Bitdefender®
ANTIVIRUS FOR MAC

GHIDUL UTILIZATORULUI

I

Mac

Bitdefender Antivirus for Mac

Ghidul utilizatorului

Data publicării 21.11.2022

Aviz juridic

Bitdefender

Cuprins

Despre acest ghid **1**
Scopul și publicul țintă 1
Cum să folosiți acest ghid 1
Convenții utilizate în acest ghid 1
Convenții tipografice 1
Atenționări 2
Comentarii 2
1. Ce Bitdefender Antivirus for Maceste **4**
2. Instalare și dezinstalare **5**
2.1. Cerințe de sistem 5
2.2. Instalarea Bitdefender Antivirus for Mac 5
2.2.1. Proces de instalare 6
2.3. Dezinstalarea Bitdefender Antivirus for Mac 10
3. Introducere **11**
3.1. Deschiderea Bitdefender Antivirus for Mac 11
3.2. Fereastră principală aplicație 12
3.3. Pictogramă aplicație în Dock 13
3.4. Meniu de navigare 13
3.5. Mod întunecat 14
4. Protecția împotriva softurilor periculoase **15**
4.1. Recomandări de utilizare 15
4.2. Scanarea Mac-ului dumneavoastră 16
4.3. Asistent scanare 17
4.4. Carantină 18
4.5. Bitdefender Shield (protecție în timp real) 19
4.6. Excepții scanare 19
4.7. Protecție web 20
4.7.1. Activarea extensiilor TrafficLight 20
4.7.2. Administrarea setărilor extensiilor 21
4.7.3. Rating-ul de pagină și alerte 21
4.8. Anti-tracker 22
4.8.1. Activarea Bitdefender Anti-tracker 22
4.8.2. Interfața Anti-tracker 23
4.8.3. Dezactivarea Bitdefender Anti-tracker 23
4.8.4. Permiterea urmăririi unui site web 24
4.9. Protecție fișiere 24
4.9.1. Acces aplicație 25
4.10. Protecție Time Machine 26
4.10.1. Activarea sau dezactivarea protecției Time Machine 26

4.11. Remedierea problemelor 26
4.12. Notificări 28
4.13. Actualizări 29
4.13.1. Cererea unei actualizări 29
4.13.2. Obținerea actualizărilor prin intermediul unui server proxy 29
4.13.3. Fă upgrade la o versiune nouă 30
4.13.4. Găsirea informațiilor despre Bitdefender Antivirus for Mac 30
5. VPN 31
5.1. Despre VPN 31
5.2. Activarea conexiunii VPN 31
5.3. Interfata 32
5.4. Abonamente 34
6. Configurarea preferințelor 35
6.1. Accesarea preferințelor 35
6.2. Preferințe de protecție 35
6.3. Preferințe avansate 36
6.4. Oferte speciale 36
7. Despre Bitdefender CENTRAL 37
7.1. Accesează Bitdefender Central 37
7.2. Autentificare în doi pași 38
7.2.1. Activați autentificarea de tip „two-factor" 38
7.3. Adăugarea dispozitivelor sigure 40
7.4. Dispozitivele mele 40
7.4.1. Adăugarea unui dispozitiv nou 40
7.4.2. Personalizează-ți dispozitivul 41
7.4.3. Acțiuni de la distanță 42
7.5. Activitate 43
7.6. Abonamentele mele 44
7.6.1. Verifică abonamentele disponibile 44
7.6.2. Activare abonament 44
7.6.3. Reînnoire abonament 45
7.7. Notificări 46
8. Întrebări frecvente 47
9. Obține ajutor 52
9.1. Solicitarea ajutorului 52
9.2. Resurse online 52
9.2.1. Centrul de asistență Bitdefender 52
9.2.2. Comunitatea de experți Bitdefender 53
9.2.3. Bitdefender Cyberpedia 53
9.3. Informații de contact 54

9.3.1. Distribuitori locali 54
Glosar 55

DESPRE ACEST GHID

Scopul și publicul țintă

Acest manual se adresează tuturor utilizatorilor care au ales Bitdefender Antivirus for Mac ca soluție de securitate pentru calculatoarele personale. Informațiile incluse în acest manual sunt destinate nu numai utilizatorilor avansați, ci și oricărei persoane care poate lucra în sistemul Macintosh.

Vei afla cum să configurezi și să utilizezi Bitdefender Antivirus for Mac pentru a te proteja împotriva amenințărilor și împotriva altor software-uri periculoase. Vei afla cum poți valorifica la maxim Bitdefender.

Vă dorim o lectură plăcută și utilă.

Cum să folosiți acest ghid

Acest ghid este organizat în mai multe teme majore:

Introducere (page 11)

Faceți cunoștință cu produsul Bitdefender Antivirus for Mac și interfața sa pentru utilizatori.

Protecția împotriva softurilor periculoase (page 15)

Află cum poți utiliza BitDefender Antivirus for Mac pentru a te proteja împotriva software-urilor periculoase.

Configurarea preferințelor (page 35)

Aflați mai multe informații despre setările favorite pentru Bitdefender Antivirus for Mac.

Obține ajutor (page 52)

Unde să căutați și unde să cereți ajutor în cazul în care apar situații neprevăzute.

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 (page 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. CE BITDEFENDER ANTIVIRUS FOR MACESTE

Bitdefender Antivirus for Mac este un scanner antivirus puternic, care poate detecta și elimina toate tipurile de programe periculoase ("amenințări"), incluzând:

- ransomware
- adware
- viruși
- spyware
- Troieni
- keylogger
- viermi

Această aplicație detectează și elimină nu numai amenințările pentru Mac, ci și amenințările pentru Windows, împiedicându-te astfel să transmiți fișiere infectate familiei, prietenilor și colegilor care utilizează calculatoare.

2. INSTALARE ȘI DEZINSTALARE

Acest capitol acoperă următoarele subiecte:

- Cerințe de sistem (page 5)
- Instalarea Bitdefender Antivirus for Mac (page 5)
- Dezinstalarea Bitdefender Antivirus for Mac (page 10)

2.1. Cerințe de sistem

Poți instala Bitdefender Antivirus for Mac pe computerele Macintosh cu sistem de operare OS X Yosemite (10.10) sau o versiune mai nouă.

Mac-ul tău trebuie să aibă minimum 1 GB de spațiu disponibil pe hard disk.

Este necesar să fiți conectați la internet pentru a înregistra și actualiza Bitdefender Antivirus for Mac.

Nota
Bitdefender Anti-tracker și Bitdefender VPN pot fi instalate doar pe sistemele de operare macOS 10.12 sau versiuni mai noi.

Cum să afli versiunea de macOS și informații hardware despre Mac-ul tău
Efectuează clic pe pictograma Apple din colțul din stânga sus al ecranului și selectează Despre **acest Mac**. În fereastra care apare, vei vedea detalii despre versiunea sistemului tău de operare, precum și alte informații utile. Efectuează clic pe **Raport sistem** pentru a vedea informații detaliate despre componentele hardware.

2.2. Instalarea Bitdefender Antivirus for Mac

Aplicația Bitdefender Antivirus for Mac poate fi instalată prin accesarea contului tău Bitdefender astfel:

1. Conectează-te ca administrator.
2. Accesează: https://central.bitdefender.com.
3. Conectează-te la contul Bitdefender folosind adresa ta de e-mail și parola.

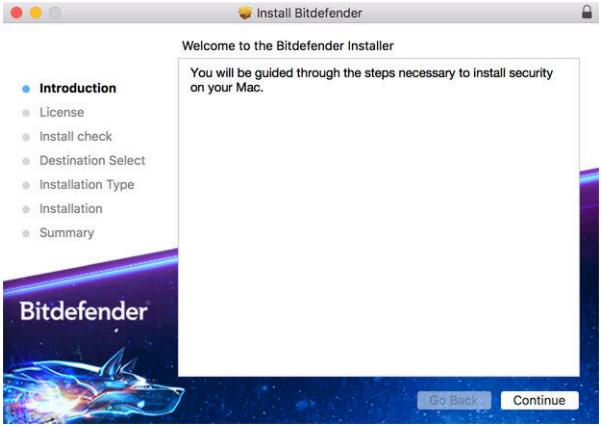
4. Accesează secțiunea **Dispozitivele mele** și apoi apasă pe **INSTALEAZĂ PROTECȚIA**.
5. Alege una dintre cele două opțiuni disponibile:
   - **Protejează acest dispozitiv**
     a. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea 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. Efectuează clic 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.
6. Rulați produsul Bitdefender descărcat.
7. Urmează pașii de instalare.

