Fișă de produs

Bitdefender
BUILT FOR RESILIENCE

GravityZone Security EDR Cloud

Advanced Endpoint Detection and Response

Infractorii cibernetici folosesc metode din ce în ce mai sofisticate, iar atacurile avansate de astăzi sunt din ce în ce mai greu de detectat. Folosind tehnici ce imită comportamentele din viața de zi cu zi, un atacator poate accesa infrastructura dvs. și poate rămâne nedetectat luni de zile, crescând semnificativ riscul apariției unei breșe costisitoare de securitate a datelor. Atunci când soluția dvs. actuală de securitate la nivel de endpoint nu vă oferă caracteristicile de detecție și răspuns de care aveți nevoie pentru combaterea atacurilor avansate – adăugarea soluției GravityZone EDR Cloud consolidează rapid și eficient operațiunile dvs. de securitate.

GravityZone EDR Cloud vă monitorizează rețeaua pentru a descoperi din timp activitățile suspecte și vă oferă instrumentele de care aveți nevoie pentru a combate atacurile cibernetice. Prin integrarea tehnologiei premiate de machine learning, a caracteristicilor de scanare în cloud și a soluției sandbox analyzer de la Bitdefender, ea poate detecta activitatea care se sustrage mecanismelor tradiționale de prevenție a atacurilor la nivel de endpoint. Oferă vizibilitate deplină asupra tehnicilor, tacticilor și procedurilor (TTP) utilizate în atacurile active, oferind în același timp capabilități de căutare cuprinzătoare pentru indicatori specifici de compromis (IoC), tehnici MITRE ATT&CK și alte artefacte pentru descoperirea atacurilor în stadiu incipient.

GravityZone EDR Cloud oferă o vizualizare inovativă și ușor de înțeles, cu contexte ample și informații privind amenințările care să ajute personalul IT să înțeleagă căile de atac și să identifice lacunele sistemului protecție. Aceste vizualizări optimizează investigațiile și răspunsurile, minimizând sarcinile personalului IT. Sandbox Analyzer permite personalului să execute automat payload-uri suspecte într-un mediu izolat și virtual, pentru a izola și neutraliza fișierele suspecte. Capacitățile GravityZone EDR Cloud protejează companiile împotriva amenințărilor avansate, permițând în același timp căutarea proactivă a amenințărilor și analiza cauzelor principale.

Cum ajută GravityZone EDR Cloud?

- **Detecție și răspuns la atacurile avansate.** Monitorizează rețeaua dumneavoastră pentru a descoperi activitatea suspectă din timp și vă oferă instrumentele de care aveți nevoie pentru a combate atacurile cibernetice.
- **Eliminați lacunele în materie de competențe.** Permite echipelor să răspundă eficient datorită ierarhizării automate a alertelor și opțiunii de răspuns cu un singur clic.
- **Reducerea riscurilor la adresa companiei.** Analizează în mod continuu infrastructura pentru a identifica riscurile pe baza a sute de factori. Contribuie la remedierea riscurilor la nivel de utilizator, rețea și sistem de operare.
- **Reduce efortul operațional.** Livrați în cloud și necesitând un efort redus de întreținere, agenții sunt ușor de implementat și integrat în arhitectura de securitate existentă și sunt complet compatibili cu soluția dumneavoastră antivirus pentru endpoint-uri.

Inovație pentru eficiență și eficacitate

Tehnologia Bitdefender de corelare la nivelul endpoint-urilor duce detecția și vizibilitatea asupra amenințărilor la un nou nivel, aplicând capabilitățile XDR pentru detectarea atacurilor avansate care implică mai multe endpoint-uri din infrastructurile hibride (stații de lucru, servere sau containere cu diferite

Pe scurt

GravityZone EDR Cloud detectează în timp real amenințările avansate, inclusiv atacurile fără fișiere, ransomware-ul și alte amenințări de tip „zero-day”. Caracteristica sa de înregistrare a evenimentelor pe baza analizei amenințărilor și pe bază de cloud monitorizează în permanență endpoint-urile și ierarhizează evenimentele de securitate într-o listă de incidente pentru investigații și răspuns. Bitdefender EDR oferă o vizualizare inovativă și ușor de înțeles, cu contexte ample și informații privind amenințările care să ajute personalul IT să înțeleagă căile de atac și să identifice lacunele de protecție. Aceste vizualizări optimizează investigațiile și răspunsurile, minimizând sarcinile personalului IT.

