Pokročilé bezpečnostní řešení pro podniky

GravityZone Business Security Enterprise 2025

Kategorie:
Bezpečnostní řešení
Bitdefender, *www.bitdefender.cz*

Přihlašovatel:
IS4 security, *www.is4security.cz*
Bitdefender Country partner pro ČR a Slovensko

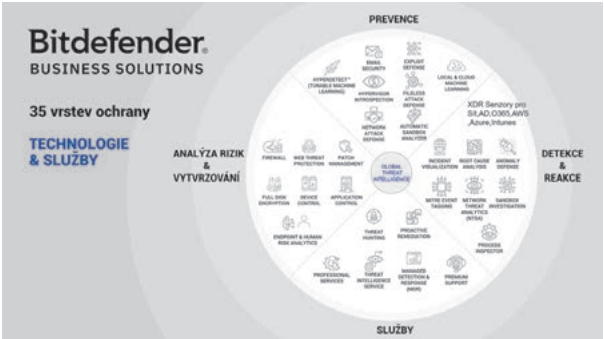
Použití produktu: GravityZone Business Security Enterprise poskytuje organizacím jednotnou ochranu i proti sofistikovaným kybernetickým útokům, přičemž pomáhá účinně zasahovat v každé fázi útoku. Nabízí rozpoznávání hrozeb v reálném čase včetně automatické nápravy problémů, zobrazení časového rámce útoku před a po kompromitaci, rychlé vyšetřování i reakci na incidenty, odhalení a zneškodnění malwaru ještě před jeho spuštěním pomocí přizpůsobitelného strojového učení, omezení plochy útoku pomocí kontroly aplikací a obsahu i patch managementu, dále monitorování procesů v reálném čase a sandboxovou analýzu nebo šifrování celých disků.

Popis produktu: Gravity Zone Business Security Enterprise je komplexní bezpečnostní řešení, které kombinuje pokročilou platformu pro ochranu koncových bodů s funkcemi detekce a reakce na koncové body (EDR). To umožňuje chránit infrastrukturu koncových bodů (tedy pracovní stanice, servery a kontejnery) v celém životním cyklu hrozeb, a to s vysokou efektivitou. Nabízí také prevenci kompromitace napříč koncovými body, detekci hrozeb a automatickou reakci na ně, vizualizaci útoku před a po kompromitaci, třídění výstrah, vyšetřování, pokročilé vyhledávání a možnosti řešení pomocí jediného kliknutí.

Zajímavé vlastnosti produktu:
- Dodává se jako cloudové řešení i on-premise s jednotnou správou
- Snadná instalace
- Propracovaná detekce hrozeb s komplexními možnostmi vyhledávání pro odhalení už raných fází útoků
- Integrované monitorování izolovaných sítí, např. OT
- Analýza rizik v ceně
- Lokální distribuce chybějících patchů
- Integrace se SIEM
- Podpora funkcí XDR (síťová, cloudová, identitní sonda), EASM či CIEM
- K dispozici mnoho add-ons

Záruka: podle délky předplatného

Cena (bez DPH): od 1761 Kč (1 zařízení/rok)



Bezpečnostní platforma s podporou AI

Progress Flowmon 12.5

Kategorie:
Bezpečnostní řešení
Progress, *www.progress.com/flowmon*

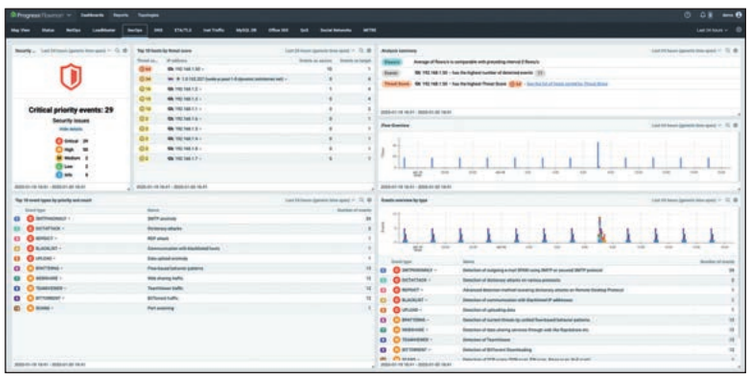
Přihlašovatel:
Progress, *www.progress.com*
výrobce