2.2.1. Proces de instalare

Pentru a instala Bitdefender Antivirus for Mac:

1. Faceți clic pe fișierul descărcat. Veți lansa astfel programul de instalare, care vă va ghida pe parcursul procesului de instalare.
2. Urmează indicațiile programului asistent de instalare.

Pasul 1 - Fereastra de întâmpinare



Efectuează clic pe **Continuare**.

Pasul 2 - Citește Contractul de abonament

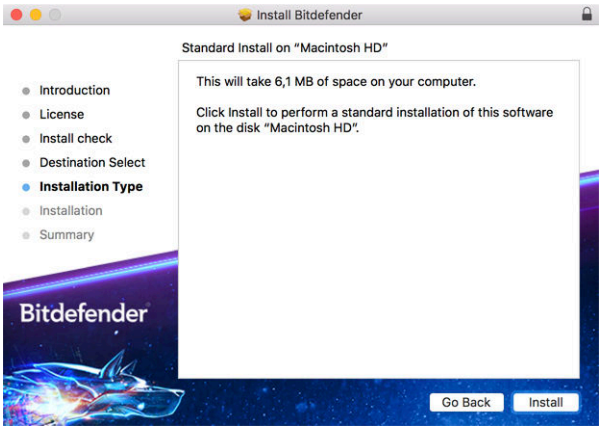
Înainte de a contninua instalarea, este necesar să îți exprimi acordul cu privire la clauzele Contractului de abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Antivirus for Mac.

Din această fereastră poți selecta și limba în care dorești să instalezi produsul.

Efectuează clic pe **Continuare**, apoi pe **De acord**.

Important
Dacă nu ești de acord cu acești termeni, efectuează clic pe **Continuare** și apoi pe **Nu sunt de acord** pentru a anula procesul de instalare.

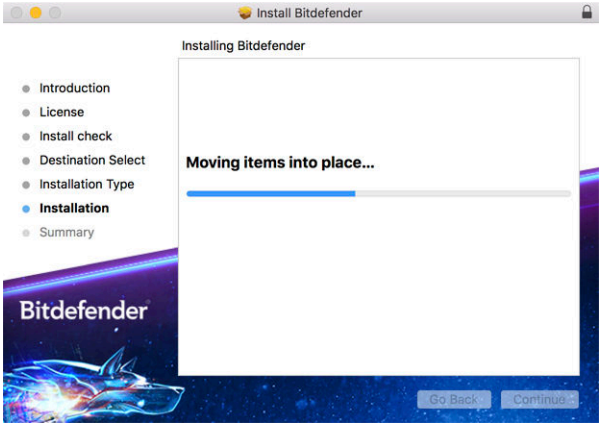
Pasul 3 - Inițiază instalarea



Bitdefender Antivirus for Mac va fi instalat în `Macintosh HD/Library/Bitdefender`. Calea de instalare nu poate fi modificată.

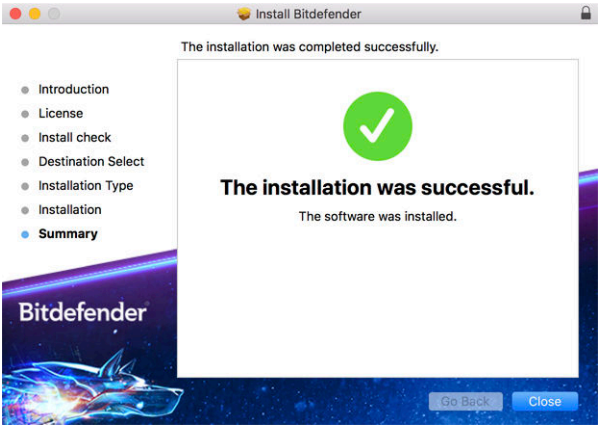
Faceți clic pe **Instalează** pentru a iniția instalarea.

Pasul 4 - Instalarea Bitdefender Antivirus for Mac



Așteptați până când instalarea este finalizată și apoi faceți clic pe **Continuă**.

Pasul 5 - Finalizare



Faceți clic pe **Închide** pentru a închide fereastra programului de instalare.

Procesul de instalare s-a încheiat.

Important

- Dacă instalezi Bitdefender Antivirus for Mac pe un sistem de operare macOS High Sierra 10.13.0 sau o versiune mai nouă, va apărea notificarea **Extensie sistem blocată**. Această notificare te informează că extensiile semnate de Bitdefender au fost blocate și trebuie activate manual. Apasă pe OK pentru a continua. În fereastra Bitdefender Antivirus for Mac care apare, apasă pe linkul **Securitate și Confidențialitate**. Apasă pe **Permite** din partea de jos a ferestrei sau selectează Bitdefender SRL din listă și apoi apasă pe **OK**.
- Dacă instalezi Bitdefender Antivirus for Mac pe sistemul de operare macOS Mojave 10.14 sau o versiune mai nouă, se afișează o fereastră nouă care te informează că trebuie să **Permiți accesul Bitdefender la întregul disc** și să **Permiți încărcarea Bitdefender**. Urmează instrucțiunile de pe ecran pentru a configura corespunzător produsul.

2.3. Dezinstalarea Bitdefender Antivirus for Mac

Deoarece este o aplicație complexă, Bitdefender Antivirus for Mac nu poate fi dezinstalat în modul obișnuit, prin transferarea pictogramei aplicației din directorul **Aplicații** în directorul Trash.

Pentru a dezinstala Bitdefender Antivirus for Mac, urmează acești pași:

1. Deschide o fereastră **Finder**, apoi accesează directorul **Aplicații**.
2. Deschide directorul Bitdefender în **Aplicații** apoi efectuează dublu clic pe **BitdenderUninstaller**.
3. Selectează opțiunea de dezinstalare preferată.

   Notă
   Dacă încerci să dezinstalezi doar aplicația Bitdefender VPN, selectează **Dezinstalare VPN**.

4. Fă clic pe **Dezinstalare** și așteaptă finalizarea procesului.
5. Apasă pe **Închidere** pentru a finaliza.

   Important
   În cazul apariției unei erori, puteți contacta serviciul de asistență clienți al Bitdefender, așa cum se descrie în Solicitarea ajutorului (page 52).

3. INTRODUCERE

Acest capitol include următoarele subiecte:

- Deschiderea Bitdefender Antivirus for Mac (page 11)
- Fereastră principală aplicație (page 12)
- Pictogramă aplicație în Dock (page 13)
- Meniu de navigare (page 13)
- Mod întunecat (page 14)

3.1. Deschiderea Bitdefender Antivirus for Mac

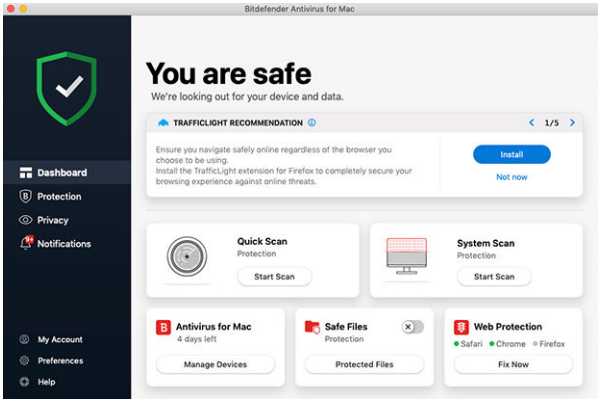
Aveți mai multe modalități prin care puteți deschide Bitdefender Antivirus for Mac.

