

Extended Detection & Response (XDR)

Intuitívny, prediktívny, bezpečný, jednoduchý.

Organizácie musia chrániť stále väčšiu útočnú plochu s väčším počtom zariadení, identít a dát v rastúcej a heterogénnej infraštruktúre, ktorá sa stáva terčom inovatívnych útočných techník.

Mnoho bezpečnostných riešení vyžaduje niekoľko ďalších bezpečnostných technológií a integráciu s tretími stranami z dôvodu prevencie, detekcie a reakcie na hrozby.

GravityZone XDR je integrovaný do špičkových preventívnych a detekčných technológií spoločnosti Bitdefender a je navrhnutý tak, aby maximalizoval efektivitu a účinnosť bezpečnostných tímov, minimalizoval dobu pobytu útočníkov a zaistil kybernetickú bezpečnosť organizácie.

Riešenie monitoruje širokú škálu fyzických a virtuálnych zdrojov, pripojených zariadení, cloudových platforiem a pracovných záťaží. Užívatelia môžu využívať výhod analytiky out-of-the-box a pokročilej heuristiky, ktorá koreluje rôznorodé upozornenia, čo umožňuje rýchle triedenie incidentov a rýchle obmedzenie útokov prostredníctvom automatizovanej a riadenej reakcie.

Platforma GravityZone XDR detekuje útoky rýchlejšie a presnejšie, odhaľuje celý rozsah útoku prepojením udalostí a incidentov v čase a poskytuje hlbší kontext a užitočné rady prostredníctvom nástroja Incident Advisor.

- Konsoliduje monitorovanie a udalosti v celom podnikovom prostredí.
- Vstavané algoritmy strojového učenia pre detekciu s vysokou spoľahlivosťou.
- Analýza hlavných príčin a kontextu naprieč zdrojmi pre rýchle triedenie incidentov a prijímanie opatrení.
- Riadená alebo automatizovaná reakcia na hrozby priamo z platformy.

Prehľadne

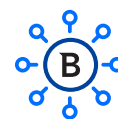
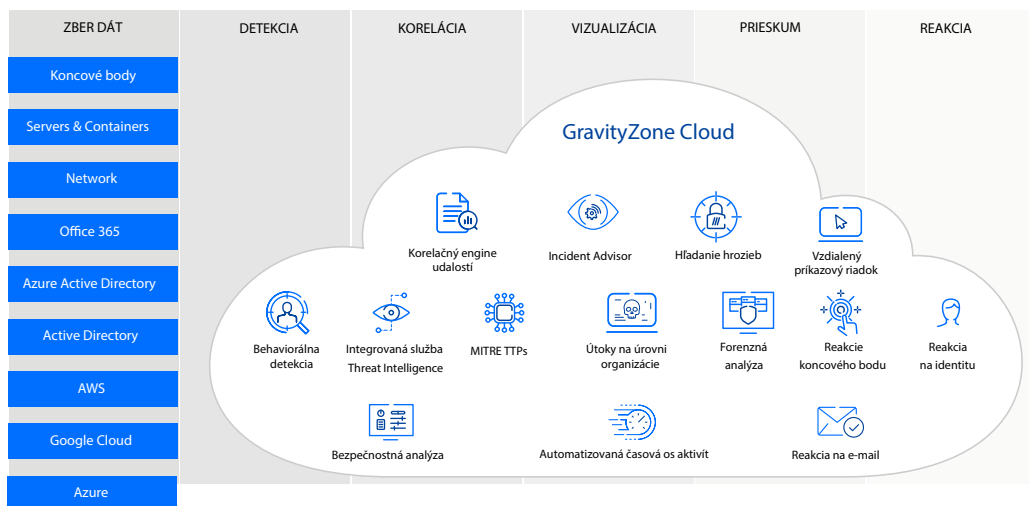
Bitdefender GravityZone XDR je cloudové riešenie určené na zabezpečenie celého podnikového prostredia. Riešenie poskytuje možnosti detekcie a reakcie naprieč všetkými užívateľmi a systémami organizácie, vrátane koncových bodov, siete a cloudu. GravityZone XDR sa ľahko používa a je navrhnuté tak, aby inteligentne analyzovalo a automaticky korelovalo a triedilo bezpečnostné udalosti z celej organizácie, čo prináša kľúčovú výhodu pre organizácie, ktoré chcú zabezpečiť komplexné prostredie.

Hlavné výhody

- Komplexný prehľad vďaka ľahko nasaditeľným a jednoducho spravovaným senzorm, ktoré zbierajú dáta z celej organizácie.
- Automatická detekcia a triedenie výstrah na základe korelačných a detekčných algoritmov, poskytovaných ako lokálne v senzore, tak na úrovni cloudovej platformy.
- Jednoduché vyhodnocovanie pomocou nástroja Incident Advisor, jediného panelu s komplexnou analýzou a odporúčanými automatickými alebo asistovanými reakciami.
- Rýchla reakcia pre kompletné potlačenie incidentu, vykonávaná priamo z platformy XDR.

Detekcia, odhaľovanie, vyhľadávanie a reakcia v rámci celej organizácie

GravityZone XDR je cloudový produkt pre organizácie, ktoré chcú túto technológiu prevádzkovať vo vlastnej réžii. Prenesenie dát o koncových bodoch, cloud, identitách, sieti a aplikáciách produktivity do platformy GravityZone, rozširuje visibilitu ďaleko za hranice spravovaných koncových bodov.



Aplikácie produktivity	Cloud	Identita	Sieť
Senzory, ktoré zhromažďujú a predbežne spracúvajú dáta o e-mailovej prevádzke a obsahu.	Zhromažďuje a spracováva informácie o zmenách konfigurácie a činnosti užívateľov.	Senzory zhromažďujú a spracúvajú prihlasovacie aktivity užívateľov, zmeny konfigurácie a ďalšie aktivity.	Zhromažďuje a spracováva sieťovú prevádzku v celom prostredí.

Organizáciám, ktoré hľadajú spravovanú službu, ponúka Bitdefender MDR, s využitím GravityZone XDR, nepretržitý bezpečnostný monitoring, pokročilú prevenciu, detekciu a nápravné opatrenia a ciele vyhľadávanie hrozieb na základe rizík certifikovaným tímom bezpečnostných expertov.