentație în engleză, astfel încât să le putem procesa eficient.

1. INSTALARE

1.1. Pregătirea pentru instalare

Pentru a instala Bitdefender Antivirus Plus fără probleme, trebuie sa parcurgi acești pași prealabili:

- Asigurați-vă dacă dispozitivul pe care doriți să instalați Bitdefender îndeplinește cerințele de sistem. În cazul în care dispozitivul nu întrunește toate cerințele de sistem, Bitdefender nu va fi instalat sau nu va funcționa în mod corespunzător, determinând reducerea vitezei de funcționare și instabilitatea sistemului. Pentru o listă completă a cerințelor de sistem, consultă Cerințe de sistem (pagina 4).
- Autentifica-te pe dispozitiv cu datele unui cont de administrator.
- Dezinstalează orice alt program similar de pe dispozitiv. Dacă se detectează ceva în timpul procesului de instalare Bitdefender, vei primi o notificare de dezinstalare. Rularea simultană a două programe de securitate poate afecta funcționarea lor și poate provoca probleme majore ale sistemului. Windows Defender va fi dezactivat în timpul instalării.
- Dezactivează sau dezinstalează orice alt program firewall de pe dispozitiv. Rularea simultană a două programe firewall poate afecta funcționarea lor și poate provoca probleme majore ale sistemului. Windows Firewall va fi dezactivat în timpul instalării.
- Se recomandă ca, în timpul instalării, dispozitivul tău să fie conectat la internet, chiar atunci când instalarea se face de pe un CD/DVD. Dacă sunt disponibile versiuni mai noi ale fișierelor aplicației decât cele incluse în pachetul de instalare, Bitdefender le va descărca și le va instala.

1.2. Cerințe de sistem

Poți instala Bitdefender Antivirus Plus doar pe dispozitive pe care rulează următoarele sisteme de operare:

- Windows 7 cu Service Pack 1
- Windows 8

- Windows 8.1
- Windows 10
- 2,5 GB spațiu liber disponibil pe hard disk (cel puțin 800 MB pe unitatea de sistem)
- 2 GB de memorie (RAM)

Important

* Performanța sistemului poate fi afectată pe dispozitivele care au procesoare de generație mai veche.

Notă

Pentru a afla pe ce sistem de operare funcționează dispozitivul tău și informațiile referitoare la hardware:

- În **Windows 7** fă clic dreapta pe **Computerul meu** de pe desktop și apoi selectează **Proprietăți** din meniu.
- În **Windows 8**, din ecranul de start, identifică **Computer** (de exemplu, poți începe să tastezi „Computer" direct în ecranul Start), apoi fă clic dreapta pe pictograma sa. În **Windows 8.1**, identifică **Acest PC**.

  Selectează **Proprietăți** din meniul din partea de jos. Caută în zona **Sistem** pentru a afla informații referitoare la tipul de sistem.
- În **Windows 10**, tastează **Sistem** în câmpul de căutare din bara de activități și apoi fă clic pe pictograma sa. Consultă zona **Sistem** pentru a afla informații despre tipul tău de sistem.

1.3. Cerințe software

Pentru a putea utiliza Bitdefender și toate funcțiile sale, dispozitivul tău trebuie să întrunească următoarele cerințe software:

- Microsoft Edge 40 sau superior
- Internet Explorer 10 sau o variantă mai recentă
- Mozilla Firefox 51 și o versiune mai recentă
- Google Chrome 34 și o versiune mai recentă
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 sau mai recent

1.4. Instalarea produsului dumneavoastră Bitdefender

Poți instala Bitdefender folosind CD-ul de instalare sau aplicația web descărcată pe dispozitivul tău **Bitdefender Central**.

Dacă produsul achiziționat acoperă mai multe dispozitive, repetă procesul de instalare și activează produsul utilizând același cont pe fiecare dispozitiv. Contul pe care trebuie să îl utilizezi este cel care conține abonamentul tău activ Bitdefender.

1.4.1. Instalare din Bitdefender Central

Din Bitdefender Central puteți descărca kitul de instalare corespunzător abonamentului achiziționat. Odată ce procesul de instalare s-a finalizat, Bitdefender Antivirus Plus este dezactivat.

Pentru a descărca Bitdefender Antivirus Plus din Bitdefender Central:

1. Accesează **Bitdefender Central**.
2. Accesează secțiunea **Dispozitivele mele** și apoi apasă pe **INSTALEAZĂ PROTECȚIA**.
3. Alege una dintre cele doua opțiuni disponibile:
   - **Protejează acest dispozitiv**
     a. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
     b. Salvează fișierul de instalare.
   - **Protejează alte dispozitive**
     a. Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
     b. Apăsați pe **TRIMITE LINK DE DESCĂRCARE**.
     c. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**.

Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

d. Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

4. Așteaptă să se finalizeze descărcarea și apoi execută aplicația de instalare.

Validarea instalării

Bitdefender va verifica mai întâi sistemul tău pentru a valida instalarea.

Dacă sistemul tău nu îndeplinește cerințele pentru instalarea Bitdefender, vei fi informat cu privire la aspectele care trebuie îmbunătățite înainte de a putea continua.

Dacă este detectat o soluție antivirus necompatibilă sau o versiune mai veche a Bitdefender, vi se va cere să le ștergeți de pe sistemul dumneavoastră. Vă rugăm să urmați instrucțiunile pentru a șterge software-ul din sistemul dumneavoastră, evitând astfel apariția problemelor pe viitor. Este posibil să fie nevoie să pornești dispozitivul pentru a finaliza dezinstalarea soluțiilor antivirus detectate.

Actualizăm în permanență pachetul de instalare al Bitdefender Total Security.

Notă
Descărcarea fișierelor de instalare poate dura foarte mult, cu precădere în cazul conexiunilor internet mai lente.

Odată ce instalarea a fost validată, se afișează asistentul de configurare. Urmează pașii pentru a instala Bitdefender Antivirus Plus.

Pasul 1 - Instalarea Bitdefender

Înainte de a începe instalarea, este necesar să îți exprimi acordul cu privire la Contractul de abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Antivirus Plus.

Dacă nu ești de acord cu acești termeni, închide fereastra. Procesul de instalare va fi abandonat și vei ieși din fereastra de instalare.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Menține opțiunea **Trimite rapoarte despre produs** activă. Prin permiterea acestei opțiuni, sunt trimise rapoarte către serverele Bitdefender, conținând informații despre modul în care utilizezi produsul. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să îți oferim produse și mai bune pe viitor. Rapoartele nu conțin date confidențiale, cum ar fi numele tău sau adresa IP, și nu vor fi folosite în scopuri comerciale.
- Selectează limba în care dorești să instalezi produsul.

Efectuează clic pe **INSTALARE** pentru a lansa procesul de instalare al produsului tău Bitdefender.

Pasul 2 - Instalare în curs de desfășurare

Așteaptă până când instalarea este finalizată. Sunt afișate informații detaliate cu privire la evoluția instalării.

Pasul 3 - Instalare finalizată

Produsul tău Bitdefender a fost instalat cu succes.

Este afișat rezumatul instalării. Dacă, în timpul instalării, este detectată și dezinstalată o amenințare, poate fi necesară o repornire a sistemului.

Pasul 4 - Analiza dispozitivului

Acum vei fi întrebat dacă dorești să efectuezi o analiză a dispozitivului tău, pentru a te asigura că este în siguranță. În timpul acestui pas, Bitdefender va scana zonele critice ale sistemului. Selectează **Începe analiza dispozitivului** pentru a o iniția.

Poți ascunde interfața de scanare selectând **Rulează scanarea în fundal**. Apoi, alege dacă vrei să fii anunțat când se va încheia scanarea sau nu.

După finalizarea scanării, selectează **Deschide interfața Bitdefender**.

> **Notă**
> În mod alternativ, dacă nu dorești să efectuezi scanarea, poți selecta **Omite**.

Pasul 5 - Primii pași

În fereastra **Primii pași**, poți vizualiza detaliile abonamentului tău activ.

Apasă pe **FINALIZARE** pentru a accesa interfața Bitdefender Antivirus Plus.

1.4.2. Instalare de pe discul de instalare

Pentru a instala Bitdefender de pe discul de instalare, introdu CD-ul în unitatea optică.

În câteva momente se va afișa fereastra de instalare. Urmează instrucțiunile pentru a începe instalarea.

Dacă nu apare ecranul de instalare, utilizează Windows Explorer pentru a parcurge directorul rădăcină al CD-ului și efectuează dublu clic pe fișierul `autorun.exe`.

În cazul în care viteza ta de internet este slabă sau sistemul tău nu este conectat la internet, efectuează clic pe butonul **Instalare de pe CD/DVD**. În acest caz, va fi instalat produsul Bitdefender disponibil pe disc și o versiune mai nouă se va descărca de pe serverele Bitdefender prin intermediul actualizărilor de produs.

Validarea instalării

Bitdefender va verifica mai întâi sistemul tău pentru a valida instalarea.

Dacă sistemul tău nu îndeplinește cerințele pentru instalarea Bitdefender, vei fi informat cu privire la aspectele care trebuie îmbunătățite înainte de a putea continua.

Dacă este detectat o soluție antivirus necompatibilă sau o versiune mai veche a Bitdefender, vi se va cere să le ștergeți de pe sistemul dumneavoastră. Vă rugăm să urmați instrucțiunile pentru a șterge software-ul din sistemul dumneavoastră, evitând astfel apariția problemelor pe viitor. Este posibil să fie nevoie să pornești dispozitivul pentru a finaliza dezinstalarea soluțiilor antivirus detectate.

Actualizăm în permanență pachetul de instalare al Bitdefender Total Security.

Notă
Descărcarea fișierelor de instalare poate dura foarte mult, cu precădere în cazul conexiunilor internet mai lente.

Odată ce instalarea a fost validată, se afișează asistentul de configurare. Urmează pașii pentru a instala Bitdefender Antivirus Plus.

Pasul 1 - Instalarea Bitdefender

Înainte de a continua cu instalarea, trebuie să fiți de acord cu Acordul de abonament. Vă rugăm să luați ceva timp pentru a citi Acordul de abonare, deoarece conține termenii și condițiile în care puteți utiliza Bitdefender Antivirus Plus.

Dacă nu sunteți de acord cu acești termeni, închideți fereastra. Procesul de instalare va fi abandonat și veți părăsi configurarea.

Două sarcini suplimentare pot fi efectuate la acest pas:

- Păstrează **Trimite rapoarte despre produse** opțiunea activată. Permițând această opțiune, rapoartele care conțin informații despre modul în care utilizați produsul sunt trimise către serverele Bitdefender. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să oferim o experiență mai bună în viitor. Rețineți că aceste rapoarte nu conțin date confidențiale, cum ar fi numele sau adresa dvs. IP și că nu vor fi utilizate în scopuri comerciale.
- Selectați limba în care doriți să instalați produsul.

Clic **INSTALARE** pentru a lansa procesul de instalare a produsului dvs. Bitdefender.

Pasul 2 - Instalare în curs

Așteptați finalizarea instalării. Sunt afișate informații detaliate despre progres.

Pasul 3 - Instalarea s-a încheiat

Este afișat un rezumat al instalării. Dacă orice amenințare activă a fost detectată și eliminată în timpul instalării, poate fi necesară o repornire a sistemului.

Pasul 4 - Analiza dispozitivului

Acum veți fi întrebat dacă doriți să efectuați o analiză a dispozitivului dvs., pentru a vă asigura că este în siguranță. În timpul acestui pas, Bitdefender va scana zonele critice ale sistemului. Clic **Porniți Analiza dispozitivului** pentru a-l iniția.

Puteți ascunde interfața de scanare făcând clic pe **Rulați Scanarea în fundal**. După aceea, alegeți dacă doriți să fiți informat când scanarea este terminată sau nu.

După finalizarea scanării, selectează **Continuă cu Creare cont**.

> **Notă**
> Alternativ, dacă nu doriți să efectuați scanarea, puteți pur și simplu să faceți clic pe **Ocolire**.

Pasul 5 - Contul Bitdefender

După terminarea configurării inițiale vei vedea fereastra Bitdefender Account. Ai nevoie de un cont Bitdefender pentru a activa produsul și pentru a utiliza funcționalitățile online ale acestuia. Pentru mai multe informații, consultă capitolul Bitdefender Central (pagina 30).

Continuă în funcție de situația ta.

- **Vreau să creez un cont Bitdefender**

  1. Introduceți informațiile solicitate în câmpurile corespunzătoare. Informațiile furnizate aici vor rămâne confidențiale. Parola trebuie să aibă o lungime de minimum 8 caractere, să includă cel puțin o cifră sau un simbol și să includă litere mici și mari.
  2. Înainte de a merge mai departe este necesar să îți exprimi acordul cu privire la Condițiile de utilizare. Accesează secțiunea Condiții de utilizare și citește-le cu atenție întrucât conțin termenii și condițiile care îți permit utilizarea Bitdefender.
     Suplimentar, poți accesa și citi Politica de confidențialitate.
  3. Fă clic pe **CREARE CONT**.

     > **Notă**
     > O dată ce contul este creat, poți utiliza adresa de e-mail și parola furnizate pentru a te autentifica în contul tău la https://central.bitdefender.com sau în aplicația Bitdefender Central dacă aceasta este instalată pe unul dintre dispozitivele tale Android sau iOS. Pentru a instala aplicația Bitdefender Central pe Android, este necesar să accesezi Google Play, să cauți Bitdefender Central, iar apoi să apeși pe opțiunea de instalare corespunzătoare. Pentru a instala aplicația Bitdefender Central pe iOS, este necesar să accesezi App Store, să cauți Bitdefender Central, iar apoi să apeși pe opțiunea de instalare corespunzătoare.

- **Am deja un cont Bitdefender**

1. Fă clic pe **Autentificare**.
2. Introdu adresa de e-mail în câmpul corespunzător, apoi fă clic pe **MAI DEPARTE**.
3. Introdu parola și apoi efectuează clic pe **AUTENTIFICARE**.
   Dacă ai uitat parola contului tău sau dacă pur și simplu dorești să o resetezi pe cea existentă deja:
   a. Fă clic pe **Ai uitat parola?**.
   b. Introdu adresa ta de e-mail, apoi selectează opțiunea **ÎNAINTE**.
   c. Verificați-vă contul de e-mail, introduceți codul de securitate primit și apoi faceți clic pe **MAI DEPARTE**.
      Alternativ, puteți face clic pe **Schimbare parolă** din mesajul e-mail pe care vi l-am trimis.
   d. Tastează noua parolă pe care vrei să o setezi, apoi tasteaz-o din nou. Apasă pe **SALVARE**.

   Notă
   Dacă ai deja un cont MyBitdefender, îl poți utiliza pentru a te conecta la contul Bitdefender. Dacă ți-ai uitat parola, întâi trebuie să mergi la https://my.bitdefender.com pentru a o reseta. Apoi, utilizează datele de autentificare actualizate pentru a te conecta la contul Bitdefender.

○ **Doresc să mă autentific prin intermediul contului de Microsoft, Facebook sau Google**

Pentru autentificare cu contul tău de Microsoft, Facebook sau Google:

1. Selectați serviciul pe care doriți să îl utilizați. Veți fi redirecționat către pagina de autentificare a acelui serviciu.
2. Urmați instrucțiunile oferite de serviciul selectat pentru a face legătura dintre contul dumneavoastră și Bitdefender.

Notă
Bitdefender nu are acces la informații confidențiale, precum parola contului pe care te autentifici de obicei sau datele personale ale prietenilor și contactelor.

Pasul 6 - Activați-vă produsul

Notă
Această etapă apare dacă ai selectat crearea unui nou cont Bitdefender pe parcursul etapei anterioare sau dacă te-ai autentificat utilizând un cont aferent unui abonament care a expirat.

Este necesară o conexiune activă la internet pentru a finaliza activarea produsului.

Procedează în funcție de situația ta:

- Am un cod de activare
  În acest caz, activează produsul urmând acești pași:

  1. Introdu codul de activare în câmpul Am un cod de activare și apoi fă clic pe **CONTINUĂ**.

     Notă
     Iată cum poți găsi codul tău de activare:

     - pe eticheta de la CD/DVD.
     - pe certificatul de înregistrare al produsului.
     - în e-mailul de achiziționare online.

  2. **Vreau să evaluez Bitdefender**
     În acest caz, poți utiliza produsul pentru o perioadă de 30 de zile. Pentru a începe perioada de evaluare, selectează **Nu am un abonament, vreau să încerc gratuit produsul** apoi fă clic pe **CONTINUĂ**.

Pasul 7 - Primii pași

În fereastra **Primii pași**, poți vizualiza detaliile abonamentului tău activ.

Clic **FINALIZAREA** pentru a accesa Bitdefender Antivirus Plus interfata.

2. INTRODUCERE

2.1. Informații de bază

Odată ce ai instalat Bitdefender Antivirus Plus, dispozitivul tău este protejat împotriva tuturor tipurilor de amenințări (cum ar fi programe periculoase, programe spion, ransomware, exploit-uri, botnet-uri și troieni) și a amenințărilor de pe internet (cum ar fi hackeri, atacurile de tip phishing și mesajele spam).

Aplicația utilizează tehnologia Photon pentru a mări viteza și performanțele procesului de scanare a amenințărilor. Funcționează prin preluarea modelelor de utilizare ale aplicațiilor din sistemul dvs. pentru a ști ce anume și când să scaneze, reducând astfel la minimum impactul asupra performanțelor sistemului dvs.

Conectarea fără protecție la rețele wireless publice din aeroporturi, mall-uri, cafenele sau hoteluri poate fi periculoasă pentru dispozitivul și datele tale. Principalul motiv pentru aceasta este faptul că cei care comit fraude ar putea să-ți monitorizeze activitatea și să găsească cel mai bun moment pentru a-ți fura fura datele personale, dar și faptul că oricine îți poate vedea adresa IP, transformând astfel sistemul tău într-o victimă a viitoarelor atacuri cibernetice. Pentru a evita astfel de situații nefericite, instalează și utilizează aplicația VPN (pagina 84).

Protecție cameră web Împiedică aplicațiile nesigure să acceseze camera ta video, evitând astfel orice încercare de hacking. În funcție de alegerea utilizatorilor Bitdefender, accesul aplicațiilor folosite în mod frecvent la camera dvs. web va fi permis sau blocat.

Pentru a te proteja de potențialii curioși și spioni atunci când dispozitivul tău este conectat la o rețea wireless nesecurizată, Bitdefender analizează nivelul său de securitate și, dacă este necesar, oferă recomandări pentru a spori siguranța activităților tale online. Pentru instrucțiuni despre cum îți poți păstra în siguranță datele personale, consultați secțiunea Evaluare securitate Wi-Fi (pagina 75).

Fișierele criptate de ransomware pot fi acum recuperate fără a cheltui bani pe recompense. Pentru informații despre modul de recuperare a fișierelor criptate, accesează Remediere ransomware (pagina 79).

În timp ce lucrați, jucați jocuri sau vizionați filme, Bitdefender vă poate oferi o experiență neîntreruptă a utilizatorului prin amânarea sarcinilor

de întreținere, eliminarea întreruperilor și ajustarea efectelor vizuale ale sistemului. Puteți beneficia de toate acestea activând și configurând opțiunea Profiluri (pagina 94).

Bitdefender va lua majoritatea deciziilor legate de securitate în locul dumneavoastră și va afișa rareori alerte pop-up. În fereastra Notificări sunt disponibile detalii despre acțiunile aplicate și informații cu privire la funcționarea programului. Pentru mai multe informații, consultă capitolul Notificări (pagina 15).

Din când în când, va trebui să deschizi Bitdefender și să remediezi problemele existente. Este posibil să trebuiască să configurezi anumite componente Bitdefender sau să iei măsuri de prevenție pentru a-ți proteja dispozitivul și datele.

Pentru a folosi caracteristicile online ale Bitdefender Antivirus Plus și pentru administrarea abonamentelor și dispozitivelor dumneavoastră, accesați-vă contul Bitdefender. Pentru mai multe informații, consultă capitolul Bitdefender Central (pagina 30).

În secțiunea Cum să (pagina 102) vei găsi instrucțiuni pas cu pas despre cum să realizezi cele mai obișnuite sarcini. Dacă întâmpini probleme atunci când utilizezi Bitdefender, verifică secțiunea Soluționarea problemelor frecvente (pagina 130) pentru a vedea soluții posibile la cele mai des întâlnite probleme.

2.1.1. Notificări

Bitdefender menține un jurnal detaliat al evenimentelor legate de activitatea sa pe dispozitivul tău. Ori de câte ori se întâmplă un lucru relevant pentru securitatea sistemului sau datelor tale, în zona Notificări Bitdefender apare un mesaj nou, ca și când ai primi un e-mail nou în Inboxul tău.

Notificările reprezintă un instrument important pentru monitorizarea și gestionarea protecției Bitdefender. De exemplu, poți verifica cu ușurință dacă actualizarea a fost efectuată cu succes, dacă au fost detectate amenințări sau vulnerabilități pe dispozitvul tău, etc. În plus, puteți lua măsuri suplimentare, dacă este cazulsau modifica măsurile luate de Bitdefender.

Pentru a accesa jurnalul de **Notificări**, fă clic pe Notificări din meniul de navigare al **interfeței Bitdefender**. De fiecare dată când se produce un

eveniment critic, se poate observa modificarea contorului pe pictograma .

În funcție de tip și severitate, notificările sunt grupate în:

- Evenimentele **importante** indică problemele principale. Acestea ar trebui verificate imediat.
- Evenimentele de tip **Avertizare** indică probleme care nu sunt de foarte mare importanță. Puteți să le verificați și să le remediați oricând aveți timp.
- Evenimentele de tip **Informații** indică operațiile finalizate cu succes.

Fă clic pe fiecare filă pentru mai multe detalii despre evenimentele generate. Detaliile pe scurt sunt afișate la un singur clic pe titlul fiecărui eveniment, respectiv: o scurtă descriere, acțiunea pe care Bitdefender a întreprins-o atunci când a survenit, precum și data și ora producerii evenimentului. Pot fi setate diverse opțiuni prin intermediul cărora să fie aplicații și alte acțiuni, dacă este necesar.

Pentru a te ajuta să gestionezi cu ușurință evenimentele înregistrate, ferestra Notificări oferă opțiuni de ștergere sau marcare ca citite a tuturor evenimentelor din secțiunea respectivă.

2.1.2. Profiluri

Unele activități efectuate pe calculator, cum ar fi jocurile online sau prezentările video, necesită o viteză sporită de reacție și funcționare superioară a sistemului, fără întreruperi. Când laptopul dvs se alimentează de la baterie, este recomandat să amânați operațiile cu consum mare de energie până când laptopul este conectat din nou la o priză.

Bitdefender Profiles alocă mai multe resurse de sistem aplicațiilor care rulează prin modificarea temporară a setărilor de protecție și prin ajustarea configurației sistemului. Prin urmare, impactul sistemului asupra activității tale este redus la minimum.

Pentru adaptarea la diferite activități, Bitdefender este furnizat cu următoarele profiluri:

Profil Lucru

Optimizează eficiența activității tale prin identificarea și ajustarea setărilor produsului și ale sistemului.

Profil Film

Sporește efectele vizuale și elimină întreruperile în timpul vizionării filmelor.

Profil Joc

Sporește efectele vizuale și elimină întreruperile în timpul jocurilor.

Profil rețea Wi-FI publică

Aplică setările de produs pentru a beneficia de protecție completă în timpul conexiunii la o rețea wireless nesecurizată.

Profil Mod baterie

Aplică setările de produs și menține redusă activitatea din fundal pentru a economisi bateria.

Configurează activarea automată a profilurilor

Pentru o experiență ușor de utilizat, poți configura Bitdefender pentru gestionarea profilului tău de lucru. În acest caz, Bitdefender detectează automat activitatea derulată și aplică setările de optimizare a sistemului și produsului.

Prima dată când accesezi **Profiluri** ți se va solicita să activezi profilurile automate. Pentru aceasta, poți selecta **ACTIVARE** în fereastra afișată.

Poți selecta **NU ACUM** dacă dorești să activezi funcția mai târziu.

Pentru a permite Bitdefender să activeze automat profilurile:

1. Efectuează clic pe **Instrumente** din meniul de navigare al interfeței **Bitdefender**.
2. În fila **Profiluri**, apasă pe **Setări**.
3. Folosiți butonul corespunzător pentru a activa funcția **Activați profilurile automat**.

Dacă nu dorești activarea automată a Profilurilor, oprește funcția de la buton.

Pentru a activa manual un profil, pornește butonul corespunzător. Dintre primele trei profiluri, doar unul poate fi activat manual imediat.

Pentru mai multe informații despre Profiluri, consultă Profiluri (pagina 94).

2.1.3. Protecție cu parolă pentru setările Bitdefender

Dacă nu ești singura persoană cu drepturi administrative care folosește acest dispozitiv, este recomandat să îți protejezi setările Bitdefender cu o parolă.

Pentru a configura protecția cu parolă pentru setările Bitdefender:

1. Fă clic pe **Setări** din meniul de navigare al **interfeței Bitdefender**.
2. În fereastra **Setări generale**, activează **Protecție prin parolă**.
3. Introdu parola în cele două câmpuri și efectuează clic pe OK. Parola trebuie să aibă cel puțin 8 caractere.

După ce ați setat o parolă, aceasta va trebuie introdusă de fiecare dată când cineva încearcă să modifice setările Bitdefender.

Important
Vă sfătuim să rețineți parola sau să o notați și să o păstrați într-un loc sigur. Dacă ați uitat parola, trebuie să reinstalați programul sau să contactați Bitdefender pentru asistență.

Pentru a elimina protecția cu parolă:

1. Clic **Setări** din meniul de navigare de pe Interfața Bitdefender.
2. În fereastra **Setări generale**, dezactivează **Protecție prin parolă**.
3. Introdu parola și efectuează clic pe **OK**.

Notă
Pentru a modifica parola produsului tău, efectuează clic pe **Modificare parolă**. Introdu parola actuală și apoi efectuează clic pe **OK**. În fereastra afișată, introduceți noua parolă pe care doriți să o utilizați de acum înainte pentru a restricționa accesul la setările produsului dumneavoastră Bitdefender.

2.1.4. Rapoarte despre produs

Rapoartele de produs conțin informații despre modul în care utilizezi produsul Bitdefender pe care l-ai instalat. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să vă oferim produse și mai bune pe viitor.

Te rugăm să reții că aceste rapoarte nu conțin date confidențiale, cum ar fi numele sau adresa ta IP și că acestea nu vor fi utilizate în scopuri comerciale.

Dacă ai ales în timpul procesului de instalare să expediezi astfel de rapoarte către serverele Bitdefender, iar acum dorești să oprești procesul:

1. Clic **Setări** din meniul de navigare de pe Interfața Bitdefender.
2. Selectează fila **Setări avansate**.
3. Dezactivează **Rapoarte produs**.

2.1.5. Notificări privind ofertele speciale

Atunci când sunt disponibile oferte promoționale, produsul Bitdefender este configurat să te notifice prin intermediul unei ferestre de tip pop-up. Aceasta îți oferă oportunitatea de a beneficia de prețuri avantajoase și de a-ți menține dispozitivele protejate pentru o perioadă mai lungă de timp.

Pentru a activa sau dezactiva notificările privind ofertele speciale:

1. Clic **Setări** pe meniul de navigare de pe Interfața Bitdefender.
2. În fereastra **General**, pornește sau oprește butonul corespunzător.

Opțiunea de Oferte speciale și notificări de produse este activată implicit.

2.2. Interfața Bitdefender

Bitdefender Antivirus Plus îndeplinește deopotrivă cerințele persoanelor experimentate și pe cele ale începătorilor în utilizarea calculatorului. Interfața sa grafică este proiectată pentru a se potrivi fiecărei categorii de utilizatori.

Pentru a parcurge interfața Bitdefender, în partea din stânga sus este afișat un asistent de introducere care conține detalii despre cum să interacționezi cu produsul și cum să îl configurezi. Selectează săgeata dreapta pentru a continua să primești indicații sau **Renunță la tur** pentru a închide asistentul.

Pictograma din bara de sistem Bitdefender este disponibilă în orice moment, indiferent dacă dorești să deschizi fereastra principală, să rulezi o actualizare de produs sau să vizualizezi informațiile referitoare la versiunea instalată.

Fereastra principală îți oferă informații cu privire la starea ta de securitate. În funcție de utilizarea și necesitățile dispozitivului tău, **Autopilot** afișează aici diferite tipuri de recomandări care să te ajute să îmbunătățești securitatea și performanța dispozitivului tău. Mai mult, poți adăuga

acțiunile rapide pe care le utilizezi cel mai mult, astfel încât să le poți avea la îndemână oricând ai nevoie de ele.

Din meniul de navigare din partea stângă poți accesa zona de setări, notificări și **secțiunile Bitdefender** pentru o configurare detaliată și sarcini administrative avansate.

Din partea superioară a interfeței principale, poți accesa contul tău **Bitdefender**. De asemenea, ne poți contacta pentru asistență în cazul în care ai întrebări sau intervine ceva neașteptat.

2.2.1. Pictograma barei de sistem

Pentru a administra întregul produs mai rapid, poți utiliza pictograma Bitdefender din bara de sistem.

Notă

Este posibil ca pictograma Bitdefender să nu fie mereu vizibilă. Pentru ca pictograma să fie afișată permanent:

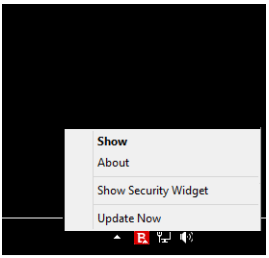
- În **Windows 7, Windows 8 și Windows 8.1**
  1. Apasă pe săgeata din colțul din dreapta jos al ecranului.
  2. Faceți clic pe **Personalizare...** pentru a deschide fereastra Pictogramelor din zona notificărilor.
  3. Selectează opțiunea **Arată pictograme și notificări** pentru a vedea pictograma **Agent Bitdefender**.
- În **Windows 10**
  1. Clic dreapta pe bara de activități și selectează **Setări bară de activități**
  2. Derulează în jos și fă clic pe linkul **Selectează ce pictograme apar în bara de activități** din **Zona de notificări**.
  3. Activează butonul de lângă **Agent Bitdefender**.

Dacă faceți dublu-clic pe această iconiță, se va deschide fereastra BitDefender. De asemenea, făcând clic-dreapta pe iconiță, un meniu contextual vă va oferi posibilitatea unei administrări rapide a BitDefender.

- **Afișează** - deschide fereastra principală a Bitdefender.
- **Despre** - se deschide o fereastră din care poți afla informații despre Bitdefender, poți afla unde poți căuta dacă ai nevoie de ajutor în cazul în care apare o situație neașteptată, unde poți accesa și

vizualiza Contractul de abonament, Componentele Terților și Politica de Confidențialitate.

- **Actualizează acum** - inițiază o actualizare imediată. Poți urmări starea actualizării în secțiunea Actualizare din **fereastra Bitdefender** principală.



Iconița Bitdefender din bara de sistem te informează despre problemele care îți afectează dspozitivul sau despre funcționarea produsului, prin afișarea unui simbol special, după cum urmează:

Nu există probleme care afectează securitatea sistemului tău.

Probleme grave de securitate afectează sistemului tău. Acestea necesită atenția ta imediat și trebuie remediate în cel mai scurt timp.

Dacă Bitdefender nu funcționează, pictograma barei de sistem este afișată pe un fundal gri: . Acest lucru se întâmplă de obicei atunci când expiră abonamentul. De asemenea, se poate întâmpla și când serviciile Bitdefender nu răspund sau când alte erori afectează funcționarea normală a Bitdefender.