Použití produktu: Řešení Flowmon umožňuje zákazníkům efektivně spravovat a zabezpečovat jejich síťovou infrastrukturu, zlepšovat výkon aplikací a chránit se před pokročilými kybernetickými hrozbami. Funguje v jakémkoli podnikovém prostředí (on-premise, hybridním nebo cloudovém) a škálovatelně se přizpůsobí velikosti a odvětví každé firmy. Nabízí intuitivní uživatelské rozhraní, které umožňuje specialistům snadno přecházet od celkového přehledu bezpečnosti k podrobné analýze výkonu a zabezpečení sítě, pro vedení společnosti navíc automaticky vytváří a doručuje reporty přizpůsobené podle aktuálních potřeb.

Popis produktu: Flowmon je platforma pro kybernetickou bezpečnost určená firmám, které pracují s citlivými daty, kritickými aplikacemi, a pro vedoucí pracovníky, pro něž je klíčová reputace jejich firmy. Díky kombinaci umělé inteligence a sofistikovaných detekčních metod Flowmon dokáže zachytit i nepatrné stopy podezřelého chování ihned po jejich výskytu v síti. Analýza využívající AI poskytuje specialistům seznam priorit, čímž šetří čas, urychluje reakci na hrozby a minimalizuje potenciální dopady.

Zajímavé vlastnosti produktu:
- Asistovaná analýza – úspora času díky automatické analýze podezřelých událostí v síti a inteligentnímu stanovení priorit
- Unikátní detekční metody – odhalují celou škálu taktik a technik útočníků, snižují dopad hrozeb díky pokročilé AI a strojovému učení
- Dashboardy a reporty – plně přizpůsobitelné, poskytují klíčové poznatky o stavu zabezpečení sítě
- Nativní viditelnost v IoT/ICS/SCADA

Cena (bez DPH): podle velikosti instalace, obvyklé náklady na projekt od 250 000 Kč



Bezpečnostní školení s podporou virtuální reality

Company (Un)Hacked

Kategorie:
Bezpečnostní řešení
Sun Capital (PL), *www.suncapital.pl*

Přihlašovatel:
Zebra Systems, *www.companyunhacked.cz*
výhradní distributor pro ČR a SR

Použití produktu: Company (Un)Hacked představuje formu kyberbezpečnostního tréninku, která se uskutečňuje ve virtuální realitě. U zaměstnanců pomáhá zvyšovat povědomí o kybernetické bezpečnosti a ochraně dat. Účastník tréninku se vžije do role hackera a plní vybrané úkoly speciálně zaměřené na kancelářské a průmyslové prostředí. Trénink se děje formou hry ve virtuální realitě, účastníci ho proto mohou absolvovat kdykoli a kdekoli podle vlastních časových potřeb. Zástupci HR nebo IT oddělení mohou jejich progres sledovat v on-line tabulce.

Popis produktu: Company (Un)Hacked nabízí velmi efektivní učení hrou. Díky vlastnímu prožitku si zaměstnanci mohou uvědomit, jaké konkrétní triky používají hackeři, aby se dostali k citlivým informacím. Projdou deseti odlišnými, na sebe navazujícími scénáři na vlastní kůži během dramatické akce, nikoli formou nudné prezentace. Program je k dispozici ve všech běžně dostupných VR headsetech a je plně lokalizovaný do češtiny a slovenštiny. K dispozici jsou i další jazykové mutace, například k procvičení konkrétních situací v jiném jazyce.

Zajímavé vlastnosti produktu:
- Díky VR tréninku se zaměstnanci atraktivní formou seznámí s kybernetickou bezpečností
- Projekt významně přispívá ke zvyšování povědomí o současných rizicích
- Školení ve VR je podle studie PwC čtyřikrát efektivnější než běžné formy vzdělávání
- Školení lze absolvovat bez účasti lektora formou licencí nebo pomocí služby ve formě jednodenních workshopů s lektorem

Cena (bez DPH): podle počtu školených zaměstnanců či zakoupených licencí