- Efectuează clic pe pictograma Bitdefender Antivirus for Mac din bara de lansare.
- Apasă pe pictograma din bara de meniu și alege **Deschide interfața Antivirus**.
- Deschide o fereastră Finder, accesează Aplicații și efectuează dublu clic pe pictograma **Bitdefender Antivirus for Mac**.

> **Important**
> Prima dată când deschizi Bitdefender Antivirus for Mac pe macOS Mojave 10.14 sau o versiune mai nouă, se va afișa o recomandare de protecție. Această recomandare apare deoarece avem nevoie de anumite drepturi de acces pentru a scana întregul sistem în vederea identificării amenințărilor. Pentru a ne acorda aceste drepturi, este necesar să fii autentificat ca administrator și să parcurgi pașii următori:
>
> 1. Accesează linkul **Preferințe sistem**.
> 2. Apasă pe pictograma și apoi tastează datele tale de autentificare ca administrator.
> 3. Se va deschide o nouă fereastră. Trage fișierul **BDLDaemon** în lista aplicațiilor permise.

3.2. Fereastră principală aplicație

Bitdefender Antivirus for Mac 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.

Bara de stare din partea de sus a ferestrei te informează cu privire la starea de securitate a sistemului tău folosind mesaje explicite și culori sugestive. Dacă Bitdefender Antivirus for Mac nu prezintă avertismente, bara de stare este verde. Atunci când a fost detectată o problemă de securitate, culoarea barei de stare devine roșie. Pentru a vedea informații detaliate despre erori și cum să le remediezi, consultă Remedierea problemelor (page 26).

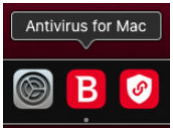
Pentru a-ți oferi o funcționare eficientă și o protecție sporită în timp ce desfășori diferite activități, **Bitdefender Autopilot** va acționa ca asistentul tău personal în materie de securitate. În funcție de activitatea pe care o desfășori, fie că e vorba de activități profesionale sau de efectuarea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

lucru te va ajuta să descoperi și să beneficiezi de avantajele aduse de caracteristicile incluse în aplicația Bitdefender Antivirus for Mac.

Din meniul de navigare din partea stângă, poți accesa secțiunile Bitdefender pentru a vedea detalii despre configurație și setări administrative avansate (filele **Protecție** și **Confidențialitate**), notificări, contul tău **Bitdefender** și secțiunea de **Preferințe**. De asemenea, ne poți contacta (fila **Asistență**) dacă ai nevoie de răspunsuri la întrebări sau în cazul în care apare ceva neașteptat.

3.3. Pictogramă aplicație în Dock

Pictograma Bitdefender Antivirus for Mac este vizibilă în Dock imediat ce deschizi aplicația. Pictograma din Dock îți oferă o metodă simplă de scanare a fișierelor și directoarelor pentru a identifica amenințările. Trebuie doar să aduci fișierul sau directorul respectiv peste pictograma Dock folosind drag & drop și scanarea va porni imediat.



3.4. Meniu de navigare

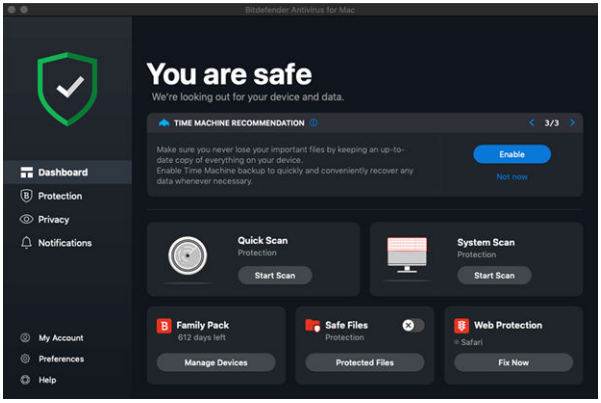
În partea stângă a interfeței Bitdefender se regăsește meniul de navigare, care îți permite să accesezi rapid caracteristicile Bitdefender de care ai nevoie pentru gestionarea produsului tău. Filele disponibile în această secțiune sunt următoarele:

- **Panoul de control**. De aici, poți rezolva rapid problemele de securitate, poți vizualiza recomandări în funcție de nevoile și tiparele de utilizare ale sistemului tău, poți efectua acțiuni rapide și accesa contul tău Bitdefender pentru a gestiona dispozitivele pe care le-ai adăugat la abonamentul tău Bitdefender.
- **Protecție**. De aici, poți lansa sarcini de scanare antivirus, poți adăuga fișiere în lista de excepții, poți proteja fișiere și aplicații împotriva atacurilor de tip ransomware, îți poți securiza backup-urile Time Machine și îți poți configura protecția în timp ce navighezi pe Internet.

- **Confidențialitate**. De aici, poți deschide aplicația Bitdefender VPN și poți instala extensia Anti-tracker în browserul tău web.
- **Notificări**. De aici, poți vedea detalii despre acțiunile întreprinse asupra fișierelor scanate.
- **Contul meu**. De aici, poți vizualiza detaliile contului tău Bitdefender și ale abonamentului care îți protejează dispozitivul și poți comuta între conturi dacă este cazul.
- **Preferințe**. De aici, poți configura setările Bitdefender.
- **Ajutor**. De aici, ori de câte ori ai nevoie de asistență pentru a rezolva o situație în legătură cu produsul Bitdefender, poți contacta departamentul de Asistență tehnică. De asemenea, ne poți trimite feedback pentru a ne ajuta să îmbunătățim produsul.

3.5. Mod întunecat

Pentru a-ți feri ochii de lumina puternică atunci când lucrezi noaptea sau într-un mediu fără lumină, Bitdefender Antivirus for Mac acceptă Modul întunecat pentru Mojave 10.14 sau mai recent. Culorile interfeței au fost optimizate astfel încât să poți utiliza Mac-ul fără a-ți obosi ochii. Interfața Bitdefender Antivirus for Mac se ajustează singură în funcție de setările de aspect ale dispozitivului tău.



4. PROTECȚIA ÎMPOTRIVA SOFTURILOR PERICULOASE

Acest capitol include următoarele subiecte:

- Recomandări de utilizare (page 15)
- Scanarea Mac-ului dumneavoastră (page 16)
- Asistent scanare (page 17)
- Carantină (page 18)
- Bitdefender Shield (protecție în timp real) (page 19)
- Excepții scanare (page 19)
- Protecție web (page 20)
- Anti-tracker (page 22)
- Protecție fișiere (page 24)
- Protecție Time Machine (page 26)
- Remedierea problemelor (page 26)
- Notificări (page 28)
- Actualizări (page 29)

4.1. Recomandări de utilizare

Pentru a îți proteja sistemul împotriva amenințărilor și pentru a preveni infectarea accidentală a altor sisteme, respectă aceste bune practici:

- Ține **Bitdefender Shield** activat pentru a permite scanarea automată a fișierelor sistemului de Bitdefender Antivirus for Mac.
- Actualizează-ți produsul Bitdefender Antivirus for Mac pentru a avea acces la cele mai recente informații despre amenințări și actualizări de produse.
- Verificați și soluționați în mod regulat problemele raportate de Bitdefender Antivirus for Mac. Pentru informații detaliate, consultați capitolul Remedierea problemelor (page 26).
- Verifică jurnalul detaliat de evenimente privind activitatea Bitdefender Antivirus for Mac pe computerul tău. De fiecare dată când are loc un

eveniment relevant pentru securitatea sistemului sau a datelor tale, se adaugă un nou mesaj în secțiunea de Notificări Bitdefender. Pentru mai multe informații, accesează Notificări (page 28).

- Vă sugerăm să urmați aceste recomandări de utilizare:
  - Obișnuiți-vă să scanați fișierele pe care le descărcați de pe o memorie externă de stocare (precum un stick USB sau un CD), în special atunci când sursa nu vă este cunoscută.
  - În cazul unui fișier DMG, instalați-l și apoi scanați conținutul acestuia (fișierele din volumul/imaginea instalată).