2.2.2. Meniu de navigare

În partea stângă a interfeței Bitdefender se află meniul de navigare, care îți permite să accesezi rapid caracteristicile și instrumentele Bitdefender de care ai nevoie pentru a îți gestiona produsul. Secțiunile disponibile în această zonă sunt:

- **Panoul de comandă**. De aici, poți rezolva rapid problemele de securitate, poți vizualiza recomandările în funcție de necesitățile sistemului tău și modelele de utilizare, poți realiza acțiuni rapide și poți instala Bitdefender pe alte dispozitive.
- **Protecție**. De aici, poți lansa și configura scanări efectuate de antivirus, accesa setările Firewall, recupera date în cazul în care sunt

criptate de ransomware și configura protecția în timp ce navighezi pe internet.

- **Confidențialitate**. De aici, poți crea configurații Password Manager pentru conturile tale online, poți proteja accesul la camera ta web împotriva privirilor indiscrete, poți efectua plăți online într-un mediu sigur, poți deschide aplicația VPN și îți poți proteja copiii prin vizualizarea și restricționarea activității lor online.
- **Utilități**. De aici poți optimiza viteza sistemului tău și poți configura caracteristica Anti-theft pentru dispozitivele tale.
- **Notificări**. De aici, ai acces la notificările generate.
- **Setări**. De aici, ai acces la setările generale.
- **Asistență**. De aici poți contacta departamentul de Asistență Tehnică de la Bitdefender, oricând ai nevoie de ajutor pentru a remedia o situație în legătură cu Bitdefender Antivirus Plus.
- **Contul meu**. De aici, îți poți accesa contul tău Bitdefender pentru a verifica abonamentele și a efectua sarcinile de securitate pe dispozitivele pe care le administrezi. Sunt de asemenea disponibile detalii despre contul Bitdefender și despre abonamentul în curs.

2.2.3. Panou de bord

Fereastra panou de control îți permite să efectuezi sarcini obișnuite, să rezolvi rapid problemele de securitate, să vizualizezi informații despre utilizarea produsului și să accesezi secțiunile din care poți configura setările produsului.

Poți accesa orice opțiune prin doar câteva clicuri.

Fereastra conține trei secțiuni principale:

Zona Stare securitate

De aici poți verifica starea de securitate a dispozitivului tău.

Autopilot

De aici poți verifica recomandările Autopilot pentru a asigura funcționarea corectă a sistemului.

Acțiuni rapide

Aici poți executa diverse sarcini pentru a-ți menține sistemul protejat și capabil să funcționeze la viteză optimă. Poți de asemenea instala

Bitdefender pe alte dispozitive, cu condiția ca abonamentul tău să aibă suficiente sloturi disponibile.

Zonă stare securitate

Bitdefender utilizează un sistem de monitorizare a problemelor pentru a detecta și pentru a vă informa în legătură cu aspectele care pot afecta securitatea dispozitivului și datelor tale. Problemele depistate pot include setări de protecție importante care au fost dezactivate, precum și alte condiții care pot reprezenta un risc de securitate.

Oricând există probleme care afectează securitatea dispozitivului tău, starea care apare în partea superioară a **interfeței Bitdefender** se modifică în roșu. Starea afișată indică tipul problemelor care îți afectează sistemul. De asemenea, pictograma **barei de sistem** se modifică în și dacă muți cursorul mouse-ului peste pictogramă, o fereastră pop-up va confirma existența unor probleme care așteaptă să fie remediate.

Întrucât problemele detectate pot împiedica Bitdefender să te protejeze împotriva amenințărilor sau reprezintă un risc major de securitate, îți recomandăm să fii atent și să le rezolvi în cel mai scurt timp. Pentru a rezolva o problemă, efectuează clic pe butonul de lângă problema detectată.

Autopilot

Pentru a-ți oferi o funcționare eficientă și o protecție sporită în timp ce desfășori diferite activități, Bitdefender Autopilot va acționa ca asistentul tău personal în materie de securitate. În funcție de activitatea pe care o desfășori, fie că e vorba de activități profesionale, de efectuarea de plăți online, vizionarea de filme sau de jocuri, Bitdefender Autopilot îți va oferi recomandări contextuale în funcție de modul de utilizare a dispozitivului tău și nevoile tale.

Recomandările propuse pot fi de asemenea legate de acțiuni pe care trebuie să le efectuezi pentru a îți menține produsul funcțional la capacitate maximă.

Pentru a începe să utilizezi o funcție sugerată sau să faci îmbunătățiri la produsul tău, efectuează clic pe butonul corespunzător.

Dezactivarea notificărilor trimise de Autopilot

Pentru a te informa cu privire la recomandările Autopilot, produsul Bitdefender este setat să te notifice printr-o fereastră pop-up.

Pentru a dezactiva notificările Autopilot:

1. Clic **Setări** din meniul de navigare de pe Interfața Bitdefender.
2. În fereastra **Setări generale**, dezactivează **Notificări de recomandare**.

Acțiuni rapide

Utilizând acțiuni rapide poți lansa rapid sarcini pe care le consideri importante pentru păstrarea protecției sistemului tău și pentru rularea la viteză optimă.

Implicit, Bitdefender sosește cu câteva acțiuni rapide care pot fi înlocuite cu cele pe care știi că le utilizezi cel mai des. Pentru a înlocui o acțiune rapidă:

1. Efectuează clic pe pictograma din colțul din dreapta sus al cardului pe care dorești să îl îndepărtezi.
2. Plasează sarcina pe care dorești să o adaugi la interfața principală și apoi efectuează clic pe **ADĂUGARE**.

Sarcinile pe care le poți adăuga în interfața principală sunt:

- **Scanare rapidă.** Efectuează o scanare rapidă pentru a detecta rapid amenințările posibile care ar putea exista pe dispozitivul tău.
- **Scanare sistem.** Efectuează o scanare de sistem pentru a te asigura că dispozitivul tău nu conține amenințări.
- **Scanarea vulnerabilităților.** Scanează-ți dispozitivul pentru a depista vulnerabilitățile și a te asigura că toate aplicațiile instalate împreună cu sistemul de operare sunt actualizate și funcționează corespunzător.
- **Funcția Asistență Securitate Wi-Fi.** Deschide fereastra Asistent de securitate Wi-Fi în modulul Vulnerabilități.
- **OpenSafepay.** Deschide Bitdefender Safepay™ pentru a-ți proteja datele confidențiale în timpul tranzacțiilor online.
- **Deschide VPN.** Deschide Bitdefender VPN pentru a adăuga un nivel suplimentar de protecție atunci când ești conectat la internet.
- **File Shredder.** Lansează instrumentul File Shredder pentru a șterge definitiv urmele datelor cu caracter sensibil din dispozitivul tău.

- **Deschide OneClick Optimizer.** Eliberează spațiu, remediază erorile din regiștri și protejează-ți confidențialitatea ștergând fișierele care nu mai sunt utile, cu un singur clic pe buton.

Pentru a începe să protejezi dispozitive suplimentare cu Bitdefender:

1. Efectuează clic pe **Instalează pe alt dispozitiv**.
   O nouă fereastră apare pe ecran.
2. Fă clic pe **TRIMITE LINK DE DESCĂRCARE**.
3. Urmează pașii de pe ecran pentru a instala Bitdefender.

În funcție de alegerea dumneavoastră, se vor instala următoarele produse Bitdefender:

- Bitdefender Antivirus Plus pe dispozitive pe platformă Windows.
- Bitdefender Antivirus for Mac pe dispozitivele care rulează macOS.
- Bitdefender Mobile Security pe dispozitivele care rulează Android.
- Bitdefender Mobile Security pe dispozitivele care rulează iOS.

2.2.4. Secțiunile Bitdefender

Produsul Bitdefender este livrat cu trei secțiuni împărțite în mai multe caracteristici utile pentru a vă ajuta să rămâneți protejat în timp ce lucrați, să navigați pe Internet sau să efectuați plăți online, să îmbunătățiți viteza sistemului și multe altele.

Atunci când dorești să accesezi caracteristicile unei anumite secțiuni sau să începi configurarea produsului tău, accesează următoarele pictograme situate în meniul de navigare al **interfeței Bitdefender**:

- **Protecție**
- **Confidențialitate**
- **Utilități**

Protecție

În secțiunea Protecție poți configura setările tale avansate de securitate, poți administra prietenii și spammerii, poți vizualiza și edita setările conexiunii la internet, poți configura caracteristicile Online Threat Prevention, poți verifica și remedia eventualele vulnerabilități ale sistemului și poți evalua securitatea rețelelor wireless la care te conectezi.

Caracteristicile pe care le poți administra în secțiunea Securitate sunt:

ANTIVIRUS

Protecția antivirus reprezintă fundația securității dumneavoastră. Bitdefender teprotejează în timp real și la cerere împotriva tuturor tipurilor de amenințări, precum malware, troieni, programe de tip spyware, adware etc.

Din funcția Antivirus, poți accesa cu ușurință următoarele sarcini de scanare:

- Scanare Rapidă
- Scanare Sistem
- Administrare Scanări
- Mediu de recuperare

Pentru mai multe informații referitoare la activitățile de scanare și modul de configurare a protecției antivirus, consultați Protecție antivirus (pagina 47).

PREVENȚIE ÎMPOTRIVA AMENINȚĂRILOR ONLINE

Online Threat Prevention te ajută să te protejezi contra atacurilor de tip phishing, tentativelor de fraudă și scurgerilor de date personale în timp ce navighezi pe internet.

Pentru mai multe informații referitoare la modul de configurare Bitdefender pentru a vă proteja activitatea online, consultați Prevenirea amenințărilor online (pagina 69).

FIREWALL

Firewall-ul te protejează în timp ce ești conectat la rețele și la internet, filtrând toate tentativele de conectare.

Pentru mai multe informații cu privire la configurarea firewall-ului, consultați Firewall.

ADVANCED THREAT DEFENSE

Funcția Advanced Threat Defense îți protejează sistemul împotriva amenințărilor precum ransomware, programe spion și troieni, analizând comportamentul tuturor aplicațiilor instalate. Procesele suspecte sunt identificate și, dacă este cazul, blocate.

Pentru mai multe informații referitoare la modul în care vă puteți menține sistemul protejat împotriva amenințărilor, consultați Apărare avansată împotriva amenințărilor (pagina 67).

ANTISPAM

Caracteristica antispam a Bitdefender se asigură că nu intră e-mail-uri nedorite în directorul cu mesaje primite, filtrând traficul de e-mail POP3.

Pentru mai multe informații referitoare la protecția antispam, consultați Antispam.

VULNERABILITATE

Modulul Vulnerabilități te ajută să-ți menții actualizarea sistemului de operare și aplicațiilor pe care le folosești în mod regulat și să identifici rețelele wireless nesigure la care te conectezi. Selectați **Deschide** în modulul Vulnerabilități pentru a accesa caracteristicile acestuia.

Funcția **Scanare vulnerabilități** îți permite să identifici actualizările Windows critice, actualizările aplicațiilor, parolele slabe aferente conturilor Windows și rețelele wireless care nu sunt sigure. Selectează **Începe scanarea** pentru a realiza o scanare pe dispozitivul tău.

Selectează **Asistent securitate Wi-Fi** pentru a vizualiza lista rețelelor wireless la care te conectezi, dar și evaluarea reputației fiecăreia dintre acestea și măsurile pe care le poți lua pentru a te proteja de eventualii curioși.

Pentru informații suplimentare referitoare la configurarea protecției la vulnerabilitate, consultați Vulnerabilități (pagina 71).

REMEDIERE RANSOMWARE

Funcția Remediere ransomware te ajută să recuperezi fișierele în cazul în care acestea sunt criptate de ransomware.

Pentru informații suplimentare despre modul de recuperare a fișierelor criptate, accesează Remediere ransomware (pagina 79).

Confidențialitate

Din secțiunea Confidențialitate, poți deschide aplicația Bitdefender VPN, îți poți cripta datele tale personale, îți poți proteja tranzacțiile online, îți poți securiza camera web și experiența de navigare și îți poți proteja copiii vizualizându-le și restricționându-le activitatea online.

Caracteristicile pe care le poți administra în secțiunea Confidențialitate sunt:

VPN

VPN îți securizează activitatea online și îți ascunde adresa IP de fiecare dată când te conectezi la rețele wireless nesecurizate în timp ce ești prin aeroporturi, mall-uri, cafenele sau hoteluri. În mod suplimentar, poți accesa conținut care în mod normal este restricționat în anumite zone.

Pentru mai multe informații despre această caracteristică, accesează VPN (pagina 84).

PROTECȚIE VIDEO & AUDIO

Protecția audio și video îți menține camera web în siguranță prin blocarea accesului aplicațiilor nesigure la aceasta și te notifică atunci când aplicațiile încearcă să obțină acces la microfonul dispozitivului tău.

Pentru informații suplimentare despre cum să îți protejezi camera web împotriva accesului neautorizat și cum să setezi Bitdefender astfel încât să-ți transmită notificări în legătură cu activitatea microfonului, accesează Protecție video și audio.

SAFEPAY

Browser-ul Bitdefender Safepay™ vă ajută să vă mențineți tranzacțiile de online, e-shopping și orice alte tipuri de tranzacții confidențiale și sigure.

Pentru informații suplimentare despre Bitdefender Safepay™, consultați Securitate Safepay pentru tranzacțiile online (pagina 87).

CONTROL PARENTAL

Modulul Controlul Parental de la Bitdefender îți permite să monitorizezi ce fac copiii atunci când utilizează dispozitivele. Dacă observi conținut necorespunzător, poți decide să le restricționezi accesul la internet sau la anumite aplicații.

Efectuați clic pe **Configurează** din secțiunea Asistență parentală pentru a începe să configurați dispozitivele copiilor dvs. și a le monitoriza activitatea indiferent unde vă aflați.

Pentru mai multe informații referitoare la configurarea aplicației Control parental, accesează Control Parental.

ANTI-TRACKER

Funcția Anti-tracker previne tracking-ul, astfel încât datele tale rămân private în timp ce navighezi online, reducând totodată timpul de încărcare al site-urilor web.

Pentru mai multe informații despre această funcție, consultă Anti-tracker (pagina 82).

Instrumente

În secțiunea Instrumente, poți îmbunătăți viteza sistemului și poți administra dispozitivele tale.

OneClick Optimizer

Bitdefender Total Security oferă mai mult decât securitate, ajutându-te să menții performanța dispozitivului tău la un nivel optim.

OneClick Optimizer te va ajuta să găsești și să elimini fișierele care nu sunt necesare din dispozitivul tău printr-un singur pas.

Pentru mai multe informații, vezi OneClick Optimizer.

Anti-furt

Bitdefender Anti-Theft îți protejează dispozitivul și datele împotriva furtului sau pierderii. În astfel de situații, acest modul îți permite să localizezi sau să blochezi dispozitivul de la distanță. De asemenea, poți șterge toate datele existente pe sistemul tău.

Bitdefender Anti-Theft oferă următoarele caracteristici:

- Localizare de la distanță
- Blocare de la distanță
- Ștergere de la distanță
- Alertă de la distanță

Pentru mai multe informații referitoare la modul în care îți poți proteja sistemul, consultă Device Anti-Theft.

Protecția datelor

Opțiunea Ștergere definitivă de la Bitdefender îți permite să ștergi definitiv date prin eliminarea fizică a acestora de pe hard disk.

Pentru mai multe informații despre acesta, consultați Data Protection (pagina 100).

Profiluri

Activitățile de serviciu zilnice, vizionarea filmelor sau jocurile pot încetini performanțele sistemului, cu precădere dacă rulează simultan cu procesele de actualizare Windows și sarcinile de actualizare.

Cu Bitdefender, puteți acum alege și aplica profilul dorit, care efectuează ajustările sistemului adecvate pentru îmbunătățirea performanțelor aplicațiilor specifice instalate.

Pentru mai multe informații despre această caracteristică, consultați Profiluri (pagina 94).

2.2.5. Modifică limba produsului

Interfața Bitdefender este disponibilă în mai multe limbi și poate fi modificată urmând acești pași:

1. Clic **Setări** pe meniul de navigare de pe Interfața Bitdefender.
2. În fereastra **General**, fă clic pe **Schimbă limba**.
3. Selectează din listă limba dorită și apoi clic pe **SALVEAZĂ**.
4. Așteaptă câteva momente până când se aplică setările.

2.3. Bitdefender Central

2.3.1. Despre Bitdefender CENTRAL

Bitdefender Central este platforma din care ai acces la caracteristicile și serviciile online ale produsului și de unde poți efectua de la distanță sarcini importante pe dispozitivele pe care este instalat Bitdefender. Te poți conecta la contul tău Bitdefender de pe orice calculator sau dispozitiv mobil conectat la internet accesând https://central.bitdefender.com sau direct din aplicația Bitdefender Central pe dispozitivele Android sau iOS.

Pentru a instala aplicația Bitdefender Central pe dispozitivele tale:

- **Pe Android** - caută Bitdefender Central în Google Play și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.
- **Pe iOS** - caută Bitdefender Central în App Store și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.

După autentificare, poți face următoarele:

- Descarcă și instalează Bitdefender pe sistemele de operare Windows, macOS, iOS și Android. Produsele disponibile pentru descărcare sunt:
  - Gama de produse Bitdefender Windows
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security for Android
  - Bitdefender Mobile Security for iOS
- Administrează și reînnoiește abonamentele Bitdefender.
- Adaugă dispozitive noi la rețeaua ta și administrează-le oriunde te-ai afla.
- Protejați-vă dispozitivele din rețea și datele de pe acestea împotriva furtului sau a pierderii cu ajutorul funcției **Anti-Theft**.
- Configurează setările de **Control parental** pentru dispozitivele copiilor tăi și monitorizează activitatea acestora oriunde te-ai afla.

2.3.2. Accesează Bitdefender Central

Există mai multe moduri de accesare aBitdefender Central. În funcție de sarcina pe care doriți să o efectuați, puteți utiliza oricare dintre următoarele posibilități:

- Din interfața principală Bitdefender:
  1. Fă clic pe **Contul meu** din meniul de navigare al **interfeței Bitdefender**.
  2. Apasă pe **Accesează Bitdefender Central**.
  3. Conectați-vă la contul Bitdefender folosind adresa dvs. de e-mail și parola.
- Din browser-ul web:
  1. Deschide un browser web pe orice dispozitiv cu acces la internet.
  2. Accesează: https://central.bitdefender.com.
  3. Conectează-te la contul tău cu ajutorul adresei de e-mail și parolei.
- De pe dispozitivul tău Android sau iOS:
  1. Deschide aplicația Bitdefender Central pe care ai instalat-o.

Notă
În acest material prezentăm opțiunile pe care le poți găsi în interfața web.

2.3.3. Autentificare în doi pași

Metoda de autentificare în doi pași adaugă un strat suplimentar de securitate contului tău Bitdefender, solicitând un cod de autentificare suplimentar pe lângă datele tale de conectare. În acest fel, vei evita ca altcineva să preia controlul asupra contului tău și veți ține la distanță atacuri cibernetice precum keyloggere, atacuri de tip „brute-force” sau pe bază de dicționar.

Activați autentificarea de tip „two-factor”

Prin activarea autentificării în doi pași, contul tău Bitdefender devine mult mai sigur. Identitatea ta va fi verificată de fiecare dată când te vei conecta de la diferite dispozitive pentru a instala unul dintre produsele Bitdefender, pentru a verifica starea abonamentului tău sau pentru a executa sarcini de la distanță pe dispozitivele tale.

Pentru a activa autentificarea de tip „two-factor”:

1. Acces Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Apasă pe **Contul Bitdefender** din meniul vertical.
4. Selectează fila **Parolă și securitate**.
5. Selectează **Autentificarea în doi pași**.
6. Apasă pe **ÎNCEPE UTILIZAREA**.
   Selectează una dintre următoarele metode:
   - **Aplicație de autentificare** - folosește o aplicație de autentificare pentru a genera un cod de fiecare dată când dorești să te conectezi la contul tău Bitdefender.
     Dacă dorești să utilizezi o aplicație de autentificare, dar nu ești sigur ce să alegi, îți punem la dispoziție o listă cu aplicațiile de autentificare pe care le recomandăm.
     a. Selectează **UTILIZEAZĂ O APLICAȚIE DE AUTENTIFICARE** pentru a începe.

b. Pentru a te autentifica pe un dispozitiv cu sistem de operare Android sau iOS, folosește dispozitivul tău pentru a scana codul QR.
   Pentru a te autentifica pe un laptop sau computer, poți adăuga manual codul afișat.
   Apasă pe **CONTINUARE**.

c. Introdu codul furnizat de aplicație sau cel afișat la pasul anterior, apoi selectează **ACTIVARE**.

- **E-mail** - de fiecare dată când te conectezi la contul tău Bitdefender, se va trimite un cod de verificare către căsuța ta de e-mail. Verifică contul de e-mail și introdu codul primit.

  a. Selectează **UTILIZEAZĂ ADRESA DE E-MAIL** pentru a începe.

  b. Verifică-ți contul de e-mail și introdu codul furnizat.

  c. Apasă pe **ACTIVARE**.

  d. Ai la dispoziție zece coduri de activare. Poți copia, descărca sau tipări lista pentru a o utiliza ulterior în cazul în care îți pierzi adresa de e-mail sau nu te poți conecta. Fiecare cod poate fi utilizat o singură dată.

  e. Fă clic pe **FINALIZAT**.

Dacă nu mai dorești să folosești Autentificarea în doi pași:

1. Selectează opțiunea **DEZACTIVEAZĂ AUTENTIFICAREA ÎN DOI PAȘI**.
2. Verifică aplicația sau contul de e-mail și introdu codul primit.
   Dacă ai optat pentru a primi codul de autentificare prin e-mail, ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a introduce codul generat. Dacă timpul expiră, va trebui să generezi un nou cod urmând aceiași pași.
3. Confirmă alegerea.

2.3.4. Adăugarea dispozitivelor sigure

Pentru a ne asigura că tu ești singura persoană care poate accesa contul tău Bitdefender, este posibil să îți solicităm mai întâi un cod de securitate. Dacă dorești să omiți acest pas de fiecare dată când te conectezi de pe același dispozitiv, îți recomandăm să îl setezi ca dispozitiv sigur.

Pentru a adăuga dispozitive marcate ca fiind sigure:

1. Acces Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Clic **Contul Bitdefender** în meniul slide.
4. Selectează **Parolă și securitate** fila.
5. Selectează **Dispozitive de încredere**.
6. Se afișează lista cu dispozitivele pe care este instalat Bitdefender. Selectează dispozitivul dorit.

Poți adăuga oricât de multe dispozitive dorești, cu condiția ca pe acestea să fie instalat Bitdefender și abonamentul tău să fie valid.

2.3.5. Activitate

În secțiunea Activitate, ai acces la informații despre dispozitivele pe care este instalat Bitdefender.

Când accesezi fereastra **Activitate**, vor deveni disponibile următoarele carduri:

- **Dispozitivele mele.** Accesând această secțiune, poți vizualiza numărul de dispozitive conectate și stările lor de protecție. Pentru a remedia de la distanță anumite probleme identificate pe dispozitivele detectate, selectează **Remediere probleme** și apoi **SCANARE ȘI REMEDIERE PROBLEME**.

  Pentru a vizualiza detaliile referitoare la problemele detectate, selectează **Vizualizează problemele**.

  Informațiile despre amenințările detectate nu pot fi extrase de pe dispozitivele cu iOS.

- **Amenințări blocate.** Aici poți vizualiza un grafic care prezintă statistici globale, ce includ informații despre amenințările blocate în ultimele 24 de ore și șapte zile. Informațiile afișate sunt preluate în funcție de comportamentul periculos detectat în cazul fișierelor, aplicațiilor și adreselor URL accesate.

- **Principalii utilizatori cu amenințări blocate.** Aici poți vedea un top al utilizatorilor la care au fost detectate cele mai multe amenințări.

- **Principalele dispozitive cu amenințări blocate.** Aici poți vedea un top al dispozitivelor pe care au fost detectate cele mai multe amenințări.

2.3.6. Abonamentele mele

Platforma Bitdefender Central vă oferă posibilitatea de a administra cu ușurință abonamentele deținute pentru toate dispozitivele.

Verifică abonamentele disponibile

Pentru a verifica abonamentele disponibile:

1. Accesează Bitdefender Central.
2. Selectați fereastra **Abonamentele mele**.

Aici găsești informații referitoare la valabilitatea abonamentelor pe care le deții și la numărul de dispozitive care utilizează fiecare dintre aceste abonamente.

Poți adăuga un dispozitiv nou unui abonament sau poți îl reînnoi selectând un card de abonament.

> **Notă**
> Poți avea mai multe abonamente în contul tău cu condiția ca acestea să fie pentru platforme diferite (Windows, macOS, iOS sau Android).

Activare abonament

Un abonament poate fi activat în timpul procesului de instalare folosind contul Bitdefender. Concomitent cu procesul de activare, începe să curgă și perioada de valabilitate a abonamentului.

Dacă ați achiziționat un cod de activare de la unul dintre distribuitorii noștri sau l-ați primit cadou, puteți adăuga valabilitatea acestuia la abonamentul Bitdefender.

Pentru a activa un abonament folosind un cod de activare, urmează pașii de mai jos:

1. Accesează Bitdefender Central.
2. Selectează **Abonamentele mele** panou.
3. Apasă pe butonul **COD DE ACTIVARE**, apoi introdu codul în câmpul corespunzător.
4. Selectează **ACTIVARE** pentru a continua.

Abonamentul este acum activat.

Reînnoire abonament

Dacă ai dezactivat reînnoirea automată a abonamentului Bitdefender, îl poți reînnoi manual parcurgând pașii următori:

1. Accesează Bitdefender Central.
2. Selectează panoul **Abonamentele mele**.
3. Selectează cardul de abonament dorit.
4. Selectează **REÎNNOIRE** pentru a continua.

Se deschide o pagină web în browser-ul dvs., de unde puteți reînnoi abonamentul Bitdefender.

2.3.7. Dispozitivele mele

Zona **Dispozitivele mele** din contul Bitdefender îți oferă posibilitatea de a instala, administra și efectua operațiuni de la distanță pe produsul Bitdefender de pe orice dispozitiv pornit și conectat la internet. Filele dispozitivelor afișează numele dispozitivului, starea protecției și dacă există riscuri de securitate ce afectează protecția dispozitivelor tale.

Adăugarea unui dispozitiv nou

Dacă abonamentul dvs. acoperă mai multe dispozitive, puteți adăuga un dispozitiv nou și puteți instala Bitdefender Antivirus Plus pe acesta, după cum urmează:

1. Accesează Bitdefender Central.
2. Selectează panoul **Dispozitivele mele**, apoi atingeți **INSTALATI PROTECTIA**.
3. Alegeți una dintre cele două opțiuni disponibile:
   - **Protejați acest dispozitiv**
     Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, atingeți butonul corespunzător.
   - **Protejați alte dispozitive**
     Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, atingeți butonul corespunzător.
     Apasă pe **TRIMITE LINK DE DESCĂRCARE**. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de

ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.
Pe dispozitivul pe care doriți să vă instalați produsul Bitdefender, verificați contul de e-mail pe care l-ați introdus, apoi atingeți butonul de descărcare corespunzător.

4. Așteaptă să se finalizeze descărcarea și apoi execută aplicația de instalare.

Personalizează-ți dispozitivul

Pentru a-ți identifica ușor dispozitivele, poți personaliza denumirile acestora:

1. Acces Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. Efectuează clic pe fila dispozitivului dorit și apoi pe pictograma ⋮ din colțul din dreapta sus al ecranului.
4. Selectează **Setări**.
5. Introdu o denumire nouă în câmpul **Denumire dispozitiv** și apoi apasă pe **SALVARE**.

Poți crea și aloca un deținător al fiecăruia dintre dispozitivele tale pentru o mai bună administrare a acestora:

1. Acces Bitdefender Central.
2. Selectează **Dispozitivele mele** panou.
3. Atingeți cardul dispozitivului dorit, apoi butonul ⋮ pictograma din colțul din dreapta sus al ecranului.
4. Selectează **Profil**.
5. Efectuează clic pe **Adăugare deținător** și completează câmpurile corespunzătoare. Personalizează-ți profilul adăugând o fotografie, selectând data nașterii și adăugând o adresă de e-mail și un număr de telefon.
6. Faceți clic pe **ADAUGĂ** pentru a salva profilul.
7. Selectează deținătorul dorit din lista **Deținător dispozitiv**, apoi apasă pe **ATRIBUIRE**.

Acțiuni de la distanță

Pentru a actualiza Bitdefender de la distanță pe un dispozitiv:

1. Accesează Bitdefender Central.
2. Selectează **Dispozitivele mele** panou.
3. Atingeți cardul dispozitivului dorit, apoi butonul ⋮ pictograma din colțul din dreapta sus al ecranului.
4. Selectează **Actualizare**.

Pentru mai multe operațiuni ce pot fi efectuate de la distanță și informații referitoare la produsul Bitdefender instalat pe un anumit dispozitiv, efectuează clic pe fila dispozitivului dorit.

După ce ai efectuat clic pe cardul dispozitivului, sunt disponibile următoarele file:

- **Panou de control.** În această fereastră, poți vizualiza detalii despre dispozitivul selectat, poți verifica starea de protecție a acestuia, statusul aplicației Bitdefender VPN și câte amenințări au fost blocate în ultimele șapte zile. Starea de protecție poate fi verde, atunci când nu există probleme care îți afectează dispozitivul, galbenă, atunci când dispozitivul necesită o intervenție din partea ta, sau roșie, atunci când există un risc la adresa dispozitivului tău. Dacă există probleme care afectează dispozitivul tău, efectuează clic pe săgeata jos din zona de status din partea de sus pentru a afla mai multe detalii. De aici, poți
- **Protecție.** Din această fereastră poți rula de la distanță o operațiune de scanare rapidă sau scanare a sistemului pe dispozitivele tale. Fă clic pe butonul **SCANARE** pentru a iniția procesul. De asemenea, poți vedea când a avut loc ultima scanare a dispozitivului și poți accesa un raport al celei mai recente scanări efectuate, care conține cele mai importante informații.
- **Optimizare.** Această funcție îți permite să îmbunătățești de la distanță performanța unui dispozitiv, prin scanarea rapidă, detectarea și ștergerea fișierelor inutile. Apasă pe butonul **INIȚIERE**, apoi selectează zonele pe care dorești să le optimizezi. Apasă din nou pe **INIȚIERE** pentru a iniția procesul de optimizare. Fă clic pe **Mai multe detalii** pentru a accesa un raport detaliat despre problemele corectate.
- **Anti-furt.** Dacă nu mai știi unde ți-ai pus dispozitivul sau dacă a fost furat sau pierdut, funcția Anti-furt îți poate localiza dispozitivul și poate

efectua acțiuni de la distanță. Fă clic pe **LOCALIZARE** pentru a afla poziția dispozitivului. Se afișează ultima poziție cunoscută, ora și data la care dispozitivul s-a aflat acolo.

- **Vulnerabilitate.** Apasă pe butonul **SCANARE** din fila Vulnerabilitate pentru a verifica dacă există vulnerabilități la nivelul unui dispozitiv, cum ar fi dacă îi lipsesc actualizări Windows sau dacă există aplicații neactualizate sau parole nesigure. Vulnerabilitățile nu pot fi corectate de la distanță. În cazul în care se detectează o vulnerabilitate, va trebui să inițiezi o scanare nouă a dispozitivului și apoi să iei măsurile recomandate. Apasă pe **Mai multe detalii** pentru a accesa un raport detaliat despre problemele identificate.

2.3.8. Notificări

Pentru a vă ajuta să fiți la curent cu ceea ce se întâmplă pe dispozitivele asociate contului dumneavoastră, aveți la dispoziție pictograma 🔔. Odată ce efectuați clic pe aceasta, veți avea o imagine de ansamblu ce constă în informații despre activitatea produselor Bitdefender instalate pe dispozitivele dumneavoastră.

2.4. Cum actualizezi Bitdefender

Zi de zi sunt descoperite și identificate noi amenințări. De aceea este foarte important ca Bitdefender să fie actualizat cu cea mai recentă bază de date cu amenințări.

Dacă sunteți conectat la internet, prin bandă largă sau ADSL, Bitdefender se ocupă singur de actualizări. În mod implicit, caută actualizări la pornirea dispozitivului, precum și după fiecare **oră**. În cazul în care este detectată o actualizare, aceasta este descărcată și instalată automat pe dispozitivul tău.

