FIȘĂ DE PRODUS

Numai pentru utilizare pe internet

Bitdefender

Detecție și răspuns la nivelul stațiilor de lucru

Detectarea amenințărilor avansate, investigații precise și răspuns eficient

www.bitdefender.ro

Provocările pe care le implică amenințările avansate cu care vă confruntați în prezent

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 care, în mod individual, sunt similare cu comportamentele de rutină, un atacator poate accesa infrastructura dumneavoastră și poate rămâne nedetectat luni de zile, crescând semnificativ riscul apariției unei breșe costisitoare de securitate a datelor.

Cum vă poate ajuta soluția Bitdefender Endpoint Detection and Response (EDR)?

Atunci când soluția dumneavoastră actuală de securitate la nivel de endpoint nu vă oferă vizibilitatea asupra atacurilor avansate și funcționalitățile de răspuns de care aveți nevoie, adăugarea rapidă și eficientă a soluției Bitdefender Endpoint Detection and Response (EDR), care este ușor de folosit, vă permite consolidarea rapidă și eficientă a operațiunilor dumneavoastră de securitate.

Detecție și răspuns la atacurile avansate

Bitdefender EDR vă monitorizează rețeaua pentru a descoperi din timp activitatea suspectă și vă oferă instrumentele de care aveți nevoie pentru a combate atacurile cibernetice.

- EDR integrează tehnologia premiată de machine learning de la Bitdefender, caracteristicile de scanare în cloud și sandbox analyzer pentru a detecta activitatea periculoasă care se sustrage mecanismelor tradiționale de prevenire a atacurilor la nivel de endpoint.
- Vizibilitate completă asupra tehnicilor, tacticilor și procedurilor (TTP) utilizate pentru a vă ataca sistemele.
- Capacități de căutare avansată în funcție de indicatori specifici de compromitere (IoC), tehnici MITRE ATT&CK și alte artefacte pentru a descoperi atacurile încă dintr-un stadiu incipient. În Evaluarea MITRE ATT&CK din aprilie 2020, Bitdefender a excelat la capitolul detecții și alerte ce stau la baza unor măsuri de remediere, în fiecare etapă a întregului lanț de atac.
- Întreprindeți măsuri de răspuns pentru a remedia vulnerabilitățile și elimina riscul apariției unor atacuri recurente.

Eliminarea lacunelor în materie de competențe de securitate cibernetică

- Fluxurile de răspuns integrate, care sunt ușor de respectat, permit echipei dumneavoastră să răspundă eficient, să limiteze răspândirea laterală și să oprească atacurile în curs.
- Caracteristicile de vizualizare a amenințărilor vă permit să vă concentrați pe anumite aspecte în cadrul investigațiilor, vă ajută să înțelegeți detecțiile complexe, să identificați cauza principală a atacurilor și să vă maximizați capacitatea de a răspunde imediat.
- Prioritizarea automatizată a alertelor cu funcții de remediere cu un singur clic.