  Cel mai ușor mod de a scana un fișier, un director sau un volum este prin folosirea drag & drop pentru a-l poziționa deasupra ferestrei Bitdefender Antivirus for Mac sau pictogramei Dock.

Nu este necesară nicio altă configurație sau acțiune. Cu toate acestea, dacă doriți, vă puteți ajusta setările și preferințele pentru a corespunde mai bine necesităților dvs. Pentru mai multe informații, consultă capitolul Configurarea preferințelor (page 35).

4.2. Scanarea Mac-ului dumneavoastră

În afara caracteristicii **Bitdefender Shield**, care monitorizează cu regularitate aplicațiile instalate în vederea identificării acțiunilor de tipul amenințărilor și împiedicării pătrunderii noilor amenințări în sistemul tău, îți poți scana Mac-ul sau anumite fișiere oricând dorești.

Cel mai ușor mod de a scana un fișier, un director sau un volum este prin folosirea drag & drop pentru a-l poziționa deasupra ferestrei Bitdefender Antivirus for Mac sau pictogramei Dock. Va apărea programul asistent de scanare, care te va ghida în procesul de scanare.

Puteți începe o operațiune de scanare și astfel:

1. Selectează **Protecție** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Antivirus**.
3. Efectuează clic pe unul dintre cele trei butoane de scanare pentru a iniția scanarea dorită.
   - **Quick Scan (Scanare rapidă)** - verifică dacă există amenințări în cele mai vulnerabile locații din sistemul tău (de exemplu,

directoarele care conțin documentele, fișierele descărcate de pe internet sau din e-mail și fișierele temporare ale fiecărui utilizator).

- **Scanare sistem** - efectuează o verificare completă pentru a identifica amenințările din întregul sistem. Toate dispozitivele conectate vor fi, de asemenea, scanate.

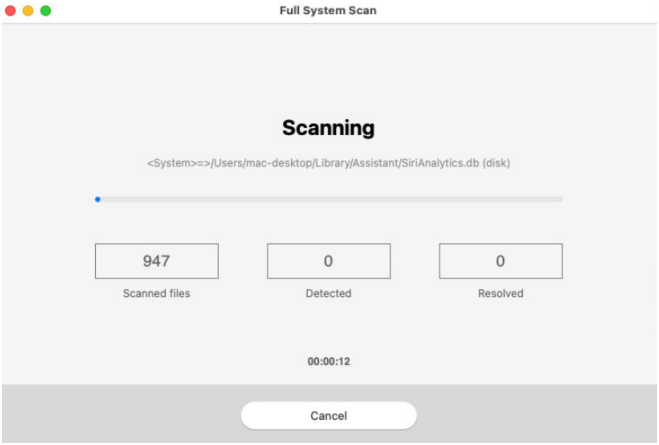
> **Notă**
> În funcție de dimensiunea hard disk-ului dumneavoastră, scanarea întregului sistem poate dura până la o oră sau chiar mai mult. Pentru o mai bună performanță, se recomandă să nu rulați această operațiune în timp ce efectuați alte operațiuni care folosesc intensiv resursele (cum ar fi editarea video).
>
> În funcție de preferințele tale, poți alege să nu scanezi anumite volume instalate prin adăugarea acestora în lista de **Excepții** din fereastra Protecție.

- **Custom Scan (Scanare personalizată)** - te ajută să verifici anumite fișiere, foldere sau volume pentru a identifica amenințările.

De asemenea, poți porni o Scanare de sistem sau o Scanare rapidă din Panoul de control.

4.3. Asistent scanare

Atunci când inițiezi o scanare, va apărea expertul de scanare Bitdefender Antivirus for Mac.



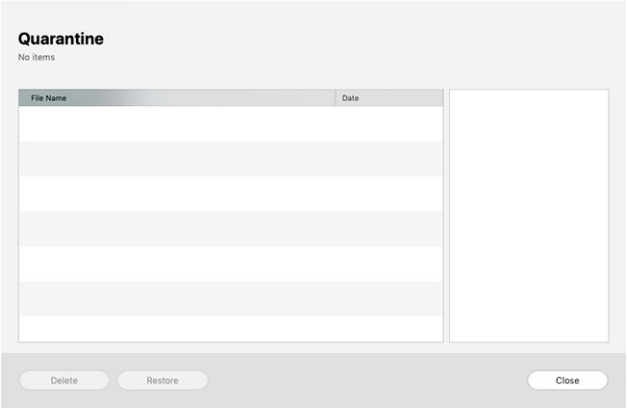
În timpul fiecărei scanări sunt afișate informații în timp real despre amenințările detectate și soluționate.

Așteaptă ca Bitdefender Antivirus for Mac să finalizeze scanarea.

> **Notă**
> Procesul de scanare poate dura cateva minute, în funcție de complexitatea scanării.

4.4. Carantină

Bitdefender Antivirus for Mac permite izolarea fișierelor infectate sau suspecte într-o zonă sigură, numită carantină. Atunci când sunt în carantină, amenințările sunt inofensive, pentru că nu pot fi executate sau citite.



Secțiunea Carantină afișează toate fișierele izolate în directorul Carantină.

Pentru a șterge un fișier aflat în carantină, selectați-l și faceți clic pe **Șterge**. Dacă doriți să restaurați un fișier aflat în carantină în locația sa originală, selectați-l și faceți clic pe **Restaurează**.

Pentru a vizualiza lista tuturor obiectelor adăugate în carantină:

1. Clic **Protecție** în meniul de navigare din interfața Bitdefender.
2. Apasă pe **Deschide** în panoul **Carantină**.

4.5. Bitdefender Shield (protecție în timp real)

Bitdefender oferă protecție în timp real împotriva unei game largi de amenințări prin scanarea tuturor aplicațiilor instalate, a versiunilor actualizate a acestora, precum și a fișierelor noi și modificate.

Pentru dezactivarea protecției în timp real:

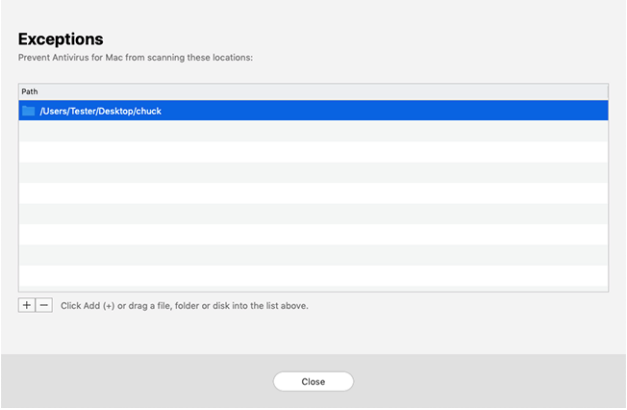
1. Selectează **Preferințe** din meniul de navigare al interfeței Bitdefender.
2. Dezactivează **Bitdefender Shield** din fereastra **Protecție**.

> **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.

4.6. Excepții scanare

Puteți configura Bitdefender Antivirus for Mac astfel încât să nu scaneze anumite fișiere, dosare sau informațiile de pe o întreagă partiție. De exemplu, ați putea exclude de la scanare:

- Fișiere identificate eronat ca infectate (cunoscute drept "fals pozitive")
- Fișierele care duc la erori de scanare
- Volume de backup



Lista de excepții conține căile de acces către fișierele ce au fost excluse de la scanare.

Pentru a accesa lista de excepții:

1. Clic **Protecție** în meniul de navigare din interfața Bitdefender.
2. Apasă pe **Deschide** în panoul **Excepții**.

Există două modalități prin care poți crea o excepție de la scanare:

- Folosește metoda drag & drop și trage un fișier, director sau volum deasupra listei de excepții.
- Apasă pe butonul marcat cu semnul plus (+), situat sub lista excepțiilor. Apoi alege fișierul, directorul sau volumul care urmează a fi exclus din operațiunea de scanare.

Pentru a șterge o excepție de la scanare, selecteaz-o din listă și apasă pe butonul marcat cu semnul minus (-), situat sub lista excepțiilor.