Procesul de actualizare este realizat progresiv, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite unul câte unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

Important
Menține funcția Actualizare automată activată pentru a fi protejat împotriva celor mai noi amenințări.

În anumite cazuri este necesară intervenția dumneavoastră pentru ca protecția oferită de Bitdefender să fie actualizată:

- Dacă dispozitivul tău este conectat la internet printr-un server proxy, trebuie să configurezi setările proxy, după cum se specifică în .
- Dacă vă conectați la internet prin dial-up, atunci este recomandat să actualizați manual Bitdefender în mod regulat. Pentru mai multe informații, consultă capitolul .

2.4.1. Cum verifici dacă Bitdefender este actualizat

Pentru a verifica data ultimei actualizări a produsului tău Bitdefender:

1. Efectuează clic pe **Notificări** din meniul de navigare al interfeței **Bitdefender**.
2. În fila **Toate**, selectează notificarea privind ultima actualizare.

Puteți afla când anume au fost inițiate actualizări, precum și informații despre acestea (dacă au fost finalizate cu succes, dacă este necesară o repornire pentru a finaliza instalarea). Dacă este necesar, reporniți sistemul cât mai curând posibil.

2.4.2. Efectuarea unei actualizări

Pentru efectuarea actualizărilor este necesară existența unei conexiuni la internet.

Pentru a iniția o actualizare, fă clic dreapta pe pictograma Bitdefender din **bara de sistem**, apoi selectează **Actualizează acum**.

Funcția Actualizare se va conecta la serverul de actualizare al Bitdefender și va căuta noi actualizări. În cazul în care este detectată o actualizare, în funcție de **setările de actualizare**, vi se va cere fie să confirmați actualizarea, fie aceasta va fi realizată automat.

Important
Pentru finalizarea actualizării, trebuie să reporniți dispozitivul. Vă recomandăm să faceți acest lucru cât mai repede cu putință.

De asemenea, poți efectua actualizări ale dispozitivelor tale și de la distanță, cu condiția ca acestea să fie pornite și conectate la internet.

Pentru a actualiza Bitdefender de la distanță pe un dispozitiv Windows:

1. Acces Bitdefender Central.
2. Selectează **Dispozitivele mele** panou.
3. Faceți clic pe cardul dispozitivului dorit, apoi pe ⋮ pictograma din colțul din dreapta sus al ecranului.
4. Selectați **Actualizați**.

2.4.3. Activarea sau dezactivarea actualizării automate

Pentru activa sau dezactiva actualizarea automată:

1. Clic **Setări** pe meniul de navigare de pe Interfața Bitdefender.
2. Selectați secțiunea **Actualizare**.

3. Activează sau dezactivează butonul corespunzător.
4. Se deschide o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării actualizarii automate.

   Poți dezactiva actualizarea automată pentru 5, 15 sau 30 de minute, pentru o oră sau până la repornirea sistemului.

   Avertizare

   Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați actualizarea automată pentru cât mai puțin timp posibil. Dacă nu este actualizat în mod regulat, BitDefender nu va putea să vă protejeze împotriva ultimelor amenințări apărute.

2.4.4. Ajustarea setărilor de actualizare

Actualizările pot fi realizate din rețeaua locală, de pe internet, direct sau printr-un server proxy. Implicit, Bitdefender va căuta actualizări la fiecare oră, pe internet, și va instala actualizările disponibile fără a vă mai avertiza.

Setările de actualizare implicite sunt potrivite pentru majoritatea utilizatorilor, și, în mod normal, nu este nevoie să le modifici.

Pentru a ajusta setările de actualizare:

1. Clic **Setări** pe meniul de navigare de pe Interfața Bitdefender.
2. Selectează fila **Actualizare** și ajustează setările conform preferințelor tale.

Frecvența actualizărilor

Bitdefender este configurat să verifice din oră în oră dacă există actualizări. Pentru a modifica frecvența actualizărilor, trageți de cursor de-a lungul scalei pentru a stabili perioada dorită de timp la care ar trebui să intervină actualizarea.

Reguli de procesare a actualizării

De fiecare dată când este disponibilă o actualizare, Bitdefender va descărca și implementa automat actualizarea fără notificări vizibile. Dezactivează opțiunea **Actualizare silențioasă** dacă dorești să fii notificat de fiecare dată când este disponibilă o nouă actualizare.

Anumite actualizări necesită o repornire a computerului pentru a finaliza procesul de instalare.

Implicit, dacă o actualizare necesită repornirea dispozitivului, Bitdefender va continua să funcționeze cu fișierele vechi până în momentul în care utilizatorul repornește computerul. În acest fel, procesul de actualizare a Bitdefender nu interferează cu operațiile utilizatorului.

Dacă dorești să fii notificat atunci când o actualizare necesită repornirea calculatorului, activează opțiunea **Repornește notificări**.

2.4.5. Actualizări permanente

Pentru a vă asigura că folosiți cea mai recentă versiune, Bitdefender verifică automat actualizările de produs. Aceste actualizări pot introduce noi caracteristici și îmbunătățiri, pot remedia erori ale produsului sau pot realiza un upgrade automat la o nouă versiune. Atunci când noua versiune Bitdefender este disponibilă prin intermediul actualizării, se salvează setările personalizate și se evită procedura de dezinstalare și reinstalare.

Aceste actualizări necesită repornirea sistemului cu scopul de a iniția instalarea de noi fișiere. Atunci când este finalizată o actualizare de produs, o fereastră pop-up vă va solicita să reporniți sistemul. Dacă rataţi această notificare, puteți fie să efectuați clic pe **REPORNEȘTE ACUM** în fereastra **Notificări** unde este menționată cea mai recentă actualizare, fie să reporniți manual sistemul.

Notă
Actualizările care includ noi caracteristici și îmbunătățiri vor fi oferite numai utilizatorilor care au Bitdefender 2020 instalat.

2.5. Asistență inteligentă prin comenzi vocale

Dacă utilizezi un smart-speaker Amazon Alexa sau aplicația Asistent Google, poți iniția comenzi vocale pentru a desfășura diferite activități sau pentru a verifica informațiile de pe dispozitivele care au Bitdefender instalat. Astfel poți efectua sarcini de scanare și optimizare, poți dezactiva internetul de pe dispozitivele conectate, poți verifica starea abonamentului tău actual sau poți vedea locația sau activitățile online ale copiilor tăi. Pentru a vedea lista completă de comenzi vocale pe care le poți iniția, consultă {1}{2}.

2.5.1. Setarea comenzilor vocale

Comenzile vocale Bitdefender pot fi configurate pentru:

- **Aplicația Google Home activată**
  - Android 5.0 sau o versiune ulterioară
  - iOS 10.0 și versiuni ulterioare
  - Chromebooks
- **Aplicația Amazon Alexa activată**
  - Echo
  - Echo Dot
  - Echo Show
  - Echo Spot
  - Fire TV Cube

Setarea comenzilor vocale Amazon Alexa pentru Bitdefender

Pentru a seta comenzile vocale Bitdefender pe Amazon Alexa:

1. Deschide aplicația Amazon Alexa.
2. Atinge pictograma **Meniu** apoi accesează **Abilități**.
3. Caută Bitdefender.
4. Atinge **Bitdefender** și apoi **ACTIVARE**.
5. Trebuie să te conectezi la contul tău Bitdefender.
   Introdu numele tău de utilizator și parola ta, iar apoi atinge **AUTENTIFICARE**.

De îndată ce sincronizarea dintre Bitdefender și Amazon Alexa este realizată, ți se prezintă comenzile vocale pe care le poți utiliza pentru a iniția sarcini sau pentru a verifica informații despre dispozitivele pe care este instalat Bitdefender.

Dacă ai nevoie ca asistentul să-ți prezinte lista tuturor comenzilor vocale sau abilităților disponibile, rostește **HELP ME** (Ajută-mă).

Setarea comenzilor vocale Google Home pentru Bitdefender

Pentru a seta comenzile vocale pe Google Home:

1. Deschide aplicația Google Home.

2. Atinge Meniu din colțul din stânga sus a ecranului Principal, apoi atinge **Explore** (Explorează).
3. Căutați Bitdefender.
4. Atinge **Bitdefender** și apoi **Link**.
5. Vi se solicită să vă conectați la contul Bitdefender.
   Introduceți numele de utilizator și parola, apoi atingeți **CONECTARE**.

De îndată ce sincronizarea dintre Bitdefender și Google Home este realizată, ți se prezintă comenzile vocale pe care le poți utiliza pentru a iniția sarcini sau pentru a verifica informații despre dispozitivele pe care este instalat Bitdefender.

Ori de câte ori aveți nevoie ca asistentul să vă ofere lista cu toate comenzile sau abilitățile vocale disponibile, de exemplu **AJUTAȚI-MĂ**.

2.5.2. Comenzi vocale prin care poți interacționa cu Bitdefender

Pentru a deschide comenzile vocale asociate Bitdefender:

- Pe Amazon Alexa: **Alexa, deschide Bitdefender**
- Pentru Google Home: **OK, Google, vorbește cu Bitdefender**

Pentru a lansa comenzile vocale asociate Bitdefender:

- Pe Amazon Alexa: **Alexa, cere Bitdefender**
- Pe Google Home: **OK, Google, cere Bitdefender**

Întrebările și sarcinile pe care le poți iniția odată ce asistentul Bitdefender este deschis sunt:

- Cum este activitatea mea astăzi?
- Care este starea abonamentului meu?
- Optimizează dispozitivele mele. (Această comandă va lansa OneClick Optimizer pe dispozitivele Windows conectate).
- Efectuează o scanare rapidă pe [tip dispozitiv] meu. (Ca tip de dispozitiv poți spune laptop, calculator, telefon sau tabletă).

Dacă ai configurat Controlul parental pe dispozitivele copiilor tăi, întrebările și activitățile pe care le poți iniția odată ce asistentul Bitdefender este deschis sunt următoarele:

- Întrerupe temporar conexiunea la internet pentru [nume profil].
- Restabilește conexiunea la internet pentru [nume profil].
- Localizează copilul meu.
- Unde este copilul meu?
- Cât timp a petrecut copilul meu pe dispozitivele lui?
- Cât timp a petrecut copilul pe Facebook astăzi?
- Cât timp a petrecut copilul meu pe Instagram astăzi?

Dacă ai mai multe profilul pe care ai configurat Controlul parental, poți menționa în comandă numele copilului. De exemplu **Localizează pe Jennifer**.

3. GESTIONAREA SECURITĂȚII

3.1. Protecție antivirus

Bitdefender îți protejează dispozitivul împotriva oricăror amenințări (malware, troieni, aplicații spyware, rootkituri și altele). Protecția oferită de BitDefender se împarte în două categorii:

- **Scanare la acces** - împiedică pătrunderea amenințărilor noi în sistemul tău. De exemplu, Bitdefender va scana un document word atunci când îl deschizi, pentru a verifica dacă conține amenințări cunoscute, precum și un mesaj e-mail atunci când îl primești.
  Procesul de scanare la accesare asigură protecție în timp real împotriva amenințărilor, fiind o componentă esențială a oricărui program de securitate pentru calculatoare.

  Important
  Pentru a preveni infectarea dispozitivului, păstrează activată funcția de **scanare la accesare**.

- **Scanarea la cerere** - permite detectarea și eliminarea amenințărilor care există deja în sistemul dumneavoastră. Acesta este modul clasic de scanare, inițiată de utilizator – dumneavoastră alegeți partițiile, directoarele sau fișierele pe care trebuie să le scaneze BitDefender, iar BitDefender le scanează – la cerere.

Bitdefender scanează în mod automat orice fișier media amovibil care este conectat la dispozitiv pentru a te asigura că este sigur să îl accesezi. Pentru mai multe informații, consultă capitolul Scanarea automată a suporturilor media amovibile (pagina 61).

Utilizatorii avansați pot configura excepțiile de scanare în cazul în care nu doresc ca anumite fișiere sau tipuri de fișiere să fie scanate. Pentru mai multe informații, consultă capitolul Configurarea excepțiilor de scanare (pagina 63).

Atunci când detectează o amenințare, Bitdefender va încerca în mod automat să elimine codul periculos din fișierul infectat și să reconstruiască fișierul original. Această operațiune este denumită dezinfectare. Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere. Pentru mai multe informații, consultă capitolul Gestionarea fișierelor aflate în carantină (pagina 65).

În cazul în care dispozitivul tău a fost infectat cu amenințări, consultă Eliminarea amenințărilor din sistemul tău (pagina 141). Pentru a te ajuta să îți cureți dispozitivul de amenințările care nu pot fi eliminate din sistemul de operare Windows, Bitdefender îți pune la dispoziție Mediu de salvare (pagina 142). Acesta este un mediu sigur, creat în special pentru eliminarea amenințărilor, care îți permite să pornești dispozitivul în mod independent de Windows. Când dispozitivul funcționează în modul de recuperare, amenințările pentru Windows sunt inactive, ceea ce înseamnă că pot fi eliminate cu ușurință.

3.1.1. Scanare la accesare (protecție în timp real)

Bitdefender oferă protecție în timp real contra unei game extinse de amenințări, scanând toate fișierele și mesajele e-mail accesate.

Activarea sau dezactivarea protecției în timp real

Pentru a activa sau dezactiva protecția în timp real împotriva amenințărilor:

1. Fă clic pe **Protecție** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **ANTIVIRUS**, apasă pe **Deschide**.
3. În fereastra **Setări avansate**, activează sau dezactivează **Bitdefender Shield**.
4. Dacă doriți să dezactivați protecția în timp real, se afișează o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 de minute, pentru o oră, permanent sau doar până la repornirea sistemului. Protecția în timp real se va activa automat la expirarea intervalului de timp selectat.

Avertizare

Aceasta este o problemă majoră de securitate. Îți recomandăm să dezactivezi protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu vei mai fi protejat împotriva amenințărilor.

Configurarea setărilor avansate de protecție în timp real

Utilizatorii avansați pot beneficia în urma ofertelor Bitdefender în ceea ce privește setările de scanare. Puteți configura setările protecției în timp real în detaliu prin crearea unui nivel de protecție personalizat.

Pentru a configura setările avansate de protecție în timp real:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Avansat** poți configura setările scanării după nevoie.

Informații cu privire la opțiunile de scanare

Aceste informații îți pot fi de folos:

- **Scanează numai aplicații.** Poți configura Bitdefender să scaneze doar aplicațiile accesate.
- **Scanează aplicațiile potențial nedorite.** Selectează această opțiune pentru a scana aplicațiile nedorite. O aplicație potențial nedorită (PUA) sau un program potențial nedorit (PUP) este un software care este, de obicei, integrat într-un software gratuit și care va afișa mesaje pop-up sau va instala o bară de instrumente în browserul implicit. Unele dintre acestea vor schimba pagina principală sau motorul de căutare, altele vor rula o serie de procese în fundal, încetinind calculatorul, sau vor afișa mai multe reclame. Aceste programe pot fi instalate fără consimțământul tău (denumite și adware) sau vor fi incluse implicit în kitul de instalare (susținute prin reclame).
- **Scanează pentru detectarea scripturilor.** Caracteristica Scanează pentru detectarea scripturilor permite Bitdefender să scaneze scripturile powershell și documentele Office care ar putea conține malware bazat pe scripturi.
- **Scanează directoare comune din rețea.** Pentru a accesa în siguranță o rețea de la distanță de pe dispozitivul tău, îți recomandăm să păstrezi activată opțiunea Scanează directoare comune din rețea.
- **Scanează memoria de procesare.** Scanează pentru a detecta activitatea periculoasă în memoria utilizată pentru rularea proceselor.
- **Scanează linie de comandă.** Scanează linia de comandă a aplicațiilor nou lansate pentru a preveni atacurile fileless.
- **Scanează arhive.** Scanarea arhivelor interne este un proces lent și care consumă resurse, prin urmare, nu este recomandat pentru a asigura protecția în timp real. Arhivele care conțin fișiere infectate nu reprezintă o amenințare imediată pentru securitatea sistemului tău. Amenințarea îți poate afecta sistemul doar dacă fișierul infectat este extras din

arhivă și executat fără o protecție activată care funcționează în timp real.
Dacă decizi să utilizezi această opțiune, activeaz-o și apoi trage cursorul pentru a exclude de la scanare arhivele care depășesc o anumită valoare în MB (megaocteți).

- **Scanează sectoarele de boot.** Poți configura Bitdefender să scaneze sectoarele de boot ale hard diskului. Acest sector al hard diskului conține codul necesar pentru a iniția procesul de boot. În momentul în care o amenințare infectează sectorul de boot, unitatea poate deveni inaccesibilă și este posibil să nu mai poți porni sistemul și accesa datele.
- **Scanează numai fișiere noi și modificate.** Prin scanarea exclusivă a fișierelor noi și a acelor modificate, poți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
- **Scanează pentru a detecta programe tip keylogger.** Selectează această opțiune pentru a scana sistemul pentru a detecta aplicații de tip keylogger. Aceste aplicații înregistrează ceea ce tastezi pe tastatura ta și trimite rapoarte pe internet către un hacker. Acesta pot afla informații confidențiale din datele furate, precum numerele conturilor bancare și parole și le poate utiliza pentru a obține beneficii personale.
- **Scanare preliminară la încărcarea sistemului.** Selectează opțiunea de **Scanare preliminară la încărcarea sistemului** pentru a scana sistemul la pornire de îndată ce se încarcă toate serviciile importante ale acestuia. Misiunea acestei caracteristici este de a îmbunătăți detecția amenințărilor la pornirea sistemului, precum și timpul de încărcare a sistemului.

Acțiuni aplicate pentru amenințările detectate

Poți configura acțiunile inițiate de protecția în timp real urmând acești pași:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Setări avansate**, derulează în jos până când vezi opțiunea **Acțiuni amenințări**.
4. Configurează setările de scanare după cum este nevoie.

Următoarele acțiuni pot fi inițiate de protecția în timp real în Bitdefender:

Aplică acțiunea adecvată

Bitdefender va aplica acțiunile recomandate în funcție de tipul fișierului detectat:

- **Fișiere infectate.** Fișierele detectate ca fiind infectate corespund unei informații privind o amenințare detectată în Baza de date cu informații despre amenințări a Bitdefender. Bitdefender va încerca automat să îndepărteze codul periculos din fișierul infectat și să reconstruiască fișierul inițial. Această operațiune este denumită ca dezinfecție.

  Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Pentru mai multe informații, consultă capitolul Gestionarea fișierelor aflate în carantină (pagina 65).

  Important
  Pentru anumite tipuri de amenințări, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

- **Fișiere suspecte.** Fișierele sunt detectate ca fiind suspecte de către analiza euristică. Fișierele suspecta nu pot fi dezinfectate, întrucât nu există nicio rutină de dezinfecție disponibilă.

  În mod implicit, fișierele în carantină sunt trimise automat la Laboratoarele Bitdefender pentru a fi analizat de cercetătorii Bitdefender experți în amenințări. Dacă se confirmă prezența unei amenințări, se emite o actualizare a mesajului de informare privind amenințarea pentru a permite eliminarea acesteia.

- **Arhive care conțin fișiere infectate.**
  - Arhivele care conțin doar fișiere infectate sunt șterse în mod automat.
  - Dacă o arhivă conține atât fișiere infectate cât și fișiere curate, Bitdefender va încerca să șteargă fișierele infectate cu condiția să poată apoi reface arhiva cu fișierele curate. Dacă reconstrucția arhivei nu este posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Mutarea în carantină

Mută fișierele detectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat. Pentru

mai multe informații, consultă capitolul Gestionarea fișierelor aflate în carantină (pagina 65).

Refuzarea accesului

În caz că un fișier este infectat, accesul la acesta va fi interzis.

Restaurarea setărilor implicite

Setările implicite de protecție în timp real asigură o bună protecție împotriva amenințărilor cu un impact minor asupra performanțelor sistemului.

Pentru a restaura setările implicite pentru protecția în timp real:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Setări avansate**, derulează în jos până vezi opțiunea **Resetare setări avansate**. Selectează această opțiune pentru a reseta antivirusul la setările prestabilite.

3.1.2. Scanare la cerere

Principalul obiectiv Bitdefender este protejarea dispozitivului tău de amenințări. Aceasta se face nepermițând amenințărilor noi să pătrundă în sistem, prin scanarea mesajelor e-mail și a fișierelor descărcate sau copiate pe dispozitiv.

Există însă riscul ca o amenințare să fi fost în sistem înainte de instalarea Bitdefender. Din acest motiv, este indicat să îți scanezi dispozitivul de amenințări după instalarea Bitdefender. Și este, de asemenea, recomandat să îți scanezi sistemul periodic.

Scanarea la cerere se bazează pe sarcinile de scanare. Sarcinile de scanare sunt cele care specifică opțiunile de scanare și obiectele care să fie scanate. Poți scana dispozitivul oricând dorești prin rularea sarcinilor implicite sau a propriilor sarcini de scanare (sarcini definite de utilizator). Dacă dorești să scanezi anumite locații de pe dispozitivul tău sau să configurezi opțiunile de scanare, poți configura și rula o scanare personalizată.

Scanarea unui fișier sau a unui director pentru detectarea amenințărilor

Se recomandă scanarea fișierelor și directoarelor în orice moment când suspectezi că ar putea fi infectate. Fă clic dreapta pe fișierul sau pe directorul pe care dorești să-l scanezi, indică **Bitdefender** cu mouse-ul și selectează **Scanare cu Bitdefender**. Se va afișa **Asistentul de scanare antivirus** care te va ghida în procesul de scanare. La finalul scanării, ți se va solicita să alegi acțiunile care trebuie implementate asupra fișierelor detectate, dacă este cazul.

Rularea unei scanări rapide

Scanarea rapidă utilizează o tehnologie de scanare "in-the-cloud" (online) pentru a detecta amenințările ce rulează pe sistemul dumneavoastră. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.

Pentru a rula o scanare rapidă:

1. Selectează Protecție din meniul de navigare al interfeței Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În ferestrele **Scanări**, apasă pe butonul **Efectuează scanare** de lângă **Scanare rapidă**.
4. Urmați **programul asistent de scanare antivirus** pentru a finaliza scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate. Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Executarea unei scanări a sistemului

Sarcina Scanare sistem scanează întregul dispozitiv pentru a depista toate tipurile de amenințări care îi pun în pericol securitatea, cum ar fi programele malware, aplicațiile spion, adware, rootkit-urile și altele.

Notă

Deoarece opțiunea de **Scanare a sistemului** efectuează o scanare atentă a întregului sistem, aceasta poate dura un timp. În consecință, este recomandat să execuți această activitate într-un moment când nu utilizezi dispozitivul.

Înainte de a executa o Scanare a sistemului, se recomandă următoarele:

- Asigurați-vă că Bitdefender are actualizate bazele de date cu informațiile privind actualizările. Scanarea dispozitivului folosind informații vechi despre amenințări poate împiedica Bitdefender să detecteze noi amenințări descoperite după ultima actualizare efectuată. Pentru mai multe informații, consultă capitolul Cum actualizezi Bitdefender (pagina 40).
- Închide toate programele deschise.

Dacă dorești să scanezi anumite locații de pe dispozitivul tău sau să configurezi opțiunile de scanare, poți configura și rula o scanare personalizată. Pentru mai multe informații, consultă capitolul Configurarea unei scanări personalizate (pagina 54).

Pentru a rula scanarea completă a sistemului:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În ferestrele **Scanări**, apasă pe butonul **Efectuează scanare** de lângă **Scanare sistem**.
4. La prima rulare a Scanării Sistemului ți se prezintă această caracteristică. Selectează **Ok, am înțeles** pentru a continua.
5. Urmează Expert scanare antivirus pentru a finaliza scanarea. Bitdefender va întreprinde automat acțiunile recomandate pentru fișierele detectate. Dacă rămân amenințări nerezolvate, vi se va solicita să alegeți acțiunile care trebuie întreprinse asupra lor.

Configurarea unei scanări personalizate

În fereastra **Administrare scanări**, poți configura Bitdefender pentru a executa scanări ori de câte ori consideri că dispozitivul tău are nevoie de o verificare pentru depistarea unor potențiale amenințări. Poți opta pentru programarea unei **Scanări de sistem** sau a unei **Scanări rapide**, sau poți crea o sarcină personalizată la alegerea ta.

Pentru a configura în detaliu o nouă scanare personalizată:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În ferestrele **Scanări**, fă clic pe **+Creează scanare**.

4. În câmpul **Nume sarcină**, introdu o denumire pentru scanarea respectivă, apoi selectează locațiile care dorești să fie scanate și fă clic pe **ÎNAINTE**.
5. Configurează următoarele opțiuni generale:
   - **Scanați numai aplicații.** Puteți seta Bitdefender să scaneze numai aplicațiile accesate.
   - **Prioritate scanare sarcină.** Poți alege ce impact ar trebui să aibă un proces de scanare asupra performanței sistemului tău.
     - Automat - Prioritatea procesului de scanare va depinde de activitatea sistemului. Pentru a te asigura că procesul de scanare nu va afecta activitatea sistemului, Bitdefender va decide dacă procesul de scanare trebuie să se execute cu prioritate mare sau mică.
     - Ridicat - Prioritatea procesului de scanare va fi ridicată. Selectând această opțiune, vei permite executarea altor programe cu o viteză redusă, micșorând perioada de timp necesară pentru finalizarea scanării.
     - Redus - Prioritatea procesului de scanare va fi redusă. Selectând această opțiune, vei permite executarea altor programe cu o viteză mai mare, mărind perioada de timp necesară pentru finalizarea scanării.
   - **Acțiuni post-scanare.** Alege ce acțiune ar trebuie să implementeze Bitdefender în cazul în care nu sunt identificate amenințări:
     - Afișează fereastra Sumar
     - Închide dispozitivul
     - Închide fereastra Scanare
6. Dacă dorești să configurezi în detaliu opțiunile de scanare, selectează **Afișează opțiuni avansate**. Poți găsi informații referitoare la scanările incluse în listă la sfârșitul acestei secțiuni.
   Apasă pe **Înainte**.
7. Dacă dorești, poți activa opțiunea **Programează sarcina de scanare** și apoi poți alege când ar trebui să pornească sarcina personalizată pe care ai creat-o.

- La pornirea sistemului
- Zilnic
- Lunar
- Săptămânal

Dacă selectezi Zilnic, Lunar sau Săptămânal, trage de cursor pentru a seta perioada de timp dorită pentru începerea scanării.

8. Selectează **Salvează** pentru a salva setările și a închide fereastra de configurare.
   Procesul de scanare poate dura ceva timp, în funcție de locațiile ce vor fi scanate. Dacă se vor găsi amenințări în timpul procesului de scanare, ți se va solicita să alegi acțiunile care trebuie întreprinse în cazul fișierelor detectate.

Informații despre opțiunile de scanare

Puteți găsi aceste informații utile:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în **glosar**. De asemenea, puteți găsi informații utile pe internet.
- **Scanați aplicații potențial nedorite.** Selectați această opțiune pentru a căuta aplicații nedorite. O aplicație potențial nedorită (PUA) sau un program potențial nedorit (PUP) este un software care vine de obicei la pachet cu un software gratuit și va afișa ferestre pop-up sau va instala o bară de instrumente în browserul implicit. Unii dintre ei vor schimba pagina de start sau motorul de căutare, alții vor rula mai multe procese în fundal încetinind PC-ul sau vor afișa numeroase reclame. Aceste programe pot fi instalate fără consimțământul dumneavoastră (numit și adware) sau vor fi incluse implicit în kitul de instalare rapidă (ad-supported).
- **Scanare arhive.** Arhivele care conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului tău. Amenințarea îți poate afecta doar dacă fișierul infectat este extras din arhivă și executat fără să fie activată o protecție în timp real. Însă, această opțiune este recomandată pentru a detecta și elimina orice amenințare potențială, chiar dacă nu reprezintă o amenințare imediată.
  Trage cursorul pentru a exclude de la scanare arhivele care depășesc o anumită valoare în MB (megaocteți).

Notă
Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

- **Scanați numai fișiere noi și modificate.** Scanând numai fișiere noi și modificate, puteți îmbunătăți considerabil capacitatea de răspuns generală a sistemului, cu un compromis minim în materie de securitate.
- **Scanați sectoarele de boot.** Puteți seta Bitdefender să scaneze sectoarele de pornire ale hard diskului. Acest sector al hard diskului conține codul computerului necesar pentru a începe procesul de pornire. Când o amenințare infectează sectorul de pornire, unitatea poate deveni inaccesibilă și este posibil să nu puteți porni sistemul și să vă accesați datele.
- **Scanare memorie.** Selectează această opțiune pentru a scana programele care rulează în memoria sistemului tău.
- **Scanare regiștri.** Selectează această opțiune pentru a scana cheile de regiștri. Windows Registry este o bază de date care stochează setările și opțiunile de configurare ale componentelor sistemului de operare Windows, precum și ale aplicațiilor instalate.
- **Scanare cookie-uri.** Selectează această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe dispozitivul tău.
- **Scanează keylogger-urile.** Selectați această opțiune pentru a vă scana sistemul pentru aplicații keylogger. Keyloggerii înregistrează ceea ce tastați pe tastatură și trimit rapoarte pe internet unei persoane rău intenționate (hacker). Hackerul poate afla informații sensibile din datele furate, cum ar fi numerele de cont bancar și parolele, și le poate folosi pentru a obține beneficii personale.

Asistentul de scanare antivirus

Oricând inițiezi o scanare la cerere (de exemplu, făcând clic dreapta pe un director, indică Bitdefender cu mouse-ul, apoi selectează **Scanare cu Bitdefender**), va apărea asistentul Bitdefender Antivirus Scan. Urmează indicațiile asistentului pentru a efectua procesul de scanare.

Notă
Dacă asistentul de scanare nu apare, scanarea poate fi configurată să fie efectuată silențios, în fundal. Caută pictograma care arată progresul scanării în **bara de sistem**.

Pasul 1 - Realizarea scanării

Bitdefender va începe scanarea obiectelor selectate. Puteți vedea informații în timp real cu privire la starea scanării precum și statistici (inclusiv timpul consumat, o estimare a timpului rămas și numărul de amenințări detectate).

Așteptați ca Bitdefender să finalizeze scanarea. Procesul de scanare poate dura cateva minute, în funcție de complexitatea scanării.

Oprirea sau întreruperea scanării. Poți opri scanarea în orice moment dorești apăsând pe **STOP**. Vei fi direcționat direct la ultimul pas al asistentului. Pentru a întrerupe temporar procesul de scanare, trebuie doar să apeși pe **PAUZĂ**. Va trebui să faci clic pe **RELUARE** pentru a relua scanarea.

Arhive protejate cu parolă. Când se detectează o arhivă protejată cu o parolă, în funcție de setările de scanare, este posibil să ți se solicite parola. Arhivele protejate prin parolă nu pot fi scanate decât dacă introduci parola. Sunt disponibile următoarele opțiuni:

- **Parola.** Dacă vrei ca Bitdefender să scaneze arhiva, selectează această opțiune și introdu parola. Dacă nu cunoști parola, alege una dintre celelalte opțiuni.
- **Nu solicita o parolă și omite acest obiect la scanare.** Selectează această opțiune pentru a omite scanarea acestei arhive.
- **Omite toate elementele protejate cu parolă fără a le scana.** Selectează această opțiune dacă nu vrei să te preocupi de arhivele protejate cu parolă. Bitdefender nu le va putea scana, însă se va păstra o evidență a acestora în jurnalul scanării.

Alegeți opțiunea dorită și faceți clic pe **OK** pentru a continua scanarea.

Pasul 2 - Selectarea acțiunilor

După finalizarea scanării, ți se va cere să selectezi acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.

Notă

Atunci când execuți o scanare rapidă sau o scanare a sistemului, Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor în timpul scanării. Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Obiectele infectate sunt afișate în grupuri, în funcție de amenințarea cu care sunt infectate. Faceți clic pe linkul corespunzător unei amenințări pentru a afla mai multe informații despre obiectele infectate.