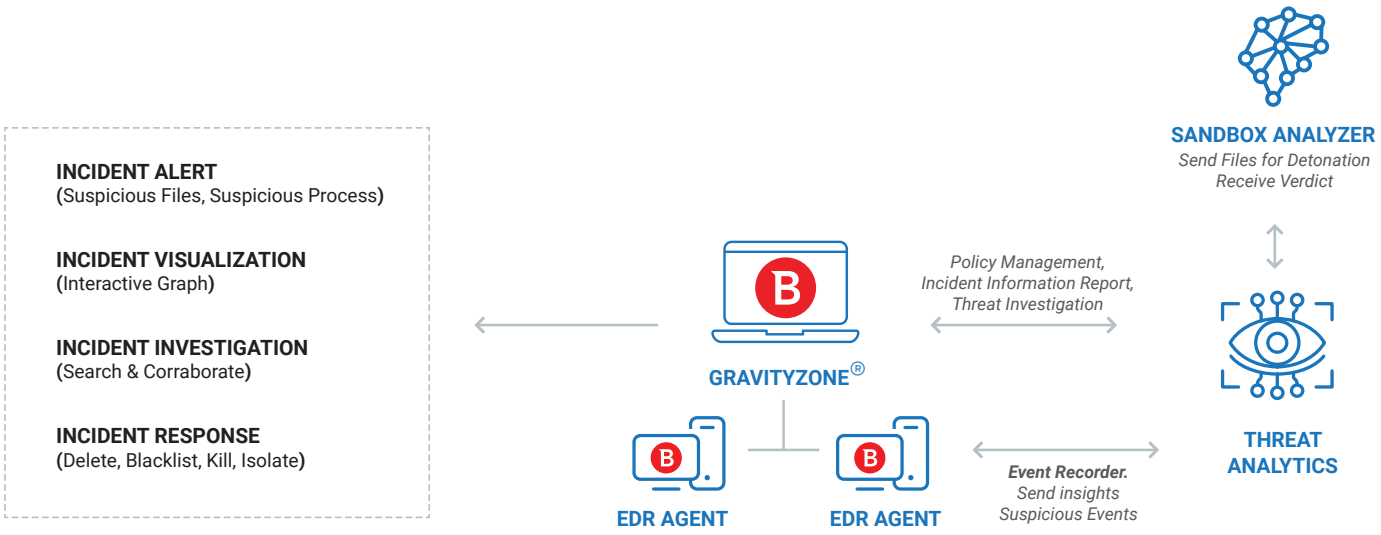
Reducerea riscului organizațional

- EDR analizează în mod continuu organizația dumneavoastră utilizând capabilități unice pentru a identifica riscul în funcție de sute de factori. Oferă îndrumări clare pentru a vă ajuta să atenuați riscurile la nivel de utilizator, rețea și sistem de operare.

Minimizarea efortului operațional

- Livrat în cloud și necesitând un efort redus de întreținere, EDR este ușor de implementat și integrat în arhitectura de securitate existentă și este complet compatibil cu soluția dumneavoastră antivirus pentru endpoint.
- Agentul, care implică un consum redus de resurse, presupune costuri administrative scăzute din punct de vedere al spațiului pe disc, memoriei, lățimii de bandă și resurselor procesorului.
- Flexibil, scalabil și cu posibilitate de upgrade la platforma completă de protecție la nivel de endpoint și serviciile administrate de detecție și răspuns (MDR) de la Bitdefender.

Cum funcționează



Mai sus: Bitdefender Endpoint Detection and Response

Bitdefender EDR este o soluție livrată din cloud, construită pe platforma Bitdefender GravityZone. Agenții EDR sunt instalați pe endpoint-urile organizației dvs. Fiecare agent EDR are o funcție de înregistrare a evenimentelor, care monitorizează continuu endpoint-ul și trimite în siguranță informații și evenimentele suspecte către cloud-ul GravityZone.

În Gravity Zone, modulul de analiză a amenințărilor colectează și filtrează evenimentele produse pe endpoint alcătuind o listă prioritară de incidente pentru investigații suplimentare și răspuns. Trimite fișierele suspecte pentru detonare în Sandbox Analyzer, apoi folosește verdictul din sandbox în rapoartele de incidente generate de EDR. Panoul de control al soluției EDR, disponibil în timp real, poate fi accesat de pe orice dispozitiv pentru a permite administratorilor să vadă alerte și să vizualizeze informațiile disponibile, apoi să investigheze și să răspundă eficient la amenințări.

Caracteristicile soluției Bitdefender Endpoint Detection and Response

Analiza riscurilor

Identificarea riscurilor la nivel de utilizator și endpoint
Analizează în permanență riscul organizațional bazându-se pe sute de factori pentru a identifica, prioritiza și a oferi îndrumări cu privire la atenuarea riscurilor la nivel de utilizator, rețea și endpoint.

Detecție

Tehnologie de vârf în materie de detecție a amenințărilor
Detectează amenințările avansate, inclusiv atacurile fără fișiere, ransomware-ul și alte amenințări de tip „zero-day”. Completează soluția dumneavoastră existentă de securitate la nivel de endpoint pentru a consolida capacitatea de detecție.

Analiza amenințărilor
Caracteristica de înregistrare a evenimentelor pe bază de cloud filtrează în permanență evenimentele produse pe endpoint, alcătuind o listă prioritară de incidente pentru investigații suplimentare și răspuns.

Înregistrare evenimente
Monitorizarea continuă a evenimentelor produse pe endpoint, care permite transmiterea evenimentelor către modulul de analiză a amenințărilor pentru a permite vizualizarea amenințărilor generate de evenimentele implicate într-un atac.

Sandbox Analyzer
Execută automat payload-urile suspecte într-un mediu virtual controlat. Modulul de analiză a amenințărilor folosește ulterior această analiză pentru a lua decizii privind fișierele suspecte.