4.7. Protecție web

Bitdefender Antivirus for Mac folosește extensii TrafficLight pentru o protecție completă a experienței tale de navigare pe internet. Extensiile TrafficLight interceptează, procesează și filtrează întregul trafic internet, blocând conținutul periculos.

Extensiile sunt compatibile și se integrează cu următoarele browsere web: Mozilla Firefox, Google Chrome și Safari.

4.7.1. Activarea extensiilor TrafficLight

Pentru a activa extensiile TrafficLight:

1. Selectează **Remediază acum** din secțiunea **Protecție web** a Panoului de control.
2. Se deschide fereastra **Protecție web**.
   Se va afișa browser-ul web instalat pe sistemul tău. Pentru a instala extensia TrafficLight în browserul tău, selectează **Obținere extensie**.
3. Se face redirecționarea către:
   https://bitdefender.com/solutions/trafficlight.html
4. Selectează **Descărcare gratuită**.

5. Urmați pașii pentru instalarea extensiei TrafficLight corespunzătoare browser-ului dumneavoastră web.

4.7.2. Administrarea setărilor extensiilor

Sunt disponibile mai multe funcții pentru protecția dumneavoastră împotriva tuturor tipurilor de amenințări pe care le puteți întâlni în timpul browsing-ului web. Pentru a le accesa, apasă pictograma în formă de semafor de lângă setările browser-ului tău și apoi apasă butonul **Setări**:

- **Setări Bitdefender TrafficLight**
  - Protecție web - împiedică accesarea site-urilor web utilizate pentru malware, phishing și atacuri frauduloase.
  - Asistență la căutare - oferă avertizări în avans cu privire la site-urile web riscante din rezultatele căutării tale.

- **Excepții**
  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 .
  Nu se vor afișa avertizări dacă paginile excluse includ amenințări. Acesta este motivul pentru care această listă trebuie cuprindă doar site-urile web în care aveți încredere deplină.

4.7.3. Rating-ul de pagină și alerte

În funcție de cum TrafficLight clasifică pagina web pe care o vizualizezi la momentul respectiv, una sau mai multe dintre următoarele pictograme sunt afișate în zona corespunzătoare:

Aceasta este o pagină sigură. Îți poți continua activitatea.

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

Ar trebui să părăsești această pagină web acum întrucât conține malware sau alte amenințări.

În Safari, pictogramele TrafficLight sunt pe fundal negru.

4.8. 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 să 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:

- Google Chrome
- Mozilla Firefox
- Safari

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.

4.8.1. Activarea Bitdefender Anti-tracker

Pentru a activa extensia Bitdefender Anti-tracker în browserul web:

1. Selectează **Confidențialitate** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Anti-tracker**.
3. Selectează opțiunea **Activare extensie** din dreptul browserului web pentru care dorești să activezi extensia.

4.8.2. 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.

4.8.3. Dezactivarea Bitdefender Anti-tracker

Pentru a dezactiva Bitdefender Anti-tracker din browserul web:

1. Deschide browserul web.
2. Efectuează clic pe pictograma de lângă bara de adresă din browserul web.
3. Efectuează clic pe pictograma din colțul din dreapta sus.
4. Utilizează butonul corespunzător pentru dezactivare.
   Pictograma Bitdefender devine gri.

4.8.4. 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. Efectuează clic pe pictograma de lângă bara de căutare.
3. Apasă pe pictograma din colțul din dreapta sus.
4. Dacă vă aflați pe site-ul web pe care doriți să îl adăugați la excepții, faceți clic pe **Adăugați site-ul web curent la listă**.
   Dacă doriți să adăugați un alt site web, introduceți adresa acestuia în câmpul corespunzător, apoi faceți clic .

4.9. Protecție fișiere

Ransomware este un program periculos care atacă sistemele vulnerabile blocându-le și solicită bani pentru a permite utilizatorului să reia controlul asupra sistemului. Acest software periculos acționează inteligent prin afișarea unor mesaje false pentru a panica utilizatorul, solicitându-i să efectueze plata cerută.

Folosind cea mai nouă tehnologie, Bitdefender asigură integritatea sistemului prin protejarea zonelor de importanță critică ale sistemului împotriva atacurilor ransomware, fără a afecta sistemul. Cu toate acestea, este posibil să vrei să-ți protejezi și fișierele personale, cum ar fi documentele, fotografiile sau filmele, împotriva accesării lor de către aplicații nesigure. Cu funcția Bitdefender Protecție fișiere, poți să-ți menții în siguranță fișierele personale și să configurezi ce aplicații ar trebui să aibă dreptul de a efectua modificări asupra fișierelor protejate și ce aplicații nu ar trebui să aibă astfel de drepturi.

Pentru a adăuga ulterior fișiere în mediul protejat:

1. Clic **Protecție** în meniul de navigare din interfața Bitdefender.
2. Selectează fila **Anti-Ransomware**.
3. Selectează **Fișiere protejate** din secțiunea Protecție fișiere.
4. Efectuează clic pe butonul marcat cu semnul plus (+), ce se află sub lista fișierelor protejate. Apoi, selectează fișierul, directorul sau

volumul de protejat în cazul în care se încearcă accesarea lor de către programele ransomware.

Pentru a evita încetinirea sistemului, îți recomandăm să adaugi cel mult 30 de directoare sau să salvezi mai multe fișiere într-un singur director.

În mod implicit, directoarele Fotografii, Documente, Desktop și Fișiere descărcate sunt protejate contra atacurilor amenințărilor.

> **Notă**
> Directoarele personalizate pot fi protejate doar pentru utilizatorii curenți. Unitățile, sistemele și fișierele aplicațiilor externe nu pot fi adăugate la mediul de protecție.

Vei fi informat de fiecare dată când o aplicație necunoscută cu un comportament neobișnuit va încerca să modifice fișierele adăugate. Apasă pe **Permite** sau **Blochează** pentru a o adăuga în lista **Administrare aplicații**.

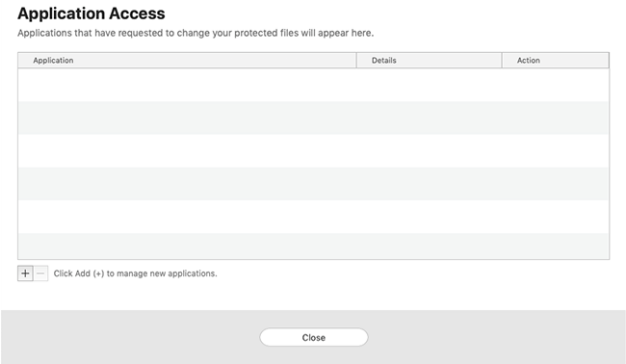
4.9.1. Acces aplicație

Aceste aplicații care încearcă să modifice sau să șteargă fișierele protejate pot fi marcate ca fiind potențial nesigure și adăugate în lista de aplicații blocate. Dacă o astfel de aplicație este blocată și ești sigur că are un comportament normal, îi poți permite accesul urmând acești pași:

1. Clic **Protecție** în meniul de navigare din interfața Bitdefender.
2. Selectează **Anti-Ransomware** fila.
3. Selectează **Acces aplicații** din secțiunea Protecție fișiere.
4. Modifică starea aplicației selectând „Permite” în dreptul aplicației blocate.

Aplicațiile cu starea Permis pot fi setate și pe valoarea Blocat.

Folosește metoda de glisare și fixare (drag&drop) sau efectuează clic pe semnul plus (+) pentru a adăuga în listă mai multe aplicații.



4.10. Protecție Time Machine

Protecția Bitdefender Time Machine are rolul unui nivel suplimentar de securitate pentru unitatea ta de backup, inclusiv pentru toate fișierele pe care ai decis să le stochezi acolo, blocând accesul oricărei surse externe. În cazul în care fișierele care se regăsesc pe unitatea Time Machine sunt criptate de un program ransomware, le vei putea recupera fără să plătești recompensa solicitată.

În cazul în care trebuie să restabilești fișiere dintr-un backup Time Machine, accesează pagina de asistență Apple pentru instrucțiuni.