Puteți alege o acțiune globală care să fie aplicată pentru rezolvarea tuturor problemelor găsite, sau puteți alege acțiuni separate pentru fiecare grup de probleme. Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

Aplică acțiunile adecvate

Bitdefender va întreprinde acțiunile recomandate în funcție de tipul de fișier detectat:

- **Fișiere infectate.** Fișierele detectate ca infectate se potrivesc cu o informație de amenințare găsită în Baza de date de informații despre amenințări Bitdefender. Bitdefender va încerca automat să elimine codul rău intenționat din fișierul infectat și să reconstruiască fișierul original. Această operație se numește dezinfecție.

  Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a conține infecția. Fișierele puse în carantină nu pot fi executate sau deschise; prin urmare, riscul de a se infecta dispare. Pentru mai multe informații, consultați Gestionarea fișierelor aflate în carantină (pagina 65).

  Important
  Pentru anumite tipuri de amenințări, dezinfecția nu este posibilă deoarece fișierul detectat este complet rău intenționat. În astfel de cazuri, fișierul infectat este șters de pe disc.

- **Fisiere suspicioase.** Fișierele sunt detectate ca suspecte de analiza euristică. Fișierele suspecte nu pot fi dezinfectate, deoarece nu este disponibilă nicio rutină de dezinfecție. Aceștia vor fi mutați în carantină pentru a preveni o potențială infecție.

  În mod implicit, fișierele în carantină sunt trimise automat la Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender experți în amenințări. Dacă se confirmă prezența unei amenințări, se emite o actualizare de informare privind amenințarea pentru a permite eliminarea acesteia.

- **Arhive care conțin fișiere infectate.**
  - Arhivele care conțin numai fișiere infectate sunt șterse automat.

- Dacă o arhivă conține atât fișiere infectate, cât și fișiere curate, Bitdefender va încerca să șteargă fișierele infectate, cu condiția să poată reconstrui arhiva cu fișierele curate. Dacă reconstrucția arhivei nu este posibilă, veți fi informat că nu poate fi luată nicio măsură pentru a evita pierderea fișierelor curate.

Ștergere

Îndepărtează fișierele identificate ca fiind infectate de pe disc.

Dacă într-o arhivă sunt stocate fișiere infectate împreună cu fișiere curate, Bitdefender va încerca să șteargă fișierele infectate și să refacă arhiva incluzând doar fișierele curate. Dacă reconstrucția arhivei nu este posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Nu efectua nicio acțiune

Nu se va lua nicio acțiune asupra fișierelor detectate. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.

Faceți clic pe **Continuă** pentru a aplica acțiunile specificate.

Pasul 3 - Rezumat

Atunci când BitDefender a remediat toate problemele apărute, rezultatele scanării vor fi afișate într-o nouă fereastră. Dacă doriți informații complete cu privire la procesul de scanare, faceți clic pe **AFIȘEAZĂ JURNAL** pentru a vizualiza jurnalul de scanare.

Important

În majoritatea cazurilor, BitDefender va dezinfecta fișierele infectate detectate sau va izola infecția. Cu toate acestea, există anumite probleme care nu pot fi rezolvate automat. Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare. Pentru mai multe informații și instrucțiuni privind modul de eliminare a amenințărilor în mod manual, consultați Eliminarea amenințărilor din sistemul tău (pagina 141).

3.1.3. Examinarea jurnalelor de scanare

De fiecare dată când efectuezi o scanare, se creează un jurnal de scanare și Bitdefender înregistrează problemele identificate în fereastra Antivirus. Raportul de scanare conține informații detaliate despre procesul

de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

Poți deschide raportul de scanare direct din asistentul de scanare, după ce scanarea a luat sfârșit, apăsând **AFIȘEAZĂ JURNAL**.

Pentru a verifica un jurnal de scanări sau orice infecție detectată ulterior:

1. Clic **Notificări** din meniul de navigare de pe Interfața Bitdefender.
2. În fila **Toate**, selectează notificarea privind ultima scanare.
   Aici poți găsi toate evenimentele de scanare, inclusiv amenințările detectate prin scanarea la accesare, prin scanarea inițiată de utilizator, precum și modificările de stare rezultate de scanările automate.
3. În lista de notificări poți verifica ce operațiuni de scanare au fost realizate recent. Efectuează clic pe o notificare pentru a vizualiza detaliile acesteia.
4. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**.

3.1.4. Scanarea automată a suporturilor media amovibile

Bitdefender detectează automat când conectezi o unitate de stocare amovibilă la dispozitivul tău și o scanează în fundal atunci când este activată opțiunea Scanare automată. Acest lucru este recomandat pentru a preveni pătrunderea amenințărilor pe dispozitivul tău.

Unitățile detectate fac parte din următoarele categorii:

- CD-uri/DVD-uri
- Unitățile de stocare USB, cum ar fi memoriile flash sau hard discurile externe
- unități de rețea mapate (la distanță)

Puteți configura scanarea automată separat pentru fiecare categorie de dispozitive de stocare. Scanarea automată a partițiilor rețelei mapate este dezactivată implicit.

Cum funcționează?

Când detectează un dispozitiv de stocare amovibil, Bitdefender inițiază scanarea pentru depistarea amenințărilor (cu condiția ca scanarea automată să fie activată pentru acel tip de dispozitiv). Veți fi notificat prin intermediul unei ferestre pop-up că a fost detectat un nou dispozitiv și că aceasta este scanat.

În **bara de sistem** va apărea o pictogramă a procesului de scanare Bitdefender. Poți apăsa pe această pictogramă pentru a deschide fereastra de scanare și pentru a vedea progresul scanării.

În momentul în care scanarea este finalizată, va apărea fereastra cu rezultatele scanării care te va informa dacă poți accesa în siguranță fișierele regăsite pe suportul media amovibil.

În majoritatea cazurilor, Bitdefender elimină automat amenințările detectate sau izolează fișierele infectate în carantină. Dacă există amenințări nesoluționate după finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Notă
Luați în considerare faptul că nu poate fi aplicată nicio acțiune în cazul fișierelor suspecte detectate pe CD-uri/DVD-uri. De asemenea, în cazul în care nu beneficiați de privilegiile corespunzătoare, nu poate fi aplicată nicio acțiune în cazul fișierelor infectate sau suspecte detectate pe unități mapate de rețea.

Următoarele informații îți pot fi de folos:

- Vă rugăm să acordați atenție maximă atunci când folosiți un CD/DVD infectat cu amenințări, deoarece o amenințare nu poate fi ștearsă de pe CD/DVD (suportul media este de tip read-only). Asigurați-vă că protecția în timp real este activată pentru a preveni răspândirea amenințărilor în cadrul sistemului dvs. Cea mai bună metodă este să copiați datele inmportante de pe CD pe sistemul dumneavoastră și apoi să aruncați CD-ul.
- Există posibilitatea ca, în unele cazuri, Bitdefender să nu poată elimina amenințările din anumite fișiere din cauza unor constrângeri tehnice sau legale. Un astfel de exemplu este reprezentat de fișierele arhivate cu ajutorul unei tehnologii brevetate (acest lucru se întâmplă din cauză că arhiva nu poate fi recreată corect).
  Pentru a afla cum poți gestiona amenințările, consultă Eliminarea amenințărilor din sistemul tău (pagina 141).

Administrarea scanării a fișierelor media amovibile

Pentru a administra scanarea automată a suporturilor media amovibile:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.

3. Selectează fereastra **Setări**.

Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție. În cazul în care sunt detectate fișiere infectate, Bitdefender va încerca să le dezinfecteze (să elimine codul malițios) sau să le mute în carantină. Dacă ambele acțiuni eșuează, asistentul de scanare Antivirus vă va permite să specificați alte acțiuni pentru a fi aplicate în cazul fișierelor infectate. Opțiunile de scanare sunt standard și nu le puteți modifica.

Pentru cea mai bună protecție, este recomandat să activezi opțiunea **Scanare automată** pentru toate tipurile de dispozitive de stocare amovibile.

3.1.5. Scanare fișier de configurare a gazdelor

Fișierul de configurare a gazdelor vine implicit cu instalarea sistemului de operare și este folosit pentru a mapa numele de gazdă pentru adresele IP de fiecare dată când accesezi o nouă pagină web, te conectezi la FTP sau la alte servere de internet. Este un fișier simplu de tip text, iar programele periculoase îl pot modifica. Utilizatorii avansați știu cum să-l utilizeze pentru a bloca reclamele deranjante, bannerele, cookie-urile terților sau hackerii.

Pentru a configura scanarea fișierului de configurare gazde:

1. Clic **Setări** pe meniul de navigare de pe Interfața Bitdefender.
2. Selectează **Avansat** fila.
3. Activează sau dezactivează opțiunea **Scanare fișier de configurare a gazdelor**.

3.1.6. Configurarea excepțiilor de scanare

Bitdefender permite excluderea de la scanare a anumitor fișiere, directoare sau extensii de fișiere. Această caracteristică are scopul de a evita interferențele cu munca dumneavoastră și poate ajuta la îmbunătățirea performanței sistemului. Excepțiile vor fi folosite de către utilizatorii care au cunoștințe avansate în ceea ce privește computerele. În caz contrar, pot fi folosite urmând recomandările unui reprezentant Bitdefender.

Poți configura setările astfel încât excepțiile să se aplice doar în cazul scanării la accesare sau al scanării la cerere, sau în cazul ambelor scanări. Obiectele excluse de la scanarea la accesare nu vor fi scanate, indiferent dacă acestea sunt accesate de către tine sau de către o aplicație.

Notă

Excepțiile NU se vor aplica în cazul scanării contextuale. Scanarea contextuală este o metodă de scanare la cerere: faceți clic-dreapta pe fișierul sau directorul pe care doriți să-l scanați și selectați **Scanează cu Bitdefender** .

Excluderea fișierelor și directoarelor de la scanare

Pentru a exclude anumite fișiere și directoare de la scanare:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Setări**, apasă pe **Gestionare excepții**.
4. Apasă pe **+Adaugă o excepție**.
5. Introdu calea directorului pe care vrei să îl excluzi de la scanare în câmpul corespunzător.
   În mod alternativ, poți naviga către director făcând clic pe butonul de navigare din partea dreaptă a interfeței, selectându-l și făcând clic pe **OK**.
6. Activează butonul de lângă caracteristica de protecție care nu trebuie să scaneze directorul. Există trei opțiuni:
   - Antivirus
   - Online Threat Prevention
   - Advanced Threat Defense
7. Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

Excluderea extensiilor de fișiere de la scanare

În momentul în care o extensie de fișier este exclusă de la scanare, Bitdefender nu va mai scana fișierele cu acea extensie, indiferent de locația acestora pe dispozitiv. Excepțiile pot fi aplicate, de asemenea, pentru fișierele aflate pe suporturi amovibile, cum ar fi CD-urile, DVD-urile, dispozitivele USB sau unitățile de rețea.

Important

Acționează cu grijă atunci când setezi excepții de scanare pentru extensiile de fișiere deoarece asemenea excepții pot face dispozitivul vulnerabil în fața amenințărilor.

Pentru a exclude extensii de fișiere de la scanare:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În **Setări** fereastra, faceți clic **Gestionați excepțiile**.
4. Clic **+ Adăugați o excepție**.
5. Introdu extensiile care dorești să fie excluse de la scanare cu un punct înaintea lor, separându-le prin punct și virgulă (;).
   `txt;avi;jpg`
6. Activează butonul de lângă caracteristica de protecție care nu trebuie să scaneze extensia.
7. Fă clic pe **Salvare**.

Administrarea excepțiilor de scanare

Dacă excepțiile de scanare configurate nu mai sunt necesare, se recomandă să le ștergi sau să dezactivezi excepțiile de scanare.

Pentru a administra excepțiile de scanare:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Setări**, apasă pe **Gestionare excepții**. Se afișează o listă cu toate excepțiile.
4. Pentru a șterge sau edita excepțiile de scanare, selectează unul dintre butoanele disponibile. Procedați astfel:
   - Pentru a șterge o înregistrare din listă, fă clic pe butonul din dreptul său.
   - Pentru a edita o înregistrare din tabel, selectează butonul **Editare** de lângă aceasta. Se afișează o nouă fereastră unde poți schimba extensia sau calea care va fi exclusă, precum și caracteristica de securitate de la care acestea să fie excluse, după caz. Efectuează modificările necesare, apoi dă clic pe **MODIFICĂ**.

3.1.7. Gestionarea fișierelor aflate în carantină

Bitdefender izolează fișierele infectate cu amenințări ce nu pot fi dezinfectate, precum și fișierele suspecte într-o zonă sigură numită

carantină. Atunci când sunt în carantină, amenințările sunt inofensive, pentru că nu pot fi executate sau citite.

În mod implicit, fișierele puse în carantină sunt trimise automat la Bitdefender Labs pentru a fi analizate de către cercetătorii Bitdefender amenințări. Dacă se confirmă prezența unei amenințări, se eliberează o actualizare a informațiilor pentru a permite eliminarea amenințării.

În plus, Bitdefender scanează fișierele din carantină după fiecare actualizare a bazei de date cu amenințări. Fișierele curățate sunt mutate automat în locația lor originală.

Pentru a verifica și gestiona fișierele din carantină:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Mergi la fereastra **Setări**.
   Aici poți vizualiza denumirile fișierelor în carantină, localizarea lor originală și denumirea amenințărilor detectate.
4. Fișierele aflate în carantină sunt gestionat în mod automat de Bitdefender, în funcție de setările implicite pentru carantină.
   Deși nu este recomandat, poți modifica setările de carantină în funcție de preferințele tale efectuând clic pe **Vizualizare setări**.
   Efectuează clic pe comutatoare pentru a activa sau dezactiva:
   Scanează din nou carantina după actualizarea informațiilor despre amenințări
   Mențineți activată această opțiune pentru a scana în mod automat fișiere aflate în carantină după fiecare actualizare a bazei de date cu informații privind amenințările. Fișierele curățate sunt mutate automat în locația lor originală.
   Ștergere conținutul mai vechi de 30 de zile
   Fișirele aflate în carantină mai vechi de 30 de zile sunt șterse automat.
   Creează excepții pentru fișierele restabilite
   Fișierele pe care le restabilești din carantină sunt mutate înapoi în locația lor inițială fără a fi reparate și sunt automat excluse de la scanările următoare.
5. Pentru a șterge un fișier aflat în carantină, selectați-l și faceți clic pe butonul **Șterge**. Dacă doriți să restaurați un fișier aflat în carantină în locația sa originală, selectați-l și faceți clic pe **Restaurează**.

3.2. Apărare avansată împotriva amenințărilor

Bitdefender Advanced Threat Defense este o tehnologie inovatoare de detecție proactivă, care folosește metode euristice avansate pentru a detecta ransomware și alte amenințări noi potențiale în timp real.

Advanced Threat Defense monitorizează continuu aplicațiile care rulează pe dispozitivul tău, căutând amenințări. Fiecare dintre aceste acțiuni are un anumit punctaj iar punctajul global este calculat pentru fiecare proces.

Ca o măsură de siguranță, vei fi anunțat de fiecare dată când se detectează și se blochează amenințări și procese potențial periculoase.

3.2.1. Activarea sau dezactivarea funcției Advanced Threat Defense

Pentru a activa sau dezactiva funcția Advanced Threat Defense

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **ADVANCED THREAT DEFENSE**, fă clic pe **DESCHIDE**.
3. Accesează fereastra **Setări** și selectează butonul de lângă **Bitdefender Advanced Threat Defense**.

> **Notă**
> Pentru a-ți menține sistemul protejat de ransomware și toate celelalte amenințări, îți recomandăm să dezactivezi funcția Advanced Threat Defense cât mai puțin timp posibil.

3.2.2. Verificarea atacurilor malware detectate

Ori de câte ori sunt detectate amenințări sau procese potențial dăunătoare, Bitdefender le va bloca pentru a preveni infectarea dispozitivului cu ransomware sau cu alte programe malware. Poți verifica în orice moment lista atacurilor malware detectate urmând acești pași:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Apărare avansată împotriva amenințărilor** panou, faceți clic **Deschis**.
3. Mergi la fereastra **Threat Defense**.
   Sunt afișate atacurile detectate în ultimele 90 de zile. Pentru a afla detalii despre tipul de ransomware detectat, calea procesului periculos,

sau dacă dezinfectarea a fost efectuată cu succes, efectuează clic pe acesta.

3.2.3. Adăugarea proceselor în lista de excepții

Poți configura regulile de excludere pentru aplicațiile sigure astfel încât funcția Advanced Threat Defense să nu le blocheze dacă întreprind acțiuni ce pot părea amenințătoare.

Pentru a începe adăugarea proceselor în lista de excepții a funcției Advanced Threat Defense:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Apărare avansată împotriva amenințărilor** panou, faceți clic **Deschis**.
3. În **Setări** fereastra, faceți clic **Gestionați excepțiile**.
4. Clic **+ Adăugați o excepție**.
5. Introduceți calea folderului pe care doriți să-l faceți, cu excepția scanării, în câmpul corespunzător.
   În mod alternativ, poți naviga către fișierul executabil făcând clic pe butonul de navigare din partea dreaptă a interfeței, selectându-l și făcând clic pe **OK**.
6. Activează butonul de lângă **Advanced Threat Defense**.
7. Clic **Salvați**.

3.2.4. Detecție exploit-uri

Una dintre metodele folosite de hackeri pentru a pătrunde în sisteme este de a profita de anumite erori sau vulnerabilități prezente în software-ul (aplicații sau plugin-uri) și hardware-ul computerelor. Pentru a te asigura că dispozitivul tău este protejat de astfel de atacuri, care în mod normal se răspândesc foarte rapid, Bitdefender utilizează cele mai noi tehnologii anti-exploit-uri.

3.2.5. Activarea sau dezactivarea funcției de detecție exploit-uri

Pentru a activa sau dezactiva funcția de detecție exploit-uri:

- Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.

- În **Apărare avansată împotriva amenințărilor** panou, faceți clic **Deschis**.
- Accesează fereastra **Setări** și selectează butonul de lângă **Detecție exploit-uri** pentru a activa sau dezactiva caracteristica.

> **Notă**
> Opțiunea Detecție exploit-uri este activată în mod implicit.

3.3. Prevenirea amenințărilor online

Bitdefender Online Threat Prevention asigură o experiență de navigare în siguranță, alertându-te cu privire la posibilele pagini web periculoase.

Bitdefender oferă funcția de prevenire în timp real a amenințărilor pentru:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Pentru a configura setările Online Threat Prevention:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **ONLINE THREAT PREVENTION**, fă clic pe **Setări**.

În secțiunile **Protecție web**, selectează butoanele pentru activare sau dezactivare:

- Funcția de prevenire a atacurilor web blochează amenințările care vin de pe internet, inclusiv descărcările neintenționate.
- Asistență pentru căutare, o componentă care clasifică rezultatele căutărilor efectuate cu ajutorul motoarelor de căutare și link-urile publicate în rețelele sociale prin afișarea unei pictograme în dreptul fiecărui rezultat:

  Nu îți recomandăm să vizitezi această pagină web.

  Această pagină poate avea conținut periculos. Procedează cu precauție dacă decizi să o vizitezi.

Aceasta este o pagină sigură.

Funcția de Asistență pentru căutare clasifică rezultatele generate de următoarele motoare de căutare:

- Google
- Yahoo!
- Bing
- Baidu

Funcția de Asistență pentru căutare clasifică link-urile publicate pe următoarele site-uri de socializare:

- Facebook
- Twitter

- Scanare web criptată.
  Atacurile mai sofisticate pot folosi trafic de web securizat pentru a induce în eroare victimele. Prin urmare, îți recomandăm să păstrezi activată opțiunea Scanare web criptată.
- Protecție antifraudă.
- Protecție antiphishing.

Derulează și vei ajunge la secțiunea **Network threat prevention**. Aici vei găsi opțiunea **Network threat prevention**. Pentru a îți păstra dispozitivul protejat împotriva atacurilor programelor periculoase (cum ar fi ransomware) prin exploatarea vulnerabilităților, păstrează activă această opțiune.

Poți crea o listă de site-uri, domenii și adrese IP care nu vor fi scanate de motoarele contra amenințărilor, tentativelor de phishing și antifraudă Bitdefender. Lista trebuie să conțină numai site-uri web, domenii și adrese IP în care aveți încredere deplină.

Pentru a configura și administra site-urile web, domeniile și adresele IP folosind funcția Online Threat Prevention pusă la dispoziție de Bitdefender:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **PREVENIREA AMENINȚĂRILOR ONLINE** panou, faceți clic **Setări**.
3. Apasă pe **Gestionare excepții**.
4. Clic **+ Adăugați o excepție**.

5. Introdu în câmpul corespunzător denumirea site-ului web, numele domeniului sau adresa IP pe care dorești să o adaugi la excepții.
6. Activează butonul de lângă **Online Threat Prevention**.
7. Pentru a elimina o intrare din listă, faceți clic pe 🗑 butonul de lângă el. Clic **Salvați** pentru a salva modificările și a închide fereastra.

3.3.1. Alertele Bitdefender din browser

De fiecare dată când încerci să vizitezi un site web clasificat ca fiind nesigur, acesta este blocat și este deschisă o pagină de avertizare în browser-ul tău.

Pagina conține informații precum URL-ul site-ului web și amenințarea detectată.

Trebuie să decideți ce veți face în continuare. Sunt disponibile următoarele opțiuni:

- Părăsește site-ul web respectiv dând clic pe **REVENIRE LA O PAGINĂ SIGURĂ**.
- Accesați site-ul web, în ciuda avertismentului, făcând clic pe **Înțeleg riscurile și doresc să accesez această pagină**.
- Dacă ești sigur că pagina web detectată este sigură, selectează **TRIMITE** pentru a o adăuga în lista de excepții. Îți recomandăm să adaugi numai pagini web în care ai deplină încredere.

3.4. Vulnerabilități

Un pas important în protejarea dispozitivului tău împotriva acțiunilor și aplicațiilor periculoase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizezi în mod regulat. Mai mult, pentru a împiedica accesul fizic neautorizat la dispozitivul tău, este necesară configurarea de parole puternice (parole ce nu pot fi ghicite cu ușurință) pentru fiecare cont de utilizator Windows, precum și pentru rețelele Wi-Fi la care te conectezi.

Bitdefender permite remedierea cu ușurință a vulnerabilităților sistemului dumneavoastră prin oricare dintre cele două metode de mai jos:

- Puteți scana sistemul pentru a identifica vulnerabilitățile acestuia și le puteți remedia pas cu pas folosind opțiunea **Scanare vulnerabilitate**.

- Prin intermediul monitorizării automate a vulnerabilităților, puteți verifica și remedia vulnerabilitățile detectate, în fereastra **Notificări**.

Ar trebui să verifici și să remediezi vulnerabilitățile sistemului săptămânal sau o dată la două săptămâni.

3.4.1. Scanarea sistemului pentru identificarea vulnerabilităților

Pentru a detecta vulnerabilitățile sistemului, Bitdefender necesită o conexiune activă la internet.

Pentru a-ți scana sistemul în vederea identificării vulnerabilităților:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **VULNERABILITATE**, apasă pe **Deschide**.
3. În secțiunea **Scanare vulnerabilitate** fă clic pe **Inițiere scanare**, apoi așteaptă ca Bitdefender să verifice dacă există vulnerabilități în sistem. Vulnerabilitățile detectate sunt grupate în trei categorii:
   - **SISTEM DE OPERARE**
     - **Securitatea sistemului de operare**
       Setările modificate ale sistemului care îți pot compromite dispozitivul și datele, cum ar fi avertismentele afișate când fișierele executate efectuează modificări asupra sistemului fără permisiunea ta sau când dispozitivele MTP, cum ar fi telefoanele sau camerele, se conectează și execută diferite operațiuni fără știrea ta.
     - **Actualizări Windows importante**
       Se afișează o listă de actualizări Windows importante care nu sunt instalate pe computerul tău. Ar putea fi necesară repornirea sistemului pentru a permite finalizarea instalării de către Bitdefender. Reține că instalarea actualizărilor poate dura câteva minute.
     - **Conturi Windows vulnerabile**
       Poți vedea lista conturilor de utilizator Windows configurate pe dispozitivul tău și nivelul de protecție asigurat de parola acestora. Puteți să-i solicitați utilizatorului să schimbe parola la următoarea autentificare sau puteți schimba dumneavoastră parola imediat. Pentru a seta o nouă parolă pentru sistemul tău, selectează **Schimbă parola acum**.

Pentru a crea o parolă puternică, îți recomandăm să utilizezi o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

- **APLICAȚII**
  - **Securitatea browserului**
    Modificări ale setărilor dispozitivului tău care permit executarea fișierelor și programelor descărcate prin Internet Explorer fără o validare a integrității, ceea ce ar putea conduce la compromiterea dispozitivului tău.
  - **Actualizări aplicații**
    Pentru a vedea informațiile despre aplicația care urmează a fi actualizată, clic pe numele acesteia din listă.
    Dacă o aplicație nu este la zi, accesează **Descărcare versiune nouă** pentru a descărca versiunea ce mai recentă.
- **REȚEA**
  - **Rețea și date de conectare**
    Setările modificate ale sistemului cum ar fi conectarea automată la rețele hotspot nesecurizate fără știrea ta sau neefectuarea criptării asupra traficului de ieșire prin canalul securizat.
  - **Rețele Wi-Fi și routere**
    Pentru a afla mai multe despre rețeaua wireless și routerul la care ești conectat, clic pe numele acesteia din listă. Dacă se recomandă să setezi o parolă mai puternică pentru rețeaua ta de acasă, asigură-te că urmezi instrucțiunile noastre, astfel încât să poți rămâne conectat fără să-ți faci griji cu privire la confidențialitatea datelor tale.
    Atunci când sunt disponibile și alte recomandări, urmează instrucțiunile pentru a te asigura că rețeaua ta de acasă este protejată de ochii iscoditori ai hackerilor.

3.4.2. Cu ajutorul monitorizării automate a vulnerabilităților

Bitdefender scanează sistemul împotriva vulnerabilităților la intervale regulate, în fundal și păstrează înregistrări ale problemelor detectate în fereastra **Notificări**.

Pentru a verifica și soluționa problemele detectate:

1. Clic **Notificări** pe meniul de navigare de pe Interfața Bitdefender.
2. În fila **Toate**, selectează notificarea privind scanarea Vulnerabilităților.
3. Puteți vizualiza informații detaliate cu privire la vulnerabilitățile sistemului detectate. În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:
   - Dacă sunt disponibile actualizări Windows, efectuează clic pe **Instalare**.
   - Dacă actualizarea automată Windows este dezactivată, faceți clic **Activare**.
   - Dacă o aplicație nu este actualizată, efectuează clic pe **Actualizează acum** pentru a găsi un link către pagina furnizorului, de unde poți instala cea mai recentă versiune a aplicației respective.
   - Dacă un cont de utilizator Windows are o parolă slabă, faceți clic pe **Modificare parolă** pentru a forța utilizatorul să modifice parola la următoarea conectare sau schimbați-o chiar dumneavoastră. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).
   - Dacă funcția de executare automată Windows este activată, faceți clic pe **Remediere** pentru a o dezactiva.
   - Dacă routerul pe care l-ai configurat are configurată o parolă slabă, efectuează clic pe **Modificare parolă** pentru a accesa interfața din care poți configura o parolă puternică.
   - Dacă rețeaua la care ești conectat conține vulnerabilități care pot supune sistemul tău unor riscuri, fă clic pe **Modificare setări Wi-Fi**.

Pentru a configura setările de monitorizare a vulnerabilităților:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.

   Important
   Pentru a primi informări automate cu privire la vulnearibilitățile sistemului sau aplicației, mențineți opțiunea **Vulnerabilitate** activată.

3. Mergi la fila **Setări**.

4. Selectează vulnerabilitățile sistemului care dorești să fie verificate în mod regulat, cu ajutorul comutatoarelor corespunzătoare.

   Actualizări Windows

   Verifică dacă sistemul de operare Windows are instalate cele mai recente actualizări de securitate importante de la Microsoft.

   Actualizări ale aplicației

   Verificați dacă aplicațiile instalate pe sistemul dvs. sunt actualizate. Aplicațiile neactualizate pot fi exploatate de software-uri periculoase, expunându-vă computerul la atacuri din exterior.

   Parolele utilizatorului

   Verifică dacă parolele pentru conturile de Windows și routerele configurate pe sistem sunt ușor de descoperit sau nu. Setând parole care sunt greu de ghicit (parole puternice), va fi mai mult mai dificil pentru hackeri să pătrundă în sistemul dumneavoastră. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

   Autoplay

   Verificați starea caracteristicii de executare automată Windows. Această caracteristică permite pornirea aplicațiilor în mod automat direct de pe CD, DVD, unități USB sau alte dispozitive externe.

   Anumite tipuri amenințări folosesc funcția de executare automată pentru a se răspândi de la suporturile media amovibile în computer. De aceea se recomandă să dezactivați această caracteristică Windows.

   Funcția Asistență Securitate Wi-Fi

   Verifică dacă rețeaua wireless de acasă la care ești conectat este sigură sau nu și dacă are vulnerabilități. De asemenea, verifică dacă parola routerului de acasă este suficient de puternică și află cum o poți face mai sigură.

   Majoritatea rețelelor wireless neprotejate sunt nesigure, permițând astfel hackerilor să aibă acces la activitățile tale private.

   Notă

   Dacă dezactivezi monitorizarea pentru o anumită vulnerabilitate, posibilele probleme aferente nu vor mai fi înregistrate în fereastra Notificări.

3.4.3. Evaluare securitate Wi-Fi

Atunci când te deplasezi, lucrezi dintr-o cafenea sau aștepți în aeroport, conectarea la o rețea wireless publică pentru a face plăți, verifica e-mail-

ul sau conturile pe rețelele sociale poate fi soluția cea mai rapidă. Însă pot exista curioși care să încerce să-ți fure datele personale, urmărind informațiile care trec prin rețea.

Datele personale includ parolele și numele de utilizator pe care le folosești pentru a-ți accesa conturile online, cum ar fi căsuțele de e-mail, conturile bancare, conturile de rețele sociale, dar și mesajele pe care le trimiți.

De obicei, rețelele wireless publice sunt cel mai probabil nesigure deoarece nu necesită parolă la autentificare sau, dacă au parolă, aceasta poate fi pusă la dispoziția oricui dorește să se conecteze. Mai mult, pot exista rețele periculoase sau de tip honeypot, care reprezintă o țintă pentru infractorii cibernetici.

Pentru a te proteja împotriva pericolelor pe care le prezintă hotspoturile wireless publice nesecurizate sau necriptate, funcția Asistentul de securitate Bitdefender pentru Wi-Fi analizează cât de sigură este o rețea wireless și, atunci când este nevoie, îți recomandă să utilizezi **Bitdefender VPN**.

Asistentul de securitate Bitdefender pentru Wi-Fi îți oferă informații despre:

- **Rețelele Wi-Fi de acasă**
- **Rețelele Wi-Fi de birou**
- **Rețelele Wi-Fi publice**

Activarea sau dezactivarea notificărilor pentru Asistență Securitate Wi-Fi

Pentru a activa sau dezactiva notificările pentru Asistență Securitate Wi-Fi:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.
3. Mergi la fereastra **Setări** și activează sau dezactivează opțiunea **Asistent de securitate Wi-Fi**.

Configurarea rețelei Wi-Fi de acasă

Pentru a porni configurarea rețelei tale de acasă:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.

3. Accesează fereastra **Asistent de securitate Wi-Fi** și selectează **Wi-Fi acasă**.
4. În fila **Wi-Fi acasă** apasă pe **SELECTEAZĂ WI-FI ACASĂ**.
   Se va afișa o listă a rețelelor wireless la care te-ai conectat până în prezent.
5. Găsește rețeaua ta de acasă și apoi fă clic pe **SELECTEAZĂ**.

Dacă o rețea de acasă este considerată nesecurizată sau nesigură, sunt afișate recomandări de configurare pentru îmbunătățirea securității.