Investigație și răspuns

Căutare IoC
Interogați baza de date a evenimentelor pentru a descoperi amenințările. Descoperiți tehnicile ATT&CK și indicatorii de compromitere. Informații actualizate privind amenințările descoperite sau alte posibile programe malware.

Vizualizare
Ghidurile vizuale ușor de înțeles, îmbogățite cu informații referitoare la context și threat intelligence, evidențiază căile critice de atac, reducând efortul personalului IT. Ajută la identificarea lacunelor de protecție și a impactului incidentelor pentru a sprijini eforturile de asigurare a conformității.

Detonare
Investigația în sandbox inițiată de operator vă ajută să luați decizii informate cu privire la fișierele suspecte

Listă de blocare

Opriți răspândirea fișierelor sau a proceselor suspecte detectate de EDR pe alte sisteme

Stoparea procesului
Opriți instantaneu procesele suspecte pentru a bloca potențialele breșe de securitate în curs de desfășurare

Izolare rețea
Blocați conexiunile la și de la endpoint pentru a opri răspândirea în rețea și alte breșe de securitate în timpul investigării incidentelor

Comenzi „shell” de la distanță
Executați comenzi de la distanță pe orice stație de lucru pentru a asigura reacția imediată la incidentele în curs

Rapoarte și alerte

Dashboard-uri și rapoarte
Panouri de control configurabile și capacități avansate de raportare instantanee și programată

Notificări
Panou de control configurabil și notificări prin e-mail

Integrare cu SIEM și API-uri disponibile
Permite integrarea avansată cu instrumentele altor producători

Performanță și administrare

Agent EDR optimizat
Impact redus asupra procesorului, memoriei RAM, spațiului pe disc

Consolă web
Caracteristici de administrare în cloud ușor de folosit

DE CE BITDEFENDER?

LIDER INCONTESTABIL ÎN INOVARE.
38% din totalul furnizorilor de securitate cibernetică la nivel global au integrat cel puțin una dintre tehnologiile Bitdefender. Suntem prezenți în 150 de țări.

PRIMA SOLUȚIE DE EVITARE COMPLETĂ A BREȘELOR DE SECURITATE DIN LUME
Prima soluție de securitate care reunește reducerea suprafeței de atac, prevenția, detecția și răspunsul pentru endpoint-uri, rețea și cloud.

SOLUȚIA DE SECURITATE COTATĂ NR. 1 PREMIATĂ ÎN TOATE DOMENIILE.

AV comparatives CERTIFIED ATP Enterprise 2019

AV comparatives Product of the Year 2019

FORRESTER WAVE LEADER 2019 Cloud Workload Security

BITDEFENDER GravityZone Ultra v6.6.7.166 ADVANCED ENDPOINT PROTECTION NSS RECOMMENDED MARCH 2019

Bitdefender

Înființat în 2001, România
Numărul angajaților 1800+

Sedii
Sediu enterprise – Santa Clara, CA, Statele Unite ale Americii
Sediu central – București, România

BIROURI ÎN ÎNTREAGA LUME
SUA și Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europa: Copenhaga, DANEMARCA | Paris, FRANȚA | München, GERMANIA | Milano, ITALIA | București, Iași, Cluj, Timișoara, ROMÂNIA | Barcelona, SPANIA | Dubai, EAU | Londra, REGATUL UNIT | Haga, ȚĂRILE DE JOS
Australia: Sydney, Melbourne

SUB SEMNUL CAPULUI DE LUP DACIC

Fiind un domeniu al inteligenței, securitatea datelor este o industrie în care doar cea mai clară viziune, cea mai sclipitoare minte și cea mai temeinică perspectivă pot câștiga — un joc cu marjă de eroare zero. Misiunea noastră este să câștigăm de fiecare dată, de o mie de ori dintr-o mie și de un milion de ori dintr-un milion.

Și reușim. Suntem lideri în industrie, nu numai datorită faptului că avem cea mai clară viziune și cea mai sclipitoare minte, ci și pentru că suntem cu un pas înaintea tuturor, fie că vorbim despre atacatori sau colegi de breaslă. Inteligența noastră colectivă strălucește precum **ochii ageri ai unui lup dacic** care ne stă mereu alături, înlesnită fiind de o intuiție studiată, creată pentru a ține piept pericolelor ce se ascund în colțurile tainice ale tărâmului digital.

Această inteligență este superputerea noastră și o așezăm la temelia tuturor produselor și soluțiilor noastre inovatoare.