4.10.1. Activarea sau dezactivarea protecției Time Machine

Pentru activa sau dezactiva Protecția Time Machine:

1. Selectează **Protecție** din meniul de navigare al **interfeței Bitdefender**.
2. Selectează **Anti-Ransomware** fila.
3. Activează sau dezactivează opțiunea **Protecție Time Machine**.

4.11. Remedierea problemelor

Bitdefender Antivirus for Mac depistează automat o serie de probleme care pot afecta securitatea sistemului și a datelor dvs. și vă informează în acest sens. În acest fel, puteți soluționa riscurile de securitate ușor și rapid.

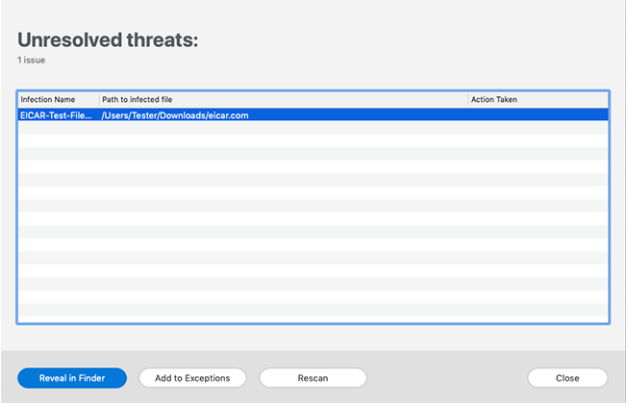
Soluționarea problemelor indicate de Bitdefender Antivirus for Mac constituie un mod rapid și ușor de a asigura protecția optimă a sistemului și a datelor dumneavoastră.

Problemele detectate includ:

- Noua actualizare a informațiilor despre amenințări nu a fost descărcată de pe serverele noastre.
- Au fost detectate amenințări pe sistemul tău și produsul nu le poate dezinfecta automat.
- Protecția în timp real este dezactivată.

Pentru a verifica și soluționa problemele detectate:

1. În cazul în care nu există avertizări din partea Bitdefender, bara de stare este de culoare verde. Atunci când este detectată o problemă de securitate, bara de stare își schimba culoarea în roșu.
2. Verificați descrierea acesteia pentru a obține mai multe informații.
3. Atunci când este detectată o problemă, apasă pe butonul corespunzător pentru a întreprinde o acțiune.



Lista amenințărilor nerezolvate este actualizată după fiecare scanare de sistem, indiferent dacă scanarea se desfășoară automat în fundal sau este inițiată de către tine.

Puteți alege să întreprindeți următoarele acțiuni cu privire la amenințările nesoluționate:

- **Ștergere manuală**. Efectuează această acțiune pentru a elimina manual infecțiile.
- **Adăugare la excepții**. Această acțiune nu este disponibilă pentru amenințările detectate în cadrul arhivelor.

4.12. Notificări

Bitdefender menține un jurnal detaliat al evenimentelor legate de activitatea sa pe computerul tău. Ori de câte ori se întâmplă un lucru important 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 calculatorul tău, etc. În plus, puteți lua măsuri suplimentare, dacă este cazulsau modifica măsurile luate de Bitdefender.

Pentru a accesa jurnalul de Notificări, efectuează 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, fereastra Notificări oferă opțiuni de ștergere sau marcare ca citite a tuturor evenimentelor din secțiunea respectivă.

4.13. Actualizări

Noi amenințări sunt găsite și identificate în fiecare zi. De aceea este foarte important să îți păstrezi Bitdefender Antivirus for Mac actualizat cu ultimele actualizări care conțin informații despre amenințări.

Actualizarea informațiilor privind amenințările se efectuează din mers, adică fișierele care trebuie actualizate sunt înlocuite progresiv. Astfel, actualizarea nu va afecta funcționarea produsului și, în același timp, se elimină orice vulnerabilitate.

- Dacă Bitdefender Antivirus for Mac este actualizat, poate detecta cele mai recente pericole descoperite și poate curăța fișierele infectate.
- Dacă Bitdefender Antivirus for Mac nu este actualizat, acesta nu va putea detecta și elimina cele mai recente amenințări descoperite de Laboratoarele Bitdefender.

4.13.1. Cererea unei actualizări

Puteți efectua o actualizare la cerere oricând doriți.

Este necesară o conexiune activă la internet pentru a verifica dacă există actualizări disponibile și pentru a le descărca.

Pentru o actualizare la cerere:

1. Faceți clic pe butonul **Acțiuni** din bara de meniu.
2. Selectează **Actualizează baza de date cu informații referitoare la amenințări**.

În mod alternativ, poți solicita o actualizare manuală tastând CMD + U.

Puteți vizualiza progresul actualizării, precum și fișierele descărcate.

4.13.2. Obținerea actualizărilor prin intermediul unui server proxy

Bitdefender Antivirus for Mac se poate actualiza numai prin servere proxy care nu necesită autentificare. Nu este necesară configurarea vreunor setări de program.

Dacă te conectexi la internet prin intermediul unui server proxy ce necesită autentificare, trebuie să treci în mod regulat la o conexiune directă la internet pentru a putea obține actualizările cu privire la informațiile despre amenințări.

4.13.3. Fă upgrade la o versiune nouă

Ocazional, lansăm actualizări de produse pentru a adăuga noi caracteristici și îmbunătățiri sau pentru a remedia anumite probleme legate de produs. Aceste actualizări pot necesita repornirea sistemului pentru a porni instalarea noilor fișiere. În mod implicit, dacă o actualizare necesită repornirea computerului, Bitdefender Antivirus for Mac va continua funcționarea folosind fișierele anterioare, până când reporniți sistemul. În acest caz, procesul de actualizare nu va interfera cu activitatea utilizatorului.

Atunci când este finalizată o actualizare de produs, o fereastră pop-up vă va solicita să reporniți sistemul. Dacă rataţi această această notificare, puteți fie să faceți clic pe **Repornește pentru upgrade** din bara de meniu sau să reporniți manual sistemul.

4.13.4. Găsirea informațiilor despre Bitdefender Antivirus for Mac

Pentru a găsi informții despre versiunea Bitdefender Antivirus for Mac pe care ai instalat-o, accesează fereastra **Despre**. Din aceeași fereastră poți accesa și vizualiza Contractul de abonament și Politica de Confidențialitate și poți vizualiza Licențele cu sursă deschisă.

Pentru a accesa fereastra Despre:

1. Deschideți Bitdefender Antivirus for Mac.
2. Apasă pe Bitdefender Antivirus for Mac din bara de meniu și selectează **Despre Antivirus for Mac**.

5. VPN

Acest capitol include următoarele subiecte:

- Despre VPN (page 31)
- Activarea conexiunii VPN (page 31)
- Interfata (page 32)
- Abonamente (page 34)

5.1. Despre VPN

Cu Bitdefender VPN îşi menţii confidenţialitatea datelor atunci când te conectezi la reţele wireless nesecurizate în aeroporturi, mall-uri, cafenele sau hoteluri. În acest fel, pot fi evitate situaţiile nefericite cum ar fi furtul de date personale sau tentativele de a face IP-ul tău accesibil de către hackeri.

Aplicaţia VPN poate fi instalată din produsul tău Bitdefender şi poate fi utilizată de fiecare dată când vrei să adaugi un nivel suplimentar de protecţie conexiunii tale. Aplicaţia VPN funcţionează ca un tunel între dispozitivul tău şi reţeaua la care te conectezi pentru a-ţi securiza conexiunea, a-ţi cripta datele utilizând criptare la un nivel care este utilizat în sistemul bancar şi pentru a-ţi ascunde adresa IP oriunde te-ai afla. Traficul tău este redirecţionat 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 eşti conectat la internet prin Bitdefender VPN, vei putea accesa conţinut care este, în mod normal, restricţionat în anumite zone.

Notă

Unele ţări cenzurează conţinutul online şi, prin urmare, utilizarea soluţiilor VPN pe teritoriul lor a fost interzisă prin lege. Pentru a evita consecinţele juridice, este posibil să se afişeze un mesaj de avertizare atunci când încercaţi să folosiţi aplicaţia VPN pentru prima dată. Prin continuarea utilizării aplicaţiei, confirmi că ai cunoştinţă de reglementările aplicabile ţării respective şi riscurile la care te-ai putea expune.