Pentru a șterge rețeaua wireless pe care ai setat-o ca fiind rețeaua ta de acasă, fă clic pe butonul **ȘTERGERE**.

Pentru a adăuga o nouă rețea wireless ca rețea de acasă, accesează opțiunea **Selectează o nouă rețea Wi-Fi acasă**.

Configurarea rețelei Wi-Fi de acasă

Pentru a începe configurarea rețelei tale de la birou:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.
3. Accesează fereastra **Asistent de securitate Wi-Fi** și selectează **Wi-Fi birou**.
4. În fila **Wi-Fi birou** apasă pe **SELECTEAZĂ WI-FI BIROU**.
   Se afișează o listă cu rețelele wireless la care v-ați conectat până acum.
5. Găsește rețeaua ta de la birou și apoi clic pe **SELECTEAZĂ**.

Dacă o rețea de birou este considerată nesecurizată sau nesigură, sunt afișate recomandări de configurare pentru îmbunătățirea securității.

Pentru a șterge rețeaua wireless pe care ai setat-o ca fiind rețeaua ta de birou, accesează opțiunea **ȘTERGE**.

Pentru a adăuga o nouă rețea wireless ca rețea de birou, accesează opțiunea **Selectează o nouă rețea Wi-Fi de birou**.

Wi-Fi Public

Atunci când ești conectat la o rețea nesecurizată sau nesigură, este activat profilul Wi-Fi public. Cât timp acest profil este activ, Bitdefender Antivirus Plus este configurat pentru a pune în aplicare automat următoarele setări:

- Funcția Advanced Threat Defense este activă
- Firewall-ul Bitdefender este pornit și următoarele setări sunt aplicate adaptorului tău wireless:
  - Mod ascuns - PORNIT
  - Tipul rețelei - Public
- Următoarele setări din Online Threat Prevention sunt activate:
  - Scanare web criptată
  - Protecție împotriva fraudelor
  - Protecție împotriva tentativelor de phishing
- Este disponibil un buton care deschide Bitdefender Safepay™. În acest caz, protecția Hotspot pentru rețele nesecurizate este activată în mod implicit.

Verifică informațiilor despre rețelele Wi-Fi

Pentru a verifica informațiile despre rețelele wireless la care te conectezi de obicei:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.
3. Accesează fereastra **Asistent de securitate Wi-Fi**.
4. În funcție de informațiile de care ai nevoie, selectează una dintre următoarele trei file: **Wi-Fi acasă**, **Wi-Fi birou** sau **Wi-Fi publică**.
5. Fă clic pe **Vizualizare detalii** din dreptul rețelei despre care dorești să afli mai multe informații.

Există trei tipuri de rețele wireless filtrate în funcție de importanța lor, fiecare marcat printr-o anumită pictogramă:

Wi-Fi nu este sigur - indică faptul că nivelul de securitate al rețelei este prea scăzut. Acest lucru înseamnă că utilizarea rețelei prezintă un risc ridicat și nu este recomandată pentru efectuarea de plăți sau pentru verificarea conturilor bancare fără o protecție suplimentară. În astfel de situații, îți recomandăm să utilizezi Bitdefender Safepay™ cu protecție Hotspot pentru rețelele nesigure activate.

Wi-Fi nu este sigur - indică faptul că nivelul de securitate al rețelei este moderat. Acest lucru înseamnă că poate prezenta vulnerabilități și

nu este recomandată pentru efectuarea de plăți sau pentru verificarea conturilor bancare fără o protecție suplimentară. În astfel de situații, îți recomandăm să utilizezi Bitdefender Safepay™ cu protecție Hotspot pentru rețelele nesigure activate.

Wi-Fi este sigur - indică faptul că rețeaua pe care o utilizezi este sigură. În acest caz, poți folosi date sensibile pentru a realiza operațiuni online.

Atunci când efectuați clic pe link-ul **Vizualizare detalii** din dreptul fiecărei rețele, se afișează următoarele detalii:

- **Securizate** - aici puteți vedea dacă rețeaua selectată este securizată sau nu. Rețelele necriptate pot face ca datele pe care le folosești să fie expuse.
- **Tip de criptare** - aici poți vedea tipul de criptare folosit de rețeaua selectată. Unele tipuri de criptare pot fi nesigure. Prin urmare, îți recomandăm să verifici informațiile despre tipul de criptare afișat pentru a te asigura că ești protejat în timp de navighezi pe internet.
- **Canal/Frecvență** - aici poți vizualiza frecvența canalului utilizat de rețeaua selectată.
- **Complexitatea parolei** - aici poți vedea cât de puternică este parola. Te rugăm să reții că rețelele cu parole slabe reprezintă o țintă pentru infractorii cibernetici.
- **Tipul autentificării** - aici poți verifica dacă rețeaua selectată este sau nu protejată prin parolă. Se recomandă să te conectezi numai la rețele cu parole puternice.
- **Tip de autentificare** - aici poți vedea tipul de autentificare folosit de rețeaua selectată.

3.5. Remediere ransomware

Bitdefender Ransomware Remediation creează backupuri pentru fișierele tale precum documente, fotografii, videoclipuri sau muzică pentru a se asigura că sunt protejate împotriva distrugerii sau pierderii lor în cazul unui atac prin criptare ransomware. De fiecare dată când se detectează un atac ransomware, Bitdefender va bloca toate procesele implicate în atac și va începe procesul de remediere. În acest fel, vei putea să recuperezi conținutul tuturor fișierelor tale fără să plătești suma solicitată de răscumpărare.

3.5.1. Activarea sau dezactivarea funcției Remediere ransomware

Pentru a activa sau dezactiva funcția Remediere ransomware:

1. 1. Apasă pe **Protecție** în meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **REMEDIERE RANSOMWARE**, activează sau dezactivează opțiunea.

> **Notă**
> Pentru a te asigura că fișierele tale sunt protejate împotriva atacurilor ransomware, îți recomandăm să păstrezi activă opțiunea Remediere ransomware.

3.5.2. Activarea sau dezactivarea restabilirii automate

Restabilirea automată se asigură că fișierele tale sunt restabilite automat în eventualitatea unei criptări ransomware.

Pentru a activa sau dezactiva restabilirea automată:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **REMEDIERE RANSOMWARE**, fă clic pe **Administrare**.
3. În fereastra Setări, activează sau dezactivează butonul **Restabilire automată**.

3.5.3. Vizualizarea fișierelor restabilite automat

Atunci când opțiunea **Restabilire automată** este activată, Bitdefender va restabili automat fișierele criptate de ransomware. Astfel, te poți bucura de o experiență fără griji de utilizare a dispozitivului știind că fișierele tale sunt în siguranță.

Pentru a vizualiza fișierele care au fost restabilite automat:

1. Clic **Notificări** din meniul de navigare de pe Interfața Bitdefender.
2. În fila **Toate**, selectează notificarea privind cel mai recent comportament ransomware remediat, apoi apasă pe **Fișiere restabilite**. Este afișată lista fișierelor restabilite. Tot aici poți vedea și locația în care au fost restabilite fișierele tale.

3.5.4. Restabilirea manuală a fișierelor criptate

În cazul în care trebuie să restabilești manual fișierele criptate de ransomware, urmează acești pași:

1. Clic **Notificări** pe meniul de navigare de pe Interfața Bitdefender.
2. În fila **Toate**, selectează notificarea privind cel mai recent comportament ransomware detectat, apoi apasă pe **Fișiere criptate**.
3. Este afișată lista fișierelor criptate.
   Selectează **Recuperare fișiere** pentru a continua.
4. În cazul în care procesul de restabilire eșuează, fie complet, fie parțial, trebuie să selectezi locația în care să fie salvate fișierele decriptate. Selectează **Restabilire locație** și apoi alege o locație din PC-ul tău.
5. Va apărea o fereastră de confirmare.
   Selectează **Finalizare** pentru a finaliza procesul de restabilire.

Fișierele cu următoarele extensii pot fi restabilite în cazul în care sunt criptate:

`.3g2;.3gp;.7z;.ai;.aif;.arj;.asp;.aspx;.avi;.bat;.bin;.bmp;.c;.cda;.cgi;.class;.com;.cpp;.cs;.css;.csv;.dat;.db;.dbf;.deb;.doc;.docx;.gif;.gz;.h264;.h;.flv;.htm;.html;.ico;.jar;.java;.jpeg;.jpg;.js;.jsp;.key;.m4v;.mdb;.mid;.midi;.mkv;.mp3;.mp4;.mov;.mpg;.mpeg;.ods;.odp;.odt;.ogg;.pdf;.pkg;.php;.pl;.png;.pps;.ppt;.pptx;.ps;.psd;.py;.rar;.rm;.rtf;.sav;.sql;.sh;.svg;.swift;.swf;.tar;.tex;.tif;.tiff;.txt;.xlr;.xls;.xlsx;.xml;.wmv;.vb;.vob;.wav;.wks;.wma;.wpl;.wps;.wpd;.wsf;.z;.zip;`

3.5.5. Adăugarea aplicațiilor în lista de excepții

Poți configura reguli de exceptare pentru aplicațiile sigure astfel încât funcția Remediere ransomware să nu le blocheze dacă efectuează acțiuni specifice programelor ransomware.

Pentru a adăuga aplicații în lista de excepții a funcției Remediere ransomware:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **REMEDIERE RANSOMWARE** panou, faceți clic **Administra**.

3. Accesează fereastra **Excepții** și selectează **+Adaugă o excepție**.

3.6. Anti-tracker

Multe dintre site-urile web pe care le accesezi utilizează instrumente de urmărire de tip tracker pentru a colecta informații despre comportamentul tău, fie pentru a le distribui unor companii terțe, fie pentru a afișa anunțuri mai relevante pentru tine. Astfel, proprietarii site-urilor web fac bani pentru a putea oferi conținut gratuit sau pentru a continua să funcționeze. Pe lângă colectarea de informații, tracker-ele pot încetini experiența ta de navigare sau îți pot afecta lățimea de bandă.

Când extensia Bitdefender Anti-tracker este activată în browserul web, aceasta te ajută eviți să fii monitorizat, astfel încât datele tale rămân confidențiale în timp ce navighezi online, precum și să reduci timpul necesar pentru încărcarea site-urilor web.

Extensia Bitdefender este compatibilă cu următoarele browsere web:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Tracker-ele pe care le detectăm sunt grupate în următoarele categorii:

- **Publicitate** - se utilizează pentru a analiza traficul de pe site-urile web, comportamentul utilizatorilor sau tiparele de trafic generat de utilizatori.
- **Interacțiunea cu clienții** - se utilizează pentru a măsura interacțiunea utilizatorilor cu diferite forme de introducere de informații, cum ar fi chat sau suport.
- **Esențiale** - se utilizează pentru a monitoriza funcționalitățile de importanță critică ale paginilor web.
- **Date de analiză site** - se utilizează pentru a colecta date referitoare la utilizarea paginilor web.
- **Rețele de socializare** - se utilizează pentru a monitoriza audiența pe rețelele de socializare, activitatea și implicarea utilizatorilor pentru diferite platforme de socializare.

3.6.1. Interfața Anti-tracker

Când extensia Bitdefender Anti-tracker este activată, pictograma apare lângă bara de căutare din browserul tău web. De fiecare dată când vizitezi

un site web, pe pictogramă vei observa un număr care se referă la trackerele detectate și blocate. Pentru a vizualiza mai multe detalii despre trackerele blocate, apasă pe pictogramă pentru a deschide interfața. În afară de numărul de trackere blocate, poți vizualiza și timpul necesar pentru încărcarea paginii și categoriile din care fac parte trackerele detectate. Pentru a vizualiza lista de site-uri web care sunt urmărite, apasă pe categoria respectivă.

Pentru a dezactiva funcția Bitdefender de blocare a tracker-elor pe site-ul pe care îl accesați în momentul respectiv, selectează opțiunea **Întrerupeți protecția pe acest site**. Această setare se aplică numai atâta timp cât site-ul este deschis și va reveni automat la starea inițială după ce părăsești site-ul web.

Pentru a permite tracker-elor dintr-o anumită categorie să îți monitorizeze activitatea, selectează activitatea dorită și apoi clic pe butonul corespunzător. Dacă te răzgândești, apasă din nou pe același buton.

3.6.2. Dezactivarea Bitdefender Anti-tracker

Pentru a dezactiva modulul Bitdefender Anti-tracker:

- Din browserul dvs. web:
  1. Deschideți browser-ul web.
  2. Apasă pe pictograma de lângă bara de adresă din browserul web.
  3. Apasă pe pictograma din colțul din dreapta sus.
  4. Utilizează butonul corespunzător pentru dezactivare.
     Pictograma Bitdefender devine gri.
- Din interfața Bitdefender:
  1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
  2. În secțiunea **ANTI-TRACKER**, fă clic pe **Setări**.
  3. Dezactivează butonul corespunzător din dreptul browserului web pentru care dorești să dezactivezi extensia.

3.6.3. Permiterea urmăririi unui site web

Dacă dorești ca activitatea ta să fie urmărită în timp ce accesezi un anumit site web, poți adăuga adresa acestuia în lista de excepții, după cum urmează:

1. Deschideți browserul web.
2. Apasă pe pictograma de lângă bara de căutare.
3. Apasă pe pictograma din colțul din dreapta sus.
4. Dacă te afli pe site-ul web pe care dorești să-l adaugi la excepții, selectează opțiunea **Adaugă în listă acest site web**.
   Dacă dorești să adaugi un alt site web, introdu adresa acestuia în câmpul corespunzător și apoi selectează .

3.7. VPN

Aplicația VPN poate fi instalată din produsul tău Bitdefender și poate fi utilizată de fiecare dată când vrei să adaugi un nivel suplimentar de protecție conexiunii tale. Aplicația VPN funcționează ca un tunel între dispozitivul tău și rețeaua la care te conectezi pentru a-ți securiza conexiunea, a-ți cripta datele utilizând criptare la un nivel care este utilizat în sistemul bancar și pentru a-ți ascunde adresa IP oriunde te-ai afla. Traficul tău este redirecționat printr-un server separat, ceea ce face ca dispozitivul tău să fie aproape imposibil de identificat din multitudinea de alte dispozitive care utilizează serviciile noastre. Mai mult, atunci când ești conectat la internet prin Bitdefender VPN, vei putea accesa conținut care este, în mod normal, restricționat în anumite zone.

Notă
Unele țări practică cenzura online, prin urmare utilizarea aplicațiilor VPN pe teritoriul lor este interzisă prin lege. Pentru a evita consecințele legale, este posibil să apară un mesaj de avertizare atunci când încerci să utilizezi aplicația VPN de la Bitdefender pentru prima dată. Prin continuarea utilizării acestei aplicații, confirmi că îți sunt cunoscute reglementările aplicabile din țara respectivă și riscurile la care ai putea fi expus.

3.7.1. Instalarea VPN

Aplicația VPN poate fi instalată din interfața Bitdefender, astfel:

1. Clic **Confidențialitate** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **VPN**, fă clic pe **Instalare VPN**.
3. În fereastra care descrie aplicația VPN, citește **Contractul de abonare** și apoi fă clic pe **INSTALARE BITDEFENDER VPN**.

   Așteaptă câteva momente până ce fișierele sunt descărcate și instalate.

   Dacă este detectată o altă aplicație VPN, îți recomandăm să o dezinstalezi. Dacă instalezi mai multe soluții VPN, este posibil să experimentezi încetiniri ale sistemului sau alte probleme de funcționalitate.
4. Efectuează clic pe **DESCHIDE BITDEFENDER VPN** pentru a finaliza procesul de instalare.

   Notă

   Bitdefender VPN necesită instalarea cadrului .Net Framework 4.5.2 sau a unei versiuni superioare. În cazul în care nu ai instalat acest pachet, se va afișa o fereastră de notificare. Apasă pe **Instalează .Net Framework** și vei fi redirecționat pe o pagină de unde poți descărca cea mai nouă versiune a acestui software.

3.7.2. Deschiderea conexiunii VPN

Pentru a accesa interfața principală a Bitdefender VPN, folosește una dintre următoarele metode:

- Din bara de sistem
  1. Fă clic dreapta pe pictograma din bara de sistem, apoi fă clic pe **Afișează**.
- Din interfața Bitdefender
  1. Clic **Confidențialitate** din meniul de navigare de pe Interfața Bitdefender.
  2. În secțiunea **VPN**, fă clic pe **Deschide VPN**.

3.7.3. Interfața VPN

Interfața VPN afișează starea aplicației, respectiv dacă este conectată sau deconectată. Locația serverului pentru utilizatorii versiunii gratuite

este setată automat de Bitdefender la cel mai adecvat server, în timp ce utilizatorii premium au posibilitatea de a schimba locația serverului la care doresc să se conecteze. Pentru mai multe informații despre abonamentele VPN, accesează Abonamente (pagina 87).

Pentru conectare sau deconectare, pur și simplu efectuează clic pe starea afișată în partea de sus a ecranului sau efectuează click dreapta pe pictograma din bara de sistem. Pictograma din bara de sistem afișează o bifă de culoare verde atunci când aplicația VPN este conectată și o bifă de culoare roșie atunci când aceasta este deconectată.

Când ești conectat, timpul scurs și lățimea de bandă utilizată sunt afișate în partea de jos a interfeței.

Pentru a vizualiza zona **Meniu** în totalitate, apasă pe pictograma din partea stângă sus. Aici vei avea următoarele opțiuni:

- **Contul meu** - sunt afișate detalii despre contul tău Bitdefender și abonamentul VPN. Efectuează clic pe **Schimbă contul** dacă dorești să te conectezi cu un alt cont.
  Selectează **Adaugă aici** pentru a adăuga un cod de activare pentru Bitdefender Premium VPN.
- **Setări** – în funcție de nevoile tale, poți personaliza comportamentul produsului tău. Setările sunt grupate în două categorii:
  - **General**
    - Notificări
    - Pornire - alege dacă vrei ca Bitdefender VPN să ruleze sau nu de la pornire
    - Rapoarte produs - trimite rapoarte anonime despre produs pentru a ne ajuta să îți îmbunătățim experiența
    - Mod întunecat
    - Limbă
  - **Avansat**
    - Comutator pentru oprirea conexiunii la internet - această caracteristică suspendă temporar întreg traficul pe internet în cazul în care conexiunea VPN se întrerupe temporar. Imediat ce revii în mediul online, conexiunea VPN va fi restabilită.

- Conectare automată - Bitdefender VPN se conectează automat când accesezi o rețea Wi-Fi publică/nesecurizată sau când este lansată o aplicație de partajare a fișierelor de tip peer-to-peer

- **Asistență** - poți accesa platforma noastră Support Center unde poți citi un articol util despre cum să folosești Bitdefender VPN sau ne poți trimite feedbackul tău.
- **Despre** – sunt afișate informații despre versiunea instalată.

3.7.4. Abonamente

Bitdefender VPN oferă gratuit o cotă de trafic zilnică de 200 MB pe dispozitiv pentru a-ți securiza conexiunea oricând ai nevoie, conectându-te automat la locația optimă a serverului.

Pentru a obține trafic nelimitat și acces nerestricționat la conținutul din întreaga lume alegând o locație de server în funcție de preferințe, efectuează upgrade la versiunea Premium.

Poți face oricând upgrade la versiunea Bitdefender Premium VPN apăsând butonul **Upgrade** din interfața produsului.

Abonamentul Bitdefender Premium VPN este separat de abonamentul Bitdefender Antivirus Plus, ceea ce înseamnă că îl vei putea utiliza cât timp este valabil, indiferent de starea abonamentului soluției de securitate. În cazul în care abonamentul Bitdefender Premium VPN expiră, dar abonamentul Bitdefender Antivirus Plus este încă activ, vei reveni la versiunea gratuită.

Bitdefender VPN este un produs pentru toate platformele, disponibil în produsele Bitdefender compatibile cu Windows, macOS, Android și iOS. Odată ce faci upgrade la planul Premium, îți vei putea folosi abonamentul pentru toate produsele, cu condiția să te conectezi cu același cont Bitdefender.

3.8. Securitate Safepay pentru tranzacțiile online

Calculatorul a început să devină principalul instrument pentru cumpărături și tranzacții bancare. Achitarea facturilor, transferul de bani, achiziționarea a cam tot ce vă puteți imagina nu au fost niciodată mai rapide sau mai ușoare.

Aceasta implică transmiterea de informații personale, date de cont și credit, parole și alte tipuri de informații personale prin Internet, cu alte

cuvinte, exact tipul de informații pe care infractorii cibernetici sunt foarte interesați să le obțină. Hackerii se străduiesc în permanență să sustragă aceste informații, deci, nu puteți fi niciodată suficient de precauți cu privire la securizarea tranzacțiilor online.

Bitdefender Safepay™ este, în primul rând, un browser protejat, un mediu izolat proiectat să se asigure că operațiunile bancare, cumpărăturile și orice alte tipuri de tranzacții online pe care le efectuezi sunt confidențiale și securizate.

Pentru cea mai bună protecție a confidențialității, Administratorul de parolă Bitdefender a fost integrat în Bitdefender Safepay™ pentru a vă proteja datele ori de câte ori doriți să accesați locații private online.

Bitdefender Safepay™ vă oferă următoarele funcții:

- Blochează accesul la calculatorul tău și orice încercări de a realiza capturi ale ecranului tău.
- Aceasta îți protejează parolele când navighezi pe internet, cu ajutorul modulului Password Manager.
- Include o tastatură virtuală care, dacă este utilizată, nu permite hackerilor să citească ceea ce introduci de pe aceasta.
- Este complet idependentă de celelalte browsere ale tale.
- Include protecție pentru punctele wireless de acces la Internet încorporată pe care o poți utiliza în cazul conectării la rețele Wi-fi nesecurizate.
- Acceptă marcajele și îți permite să navighezi pe site-urile tale preferate de tranzacții bancare/cumpărături.
- Nu se limitează la tranzacții bancare și cumpărături online. Cu Bitdefender Safepay™, poți deschide orice site web.

3.8.1. Cum să utilizezi Bitdefender Safepay™

În mod implicit, Bitdefender detectează dacă navighezi către un site de tranzacții online sau de cumpărături online în orice browser de pe dispozitivul tău și îți solicită să îl lansezi în Bitdefender Safepay™.

Pentru a accesa interfața principală a Bitdefender Safepay™, folosește una dintre următoarele metode:

- Din **interfața Bitdefender**:

1. Clic **Confidențialitate** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **SAFEPAY**, fă clic pe **Setări**.
3. În fereastra **Safepay**, fă clic pe **Lansează Safepay**.

- Din Windows:
  - În **Windows 7**:
    1. Apasă pe **Pornire** și accesează **Toate programele**.
    2. Fă clic pe **Bitdefender**.
    3. Fă clic pe **Bitdefender Safepay™**.
  - În **Windows 8** și **Windows 8.1**:
    Localizați Bitdefender Safepay™ din ecranul de Start Windows (de exemplu, puteți tasta "Bitdefender Safepay™" direct pe ecranul de Start) și apoi faceți clic pe pictograma.
  - În **Windows 10** și **Windows 11**:
    Introduceți "Bitdefender Safepay™" în caseta de căutare din bara de sarcini și faceți clic pe pictogramă.

Dacă ești obișnuit cu browserele web, nu vei avea probleme în utilizarea Bitdefender Safepay ™- acesta arată și se comportă ca un browser obișnuit:

- introdu URL-urile pe care dorești să le accesezi în bara de adrese.
- adaugă file pentru a vizita mai multe site-uri web în fereastra Bitdefender Safepay™ apăsând pe ⊞.
- navighează și reîmprospătează paginile utilizând ← →, și respectiv ↻.
- accesează **setările** Bitdefender Safepay™ printr-un clic și selectează **Setări**.
- protejează-ți parolele cu **Password Manager** făcând clic pe .
- administrează-ți **marcajele** făcând clic pe ☆ de lângă bara pentru adrese.
- deschide tastatura virtuală apăsând pe .

- mărește sau micșorează dimensiunea browserului apăsând simultan tastele **Ctrl** și **+/-** de pe tastatura numerică.
- vizualizează informații despre produsul tău Bitdefender făcând clic pe ⋯ și selectând **Despre**.
- printează informații importante făcând clic pe ⋯ și selectând **Tipărire**.

> **Notă**
> Pentru a comuta între Bitdefender Safepay™ și desktopul Windows, apasă tastele **Alt+Tab** sau fă clic pe opțiunea **Comută pe Desktop** din colțul din stânga sus al ferestrei.

3.8.2. Configurarea setărilor

Fă clic pe ⋯ și selectează **Setări** pentru a configura Bitdefender Safepay™:

Aplică regulile Bitdefender Safepay pentru domeniile accesate

Aici vor apărea site-urile web pe care le-ai adăugat la **Bookmarks** cu opțiunea **Deschidere automată în Safepay** activată. Dacă dorești să dezactivezi deschiderea automat cu Bitdefender Safepay™ a unui site web din listă, clic pe × din dreptul înregistrării dorite din coloana **Ștergere**.

Blochează ferestre pop-up

Poți opta pentru blocarea pop-up-urilor făcând clic pe comutatorul corespunzător.

De asemenea, puteți crea o listă a site-urilor pe care permiteți afișarea pop-up-urilor. Este recomandat ca lista să conțină doar site-uri web în care aveți deplină încredere.

Pentru a adăuga un site în listă, introdu adresa acestuia în câmpul corespunzător și efectuează clic pe **Adaugă domeniu**.

Pentru a șterge un site web din listă, selectează x-ul corespunzător înregistrării dorite.

Administrare plugin-uri

Poți opta pentru activarea sau dezactivarea anumitor plugin-uri din Bitdefender Safepay™.

Administrare certificate

Poți importa certificate din sistemul tău într-un magazin de certificate.

Selectează **IMPORT** și urmează instrucțiunile asistentului pentru a utiliza certificatele în Bitdefender Safepay™.

Utilizează tastatura virtuală

Tastatura virtuală va apărea automat atunci când este selectat un câmp de parolă.

Folosește butonul corespunzător pentru a activa sau dezactiva această funcție.

Confirmarea tipăririi

Activează această opțiune dacă dorești să confirmi înainte ca procesul de tipărire să înceapă.

3.8.3. Administrarea marcajelor

Dacă ați dezactivat detectarea automată a unei părți dintre site-uri sau a tuturor site-urilor sau dacă Bitdefender pur și simplu nu detectează anumite site-uri internet, puteți adăuga marcați în Bitdefender Safepay™ pentru a putea lansa cu ușurință site-urile Internet în viitor.

Urmați pașii de mai jos pentru a adăuga un URL la marcajele Bitdefender Safepay™:

1. Fă clic pe ⋯ și selectează **Marcaje** pentru a deschide pagina Marcaje.

   Notă
   Pagina Marcaje se deschide în mod implicit la lansarea Bitdefender Safepay™.

2. Faceți clic pe butonul **+** pentru a adăuga un marcaj nou.
3. Introduceți URL-ul și titlul marcajului și apoi faceți clic pe **CREEAZĂ**. Faceți clic pe opțiunea **Deschide automat în Safepay** dacă doriți ca pagina marcată să se deschidă cu Bitdefender Safepay™ de fiecare dată când o accesați. URL-ul este și el adăugat la lista Domeniilor de pe pagina setări.

3.8.4. Dezactivarea notificărilor Safepay

Când este detectat un site bancar, produsul Bitdefender este setat să te notifice prin intermediul unei ferestre pop-up.

Pentru a dezactiva notificările Safepay:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **SAFEPAY** panou, faceți clic **Setări**.
3. În fereastra **Setări**, dezactivează butonul din dreptul **Notificări Safepay**.

3.8.5. Utilizarea VPN cu Safepay

Pentru a efectua plăți online într-un mediu sigur în timp ce ești conectat la rețele nesecurizate, produsul Bitdefender poate fi setat să lanseze automat aplicația VPN în același timp cu Safepay.

Pentru a începe utilizarea aplicației VPN împreună cu Safepay:

1. Clic **Confidențialitate** din meniul de navigare de pe Interfața Bitdefender.
2. În **SAFEPAY** panou, faceți clic **Setări**.
3. În fereastra **Setări**, activează butonul din dreptul **Folosește funcția VPN cu Safepay**.

3.9. Bitdefender USB Immunizer

Funcția Autorun încorporată în sistemele de operare Windows este un instrument foarte util care permite dispozitivelor să execute automat un fișier de pe un suport conectat la acestea. De exemplu, instalările aplicațiilor pot începe automat când introduceți un CD în unitatea optică.

Din nefericire, această funcție poate fi utilizată și de amenințări pentru lansarea automată și infiltrarea în dispozitivul tău de pe medii reinscriptibile, cum ar fi unitățile USB și cardurile de memorie conectate prin cititoare de carduri. În ultimii ani au fost create numeroase atacuri bazate pe Autorun.

Cu USB Immunizer, puterți împiedica orice unități flash formatate NTFS, FAT32 sau FAT să mai execute amenințări. După ce un dispozitiv USB a fost imunizat, amenințările nu îl mai pot configura să ruleze o anumită aplicație când dispozitivul este conectat la un dispozitiv pe care rulează Windows.

Pentru a imuniza un dispozitiv USB:

1. Conectează unitatea flash la dispozitivul tău.

2. Navighează în dispozitiv pentru a localiza dispozitivul amovibil de stocare și efectuează clic dreapta pe această pictogramă.
3. În meniul contextual, așează cursorul deasupra **Bitdefender** și selectează **Imunizează această unitate**.

> **Notă**
> Dacă unitatea a fost deja imunizată, în locul opțiunii Imunizare va apărea mesajul **Dispozitivul USB este protejat împotriva amenințărilor cu executare automată**.

Pentru a preveni lansarea amenințărilor de către dispozitivul tău de pe dispozitive USB neimunizate, dezactivează funcția de rulare automată a mediilor. Pentru mai multe informații, consultă capitolul Cu ajutorul monitorizării automate a vulnerabilităților (pagina 73).

4. UTILITĂȚI

4.1. Profiluri

Activitățile de serviciu zilnice, vizionarea filmelor sau jocurile pot încetini performanțele sistemului, cu precădere dacă rulează simultan cu procesele de actualizare Windows și sarcinile de actualizare. Cu Bitdefender, puteți acum alege și aplica profilul dorit, care efectuează ajustările sistemului adecvate pentru îmbunătățirea performanțelor aplicațiilor specifice instalate.

Bitdefender oferă următoarele profiluri:

- Profil de lucru
- Profil film
- Profilul jocului
- **Profil Wi-Fi publică**
- Profilul modului bateriei

Dacă decizi să nu utilizezi **Profiluri**, se activează un profil implicit numit **Standard**, care nu îți optimizează sistemul.

În funcție de activitatea ta, se aplică următoarele setări ale produsului la activarea unui profil Lucru, Film sau Joc:

- Toate alertele și pop-upurile BitDefender sunt dezactivate.
- Actualizarea automată este amânată.
- Scanările programate sunt amânate.
- Modulul antispam este activat.
- Modulul **Asistență pentru căutare** nu este disponibil.
- Notificările privind ofertele speciale sunt dezactivate.

În funcție de activitatea ta, se aplică următoarele setări ale sistemului la activarea unui profil Lucru, Film sau Joc:

- Actualizările automate Windows sunt amânate.
- Alertele și pop-up-urile Windows sunt dezactivate.
- Programele inutile care rulează în fundal sunt suspendate.

- Efectele vizuale sunt adaptate pentru performanțe superioare.
- Sarcinile de întreținere sunt amânate.
- Setările planului de alimentare sunt ajustate.

Cât timp Profilul Wi-Fi este activ, Bitdefender Antivirus Plus este configurat pentru a pune în aplicare automat următoarele setări:

- Advanced Threat Defense este activată
- Paravanul de protecție Bitdefender este pornit și următoarele setări sunt aplicate adaptorului dvs. wireless:
  - Modul Stealth - PORNIT
  - Tip de rețea - Publică
- Următoarele setări din Prevenirea amenințărilor online sunt activate:
  - Scanare web criptată
  - Protecție împotriva fraudei
  - Protecție împotriva phishingului

4.1.1. Profil Lucru

Rularea mai multor sarcini la serviciu, cum ar fi trimiterea de e-mail-uri, comunicarea video cu colegi aflați la distanță sau lucrul cu aplicații de proiectare, vă pot afecta performanțele sistemului. Profilul de serviciu a fost proiectat pentru a vă ajuta să vă îmbunătățiți eficiența la lucru, prin dezactivarea unora dintre serviciile și sarcinile care rulează în fundal.