Beneficii principale

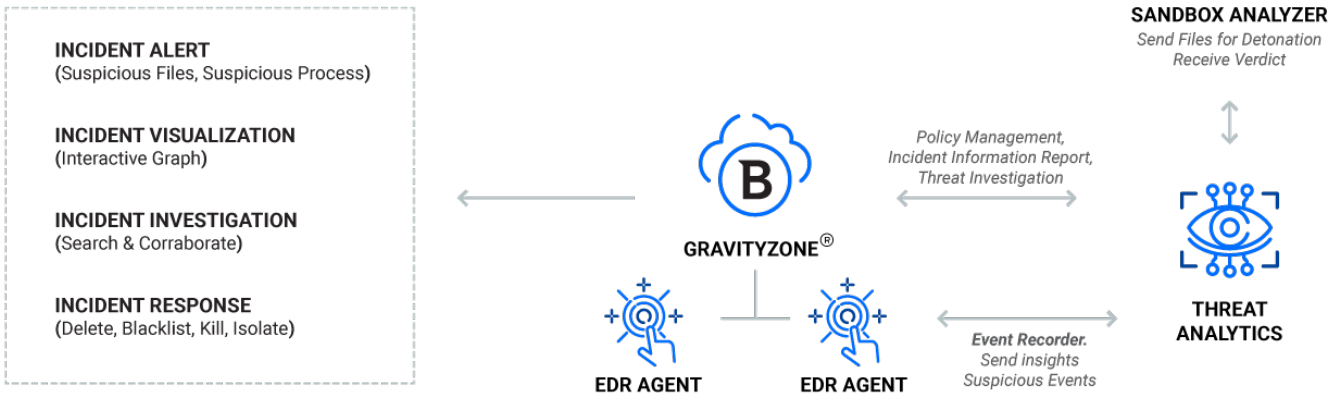
- Cea mai performantă detecție din industrie - detecție și vizibilitate îmbunătățită asupra amenințărilor, care permite capabilităților XDR să vă protejeze endpoint-urile. Capacități de căutare avansată în funcție de indicatori specifici de compromitere (IoC), tehnici MITRE ATT&CK și alte artefacte pentru a descoperi atacurile într-un stadiu incipient.
- Investigații și răspunsuri orientate – Vizualizarea incidentelor la nivel organizațional vă permite să răspundeți eficient, să limitați răspândirea laterală și să opriți atacurile în curs de desfășurare.
- Eficiență maximă - Agentul nostru ușor de instalat, cu impact redus asupra resurselor, asigură eficiență și protecție maximă, cu eforturi minime. Pentru o soluție administrată complet, puteți face ușor upgrade la serviciul administrat de detecție și răspuns (MDR) de la Bitdefender.

„Capabilitățile EDR ale GravityZone ne oferă rapoarte detaliate cu privire la modul în care au fost afectate procesele de-a lungul întregului lanț de atac. Astfel nu mai trebuie să dedicăm mult timp procesului de investigare, având în vedere că munca manuală este eliminată.”

Sascha Neuhaus,
IT Security Officer, Louis

sisteme de operare). Extinde capabilitățile EDR de vizibilitate, analiză și corelare a evenimentelor dincolo de granițele unui singur endpoint, pentru a permite echipelor de securitate să facă față mai eficient atacurilor cibernetice complexe care implică mai multe endpoint-uri. Această tehnologie de corelare a mai multor endpoint-uri combină granularitatea și contextul bogat de securitate al soluției EDR cu analiza la nivelul întregii infrastructuri a modulului Extended Detection and Response (XDR). Oferind vizualizări ale amenințărilor la nivel organizațional, XDR ajută companiile să se concentreze asupra investigațiilor și să răspundă mai eficient.

Modalitatea de funcționare



GravityZone EDR Cloud este o soluție bazată pe cloud, care valorifică platforma Bitdefender GravityZone XDR. Fiecare agent EDR instalat pe endpoint-urile companiei dumneavoastră are o funcție de înregistrare a evenimentelor, care monitorizează în permanență endpoint-ul și trimite în siguranță informații și detalii privind evenimentele suspecte către consola centralizată GravityZone Control Center. În Control Center, motorul Bitdefender de corelare între endpoint-uri colectează și distilează evenimentele de la endpoint-uri și generează vizualizări prioritare, la nivel organizațional, ale incidentelor de securitate, permițând administratorilor să investigheze rapid și să răspundă eficient la amenințări.

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Bitdefender este un lider recunoscut în domeniul securității IT, care oferă soluții superioare de prevenție, detecție și răspuns la incidente de securitate cibernetică. Milioane de sisteme folosite de utilizatori individuali, companii și instituții guvernamentale sunt protejate de Bitdefender, unul dintre cei mai de încredere experți în combaterea amenințărilor informatice, în protejarea datelor și în consolidarea rezilienței cibernetice. Ca urmare a investițiilor susținute în cercetare și dezvoltare, laboratoarele Bitdefender descoperă peste 400 de noi amenințări informatice în fiecare minut și analizează zilnic circa 40 de miliarde de amenințări. Compania a inovat constant în domenii precum antimalware, Internet of Things, analiză comportamentală și inteligență artificială, iar tehnologiile Bitdefender sunt licențiate către peste 150 dintre cele mai cunoscute branduri de securitate din lume. Fondată în 2001, compania Bitdefender are clienți în 170 de țări și birouri pe toate continentele.

Mai multe detalii sunt disponibile pe www.bitdefender.ro

Bitdefender BSS GZ EDRCloud Datasheet DEV4610ro_RO
CA v1.0 2022.10.04