5.2. Activarea conexiunii VPN

Există trei moduri prin care poţi deschide aplicaţia Bitdefender VPN:

- Apasă pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
  Apasă pe **Deschide** în panoul Bitdefender VPN.
- Apasă pe pictograma din bara de meniu.
- Accesează directorul Aplicații, deschide directorul Bitdefender și apoi efectuează dublu clic pe pictograma Bitdefender VPN.

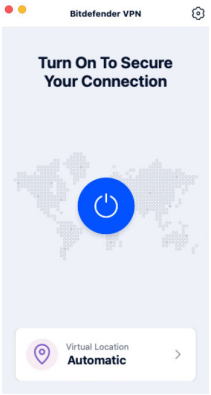
Prima dată când deschizi aplicația, ți se solicită să permiți Bitdefender să adauge configurații. Permițând Bitdefender să adauge configurații, îți exprimi acordul ca întreaga activitate din rețea a dispozitivului tău să poată fi filtrată sau monitorizată atunci când utilizezi aplicația VPN.

> **Notă**
> Aplicația Bitdefender VPN poate fi instalată doar pe versiunile macOS Sierra (10.12.6), macOS High Sierra (10.13.6) sau macOS Mojave (10.14) sau pe versiuni ulterioare ale sistemului de operare.

5.3. Interfata

Interfața VPN afișează starea aplicației, respectiv dacă este conectată sau deconectată. Locația serverului pentru utilizatorii care folosesc versiunea gratuită este setată automat de Bitdefender pe cel mai potrivit server, iar utilizatorii versiunii premium au posibilitatea de a modifica locația serverului la care doresc să se conecteze selectând-o din lista de Locații virtuale. Pentru detalii despre abonamentele VPN, accesează Abonamente (page 34).

Pentru conectare sau deconectare, nu trebuie decât să efectuezi clic pe starea afișată în partea de sus a ecranului. Pictograma din bara de meniu devine neagră atunci când conexiunea VPN este activă și albă atunci când conexiunea VPN este inactivă.



Când ești conectat, timpul scurs este afișat în partea de jos a interfeței. Pentru a avea acces la mai multe opțiuni, efectuează clic pe pictograma ⚙ din partea de sus dreapta:

- **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.
- **Setări** - în funcție de nevoile tale, poți personaliza comportamentul produsului tău:
  - **General**
    - Notificări - Afișează notificările produsului.
    - Rulare la pornire - lansează automat Bitdefender VPN în momentul conectării.
    - Rapoarte privind produsul - trimite rapoarte anonime despre produs pentru a ne ajuta să îți îmbunătățim experiența și capabilitățile de protecție.
  - **Avansat**
    - Comutator pentru oprirea conexiunii la internet - suspendă temporar întreg traficul pe internet în cazul în care conexiunea VPN se întrerupe accidental.
    - Ad blocker și Anti-tracker - blochează reclamele și trackerele pentru ca tu să te bucuri de o navigare sigură și rapidă.
    - Split tunneling - aplicațiile sau site-urile web selectate vor evita VPN-ul și vor accesa internetul direct.

> **Notă**
> Apasă pe **Administrare** și apoi pe **Adăugare site web** pentru a adăuga pagini web la această listă.

- Autoconectare - conectează la VPN automat atunci când:
  - Se efectuează o conexiune la o rețea Wi-Fi nesecurizată sau publică.
  - A fost inițiată o aplicație de partajare a fișierelor de tip peer-to-peer.

- **Asistență** - ești redirecționat către platforma noastră Support Center unde poți citi un articol util despre cum să folosești Bitdefender VPN.
- **Despre** – sunt afișate informații despre versiunea instalată.
- **Renunțare** - părăsește aplicația.

5.4. Abonamente

Bitdefender VPN oferă gratuit o cotă de trafic zilnică de 200 MB pentru fiecare dispozitiv pentru a 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 for Mac, ceea ce înseamnă că îl vei putea utiliza cât timp este valabil, indiferent de starea abonamentului pentru soluția de securitate. În cazul în care abonamentul Bitdefender Premium VPN expiră, dar abonamentul Bitdefender Antivirus for Mac este încă activ, vei reveni la versiunea gratuită.

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

6. CONFIGURAREA PREFERINȚELOR

Acest capitol include următoarele subiecte:

- Accesarea preferințelor (page 35)
- Preferințe de protecție (page 35)
- Preferințe avansate (page 36)
- Oferte speciale (page 36)

6.1. Accesarea preferințelor

Pentru deschiderea ferestrei de preferințe a Bitdefender Antivirus for Mac:

- Puteți proceda în oricare dintre următoarele modalități:
  - Clic pe **Preferințe** în meniul de navigare din interfața Bitdefender.
  - Apasă pe Bitdefender Antivirus for Mac din bara de meniu și selectează **Preferințe**.

6.2. Preferințe de protecție

Fereastra de setări preferate de protecție îți permite să configurezi abordarea generală de scanare. Puteți configura acțiunile întreprinse în cazul fișierelor infectate și suspecte detectate, precum și alte setări generale.

- **Bitdefender Shield.** Bitdefender Shield oferă protecție în timp real împotriva unei varietăți de amenințări prin scanarea tuturor aplicațiilor instalate, a versiunilor lor actualizate și a fișierelor noi și modificate. Nu îți recomandăm să dezactivezi Bitdefender Shield, însă dacă acest lucru este necesar, asigură-te că acest modul este dezactivat pentru cât mai puțin timp posibil. Dacă Bitdefender Shield este dezactivat, nu vei mai fi protejat împotriva amenințărilor.
- **Scanare doar fișiere noi și modificate.** Selectează această căsuță pentru a configura Bitdefender Antivirus for Mac să scaneze exclusiv fișierele care nu au fost scanate anterior sau care au fost modificate de la ultima scanare.
  Poți alege să nu aplici această setare în cazul scanării personalizate prin drag & drop debifând caseta corespunzătoare.

- **Nu scana conținutul din backupuri.** Selectează această căsuță pentru a exclude fișierele backup de la procesul de scanare. Dacă fișierele infectate sunt restituite ulterior, Bitdefender Antivirus for Mac le va detecta automat și va lua măsurile necesare.

6.3. Preferințe avansate

Poți selecta o acțiune generală ce urmează a fi întreprinsă pentru toate problemele și obiectele suspecte identificate în timpul procesului de scanare.

Acțiune pentru obiecte infectate

- **Încearcă dezinfectarea sau mutarea în carantină** - Dacă sunt detectate fișiere infectate, Bitdefender va încerca să le dezinfecteze (să elimine codul periculos) sau să le mute în carantină.
- **Nu întreprinde nicio acțiune** - Nu se va întreprinde nicio acțiune asupra fișierelor detectate.

Acțiune pentru obiecte suspecte

- **Mută fișierele în carantină** - Dacă sunt detectate fișiere suspecte, Bitdefender le va muta în carantină.
- **Nu luați nicio măsură** - Nu se va lua nicio acțiune asupra fișierelor detectate.

6.4. Oferte 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 **Preferințe** în meniul de navigare din interfața Bitdefender.
2. Selectează fila **Altele**.
3. Activează sau dezactivează opțiunea **Ofertele mele**.

> **Notă**
> Opțiunea **Ofertele mele** este activată implicit.

7. 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:
  - Bitdefender Antivirus pentru Mac
  - Gama de produse Bitdefender Windows
  - 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.

7.1. 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 a Bitdefender Antivirus for Mac:

1. Fă clic pe linkul **Mergi la contul tău** situat în partea din dreapta jos a ecranului.

- Din browser-ul web:
  1. Deschide un browser web pe orice dispozitiv cu acces la internet.
  2. Mergi la: 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.

7.2. 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.

7.2.1. 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. Accesează **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. 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**.

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.

7.3. 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. Accesează Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Clic pe **Contul Bitdefender** în meniul slide.
4. Selectează **Parolă și securitate**.
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.