Configurarea profilului Serviciu.

Pentru a configura măsurile implementate în Profilul Lucru:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Lucru.
4. Selectează ajustările sistemului care dorești să fie aplicate, prin bifarea opțiunilor de mai jos:
   - Crește performanța aplicațiilor de lucru
   - Optimizează setările de produs pentru Profilul Lucru

- Amână programele de fundal și activitățile de întreținere
- Amânare actualizare Windows automată

5. Efectuează clic pe **SALVEAZĂ** pentru a memora schimbările și a închide fereastra.

Adăugarea manuală a aplicațiilor la lista Profil Serviciu

Dacă Bitdefender nu intră automat în Profilul Serviciu când lansezi o anumită aplicație de serviciu, poți adăuga manual aplicația la **Lista aplicațiilor de lucru**.

Pentru a adăuga manual aplicații în Lista de aplicații de lucru din Profilul Serviciu:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Apasă pe **CONFIGURAȚI** butonul din zona Profil de lucru.
4. În fereastra **Setări profil lucru**, fă clic pe **Lista de aplicații**.
5. Fă clic pe **ADAUGĂ**.
   Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

4.1.2. Profil Film

Afișarea videoclipurilor de calitate superioară, cum ar fi filmele de înaltă definiție, necesită resurse semnificative de sistem. Profilul Film adaptează setările sistemului și ale produsului, astfel încât să vă puteți bucura de o experiență plăcută și fără întreruperi.

Configurarea Profilului Film

Pentru a configura măsurile implementate în Profilul Film:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil film.
4. Alegeți ajustările sistemului pe care doriți să le aplicați, bifând următoarele opțiuni:

- Crește performanța aplicațiilor media
- Optimizează setările de produs pentru Profilul Film
- Amânați programele de fundal și sarcinile de întreținere
- Amânați actualizările automate Windows
- Ajustează configurările planului de energie pentru filme

5. Clic **SALVA** pentru a salva modificările și a închide fereastra.

Adăugarea manuală a dispozitivelor de redare video în lista Profil Film

Dacă Bitdefender nu intră automat în Profilul Film când lansați o anumită aplicație pentru redarea video clipurilor, puteți adăuga manual aplicația în **Lista aplicațiilor de film**.

Pentru a adăuga manual jucători video în lista Aplicațiilor de film din Profilul Film:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Apasă pe **CONFIGURAȚI** butonul din zona Profil film.
4. În fereastra **Setări profil film**, fă clic pe **Lista de playere**.
5. Clic **ADĂUGA**.
   Apare o nouă fereastră. Navigați la fișierul executabil al aplicației, selectați-l și faceți clic **Bine** pentru a-l adăuga pe listă.

4.1.3. Profil Joc

Pentru o experiență plăcută a jocului trebuie reduse încărcările de sistem și încetinirile. Folosind metoda euristică comportamentală, alături de o listă de jocuri cunoscute, Bitdefender poate detecta automat jocurile active și poate optimiza resursele sistemului pentru ca dvs. să vă puteți bucura de pauza de joc.

Configurarea Profilului Joc

Pentru a configura măsurile implementate în Profilul Joc:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.

2. În **Profiluri** filă, faceți clic **Setări**.
3. Selectează butonul **Configurează** din zona Profil Joc.
4. Alegeți ajustările sistemului pe care doriți să le aplicați, bifând următoarele opțiuni:
   - Crește performanța jocurilor
   - Optimizează setările de produs pentru Profilul Joc
   - Amânați programele de fundal și sarcinile de întreținere
   - Amânați actualizările automate Windows
   - Ajustează configurările planului de energie pentru jocuri
5. Clic **SALVA** pentru a salva modificările și a închide fereastra.

Adăugare manuală de jocuri la lista de jocuri

În cazul în care Bitdefender nu intră automat în Profilul Joc atunci când ați lansat un anumit joc sau o aplicație, aveți posibilitatea să adăugați aplicația manual la **Lista de aplicații de jocuri**.

Pentru a adăuga manual jocuri în Lista de aplicații de jocuri în Profilul Joc:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Apasă pe **Configurați** butonul din zona Profil de joc.
4. În fereastra **Setări profil joc**, fă clic pe **Lista de jocuri**.
5. Clic **ADĂUGA**.
   Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil al jocului, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

4.1.4. Profil Wi-Fi public

Trimiterea de e-mailuri, introducerea unor date de autentificare sensibile sau cumpărăturile online în timp ce sunteți conectat la rețele wireless nesigure pot expune la riscuri datele dumneavoastră personale. Profilul Wi-Fi public ajustează setările produsului pentru a vă da posibilitatea de a face plăți online și de a utiliza informații sensibile într-un mediu protejat.

Configurarea profilului Wi-Fi public

Pentru a configura Bitdefender să aplice setările produsului în timpul conectării la o rețea wireless nesigură:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Wi-Fi public.
4. Permiteți **să ajusteze setările produsului pentru a optimiza protecția atunci când sunteți conectat la o rețea Wi-Fi publică nesigură căsuța** bifată.
5. Clic **Salvați**.

4.1.5. Profil mod baterie

Modul Baterie se adresează utilizatorilor de laptop si tablete. Scopul este acela de a reduce impactul sistemului și al Bitdefender asupra consumului de electricitate dacă nivelul bateriei este inferior celui implicit sau celui selectat de dumneavoastră.

Configurarea Modului Baterie

Pentru a configura profilul Mod baterie:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Selectează butonul **Configurează** din zona Mod Baterie.
4. Selectează ajustările sistemului care vor fi aplicate, prin bifarea opțiunilor de mai jos:
   - Optimizează setările de produs pentru Profilul Baterie.
   - Amână programele de fundal și activitățile de întreținere.
   - Amânare actualizare Windows automată.
   - Ajustează configurările planului de energie pentru Modul Baterie.
   - Dezactivează dispozitivele externe și porturile de rețea.
5. Clic **SALVA** pentru a salva modificările și a închide fereastra.

Introdu o valoare validă în casetă sau selectează una folosind săgețile sus/jos pentru a specifica când să intre sistemul în Modul Baterie. Implicit, modul este activat când nivelul de încărcare a bateriei scade sub 30%.

Când Bitdefender operează în Modul Baterie, se aplică următoarele setări:

- Actualizarea automată Bitdefender este amânată.
- Scanările programate sunt amânate.

Bitdefender detectează dacă laptopul a fost trecut pe alimentarea cu bateire și, în funcție de nivelul de încărcare al bateriei, intră automat în Modul Baterie. De asemenea, Bitdefender iese automat din modul pentru baterie, atunci când detectează că laptopul nu mai funcționează pe baterie.

4.1.6. Optimizare în timp real

Modulul Bitdefender Optimizare în timp real este un plugin care îmbunătățește performanța sistemului în mod silențios, în fundal, asigurându-se că nu ești întrerupt atunci când este activat un profil. În funcție de sarcina înregistrată la nivelul procesorului, pluginul monitorizează toate procesele, concentrându-se pe cele care au o sarcină mai mare, pentru a le ajusta în funcție de nevoile tale.

Pentru a activa sau dezactiva optimizarea în timp real:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Derulează în jos până când observi opțiunea de optimizare în timp real și apoi folosește butonul corespunzător pentru a o activa sau dezactiva.

4.2. Data Protection

4.2.1. Ștergerea permanentă a fișierelor

Atunci când ștergi un fișier, acesta nu mai poate fi accesat prin metodele obișnuite. Cu toate acestea, fișierul continuă să existe pe hard-disk până ce este suprascris prin copierea altor fișiere.

Bitdefender File Shredder vă ajută să ștergeți definitiv datele eliminându-le fizic de pe hard disk.

Puteți șterge definitiv și rapid fișiere și directoare din dispozitivul dumneavoastră, cu ajutorul meniul contextual Windows, urmând pașii de mai jos:

1. Efectuează clic dreapta pe un fișier sau director pe care dorești să-l ștergi definitiv.
2. Selectează **Bitdefender > Ștergere definitivă fișiere** în meniul contextual afișat.
3. Selectează **Șterge definitiv** și apoi confirmă că dorești să continui procesul.
   Așteptați până când Bitdefender finalizează procesul de ștergere.
4. Sunt afișate rezultatele. Selectează **Finalizare** pentru a părăsi asistentul.

Ca alternativă, poți șterge definitiv fișierele din interfața Bitdefender, după cum urmează:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **Protecția datelor**, fă clic pe **Ștergere definitivă fișiere**.
3. Urmează pașii asistentului de ștergere definitivă a fișierelor:
   a. Selectează butonul **Adaugă directoare** pentru a adăuga fișierele sau directoarele pe care dorești să le ștergi definitiv.
      Ca alternativă, glisează aceste fișiere sau foldere în această fereastră.
   b. Selectează **Șterge definitiv** și apoi confirmă că dorești să continui procesul.
      Așteptați ca Bitdefender să termine de distrugere fișierele.
   c. **Sumarul rezultatelor**
      Rezultatele sunt afișate. Clic **finalizarea** pentru a ieși din vrăjitor.

5. CUM SĂ

5.1. Instalare

5.1.1. Cum instalez Bitdefender pe un al doilea dispozitiv?

Dacă abonamentul achiziționat acoperă mai mult de un dispozitiv, poți utiliza contul tău Bitdefender pentru a activa un al doilea calculator.

Pentru a instala Bitdefender pe un al doilea dispozitiv:

1. Fă clic pe **Instalare pe alt dispozitiv** din colțul din stânga jos al **interfeței Bitdefender**.
   O nouă fereastră apare pe ecran.
2. Clic **SHARE LINK DE DESCARCARE**.
3. Urmează instrucțiunile de pe ecran pentru a instala Bitdefender.

Dispozitivul pe care ați instalat Bitdefender va fi afișat în secțiunea Dispozitivele mele, în Bitdefender Central.

5.1.2. Cum reinstalez Bitdefender?

Printre cazurile care ar putea necesita reinstalarea Bitdefender se numără următoarele:

- ai reinstalat sistemul de operare.
- doresc să remediez problemele care este posibil să fi cauzat încetiniri ale proceselor sau căderi de sistem.
- produsul dumneavoastră Bitdefender nu pornește sau nu funcționează corespunzător.

În eventualitatea în care te afli într-una dintre situațiile menționate mai sus, urmează acești pași:

- În **Windows 7**:
  1. Clic **start** și du-te la **Toate programele**.
  2. Găsește Bitdefender Antivirus Plus și selectează **Dezinstalare**.
  3. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
  4. După finalizarea procesului, va fi necesară repornirea dispozitivului.

- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
  2. Fă clic pe **Dezinstalare** pentru a dezinstala un program sau **Programe și caracteristici**.
  3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
  4. Clic **REINSTALA** în fereastra care apare.
  5. Trebuie să reporniți dispozitivul pentru a finaliza procesul.
- În **Windows 10** și **Windows 11**:
  1. Fă clic pe **Start**, apoi pe **Setări**.
  2. Fă clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații și caracteristici**.
  3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
  4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
  5. Fă clic pe **REINSTALARE**.
  6. Trebuie să reporniți dispozitivul pentru a finaliza procesul.

Notă
Urmând această procedură de reinstalare, setările personalizate sunt salvate și vor fi disponibile în noul produs instalat. Celelalte setări pot fi restabilite la configurația implicită.

5.1.3. De unde pot descărca produsul meu Bitdefender?

Poți instala Bitdefender folosind CD-ul de instalare sau aplicația de instalare web pe care o poți descărca pe dispozitivul tău din platforma Bitdefender Central.

Notă
Înainte de a rula aplicația de instalare, vă recomandăm să dezinstalați orice soluție de securitate de pe sistemul dumneavoastră. Atunci când utilizezi mai multe soluții de securitate pe același dispozitiv, sistemul devine instabil.

Pentru a instala Bitdefender din Bitdefender Central:

1. Acces Bitdefender Central.
2. Selectează **Dispozitivele mele** panou, apoi faceți clic **INSTALATI PROTECTIA**.
3. Alegeți una dintre cele două opțiuni disponibile:
   - **Protejați acest dispozitiv**
     Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
   - **Protejați alte dispozitive**
     Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
     Clic **TRIMITE LINK DE DESCARCARE**. Introduceți o adresă de e-mail în câmpul corespunzător și faceți clic **TRIMITE EMAIL**. Rețineți că linkul de descărcare generat este valabil doar pentru următoarele 24 de ore. Dacă linkul expiră, va trebui să generați unul nou urmând aceiași pași.
     Pe dispozitivul pe care doriți să vă instalați produsul Bitdefender, verificați contul de e-mail pe care l-ați introdus, apoi faceți clic pe butonul de descărcare corespunzător.
4. Rulați produsul Bitdefender descărcat.

5.1.4. Cum folosesc abonamentul Bitdefender după un upgrade Windows?

Această situație apare atunci când faceți un upgrade al sistemului de operare și doriți utilizați în continuare abonamentul Bitdefender.

Dacă utilizezi o versiune Bitdefender anterioară, poți face upgrade gratuit la cea mai nouă versiune Bitdefender, după cum urmează:

- De la versiunea anterioară a Antivirus Bitdefender la cea mai recentă versiune disponibilă a Antivirus Bitdefender.
- De la o versiune anterioară a Bitdefender Internet Security la cea mai recentă versiune disponibilă a Bitdefender Internet Security.
- De la o versiune anterioară a Bitdefender Total Security la cea mai recentă versiune disponibilă a Bitdefender Total Security.

Pot apărea două cazuri:

- Ați făcut upgrade la sistemul de operare folosind Windows Update și ați observat că Bitdefender nu mai funcționează.
  În acest caz, este necesar să reinstalezi produsul urmând acești pași:
  - În **Windows 7**:
    1. Fă clic pe **Start**, accesează **Panoul de control** și fă dublu clic pe **Programe și caracteristici**.
    2. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
    3. Clic **REINSTALA** în fereastra care apare.
    4. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.
       Deschideți interfața noului produs Bitdefender instalat pentru a avea acces la caracteristicile sale.
  - În **Windows 8** și **Windows 8.1**:
    1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
    2. Fă clic pe **Dezinstalează un program** sau pe **Programe și caracteristici**.
    3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
    4. Clic **REINSTALA** în fereastra care apare.
    5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
       Deschideți interfața noului dumneavoastră produs Bitdefender instalat pentru a avea acces la funcțiile acestuia.
  - În **Windows 10** și **Windows 11**:
    1. Clic **start**, apoi apasa **Setări**.
    2. Fă clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații**.
    3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
    4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.

5. Clic **REINSTALA** în fereastra care apare.
6. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
   Deschideți interfața noului dumneavoastră produs Bitdefender instalat pentru a avea acces la funcțiile acestuia.

Notă
Urmând această procedură de reinstalare, setările personalizate sunt salvate și disponibile în noul produs instalat. Alte setări pot fi comutate înapoi la configurația lor implicită.

- Ați modificat sistemul dumneavoastră și doriți să utilizați în continuare protecția Bitdefender. Prin urmare, trebuie să reinstalați produsul folosind cea mai recentă versiune.
  Pentru a rezolva această problemă:
  1. Descarcă fișierul de instalare:
     a. Acces Bitdefender Central.
     b. Selectează **Dispozitivele mele** panou, apoi faceți clic **INSTALATI PROTECTIA**.
     c. Alegeți una dintre cele două opțiuni disponibile:
        - **Protejați acest dispozitiv**
          Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
        - **Protejează un alt dispozitiv**
          Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
          Clic **TRIMITE LINK DE DESCARCARE**. Introduceți o adresă de e-mail în câmpul corespunzător și faceți clic **TRIMITE EMAIL**. Rețineți că linkul de descărcare generat este valabil doar pentru următoarele 24 de ore. Dacă linkul expiră, va trebui să generați unul nou urmând aceiași pași.
          Pe dispozitivul pe care doriți să vă instalați produsul Bitdefender, verificați contul de e-mail pe care l-ați introdus, apoi faceți clic pe butonul de descărcare corespunzător.

2. Rulați produsul Bitdefender pe care l-ați descărcat.

   Pentru mai multe informații cu privire la procesul de instalare Bitdefender, consultați Instalarea produsului dumneavoastră Bitdefender (pagina 6).

5.1.5. Cum pot face upgrade la cea mai recentă versiune Bitdefender?

De acum înainte, actualizarea la cea mai recentă versiune este posibilă fără a urma procedura de dezinstalare și reinstalare manuală. Mai exact, noul produs care include noi caracteristici și îmbunătățiri majore de produs este livrat prin intermediul actualizărilor de produs și, dacă aveți deja un abonament Bitdefender activ, produsul se activează automat.

Dacă folosești versiunea 2020, poți face upgrade la cea mai nouă versiune urmând acești pași:

1. Efectuați clic pe **REPORNEȘTE ACUM** în fereastra de notificare în care sunt afișate informațiile privind actualizarea. Dacă ați ratat-o, accesați fereastra **Notificări**, identificați cea mai recentă actualizare și apoi efectuați clic pe butonul **REPORNEȘTE ACUM**. Așteaptă ca dispozitivul să repornească.

   Se va afișa fereastra **Ce este nou** conținând informațiile despre caracteristicile noi și îmbunătățite.

2. Efectuați clic pe link-urile **Citiți mai multe** pentru redirectare către pagina noastră dedicată conținând mai multe detalii și articole utile.

3. Închideți fereastra **Ce este nou** pentru a accesa interfața noi versiuni instalate.

Utilizatorii care doresc să facă upgrade gratuit de la Bitdefender 2016 sau o versiune anterioară la cea mai recentă versiune a Bitdefender trebuie să dezinstaleze versiunea lor actuală din Panoul de control și apoi să descarce cel mai recent fișier de instalare de pe site-ul Bitdefender accesând următoarea adresă: https://www.bitdefender.com/Downloads/. Activarea este posibilă doar cu un abonament valid.

5.2. Bitdefender Central

5.2.1. Cum mă pot conecta la contul Bitdefender cu un alt cont?

Ai creat un cont Bitdefender nou și vrei să-l utilizezi pe acesta de acum încolo.

Pentru a vă autentifica cu alt cont Bitdefender:

1. Selectează numele contului tău în partea superioară a interfeței **Bitdefender**.
2. Selectează **Schimbă contul** din colțul din dreapta sus al ecranului pentru a schimba contul asociat dispoztivului respectiv.
3. Tastați adresa de e-mail în câmpul corespunzător, apoi faceți clic **URMĂTORUL**.
4. Introduceți parola, apoi faceți clic **CONECTARE**.

Notă

Produsul Bitdefender de pe dispozitivul tău se schimbă automat în funcție de abonamentul asociat noului cont Bitdefender. Dacă nu există niciun abonament disponibil asociat noului cont Bitdefender sau dacă vrei să transferi abonamentul din contul anterior, poți contacta Bitdefender pentru asistență așa cum se descrie în secțiunea Solicitarea ajutorului (pagina 149).

5.2.2. Cum dezactivez mesajele de asistență Bitdefender Central?

Pentru a te ajuta să înțelegi cum să folosești fiecare opțiune din Bitdefender Central, în panoul de bord sunt afișate mesaje de ajutor.

Dacă dorești să nu mai vezi acest tip de mesaje:

1. Acces Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Fă clic pe **Contul meu** în meniul derulant.
4. Selectează opțiunea **Setări** din meniul derulant.
5. Dezactivează opțiunea **Activează/Dezactivează mesajele de ajutor**.

5.2.3. Am uitat parola setată pentru contul meu Bitdefender. Cum se resetează?

Există două posibilități pentru a seta o nouă parolă pentru contul dumneavoastră Bitdefender:

- De la Interfața Bitdefender:
  1. Clic **Contul meu** pe meniul de navigare de pe Interfața Bitdefender.
  2. Selectează {1}Schimbă contul{2} din colțul din dreapta sus al ecranului.
     Se afișează o nouă fereastră.
  3. Introdu adresa ta de e-mail și selectează {1}ÎNAINTE{2}.
     Apare o nouă fereastră.
  4. Clic **Aţi uitat parola?**.
  5. Apasă pe {1}ÎNAINTE{2}.
  6. Verificați-vă contul de e-mail, introduceți codul de securitate pe care l-ați primit, apoi faceți clic **URMĂTORUL**.
     Alternativ, puteți face clic **Schimbaţi parola** în e-mailul pe care ți l-am trimis.
  7. Introduceți noua parolă pe care doriți să o setați, apoi introduceți-o din nou. Clic **SALVA**.

- Din browserul dvs. web:
  1. Mergi la: https://central.bitdefender.com.
  2. Fă clic pe {1}CONECTARE{2}.
  3. Introduceți adresa dvs. de e-mail, apoi faceți clic **URMĂTORUL**.
  4. Clic **Aţi uitat parola?**.
  5. Clic **URMĂTORUL**.
  6. Verifică-ți contul de e-mail și urmărește instrucțiunile furnizate pentru a seta o nouă parolă pentru contul tău Bitdefender.

Pentru a accesa ulterior contul Bitdefender, introduceți adresa e-mail și noua parolă setată.

5.2.4. Cum pot gestiona sesiunile de autentificare asociate contului meu Bitdefender?

În contul dumneavoastră Bitdefender, aveți posibilitatea de a vizualiza cele mai recente sesiuni de autentificare active și inactive de pe dispozitivele asociate contului dumneavoastră. În plus, vă puteți deconecta de la distanță urmând acești pași:

1. Acces Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Selectează **Sesiuni** din meniul derulant.
4. În secțiunea **Sesiuni active**, selectează opțiunea **DECONECTARE** din dreptul dispozitivului pe care dorești să închei sesiunea.

5.3. Scanarea cu BitDefender

5.3.1. Cum scanez un fișier sau un director?

Cea mai ușoară metodă de a scana un fișier sau un director este să faci clic dreapta pe un obiect pe care dorești să-l scanezi, să alegi Bitdefender și să selectezi **Scanează cu Bitdefender** din meniu.

Pentru finalizarea procesului de scanare, urmați pașii asistentului de scanare antivirus. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate.

Dacă rămân amenințări nesoluționate, ți se va cere să selectezi acțiunile ce vor fi aplicate în cazul acestora.

Iată câteva situații în care este recomandată folosirea acestei metode de scanare:

- Suspectezi un anumit fișier sau director că este infectat.
- Atunci când descarci fișiere de pe internet considerate că ar putea fi periculoase.
- Scanează un director comun din rețea înainte de a copia fișiere din acesta pe dispozitivul tău.

5.3.2. Cum îmi scanez sistemul

Pentru a realiza o scanare completă a sistemului:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Fă clic pe butonul **Rulează scanare** din dreptul **Scanare sistem**.
4. Urmați programul asistent Scanare Sistem pentru a încheia scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate.
   Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultă capitolul .

5.3.3. Cum programez o scanare?

Poți configura Bitdefender să activeze scanarea locațiilor importante de sistem când nu te afli la dispozitiv.

Pentru a programa o scanare:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Selectează ··· de lângă tipul scanării pe care vrei să o programezi, Scanare sistem sau Scanare rapidă, în partea inferioară a interfeței, apoi selectează **Editare**.
   Ca metodă alternativă, poți crea un tip de scanare care să corespundă necesităților tale selectând **+Creare scanare** din dreptul **Administrare scanări**.
4. Personalizează scanarea în funcție de nevoile tale, apoi selectează **Înainte**.
5. Bifează caseta de lângă **Alege când vei programa această sarcină**.
   Selectează una dintre opțiunile corespunzătoare pentru a seta un program:
   - La pornirea sistemului
   - Zilnic
   - Săptămânal
   - Lunar

Dacă alegeți Zilnic, Lunar sau Săptămânal, trageți glisorul de-a lungul scalei pentru a seta perioada dorită de timp în care ar trebui să înceapă scanarea programată.

Dacă alegi să creezi o nouă scanare personalizată, se va afișa fereastra **Sarcină de scanare**. De aici poți selecta locațiile care dorești să fie scanate.

5.3.4. Cum creez o activitate de scanare personalizată?

Dacă dorești să scanezi anumite locații de pe dispozitiv sau pentru a configura opțiunile de scanare, poți configura și rula o sarcină de scanare personalizată.

Pentru a crea o activitate de scanare personalizată, procedează după cum urmează:

1. În **ANTIVIRUS** panou, faceți clic **Deschis**.
2. Fă clic pe **+Creare scanare** din dreptul **Administrare scanări**.
3. În câmpul Nume sarcină, introdu o denumire pentru scanarea respectivă, apoi selectează locațiile care dorești să fie scanate și selectează **ÎNAINTE**.
4. Configurați aceste opțiuni generale:
   - **Scanează numai aplicații.** Poți configura Bitdefender să scaneze doar aplicațiile accesate.
   - **Prioritate scanare sarcină.** Poți alege ce impact ar trebui să aibă un proces de scanare asupra performanței sistemului tău.
     - Auto - Prioritatea procesului de scanare va depinde de activitatea sistemului. Pentru a se asigura că procesul de scanare nu va afecta activitatea sistemului, Bitdefender va decide dacă procesul de scanare ar trebui să fie rulat cu prioritate mare sau scăzută.
     - High - Prioritatea procesului de scanare va fi mare. Alegând această opțiune, veți permite altor programe să ruleze mai lent și veți reduce timpul necesar pentru finalizarea procesului de scanare.
     - Scăzută - Prioritatea procesului de scanare va fi scăzută. Alegând această opțiune, veți permite altor programe să ruleze

mai rapid și veți crește timpul necesar pentru finalizarea procesului de scanare.

- **Acțiuni post-scanare.** Alege ce acțiune ar trebuie să implementeze Bitdefender în cazul în care nu sunt identificate amenințări:
  - Afișează fereastra Rezumat
  - Dispozitiv de oprire
  - Închideți fereastra Scanare

5. Dacă dorești să configurezi în detaliu opțiunile de scanare, selectează **Afișează opțiuni avansate**.
   Clic **Următorul**.
6. Dacă dorești, poți activa opțiunea **Programează sarcina de scanare** și apoi poți alege când ar trebui să pornească sarcina personalizată pe care ai creat-o.
   - La pornirea sistemului
   - Zilnic
   - Lunar
   - Săptămânal

   Dacă alegeți Zilnic, Lunar sau Săptămânal, trageți glisorul de-a lungul scalei pentru a seta perioada dorită de timp în care ar trebui să înceapă scanarea programată.
7. Clic **Salvați** pentru a salva setările și a închide fereastra de configurare.
   În funcție de locațiile care urmează să fie scanate, scanarea poate dura ceva timp. Dacă în timpul procesului de scanare vor fi găsite amenințări, vi se va solicita să alegeți acțiunile care trebuie întreprinse asupra fișierelor detectate.

Dacă dorești, poți relua rapid rularea scanării personalizate anterioare, făcând clic pe înregistrarea corespunzătoare din lista valabilă.

5.3.5. Cum exclud un director de la procesul de scanare?

Bitdefender permite excluderea de la scanare a anumitor fișiere, directoare sau extensii de fișiere.

Excepțiile vor fi folosite de către utilizatorii care au cunoștințe avansate privind computerele sau doar în situațiile următoare:

- Ai un director mare pe sistemul tău în care există filme și muzică
- Ai o arhivă mare pe sistemul tău în care păstrezi diferite date.
- Păstrați un director în care să instalați diverse tipuri de software-uri și aplicații în scopuri de testare. Scanarea directorului poate duce la pierderea anumitor date.

Pentru a adăuga un director în lista de Excepții:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Fă clic pe fila **Setări**.
4. Fă clic pe **Gestionare excepții**.
5. Clic **+ Adăugați o excepție**.
6. Introduceți calea folderului pe care doriți să-l faceți, cu excepția scanării, în câmpul corespunzător.
   Alternativ, puteți naviga la folder făcând clic pe butonul de răsfoire din partea dreaptă a interfeței, selectați-l și faceți clic pe **Bine**.
7. Porniți comutatorul de lângă caracteristica de protecție care nu ar trebui să scaneze folderul. Există trei opțiuni:
   - Antivirus
   - Prevenirea amenințărilor online
   - Apărare avansată împotriva amenințărilor
8. Clic **Salvați** pentru a salva modificările și a închide fereastra.

5.3.6. Ce să fac atunci când Bitdefender a detectat un fișier curat ca fiind infectat?

Pot exista situații în care Bitdefender marchează greșit un fișier legitim ca fiind o amenințare (un rezultat fals pozitiv). Pentru a corecta această eroare, adaugă fișierul în secțiunea de excepții:

1. Dezactivează protecția antivirus în timp real a Bitdefender:
   a. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. În fereastra **Setări avansate**, dezactivează **Scutul Bitdefender**.

Se deschide o fereastră de avertizare. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 de minute, pentru o oră, permanent sau doar până la repornirea sistemului.

2. Afișează obiecte ascunse în Windows. Pentru a afla cum să faci acest Cum pot afișa elementele ascunse din Windows? (pagina 125)lucru, consultă .
3. Restaurează fișierul din zona de carantină:
   a. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. Accesează ferestrele **Setări** și fă clic pe **Administrare carantină**.
   d. Selectează fișierul și apoi fă clic pe **Restabilire**.
4. Adaugă fișierul în lista de excepții. Pentru a afla cum să faci acest lucru, consultă Cum exclud un director de la procesul de scanare? (pagina 113).
5. Activați protecția antivirus în timp real a Bitdefender.
6. Contactează un reprezentant al echipei noastre de asistență tehnică și solicită eliminarea mesajului de informare privind amenințările. Pentru a afla cum să faci acest lucru, consultă Solicitarea ajutorului (pagina 149).

5.3.7. Cum aflu ce amenințări au fost detectate de Bitdefender?

De fiecare dată când se efectuează o operațiune de scanare, se creează un jurnal în care Bitdefender înregistrează toate problemele detectate.

Raportul de scanare conține informații detaliate despre procesul de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

Puteți deschide jurnalul de scanare direct din expertul de scanare, odată ce scanarea este finalizată, făcând clic **ARATĂ JURNAL**.

Pentru a verifica mai târziu un jurnal de scanare sau orice infecție detectată:

1. Clic **Notificări** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Toate** fila, selectați notificarea privind cea mai recentă scanare.
   Aici puteți găsi toate evenimentele de scanare a amenințărilor, inclusiv amenințările detectate prin scanarea la acces, scanările inițiate de utilizator și modificările de stare pentru scanările automate.
3. În lista de notificări, puteți verifica ce scanări au fost efectuate recent. Faceți clic pe o notificare pentru a vedea detalii despre aceasta.
4. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**.

5.4. Control date personale

5.4.1. Cum mă asigur că tranzacțiile mele online sunt securizate?

Pentru a asigura confidențialitatea operațiunilor pe care le efectuați online, puteți folosi browserul furnizat de Bitdefender, care vă protejează tranzacțiile și aplicațiile de home banking.

Bitdefender Safepay™ este un browser securizat, proiectat pentru a-ți proteja informațiile privind cardurile bancare, numărul de cont sau orice alte date confidențiale pe care le-ai introdus atunci când accesezi diferite locații online.

Pentru a menține securitatea și confidențialitatea activității tale online:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **SAFEPAY** panou, faceți clic **Setări**.
3. În **Safepay** fereastra, faceți clic **Lansați Safepay**.
4. Fă clic pe butonul pentru a accesa **Tastatura virtuală**.
   Folosiți **Tastatura virtuală** atunci când introduceți informații confidențiale, cum ar fi parolele.

5.4.2. Ce pot face dacă mi-a fost furat dispozitivul?

Furtul de dispozitive mobile - indiferent dacă este vorba despre un smartphone, o tabletă sau un laptop - este una dintre principalele probleme care afectează în prezent indivizii și organizațiile din întreaga lume.

Bitdefender Anti-Theft îți permite nu numai să localizezi și să blochezi dispozitivul furat, dar și să ștergi toate datele pentru a te asigura că acestea nu vor fi folosite de autorii furtului.

Pentru a accesa caracteristicile Anti-Theft din contul tău:

1. Acces Bitdefender Central.
2. Selectează **Dispozitivele mele** panou.
3. Efectuează clic pe fila dispozitivului dorit și selectează **Antifurt**.
4. Selectează funcția pe care dorești să o folosești:
   - **LOCALIZARE** - afișează locația dispozitivului dumneavoastră pe Google Maps.
     Afișează IP - afișează ultima adresă IP a dispozitivului selectat.
   - **Alertă** - trimite o alertă pe dispozitiv.
   - **Blocare** - blochează-ți dispozitivul și setează un cod PIN numeric pentru a-l debloca. De asemenea, poți activa o opțiune corespunzătoare care îi permite Bitdefender să facă fotografii instantanee ale persoanei care încearcă să-ți acceseze dispozitivul.
   - **Ștergere** - șterge toate datele din dispozitivul tău.

> **Important**
> După ce ștergi un dispozitiv, este oprită funcționarea tuturor funcțiilor Anti-Theft.

5.4.3. Cum șterg definitiv un fișier cu ajutorul Bitdefender?

Dacă dorești să ștergi definitiv un fișier din sistemul tău, este necesar să ștergi fizic datele de pe hard disk.

Funcția Ștergere definitivă fișiere a Bitdefender te va ajuta să ștergi rapid fișiere sau directoare din dispozitivul tău prin accesarea meniului contextual Windows, urmând pașii de mai jos:

1. Faceți clic dreapta pe fișierul sau directorul pe care doriți să-l ștergeți definitiv, alegeți Bitdefender și selectați **Ștergere definitivă fișiere**.
2. Clic **Sterge Permanent**, apoi confirmați că doriți să continuați procesul. Așteptați ca Bitdefender să termine de distrugere fișierele.

3. Sunt afișate rezultatele. Efectuați clic pe **Finalizare** pentru a părăsi asistentul.

5.4.4. Cum îmi protejez de hackeri camera web?

Puteți configura produsul Bitdefender pentru a permite sau bloca accesul aplicațiilor instalate la camera web urmând acești pași:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **PROTECTIE VIDEO & AUDIO** panou, faceți clic **Setări**.
3. Mergi la fereastra {1}Protecția cameră web{2} și vei vedea lista cu aplicațiile care au solicitat accesul la camera ta.
4. Îndreaptă cursorul spre aplicația căreia vrei să îi permiți sau să îi blochezi accesul și apoi selectează butonul reprezentat printr-o cameră video care se află lângă aceasta.
   Pentru a vizualiza opțiunile alese de alți utilizatori Bitdefender în legătură cu aplicația selectată, apasă pe pictograma {1}{2}{3}{4}{5}{6}. Vei fi notificat de fiecare dată când aplicațiile selectate sunt blocate de utilizatori Bitdefender.

Pentru a adăuga manual aplicații în această listă selectează butonul {1}Adaugă aplicație{2} și apoi selectează una dintre cele două opțiuni.

- Din Windows Store
- Dintre aplicațiile tale

5.4.5. Cum pot restabili manual fișierele criptate atunci când procesul de restabilire eșuează?

În cazul în care fișierele criptat nu pot fi restabilite automat, le poți restabili manual urmând acești pași:

1. Clic **Notificări** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Toate** fila, selectați notificarea cu privire la cel mai recent comportament ransomware detectat, apoi faceți clic **Fișiere criptate**.
3. Se afișează lista cu fișierele criptate.
   Selectează **Recuperare fișiere** pentru a continua.

4. În cazul în care întregul sau o parte a procesului de restaurare eșuează, trebuie să alegeți locația în care ar trebui să fie salvate fișierele decriptate. Clic **Restaurați locația**, apoi alegeți o locație pe computer.
5. Apare o fereastră de confirmare.
   Clic **finalizarea** pentru a încheia procesul de restaurare.

Fișierele cu următoarele extensii pot fi restaurate în cazul în care sunt criptate:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

5.5. Informații utile

5.5.1. Cum îmi testez soluția de securitate?

Pentru a vă asigura că produsul Bitdefender funcționează corespunzător, vă recomandăm să utilizați testul Eicar.

Testul Eicar îți permite să îți verifici soluția de securitate folosind un fișier de siguranță conceput special pentru acest scop.

Pentru a testa soluția de securitate:

1. Descarcă testul de pe pagina web oficială a organizației EICAR http://www.eicar.org/.
2. Faceți clic pe fila **Fișier de testare anti-malware**.
3. Faceți clic pe **Descărcare** în meniul din stânga.
4. Din zona de **Descărcare folosind protocolul standard http** fă clic pe fișierul de testare **eicar.com**.
5. Vei primi notificarea că pagina pe care încerci să o accesezi conține fișierul de testare EICAR (și nu o amenințare).
   Dacă faceți clic pe **Înțeleg riscurile, vreau să continui oricum**, descărcarea pachetului de testare va începe automat și o fereastră pop-up Bitdefender vă va informa că a fost detectată o amenințare.

Faceți clic pe **Mai multe detalii** pentru a afla mai multe informații despre această acțiune.

Dacă nu primiți nicio alertă Bitdefender, vă recomandăm să contactați Bitdefender pentru asistență, așa cum este indicat la secțiunea Solicitarea ajutorului (pagina 149).

5.5.2. Cum să dezinstalati Bitdefender

Dacă vrei să elimini Bitdefender Antivirus Plus:

- În **Windows 7**:
  1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
  2. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
  3. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
  4. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  2. Clic **Dezinstalează un program** sau **Programe si caracteristici**.
  3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
  4. Clic **ELIMINA** în fereastra care apare.
  5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
- În **Windows 10** și **Windows 11**:
  1. Faceți clic pe **Start**, apoi pe Setări.
  2. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații**.
  3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
  4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
  5. Clic **ELIMINA** în fereastra care apare.

6. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

Notă
Această procedură de reinstalare va șterge definitiv setările personalizate.

5.5.3. Cum să dezinstalati Bitdefender VPN

Procedura de dezinstalare a aplicației Bitdefender VPN este similară celei utilizate pentru eliminarea altor programe din dispozitivul tău:

- În **Windows 7**:
  1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
  2. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.
     Așteaptă până când procesul de dezinstalare este finalizat.
- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  2. Clic **Dezinstalează** un program sau **Programe si caracteristici**.
  3. Găsi **Bitdefender VPN** și selectați **Dezinstalează**.
     Așteptați finalizarea procesului de dezinstalare.
- În **Windows 10** și **Windows 11**:
  1. Clic **start**, apoi faceți clic pe Setări.
  2. Fă clic pe pictograma **Sistem** din secțiunea Setărilor, apoi selectează **Aplicații instalate**.
  3. Găsi **Bitdefender VPN** și selectați **Dezinstalează**.
  4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
     Așteptați finalizarea procesului de dezinstalare.

5.5.4. Cum dezinstalez extensia Bitdefender Anti-tracker?

În funcție de browserul web pe care îl utilizezi, urmează acești pași pentru a dezinstala extensia Bitdefender Anti-tracker:

- Internet Explorer
  1. Fă clic pe ⚙ de lângă bara de căutare, apoi selectează Gestionare add-on. Se afișează lista extensiilor instalate.
  2. Fă clic pe Bitdefender Anti-tracker.
  3. Selectează **Dezactivare** din dreapta jos.
- Google Chrome
  1. Fă clic pe ⋮ din dreptul barei de căutare.
  2. Selectează **Mai multe instrumente** și apoi **Extensii**.
     Se va afișa o listă cu extensiile instalate.
  3. Apasă pe **Eliminare** în căsuța Bitdefender Anti-tracker card.
  4. Selectează opțiunea **Dezinstalează** din fereastra care se deschide.
- Mozilla Firefox
  1. Clic ≡ lângă bara de căutare.
  2. Selectează **Add-on** și apoi **Extensii**.
     Apare o listă cu extensiile instalate.
  3. Fă clic pe ··· și apoi selectează **Eliminare**.

5.5.5. Cum închid automat dispozitivul după finalizarea operațiunii de scanare?

Bitdefender oferă mai multe opțiuni de scanare pe care le puteți folosi pentru a vă asigura că sistemul dumneavoastră nu este infectat cu amenințări. Scanarea întregului dispozitiv poate dura destul de mult timp, în funcție de configurația hardware și software a sistemului tău.

Din acest motiv, Bitdefender vă permite să vă configurați produsul să închidă sistemul imediat după finalizarea scanării.

Spre exemplu: ți-ai terminat treaba și vrei să mergi la culcare. Doriți să efectuați o verificare integrală a sistemului dumneavoastră în vederea detectării amenințărilor cu ajutorulBitdefender.

Pentru a opri dispozitivul în momentul finalizării unei sarcini de Scanare rapidă sau Scanare de sistem:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Scanări**, fă clic pe ··· din dreptul opțiunii Scanare rapidă sau Scanare sistem și apoi selectează **Editare**.
4. Personalizează scanarea în funcție de nevoile tale, apoi selectează **Înainte**.
5. Bifează caseta de lângă **Alege când vei programa această sarcină** și apoi alege când va începe această sarcină.
   Dacă alegeți Zilnic, Lunar sau Săptămânal, trageți glisorul de-a lungul scalei pentru a seta perioada dorită de timp în care ar trebui să înceapă scanarea programată.
6. Clic **Salvați**.

Pentru a închide dispozitivul după finalizarea scanării personalizate:

1. Apasă pe ··· din dreptul opțiunii de scanare personalizată pe care ai creat-o.
2. Fă clic pe **Înainte** și apoi pe **Înainte** din nou.
3. Bifează caseta de lângă **Alege când vei programa această sarcină** și apoi alege când va începe această sarcină.
4. Clic **Salvați**.

Dacă nu este detectată nicio amenințare, dispozitivul se va închide.

Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultă capitolul Asistentul de scanare antivirus (pagina 57).

5.5.6. Cum configurez Bitdefender să utilizeze o conexiune de internet prin proxy?

Dacă dispozitivul tău se conectează la internet prin intermediul unui server proxy, trebuie să configurezi Bitdefender cu setările proxy. În mod normal, Bitdefender detectează și importă în mod automat setările proxy ale sistemului dumneavoastră.

Important
Conexiune de internet de acasă nu sunt folosite, în mod normal, ca server proxy. Ca regulă de bază, verificați și configurați setările conexiunii proxy ale programului Bitdefender atunci când nu funcționează actualizările. Dacă Bitdefender poate folosi actualizări, înseamnă că este configurat corespunzător pentru a se conecta la internet.

Pentru a administra setările proxy:

1. Clic **Setări** pe meniul de navigare de pe Interfața Bitdefender.
2. Selectează **Avansat** fila.
3. Activează **Server proxy**.
4. Fă clic pe **Schimbă proxy**.
5. Există două opțiuni de configurare a setărilor proxy:
   - **Importă setări proxy din browserul implicit** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy necesită un nume de utilizator și o parolă, atunci va trebui să le specificați în câmpurile corespunzătoare.

     Notă
     Bitdefender poate importa setări proxy de la browserele cele mai des folosite, inclusiv cele mai noi versiuni de Microsoft Edge,Internet Explorer, Mozilla Firefox și Google Chrome.

   - **Setări proxy personalizate** - setări proxy pe care le puteți configura cum doriți.
     Următoarele setări trebuie specificate:
     - **Adresă** - tastează IP-ul serverului proxy.
     - **Port** - introdu portul utilizat de Bitdefender pentru a se conecta la serverul proxy.
     - **Nume de utilizator** - introdu numele de utilizator recunoscut de proxy.
     - **Parola** - introdu parola validă a utilizatorului anterior.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Bitdefender va folosi setările proxy disponibile până când va reuși să se conecteze la internet.

5.5.7. Utilizez o versiune Windows pe 32 biți sau pe 64 biți?

Pentru a afla dacă ai un sistem de operare pe 32 sau 64 de biți:

- În **Windows 7**:
  1. Fă clic pe **Start**.
  2. Găsește **Computer** în meniul **Start**.
  3. Fă clic dreapta pe **Computer** și apoi selectează **Proprietăți**.
  4. Sub **System** veți găsi informații referitoare la sistemul dumneavoastră.
- În **Windows 8**:
  1. Din ecranul de Start al Windows, localizați **Computer** (de exemplu, puteți începe să tastați „Computer” direct în ecranul de Start) și faceți clic dreapta pe pictograma acestuia.
     În **Windows 8.1**, găsește **Acest PC**.
  2. Selectează **Proprietăți** din meniul din partea de jos.
  3. Mergi la secțiunea Sistem pentru a vedea tipul sistemului.
- În **Windows 10** și **Windows 11**:
  1. Introdu "System" în caseta de căutare din bara de sarcini și efectuează clic pe pictogramă.
  2. Caută în zona System pentru a afla informații referitoare la tipul de sistem.

5.5.8. Cum pot afișa elementele ascunse din Windows?

Acești pași sunt utili în acele cazuri în care ai de-a face cu o situație în care este implicată o amenințare și trebuie să găsesti și să elimini fișierele infectate, care pot fi ascunse.

Urmează acești pași pentru a afișa obiectele ascunse din Windows:

1. Fă clic pe **Start**, mergi la **Panoul de control**.
   În **Windows 8** și **Windows 8.1**: din ecranul de Start al Windows, găsește **Panoul de control** (de exemplu, poți începe să tastezi „Control panel/ Panoul de control” direct în ecranul de Start) și fă clic pe pictograma acestuia.

2. Selectează **Opțiuni director**.
3. Mergi la fila **Vizualizare**.
4. Selectați **Show hidden files and folders**.
5. Debifați **Hide extensions for known file types**.
6. Debifați **Hide protected operating system files**.
7. Fă clic pe **Aplică**, apoi pe **OK**.

În **Windows 10** și **Windows 11**:

1. Introdu "Show hidden files and folders" în caseta de căutare din bara de sarcini și efectuează clic pe pictogramă.
2. Selectați **Show hidden files, folders, and drives**.
3. clar **Ascunde extensiile pentru tipurile de fișiere cunoscute**.
4. clar **Ascundeți fișierele protejate ale sistemului de operare**.
5. Clic **aplica**, apoi apasa **Bine**.

5.5.9. Cum elimin celelalte soluții de securitate?

Principalul motiv pentru utilizarea unei soluții de securitate este de a asigura protecția și siguranța datelor dumneavoastră. Ce se întâmplă însă când aveți mai multe produse de securitate instalate în același sistem?

Atunci când utilizezi mai multe soluții de securitate pe același dispozitiv, sistemul devine instabil. Programul de instalare al Bitdefender Antivirus Plus detectează în mod automat alte programe de securitate și vă oferă opțiunea de a le dezinstala.

Dacă nu ai dezinstalat celelalte soluții de securitate în timpul instalării inițiale:

- În **Windows 7**:
  1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
  2. Așteaptă câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Dezinstalare**.

4. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  2. Clic **Dezinstalați un program** sau **Programe si caracteristici**.
  3. Așteptați câteva momente până când este afișată lista de software instalat.
  4. Găsiți numele programului pe care doriți să îl eliminați și selectați **Dezinstalează**.
  5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 10** și **Windows 11**:
  1. Clic **start**, apoi faceți clic pe Setări.
  2. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații**.
  3. Găsiți numele programului pe care doriți să îl eliminați și selectați **Dezinstalează**.
  4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
  5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

Dacă nu reușești să elimini cealaltă soluție de securitate, descarcă instrumentul de dezinstalare de pe site-ul furnizorului sau contactează-l direct pentru a-ți oferi instrucțiuni cu privire la dezinstalare.

5.5.10. Cum pot să repornesc sistemul în Safe Mode?

Safe Mode este un mod de funcționare de diagnosticare, utilizat în principal pentru depanarea problemelor care afectează funcționarea normală a sistemului Windows. Printre astfel de probleme se numără driverele incompatibile și amenințările ce împiedică pornirea normală a sistemului Windows. În Safe Mode funcționează numai câteva aplicații, iar Windows încarcă doar driverele de bază și un minim de componente

ale sistemului de operare. Acesta este motivul pentru care majoritatea amenințărilor sunt inactive atunci când Windows se află în Safe Mode și pot fi eliminate cu ușurință.

Pentru a porni Windows în Safe Mode:

- În **Windows 7**:
  1. Repornește dispozitivul
  2. Apăsați tasta **F8** de mai multe ori înainte ca Windows să pornească pentru a avea acces la meniul de pornire.
  3. Selectează **Safe Mode** (Mod de siguranță) în meniul de pornire sau **Safe Mode with Networking** (Mod de siguranță cu rețea) dacă dorești să ai acces la internet.
  4. Apăsați **Enter** și așteptați până când Windows se încarcă în Safe Mode.
  5. Acest proces este finalizat cu un mesaj de confirmare. Apasă pe **OK** pentru a confirma.
  6. Pentru a porni Windows în mod normal, repornește pur și simplu sistemul.

- În **Windows 8**, **Windows 8.1**, **Windows 10** și **Windows 11**:
  1. Lansează aplicația **System Configuration** (Configurație sistem) din Windows apăsând simultan tastele **Windows + R**.
  2. Introdu **msconfig** în caseta de dialog **Open** (Deschide) apoi apasă pe **OK**.
  3. Selectează fila **Boot** (Pornire).
  4. În secțiunea **Boot options** (Opțiuni pornire), bifează caseta **Safe boot** (Pornire în mod de siguranță).
  5. Fă clic pe **Network** (Rețea) și apoi pe **OK**.
  6. Fă clic pe **OK** în fereastra **System Configuration** (Configurare sistem) care te informează că sistemul trebuie repornit pentru ca modificările să poată fi implementate.
     Sistemul tău este în curs de repornire în Safe Mode with Networking.

Pentru a reporni dispozitivul în modul normal, modifică din nou setările lansând **System Operation** (Operațiune sistem) și debifând **Safe boot**

(Pornire în mod de siguranță). Fă clic pe **OK** și apoi pe **Restart** (Repornire). Așteaptă ca noile setări să fie aplicate.

6. REMEDIEREA PROBLEMELOR

6.1. Soluționarea problemelor frecvente

Acest capitol prezintă unele probleme care pot apărea atunci când folosiți BitDefender și vă oferă soluții posibile. Majoritatea acestor probleme pot fi remediate prin configurarea adecvată a setărilor de produs.

Dacă problema dvs nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic BitDefender folosind informațiile din capitolul {1}{2}.

6.1.1. Sistemul meu funcționează lent

De obicei, după instalarea unui program de securitate, este posibil să se producă o ușoară încetinire a funcționării sistemului, fapt ce este normal într-o anumită măsură.

În cazul în care observi o încetinire semnificativă, această problemă poate apărea din următoarele motive:

- **Bitdefender nu este singurul program de securitate instalat pe sistem.**
  Deși Bitdefender caută și dezinstalează programele de securitate detectate în timpul instalării, se recomandă să îndepărtați orice alte

soluții de securitate pe care le-ați utilizat înainte de a iniția instalarea Bitdefender. Pentru mai multe informații, consultă capitolul Cum elimin celelalte soluții de securitate? (pagina 126).

- **Cerințele de sistem pentru rularea Bitdefender nu sunt îndeplinite.**
  Dacă dispozitivul tău nu îndeplinește cerințele de sistem, dispozitivul va fi afectat de încetiniri, mai ales atunci când mai multe aplicații rulează în același timp. Pentru mai multe informații, consultă capitolul Cerințe de sistem (pagina 4).
- **Ai instalat aplicații pe care nu le utilizezi.**
  Orice dispozitiv are programe sau aplicații pe care nu le folosești. Și multe programe nedorite rulează în fundal, ocupând spațiu pe disc și încărcând memoria calculatorului. Dacă nu folosiți un program, dezinstalați-l. Acest lucru este valabil și pentru orice alte programe software sau aplicații de evaluare pe care omiteți să le ștergeți.

  Important
  Dacă suspectezi că un program sau o aplicație este o componentă esențială a sistemului tău de operare, nu le dezinstala, ci contactează Serviciul de asistență clienți al Bitdefender.

- **Sistemul dumneavoastră poate fi infectat.**
  Viteza cu care funcționează sistemul tău și comportamentul general al acestuia pot fi afectate și de amenințări. Programele precum spyware, malware, troieni și adware generează un impact asupra performanței dispozitivului tău. Asigură-te că scanezi periodic sistemul, cel puțin o dată pe săptămână. Se recomandă să utilizezi Bitdefender System Scan pentru că scanează toate tipurile de amenințări care pun în pericol securitatea sistemului tău.
  Pentru a porni Scanarea sistemului:
  1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
  2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
  3. În fereastra **Scanări**, fă clic pe **Efectuează scanare** de lângă **Scanare sistem**.
  4. Urmează pașii asistentului.

6.1.2. Nu începe scanarea

Acest tip de problemă poate avea două cauze principale:

- {1}O instalare anterioară a Bitdefender care nu a fost complet eliminată sau o instalare necorespunzătoare a Bitdefender.{2}
  În acest caz, reinstalează Bitdefender:
  - În **Windows 7**:
    1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
    2. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
    3. Clic **REINSTALA** în fereastra care apare.
    4. Așteaptă finalizarea procesului de reinstalare și apoi repornește sistemul.
  - În **Windows 8** și **Windows 8.1**:
    1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
    2. Clic **Dezinstalează** un program sau **Programe si caracteristici**.
    3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
    4. Clic **REINSTALA** în fereastra care apare.
    5. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.
  - În **Windows 10** și **Windows 11**:
    1. Clic **start**, apoi apasa **Setări**.
    2. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.
    3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
    4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
    5. Clic **REINSTALA** în fereastra care apare.
    6. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.

Notă
Urmând această procedură de reinstalare, setările personalizate sunt salvate și disponibile în noul produs instalat. Alte setări pot fi comutate înapoi la configurația lor implicită.

- **Bitdefender nu este singura soluție de securitate instalată pe sistemul tău.**
  În acest caz:

  1. Dezinstalați cealaltă soluție de securitate. Pentru mai multe informații, consultă capitolul Cum elimin celelalte soluții de securitate? (pagina 126).
  2. Reinstalare Bitdefender:
     - În **Windows 7**:
       a. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
       b. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
       c. Clic **REINSTALA** în fereastra care apare.
       d. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.
     - În **Windows 8** și **Windows 8.1**:
       a. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
       b. Clic **Dezinstalează** un program sau **Programe si caracteristici**.
       c. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
       d. Clic **REINSTALA** în fereastra care apare.
       e. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.
     - În **Windows 10** și **Windows 11**:
       a. Clic **start**, apoi apasa **Setări**.

b. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.

c. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.

d. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.

e. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată

f. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.

Notă
Urmând această procedură de reinstalare, setările personalizate sunt salvate și disponibile în noul produs instalat. Alte setări pot fi comutate înapoi la configurația lor implicită.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru suport, conform descrierii din secțiunea Solicitarea ajutorului (pagina 149).

6.1.3. Nu mai pot utiliza o aplicație

Această problemă apare când încercați să utilizați un program care a funcționat normal înainte de instalarea Bitdefender.

După instalarea Bitdefender ar putea apărea următoarele situații:

- Este posibil să primiți un mesaj din partea Bitdefender referitor la faptul că programul încearcă să efectueze o modificare asupra sistemului.
- Este posibil să primiți un mesaj de eroare din partea programului pe care încerci să-l utilizezi.

Acest tip de situație apare când Advanced Threat Defense detectează din greșeală anumite aplicații ca fiind rău intenționate.

Advanced Threat Defense este un modul Bitdefender care monitorizează în mod constant aplicațiile care rulează pe sistemul dumneavoastră și raportează acele aplicații care sunt posibil rău intenționate. Deoarece această opțiune se bazează pe un sistem euristic, pot exista situații în care aplicații legitime să fie raportate de Advanced Threat Defense.

Atunci când se întâmplă aceasta, poți exclude aplicația respectivă de la monitorizarea efectuată de Advanced Threat Defense.

Pentru a adăuga programul în lista de excepții:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Apărare avansată împotriva amenințărilor** panou, faceți clic **Deschis**.
3. În **Setări** fereastra, faceți clic **Gestionați excepțiile**.
4. Clic **+ Adăugați o excepție**.
5. Introdu calea fișierului executabil pe care vrei să îl excluzi de la scanare în câmpul corespunzător.
   Alternativ, puteți naviga la executabil făcând clic pe butonul de răsfoire din partea dreaptă a interfeței, selectați-l și faceți clic pe **Bine**.
6. Porniți comutatorul de lângă **Apărare avansată împotriva amenințărilor**.
7. Clic **Salvați**.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 149).

6.1.4. Ce trebuie să faci atunci când Bitdefender blochează un site web, un domeniu, o adresă IP sau o aplicație online care este sigură

Bitdefender oferă o experiență de navigare web sigură prin filtrarea întregului trafic web și blocarea oricărui conținut periculos. Cu toate acestea, este posibil ca Bitdefender să considere nesigure un site web, un domeniu, o adresă IP sau o aplicație online care sunt, de fapt, sigure, ceea ce va face ca funcția Bitdefender de scanare a traficului HTTP să le blocheze în mod incorect.

În cazul în care aceleași pagini, domenii, adrese IP sau aplicații online sunt blocate în mod repetat, acestea pot fi adăugate în lista de excepții astfel încât să nu fi scanate de motoarele Bitdefender, asigurând o experiență de navigare pe internet fără probleme.

Pentru a adăuga un site web la **Excepții**:

1. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
2. În **PREVENIREA AMENINȚĂRILOR ONLINE** panou, faceți clic **Setări**.
3. Clic **Gestionați excepțiile**.
4. Clic **+ Adăugați o excepție**.

5. Introduceți în câmpul corespunzător numele site-ului web, numele domeniului sau adresa IP pe care doriți să o adăugați la excepții.
6. Faceți clic pe comutatorul de lângă **Prevenirea amenințărilor online**.
7. Clic **Salvați** pentru a salva modificările și a închide fereastra.

Numai site-urile, domeniile, adresele IP și aplicațiile în care ai deplină încredere ar trebui adăugate în această listă. Acestea vor fi excluse din procesul de scanare de către motoarele contra amenințărilor, a tentativelor de phishing și fraudelor.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 149).

6.1.5. Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet

Dacă dispui de o conexiune lentă la internet (cum ar fi cea de tip dial-up), în timpul procesului de actualizare pot apărea erori.

Pentru a îți păstra sistemul actualizat cu cea mai recentă bază de date cu informațiile privind amenințările a Bitdefender:

1. Clic **Setări** din meniul de navigare de pe Interfața Bitdefender.
2. Selectează **Actualizați** fila.
3. Dezactivează butonul **Actualizare discretă**.
4. Data viitoare când va fi disponibilă o actualizare, ți se va solicita să selectezi actualizarea pe care dorești să o descarci. Selectează doar **Actualizare semnături**.
5. Bitdefender va descărca și instala numai baza de date cu informații privind amenințările.

6.1.6. Serviciile Bitdefender nu răspund

Acest articol vă ajută să remediați problema **Serviciile Bitdefender nu răspund**. Această problemă poate apărea în următoarele situații:

- Pictograma Bitdefender din **bara de sistem** este inactivă și se afișează notificarea că serviciile Bitdefender nu răspund.

- Fereastra BitDefender indică faptul că serviciile BitDefender nu răspund.

Problema poate fi cauzată de:

- erori temporare de comunicare între serviciile BitDefender.
- unele dintre serviciile BitDefender sunt oprite.
- alte soluții de securitate rulează pe dispozitivul tău, în același timp cu Bitdefender.

Pentru a remedia această problemă, încearcă următoarele soluții:

1. Așteptați câteva momente pentru a vedea dacă apar schimbări. Eroarea poate fi temporară.
2. Repornește dispozitivul și așteaptă câteva momente până când se încarcă Bitdefender. Deschideți BitDefender pentru a vedea dacă eroarea persistă. De obicei, repornirea dispozitivului rezolvă problema.
3. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a BitDefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați BitDefender.
   Pentru mai multe informații, consultă capitolul Cum elimin celelalte soluții de securitate? (pagina 126).

Dacă eroarea persistă, vă rugăm să contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea Solicitarea ajutorului (pagina 149).

6.1.7. Nu s-a reușit dezinstalarea Bitdefender

Dacă doriți să ștergeți produsul Bitdefender și observați că procesul este suspendat sau sistemul se blochează, faceți clic pe **Anulare** pentru a abandona acțiunea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, în sistemul dumneavoastră pot rămâne unele chei de regiștri și fișiere Bitdefender. Aceste rămășite pot împiedica instalarea ulterioară a Bitdefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului.

Pentru a șterge definitiv Bitdefender de pe sistemul tău:

- În **Windows 7**:

1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
2. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
3. Clic **ELIMINA** în fereastra care apare.
4. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 8** și **Windows 8.1**:

1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control" direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
2. Clic **Dezinstalează un program** sau **Programe si caracteristici**.
3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
4. Clic **ELIMINA** în fereastra care apare.
5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 10** și **Windows 11**:

1. Clic **start**, apoi faceți clic pe Setări.
2. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.
3. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
5. Clic **ELIMINA** în fereastra care apare.
6. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

6.1.8. Sistemul meu nu pornește după ce am instalat Bitdefender

Dacă se întâmplă ca, după ce tocmai ați instalat Bitdefender,să nu puteți reporni sistemul în modul normal, pot exista mai multe motive pentru această problemă.

Cel mai probabil această problemă este cauzată fie de o instalare anterioară a Bitdefender care nu a fost dezinstalată corespunzător fie de o altă soluție de securitate care este instalată pe sistem.

Mai jos sunt prezentate modurile în care să acționezi pentru fiecare situație:

- **O soluție Bitdefender a fost instalată anterior și nu ai dezinstalat-o în mod corespunzător.**
  Pentru a remedia această problemă:

  1. Repornește sistemul și accesează-l în Safe Mode. Pentru a afla cum să faci acest lucru, consultă Cum pot să repornesc sistemul în Safe Mode? (pagina 127).
  2. Dezinstalează soluția Bitdefender de pe sistemul tău:
     - În **Windows 7**:
       a. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
       b. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
       c. Clic **ELIMINA** în fereastra care apare.
       d. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
       e. Repornește sistemul în modul normal.
     - În **Windows 8** și **Windows 8.1**:
       a. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
       b. Clic **Dezinstalați un program** sau **Programe si caracteristici**.
       c. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
       d. Clic **ELIMINA** în fereastra care apare.
       e. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
       f. Reporniți sistemul în modul normal.

- În **Windows 10** și **Windows 11**:
  a. Clic **start**, apoi faceți clic pe Setări.
  b. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.
  c. Găsi **Bitdefender Antivirus Plus** și selectați **Dezinstalează**.
  d. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
  e. Clic **ELIMINA** în fereastra care apare.
  f. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
  g. Reporniți sistemul în modul normal.

3. Reinstalează-ți produsul Bitdefender.

- **Ați avut instalată o altă soluție de securitate înainte, iar aceasta nu a fost dezinstalată corespunzător.**
  Pentru a rezolva asta:
  1. Reporniți sistemul și intrați în modul Safe. Pentru a afla cum să faceți acest lucru, consultați Cum pot să repornesc sistemul în Safe Mode? (pagina 127).
  2. Șterge cealaltă soluție de securitate din sistem:
     - În **Windows 7**:
       a. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
       b. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Ștergere**.
       c. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
     - În **Windows 8** și **Windows 8.1**:
       a. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.

b. Clic **Dezinstalează un program** sau **Programe si caracteristici**.

c. Găsiți numele programului pe care doriți să îl eliminați și selectați **Elimina**.

d. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 10** și **Windows 11**:

a. Clic **start**, apoi faceți clic pe Setări.

b. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.

c. Găsiți numele programului pe care doriți să îl eliminați și selectați **Dezinstalează**.

d. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

Pentru a dezinstala celălalt software în mod corect, mergi pe site-ul web al producătorului și lansează instrumentul de dezinstalare sau contactează direct producătorul, solicitând instrucțiunile de dezinstalare.