7.4. 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.

7.4.1. Adăugarea unui dispozitiv nou

Dacă abonamentul dvs. acoperă mai multe dispozitive, puteți adăuga un dispozitiv nou și puteți instala Bitdefender Antivirus for Mac 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.

7.4.2. 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**.

7.4.3. 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.

7.5. 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.

7.6. Abonamentele mele

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

7.6.1. 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).

7.6.2. 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.

7.6.3. 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.

7.7. 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.

8. ÎNTREBĂRI FRECVENTE

Cum pot încerca Bitdefender Antivirus for Mac înainte de a solicita un abonament?

Ești un client nou Bitdefender și dorești să încerci produsul nostru înainte de a-l cumpăra. Perioada de evaluare este de 30 de zile și poți utiliza în continuare produsul instalat numai dacă achiziționezi un abonament Bitdefender. Pentru a încerca Bitdefender Antivirus for Mac, trebuie să:

1. Creează-ți un cont Bitdefender urmând acești pași:
   a. Mergi la: https://central.bitdefender.com.
   b. Introdu informațiile solicitate în câmpurile corespunzătoare. Datele furnizate aici vor rămâne confidențiale.
   c. 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.
   d. Fă clic pe **CREARE CONT**.

2. Descarcă Bitdefender Antivirus for Mac astfel:
   a. Selectează **Dispozitivele mele** panou, apoi faceți clic **INSTALATI PROTECTIA**.
   b. Alegeți una dintre cele două opțiuni disponibile:
      - **Protejați acest dispozitiv**
        i. Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
        ii. Salvați fișierul de instalare.
      - **Protejați alte dispozitive**
        i. Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
        ii. Clic **TRIMITE LINK DE DESCARCARE**.

iii. 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.

iv. 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.

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

Am deja un cont de activare. Cum adaug valabilitatea acestuia la abonamentul meu?

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

Pentru a activa un abonament folosind un cod de activare, urmați acești pași:

1. Acces Bitdefender Central.
2. Selectează **Abonamentele mele** panou.
3. Apasă pe **COD DE ACTIVARE** butonul, apoi introduceți codul în câmpul corespunzător.
4. Clic **ACTIVATI** a continua.

Extensia este acum vizibilă în contul tău Bitdefender și în produsul tău Bitdefender Antivirus for Mac instalat, în partea din dreapta jos a ecranului.

Jurnalul de scanare indică faptul că există încă o serie de obiecte nesoluționate. Cum le șterg?

Obiectele nesoluționate din jurnalul de scanare pot fi:

- acces restricționat arhive (xar, rar, etc.)
  Soluție: utilizează opțiunea **Arată în Finder** pentru a identifica fișierul și pentru a-l șterge manual. Golește folderul Trash.
- acces restricționat cutii poștale (Thunderbird, etc.)

Soluție: Utilizați aplicația pentru a șterge înregistrarea care conține fișierul infectat.

- Conținut din back-up-uri
  Soluție: activează opțiunea **Nu scana conținutul backupurilor** din Preferințele privind protecția sau **Adaugă la excepții** fișierele detectate.
  Dacă fișierele infectate sunt restabilite ulterior, Bitdefender Antivirus for Mac le va detecta automat și va acționa în mod corespunzător.

> **Notă**
> Fișierele cu acces restricționat sunt fișiere pe care Bitdefender Antivirus pentru Mac doar le poate deschide, nu le poate modifica.

Unde pot vedea detalii despre activitatea produsului?

Bitdefender păstrează un jurnal al tuturor acțiunilor importante, modificărilor de stare și al altor mesaje critice legate de activitatea sa. Pentru a accesa aceste informații, selectați opțiunea **Notificări** din meniul de navigare al interfeței Bitdefender.

Pot actualiza Bitdefender Antivirus for Mac prin intermediul unui Server Proxy?

Bitdefender Antivirus pentru Mac se poate actualiza numai prin servere proxy care nu necesită autentificare. Nu trebuie să configurați nicio setare a programului.

Dacă vă conectați la internet printr-un server proxy care necesită autentificare, trebuie să treceți la o conexiune directă la internet în mod regulat pentru a obține actualizări ale informațiilor despre amenințări.

Cum dezactivez Bitdefender Antivirus for Mac?

Pentru a elimina Bitdefender Antivirus pentru Mac, urmați acești pași:

1. Deschide o fereastră **Finder**, apoi accesează directorul Aplicații.
2. Deschide directorul Bitdefender și efectuează dublu-clic pe BitdefenderUninstaller.
3. Clic **Dezinstalează** și așteptați finalizarea procesului.
4. Clic **Închide** a termina.

Important
Dacă apare o eroare, puteți contacta Serviciul pentru clienți Bitdefender, așa cum este descris în Solicitarea ajutorului (page 52).

Cum șterg extensiile TrafficLight din browser-ul meu web?

- Pentru a șterge extensiile TrafficLight din Mozilla Firefox, urmați pașii de mai jos:
  1. Accesează **Instrumente** și selectează **Add-on**.
  2. Selectați **Extensii** din coloana din partea stângă.
  3. Selectați extensia și faceți clic pe **Ștergere**.
  4. Reporniți browser-ul pentru finalizarea procesului de ștergere.
- Pentru a șterge extensiile TrafficLight din Google Chrome, urmați pașii de mai jos:
  1. În partea dreaptă de sus, apasă pe **Mai multe** ⋮.
  2. Accesează **Mai multe instrumente** și selectează **Extensii**.
  3. Fă clic pe pictograma **Dezinstalare** de lângă extensia pe care dorești să o dezinstalezi.
  4. Efectuează clic pe **Dezinstalare** pentru a confirma procesul de ștergere.
- Pentru a elimina Bitdefender TrafficLight din Safari, urmați pașii de mai jos:
  1. Accesează **Preferințe** sau apasă pe **Command-Comma(,)**.
  2. Selectează **Extensii**.
     Se va afișa o listă cu extensiile instalate.
  3. Selectează extensia Bitdefender TrafficLight, apoi **Dezinstalare**.
  4. Selectează **Dezinstalare** încă o dată pentru a confirma procesul de ștergere.

Când ar trebui să utilizez Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe internet. Ca să fii sigur că ești protejat atunci când navighezi pe web, îți recomandăm să folosești Bitdefender VPN când:

- când dorești să te conectezi la rețele wireless publice
- când dorești să accesezi conținut care în mod normal este restricționat în anumite zone, indiferent dacă ești acasă sau în străinătate
- când dorești să-ți păstrezi confidențialitatea datelor tale personale (nume de utilizator, parole, datele cardului de credit etc.)
- când dorești să-ți ascunzi adresa IP

Bitdefender VPN va avea un impact negativ asupra autonomiei bateriei dispozitivului meu?

Bitdefender VPN este conceput să îți protejeze datele personale, să îți ascundă adresa IP în timp ce ești conectat la rețele wireless nesecurizate și la conținutul cu acces restricționat din anumite țări. Pentru a evita consumarea inutilă a bateriei, îți recomandăm să folosești funcția VPN numai atunci când ai nevoie de ea și să te deconectezi atunci când ești offline.

De ce încetinește viteza de internet atunci când sunt conectat cu Bitdefender VPN?

Bitdefender VPN este conceput să îți ofere o navigare ușoară pe web; totuși, conexiunea ta la internet sau distanța față de serverul la care te conectezi pot cauza o încetinire. În acest caz, dacă nu trebuie neapărat să te conectezi din locația ta la un server îndepărtat (de ex. din SUA sau China), îți recomandăm să permiți Bitdefender VPN să te conecteze automat la cel mai apropriat server, sau să găsești un server mai apropiat de locația ta curentă.

9. OBȚINE AJUTOR

9.1. 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.

9.2. 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.

9.2.1. 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/.

9.2.2. 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

9.2.3. 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/.

9.3. 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 (page 52).

https://www.bitdefender.ro/consumer/support/

9.3.1. 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.

Dicționar 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 acționează şi să identifice metodele eretice pe care le folosesc pentru a colecta informații 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.