3. Reporniți sistemul în modul normal și reinstalați Bitdefender.

Situația nu s-a rezolvat deși ați urmat toți pașii de mai sus.

Pentru a rezolva asta:

1. Reporniți sistemul și intrați în modul Safe. Pentru a afla cum să faceți acest lucru, consultați Cum pot să repornesc sistemul în Safe Mode? (pagina 127).
2. Cu ajutorul funcției System Restore din Windows poți restabili dispozitivul la o dată anterioară instalării produsului Bitdefender.
3. Reporniți sistemul în modul normal și contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea Solicitarea ajutorului (pagina 149).

6.2. Eliminarea amenințărilor din sistemul tău

Amenințările vă pot afecta sistemul în moduri diferite, iar modul de acțiune al Bitdefender depinde de tipul de atac al amenințării. Deoarece

amenințările își schimbă comportamentul în mod frecvent, este dificil de stabilit un model privind comportamentul și acțiunile acestora.

Există cazuri când Bitdefender nu poate elimina în mod automat amenințarea din sistemul dumneavoastră. În astfel de cazuri, este necesară intervenția dumneavoastră.

Dacă nu puteți găsi problema dvs. aici sau dacă soluțiile prezentate nu o rezolvă, puteți contacta reprezentanții de asistență tehnică Bitdefender, așa cum este prezentat în capitolul Solicitarea ajutorului (pagina 149).

6.2.1. Mediu de salvare

Mediu de recuperare este o caracteristică a Bitdefender care îți permite să scanezi și să dezinfectezi toate partițiile unității hard din/ de pe sistemul de operare.

Mediul de recuperare Bitdefender este integrat cu Windows RE.

Pornirea sistemului în Modul de recuperare

Poți intra în Modul de recuperare numai din produsul tău Bitdefender, după cum urmează:

1. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.

2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Selectează **Deschide** din dreptul opțiunii **Mediu de recuperare**.
4. Selectează **REPORNIRE** în fereastra care se deschide.
   Mediul de recuperare Bitdefender se încarcă în câteva momente.

Scanarea sistemului în Modul de recuperare

Pentru scanarea sistemului în Modul de recuperare:

1. Accesează Mediul de recuperare, conform descrierii din Pornirea sistemului în Modul de recuperare (pagina 142).
2. Procesul de scanare Bitdefender începe automat imediat ce sistemul este încărcat în Mediul de recuperare.
3. Așteptați finalizarea procesului de scanare. Dacă este detectată o amenințare, urmează instrucțiunile pentru îndepărtarea acesteia.
4. Pentru a ieși din Mediul de recuperare, efectuează clic pe butonul Închidere din fereastra cu rezultatele scanării.

6.2.2. Ce poți face când Bitdefender găsește amenințări pe dispozitivul tău?

Este posibil să afli că există amenințări pe dispozitivul tău într-unul din următoarele moduri:

- Ți-ai scanat dispozitivul și Bitdefender a găsit elemente infectate pe acesta.
- O alertă de amenințări te informează că Bitdefender a blocat una sau mai multe amenințări pe dispozitivul tău.

În astfel de situații, actualizează Bitdefender pentru a te asigura că ai cele mai recente baze de date cu informații privind amenințările și efectuează o scanare a sistemului pentru analizarea acestuia.

După finalizarea scanării sistemului, selectează acțiunea dorită pentru elementele infectate (dezinfectare, ștergere, mutare în carantină).

Avertizare
În cazul în care consideri că fișierul face parte din sistemul de operare Windows sau că nu este un fișier infectat, nu urma acești pași și contactează serviciul de asistență clienți Bitdefender cât mai curând posibil.

Dacă acțiunea selectată nu a putut fi efectuată, iar jurnalul de scanare indică o infectare care nu a putut fi eliminată, trebuie să ștergi fișierul/fișierele manual:

Prima metodă poate fi utilizată în modul normal:

1. Dezactivați protecția antivirus în timp real Bitdefender:
   a. Clic **Protecţie** pe meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. În **Avansat** fereastra, stinge **Bitdefender Shield**.
2. Afișează obiecte ascunse în Windows. Pentru a afla cum să faceți acest lucru, consultați Cum pot afișa elementele ascunse din Windows? (pagina 125).
3. Mergi la locația unde se găsește fișierul infectat (verifică jurnalul de scanare) și șterge-l.
4. Activați protecția antivirus în timp real Bitdefender.

În cazul în care prima metodă nu a reușit să elimine infecția:

1. Reporniți sistemul și intrați în modul Safe. Pentru a afla cum să faceți acest lucru, consultați Cum pot să repornesc sistemul în Safe Mode? (pagina 127).
2. Afișează obiecte ascunse în Windows. Pentru a afla cum să faceți acest lucru, consultați Cum pot afișa elementele ascunse din Windows? (pagina 125).
3. Navigați la locația fișierului infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Repornește sistemul în mod normal.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 149).

6.2.3. Cum elimin o amenințare dintr-o arhivă?

O arhivă este un fișier sau o colecție de fișiere comprimate într-un format special, în scopul reducerii spațiului de pe hard-disc necesar stocării fișierelor.

Unele dintre aceste formate sunt formate deschise, ceea ce permite Bitdefender să scaneze în interiorul acestora și apoi să ia măsurile corespunzătoare pentru eliminarea infecțiilor.

Alte formate de arhivă sunt închise complet sau parțial, iar Bitdefender poate identifica numai prezența amenințărilor din acestea însă nu poate lua niciun fel de măsură în acest sens.

Dacă Bitdefender anunță că a fost detectată o amenințare într-o arhivă și nu este disponibilă nicio acțiune, aceasta înseamnă că eliminarea amenințării nu este posibilă din cauza restricțiilor legate de setările referitoare la permisiunile arhivelor.

Iată cum poți elimina o amenințare stocată într-o arhivă:

1. Identifică arhiva care conține amenințarea în urma unei scanări a sistemului.
2. Dezactivați protecția antivirus în timp real Bitdefender:
   a. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. În **Avansat** fereastra, stinge **Bitdefender Shield**.
3. Accesează locația arhivei și dezarhiveaz-o utilizând o aplicație de arhivare, cum ar fi WinZip.
4. Identifica fișierul infectat și șterge-l.
5. Șterge arhiva inițială pentru a te asigura că fișierul infectat este eliminat în totalitate.
6. Recomprimă fișierele într-o nouă arhivă utilizând o aplicație de arhivare, cum ar fi WinZip.
7. Activați protecția antivirus în timp real a Bitdefender și executați o scanare a sistemului pentru a vă asigura că sistemul nu este infectat.

Notă
Este important de reținut faptul că o amenințare aflată într-o arhivă nu reprezintă o amenințare imediată la adresa sistemului tău deoarece trebuie să fie dezarhivată și executată pentru a putea infecta calculatorul.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 149).

6.2.4. Cum elimin o amenințare dintr-o arhivă de e-mail?

Bitdefender poate de asemenea să identifice amenințări din bazele de date de e-mail și arhivele de e-mail stocate pe disc.

Uneori este necesară identificarea mesajului infectat utilizând informațiile puse la dispoziție în raportul de scanare și ștergerea acestuia în mod manual.

Iată cum poți elimina o amenințare stocată într-o arhivă de e-mail:

1. Scanează baza de date de e-mailuri cu Bitdefender.
2. Dezactivați protecția antivirus în timp real Bitdefender:
   a. Clic **Protecţie** din meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. În **Avansat** fereastra, stinge **Bitdefender Shield**.
3. Deschide raportul de scanare și utilizeaza informațiile de identificare (Subiect, De la, Către) aferente mesajelor infectate pentru a le localiza în clientul de e-mail.
4. Ștergeți mesajele infectate. Majoritatea clienților de e-mail mută mesajul șters într-un director de recuperare, de unde acesta poate fi recuperat. Trebuie să vă asigurați că mesajul este șters și din acest director de recuperare.
5. Arhivează directorul în care se află mesajul infectat.
   - În Microsoft Outlook 2007: Din meniul File (Fișier), selectează Data File Management (Administrare fișiere de date). Alege fișierele (.pst) pe care intenționezi să le compactezi, apoi selectează Settings (Setări). Clic pe Compact Now (Compactează acum).
   - În Microsoft Outlook 2010/2013/2016: Din meniul File (Fișier), selectează Info (Informații), apoi Account settings (Add and remove accounts or change existing connection settings) [Setări cont (Adăugare și eliminare conturi sau modificare setări de conectare existente)]. Apoi selectează Data File (Fișier de date), fișierele (.pst) pe care intenționezi să le compactezi și alege opțiunea Settings (Setări). Clic pe Compact Now (Compactează acum).
6. Activați protecția antivirus în timp real Bitdefender.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 149).

6.2.5. Ce trebuie să fac dacă suspectez că un fișier este periculos?

Există posibilitatea să considerați că un anumit fișier din sistemul dumneavoastră este periculos chiar dacă Bitdefender nu l-a detectat.

Pentru a te asigura că sistemul tău este protejat:

1. Execută o **Scanare de sistem** cu Bitdefender. Pentru a afla cum să faci acest lucru, consultă How do I scan my system?.
2. Dacă procesul de scanare nu a detectat nimic, dar încă ai dubii cu privire la fișier, contactează reprezentanții serviciul de asistență pentru ajutor.
   Pentru a afla cum să faci acest lucru, consultă Solicitarea ajutorului (pagina 149).

6.2.6. Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?

Aceasta reprezintă doar o notificare referitoare la faptul că Bitdefender a detectat aceste fișiere ca fiind protejate fie prin parolă, fie cu o anumită formă de criptare.

Cel mai frecvent, elementele protejate prin parolă sunt următoarele:

- Fișiere care aparțin unei alte soluții de securitate.
- Fișiere care aparțin sistemului de operare.

Pentru a putea scana conținutul, aceste fișiere trebuie să fie extrase sau decriptate.

În cazul în care conținutul respectiv este extras, Bitdefender va scana automat conținutul pentru a-ti proteja dispozitivul. Dacă doriți să scanați acele fișiere folosind Bitdefender, trebuie să contactați producătorul produsului pentru a obține mai multe detalii despre respectivele fișiere.

Noi îți recomandăm să ignori acele fișiere deoarece acestea nu reprezintă o amenințare pentru sistemul tău.

6.2.7. Ce reprezintă elementele omise din jurnalul de scanare?

Toate fișierele care apar ca fiind omise în raportul de scanare nu conțin niciun fel de viruși.

Pentru performanțe sporite, Bitdefender nu scanează fișiere care nu au fost modificate de la ultima scanare.

6.2.8. Ce reprezintă fișierele supracomprimate din jurnalul de scanare?

Elementele supracomprimate sunt elemente care nu au putut fi extrase de către motorul de scanare sau elemente pentru care timpul necesar decriptării ar fi fost prea lung ducând la instabilitatea sistemului.

Supracomprimarea se referă la faptul că Bitdefender a sărit peste scanarea respectivei arhive deoarece dezarhivarea acesteia s-a dovedit a consuma prea mult din resursele sistemului. Conținutul va fi scanat în timp real, la accesare, dacă este cazul.

6.2.9. De ce Bitdefender a șters în mod automat un fișier infectat?

În cazul în care este detectat un fișier infectat, Bitdefender va încerca în mod automat să-l dezinfecteze. Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

Pentru anumite tipuri de amenințări, dezinfecția nu este posibilă deoarece fișierul detectat este complet rău intenționat. În astfel de cazuri, fișierul infectat este șters de pe disc.

Acesta este cazul fișierelor de instalare care sunt descărcate de pe site-uri web nesigure. Dacă vă aflați într-o astfel de situație, descărcați fișierul de instalare de pe site-ul web al producătorului sau de pe un alt site web sigur.

7. OBȚINE AJUTOR

7.1. Solicitarea ajutorului

Bitdefender le oferă clienților săi un serviciu rapid și precis de asistență, la un nivel inegalabil. Dacă întâmpini probleme sau dacă ai întrebări legate de produsul tău Bitdefender, poți utiliza o serie de resurse online pentru a identifica o soluție sau un răspuns. De asemenea, poți contacta echipa Serviciului de asistență pentru clienți. Reprezentanții noștri îți vor răspunde la întrebări în timp util și îți vor oferi sprijinul de care ai nevoie.

7.2. Resurse online

Sunt disponibile mai multe resurse online pentru a vă ajuta la soluționarea problemelor și întrebărilor referitoare la produsul Bitdefender.

- Centrul de asistență Bitdefender:
  https://www.bitdefender.ro/consumer/support/
- Comunitatea de experți Bitdefender:
  https://community.bitdefender.com/ro
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare referitoare la securitatea informatică, produsele și compania Bitdefender.

7.2.1. Centrul de asistență Bitdefender

Centrul de Asistență Bitdefender este un depozit online ce conține informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea amenințărilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Bitdefender Support Center este pusă la dispoziția publicului. Această multitudine de informații reprezintă încă o cale de a oferi clienților BitDefender asistența tehnică de care au nevoie. Toate cererile valide de

informații sau rapoarte despre bug-uri venind de la clienții BitDefender ajung în cele din urmă în Bitdefender Support Center, ca rapoarte asupra eliminării bug-urilor, fișe de lucru sau articole informative pentru a suplimenta fișierele de suport ale produsului.

Centrul de asistență Bitdefender este disponibil oricând la următoarea adresă: https://www.bitdefender.ro/consumer/support/.

7.2.2. Comunitatea de experți Bitdefender

Comunitatea de experți este un mediu în care utilizatorii, pasionații și fanii Bitdefender pot interacționa, face schimb de idei, se pot ajuta reciproc și își pot împărtăși cunoștințele și soluțiile. De asemenea, acesta este un loc în care se nasc idei și de unde echipele noastre de dezvoltare pot obține un feedback valoros. Membrii comunității sunt utilizatori Bitdefender cu experiență, dornici să-și ajute colegii, în timpul liber. Cu contribuția lor impresionantă și prin eforturi voluntare sincere, am creat o bază de cunoștințe unde utilizatorii pot găsi răspunsuri și îndrumări, prin interacțiune.

Aici veți găsi conversații relevante cu persoane care utilizează Bitdefender pe dispozitivele lor. Comunitatea oferă o legătură reală cu membrii noștri și îți permite să te faci auzit. Este un loc unde ești încurajat să participi, având siguranța că opinia și aportul tău sunt respectate și prețuite. Pentru că activitatea noastră este apreciată, depunem eforturi pentru a asigura o asistență rapidă și precisă, la un nivel incomparabil, și ne dorim să-i aducem pe utilizatorii noștri mai aproape de noi. Cu acest scop în minte, am creat această comunitate.

Accesează pagina Comunității noastre de experți aici:

https://community.bitdefender.com/ro

7.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia conține toate informațiile de care ai nevoie despre cele mai noi amenințări cibernetice. Acesta este locul unde experții Bitdefender își împărtășesc sfaturi și recomandări despre cum să se protejeze împotriva hackerilor, breșelor de securitate a datelor, furtului de identitate și încercărilor de asumare a identității.

Accesează pagina Bitdefender Cyberpedia aici:

https://www.bitdefender.com/cyberpedia/.

7.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. Din 2001, BITDEFENDER și-a stabilit o reputație incontestabilă prin străduința constantă pentru o mai bună comunicare, astfel încât să depășească așteptările clienților și partenerilor noștri. Dacă aveți întrebări, nu ezitați să ne contactați direct prin intermediul nostru Centrul de asistență Bitdefender (pagina 149).

https://www.bitdefender.ro/consumer/support/

7.3.1. Distribuitori locali

Distribuitorii locali Bitdefender sunt pregătiți să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergi la https://www.bitdefender.com/partners/partner-locator.html.
2. Selectează țara și orașul folosind opțiunile corespunzătoare.

GLOSAR

Cod de activare

Este o cheie unică care poate fi cumpărată de la retail și utilizată pentru a activa un anumit produs sau serviciu. Un cod de activare permite activarea unui abonament valabil pentru o anumită perioadă de timp și număr de dispozitive și poate fi folosit și pentru a prelungi un abonament cu condiția să fie generat pentru același produs sau serviciu.

ActiveX

ActiveX este un model de scriere a programelor, astfel încât alte programe și sistemul de operare să le poată apela. Tehnologia ActiveX este utilizată cu Microsoft Internet Explorer pentru a crea pagini web interactive care arată și se comportă ca niște programe de calculator, mai degrabă decât ca pagini statice. Cu ActiveX, utilizatorii pot pune sau răspunde la întrebări, pot folosi butoane și pot interacționa în alte moduri cu pagina web. Controalele ActiveX sunt adesea scrise folosind Visual Basic. Active X se remarcă prin lipsa completă a controalelor de securitate; experții în securitatea computerelor descurajează utilizarea acestuia pe internet.

Amenințare persistentă avansată

Amenințarea persistentă avansată (APT) exploatează vulnerabilitățile sistemelor pentru a fura informații importante pentru a le livra la sursă. Grupurile mari, cum ar fi organizațiile, companiile sau guvernele, sunt vizate de această amenințare. Obiectivul unei amenințări persistente avansate este de a rămâne nedetectat pentru o lungă perioadă de timp, putând monitoriza și aduna informații importante fără a deteriora mașinile vizate. Metoda folosită pentru a injecta amenințarea în rețea este printr-un fișier PDF sau un document Office care arată inofensiv, astfel încât fiecare utilizator să poată rula fișierele.

Adware

Adware-ul este adesea combinat cu o aplicație gazdă care este furnizată gratuit, atâta timp cât utilizatorul este de acord să accepte adware-ul. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord cu un acord de licență care precizează scopul aplicației, nu se comite nicio infracțiune. Cu toate acestea, reclamele pop-up pot deveni o supărare și, în unele cazuri, pot degrada performanța sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații

le colectează pot cauza probleme de confidențialitate pentru utilizatorii care nu cunoșteau pe deplin termenii din acordul de licență.

Arhiva

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Ușa din spate

O gaură în securitatea unui sistem lăsată în mod deliberat de proiectanți sau întreținători. Motivația pentru astfel de găuri nu este întotdeauna sinistră; unele sisteme de operare, de exemplu, ies din cutie cu conturi privilegiate destinate utilizării de către tehnicienii de service pe teren sau programatorii de întreținere ai furnizorului.

Sectorul de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (dimensiunea sectorului, dimensiunea clusterului și așa mai departe). Pentru discurile de pornire, sectorul de boot conține și un program care încarcă sistemul de operare.

Virus de pornire

O amenințare care infectează sectorul de pornire al unui disc fix sau al unei dischete. O încercare de pornire de pe o dischetă infectată cu un virus din sectorul de boot va face ca amenințarea să devină activă în memorie. De fiecare dată când porniți sistemul din acel moment, veți avea amenințarea activă în memorie.

botnet

Termenul „botnet” este compus din cuvintele „robot” și „rețea”. Rețelele bot sunt dispozitive conectate la internet infectate cu amenințări și pot fi folosite pentru a trimite e-mailuri spam, a fura date, a controla de la distanță dispozitive vulnerabile sau a răspândi programe spyware, ransomware și alte tipuri de amenințări. Obiectivul lor este de a infecta cât mai multe dispozitive conectate, precum PC-uri, servere, dispozitive mobile sau IoT aparținând marilor companii sau industrii.

Browser

Prescurtare pentru browser web, o aplicație software folosită pentru a localiza și afișa pagini web. Printre browserele populare se numără Microsoft Internet Explorer, Mozilla Firefox și Google Chrome. Acestea sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafică, cât și text. În

plus, majoritatea browserelor moderne pot prezenta informații multimedia, inclusiv sunet și video, deși necesită plug-in-uri pentru unele formate.

Atac de forță brută

Atacul de ghicire a parolei folosit pentru a pătrunde într-un sistem computerizat prin introducerea de combinații posibile de parole, de cele mai multe ori începând cu parola cel mai ușor de ghicit.

Linie de comanda

Într-o interfață de linie de comandă, utilizatorul tastează comenzi în spațiul oferit direct pe ecran folosind limbajul de comandă.

Cookie-uri

În industria internetului, cookie-urile sunt descrise ca fișiere mici care conțin informații despre computere individuale care pot fi analizate și utilizate de agenții de publicitate pentru a urmări interesele și gusturile dvs. online. În acest domeniu, tehnologia cookie-urilor este încă în curs de dezvoltare și intenția este de a direcționa anunțurile direct către ceea ce ați spus că sunt interesele dvs. Este o sabie cu două tăișuri pentru mulți oameni, deoarece, pe de o parte, este eficientă și pertinentă, deoarece vedeți doar reclame despre ceea ce vă interesează. Pe de altă parte, implică de fapt „urmărirea” și „urmărirea” unde mergeți și pe ce dai click. De înțeles, există o dezbatere asupra confidențialității și mulți oameni se simt jigniți de ideea că sunt priviți ca un „număr SKU” (știți, codul de bare de pe spatele pachetelor care este scanat la linia de check-out de la băcănie) . Deși acest punct de vedere poate fi extrem, în unele cazuri este precis.

Hărțuirea cibernetică

Când colegii sau străinii comit acte abuzive împotriva copiilor intenționat pentru a-i răni fizic. Pentru a dăuna emoțional, agresorii trimit mesaje răutăcioase sau fotografii nemăgulitoare, făcând astfel victimele lor să se izoleze de ceilalți sau să se simtă frustrate.

Dicţionar Attack

Atacurile de ghicire a parolelor erau folosite pentru a pătrunde într-un sistem informatic prin introducerea unei combinații de cuvinte comune pentru a genera parole potențiale. Aceeași metodă este folosită pentru a ghici cheile de decriptare ale mesajelor sau documentelor criptate. Atacurile de dicționar reușesc, deoarece mulți oameni înclină să aleagă parole scurte și simple, care sunt ușor de ghicit.

Unitate disc

Este o mașină care citește și scrie date pe un disc. Un hard disk citește și scrie hard disk-uri. O unitate de dischetă accesează dischetele. Unitățile de disc pot fi fie interne (găzduite într-un computer), fie externe (găzduite într-o cutie separată care se conectează la computer).

Descarca

Pentru a copia date (de obicei un fișier întreg) de la o sursă principală pe un dispozitiv periferic. Termenul este adesea folosit pentru a descrie procesul de copiere a unui fișier dintr-un serviciu online pe propriul computer. Descărcarea se poate referi și la copierea unui fișier de pe un server de fișiere din rețea pe un computer din rețea.

E-mail

Poștă electronică. Un serviciu care trimite mesaje pe computere prin rețele locale sau globale.

Evenimente

O acțiune sau o apariție detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi clic pe un buton al mouse-ului sau apăsarea unei taste, sau apariții ale sistemului, cum ar fi epuizarea memoriei.

Exploatările

O modalitate de a profita de diferite erori sau vulnerabilități care sunt prezente într-un computer (software sau hardware). Astfel, hackerii pot obține controlul asupra computerelor sau rețelelor.

Fals pozitiv

Apare atunci când un scaner identifică un fișier ca fiind infectat, când de fapt nu este.

Extensie de nume de fișier

Porțiunea dintr-un nume de fișier, care urmează punctului final, care indică tipul de date stocate în fișier. Multe sisteme de operare folosesc extensii de nume de fișiere, de exemplu Unix, VMS și MS-DOS. Acestea sunt de obicei de la una la trei litere (unele sisteme de operare vechi triste nu acceptă mai mult de trei). Exemplele includ „c” pentru codul sursă C, „ps” pentru PostScript, „txt” pentru text arbitrar.

Euristică

O metodă bazată pe reguli de identificare a noilor amenințări. Această metodă de scanare nu se bazează pe baza de date cu informații despre amenințări specifice. Avantajul scanării euristice este că nu este păcălit de o nouă variantă a unei amenințări existente. Cu toate acestea, poate raporta ocazional cod suspect în programele normale, generând așa-numitul „fals pozitiv”.

Borcan cu miere

Un sistem informatic momeală creat pentru a atrage hackerii să studieze modul în care acţionează și să identifice metodele eretice pe care le folosesc pentru a colecta informaţii despre sistem. Companiile și corporațiile sunt mai interesate de implementarea și utilizarea honeypot-urilor pentru a-și îmbunătăți starea generală de securitate.

IP

Internet Protocol - Un protocol rutabil din suita de protocoale TCP/IP care este responsabil pentru adresarea IP, rutarea și fragmentarea și reasamblarea pachetelor IP.

applet Java

Un program Java care este proiectat să ruleze numai pe o pagină web. Pentru a utiliza un applet pe o pagină web, trebuie să specificați numele applet-ului și dimensiunea (lungime și lățime, în pixeli) pe care le poate utiliza applet-ul. Când pagina web este accesată, browserul descarcă appletul de pe un server și îl rulează pe computerul utilizatorului (clientul). Appleturile diferă de aplicații prin faptul că sunt guvernate de un protocol de securitate strict.

De exemplu, chiar dacă aplicațiile rulează pe client, acestea nu pot citi sau scrie date pe computerul clientului. În plus, applet-urile sunt restricționate în continuare, astfel încât să poată citi și scrie numai date de pe același domeniu din care sunt servite.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați. Keylogger-urile nu sunt rău intenționate în natură. Ele pot fi folosite în scopuri legitime, cum ar fi monitorizarea angajaților sau a activității copiilor. Cu toate acestea, acestea sunt din ce în ce mai folosite de infractorii cibernetici în scopuri rău intenționate (de exemplu, pentru a colecta date private, cum ar fi datele de conectare și numerele de securitate socială).

Virus macro

Un tip de amenințare informatică care este codificată ca macrocomandă încorporată într-un document. Multe aplicații, cum ar fi Microsoft Word și Excel, acceptă limbaje macro puternice. Aceste aplicații vă permit să încorporați o macrocomandă într-un document și să executați macrocomandă de fiecare dată când documentul este deschis.

Client de mail

Un client de e-mail este o aplicație care vă permite să trimiteți și să primiți e-mail.

Memorie

Zone de stocare internă în computer. Termenul de memorie identifică stocarea de date care vine sub formă de cipuri, iar cuvântul stocare este folosit pentru memoria care există pe benzi sau discuri. Fiecare computer vine cu o anumită cantitate de memorie fizică, denumită de obicei memorie principală sau RAM.

Non-euristic

Această metodă de scanare se bazează pe baza de date cu informații despre amenințări specifice. Avantajul scanării non-euristice este că nu este păcălit de ceea ce ar putea părea a fi o amenințare și nu generează alarme false.

Prădători online

Persoane care caută să atragă minori sau adolescenți în conversații cu scopul de a-i implica în activități sexuale ilegale. Rețelele de socializare sunt locul ideal în care copiii vulnerabili pot fi vânați cu ușurință și seduși să comită activități sexuale, online sau față în față.

Programe pline

Un fișier într-un format de compresie. Multe sisteme de operare și aplicații conțin comenzi care vă permit să împachetați un fișier astfel încât să ocupe mai puțină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere spațiale consecutive. În mod normal, acest lucru ar necesita zece octeți de stocare.

Cu toate acestea, un program care împachetează fișiere ar înlocui caracterele de spațiu cu un caracter special din seria spațială, urmat de numărul de spații înlocuite. În acest caz, cele zece spații ar necesita doar doi octeți. Aceasta este doar o tehnică de ambalare - sunt multe altele.

Cale

Indicațiile exacte către un fișier de pe un computer. Aceste direcții sunt de obicei descrise prin intermediul sistemului ierarhic de evidență de sus în jos.

Ruta dintre oricare două puncte, cum ar fi canalul de comunicații între două computere.

Phishing

Acțiunea de a trimite un e-mail unui utilizator care pretinde în mod fals că este o întreprindere legitimă stabilită în încercarea de a înșela utilizatorul pentru a renunța la informații private care vor fi folosite pentru furtul de identitate. E-mailul îl direcționează pe utilizator să viziteze un site web unde i se cere să actualizeze informații personale, cum ar fi parolele și numerele de card de credit, de securitate socială și de cont bancar, pe care organizația legitimă le are deja. Totuși, site-ul web este fals și creat doar pentru a fura informațiile utilizatorului.

Foton

Photon este o tehnologie Bitdefender inovatoare, neitruzivă, proiectată pentru minimizarea impactului soluției tale de securitate asupra performanțelor. Prin monitorizarea în fundal a activității PC-ului tău, creează modele de utilizare care vor ajuta la optimizarea pornirii și a proceselor de scanare.

Virus polimorf

O amenințare care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, astfel de amenințări sunt greu de identificat.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului și a altor dispozitive periferice.

În rețelele TCP/IP și UDP, acestea reprezintă un endpoint către o conexiune logică. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Ransomware

Ransomware este un program periculos care încearcă să obțină bani de la utilizatori prin blocarea sistemelor vulnerabile. CryptoLocker, CryptoWall și

TeslaWall sunt doar câteva variante care vânează sistemele personale ale utilizatorilor.

Infecția se poate extinde prin accesarea mesajelor spam, descărcarea atașamentelor e-mail sau instalarea de aplicații, fără ca utilizator să afle ce se întâmplă pe sistemul său. Utilizatorii și companiile sunt vizate zilnic de către hackerii ransomware.

Fișier raport

Reprezintă un fișier care listează acțiunile care au avut loc. BitDefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

Rootkit

Un rootkit este un set de instrumente soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la instrumente recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, conectări și jurnale. Acestea pot, de asemenea, să intercepteze date de la terminale, conexiuni la rețea sau dispozitive periferice, dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde amenințări sau prezența intrușilor în sistem. În combinație cu amenințările, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Spam

Termen ce acoperă întreaga gamă a mesajelor electronice nesolicitate (junk). În general, acestea sunt cunoscute sub numele de mesaje electronice nesolicitate.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și o amenințare de tip cal troian este legată de faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Elemente de pornire

Orice fișier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, și nu direct fișierul.

Abonament

Contractul de cumpărare care acordă utilizatorului dreptul de a folosi un anumit produs sau serviciu pe un anumit număr de dispozitive și o anumită perioadă de timp. Un abonament expirat poate fi reînnoit automat folosind informațiile furnizate de utilizator la prima achiziție.

Zona de notificare

Introdusă odată cu apariția sistemului Windows 95, bara de sistem se află în bara de sarcini Windows (de obicei, în partea de jos, lângă ceas) și

conține pictograme miniaturale pentru accesul rapid la aplicații de sistem cum ar fi cele de fax, imprimantă, modem, volum și altele. Faceți dublu-clic sau clic-dreapta cu mouse-ul pe o pictogramă pentru a vizualiza și accesa detaliile și comenzile.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Amenințare

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a amenințărilor se pot și înmulți. Toate amenințările informatice sunt create de om. O simplă amenințare care poate realiza copii ale sale este relativ simplu de produs. Chiar și o asemenea amenințare este periculoasă întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. O amenințare și mai periculoasă este cea care este capabilă să se răspândească în rețea și poate să treacă de sistemele de securitate.

Actualizare informații despre amenințări

Modelul binar al unei amenințări, utilizat de către soluția de securitate pentru detectarea și eliminarea amenințării.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de programele malițioase și viermi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cele mai mascate tipuri de amenințări de tip cal troian este un program care pretinde că elimină amenințările de pe calculatorul tău, însă, în loc de aceasta, introduce amenințări pe calculatorul tău.

Termenul provine de la o poveste din opera „Iliada” a lui Homer, în care grecii le oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. Rutinele de instalare a actualizărilor verifică dacă pe calculatorul tău există instalată o altă versiune mai veche; dacă nu, nu vei putea instala actualizarea.

Bitdefender dispune de o funcție proprie de actualizare care îți permite să verifici manual actualizările sau să permiți actualizarea automată a produsului.

Rețea privată virtuală (VPN)

Este o tehnologie care permite o conexiune directă temporară și criptată la o anumită rețea prin intermediul unei rețele mai puțin sigure. Astfel, trimiterea și primirea de date este sigură și criptată, dificil de interceptat de către curioși. O dovadă de securitate este autentificarea, care se poate efectua numai folosind un nume de utilizator și o parolă.

Vierme

Reprezintă un program care se auto-propagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.