

Bitdefender představuje GravityZone Elite HD

Nová dimenze ochrany pro koncové body

Před množícími se sofistikovanými a cílenými kybernetickými útoky, které dnešním běžným bezpečnostním nástrojům velice jednoduše uniknou, je potřeba se chránit, a to pomocí vrstvené ochrany, která není založena jen a pouze na signaturách, ale využívá další pokročilé nástroje.

ONDŘEJ DESENSKÝ

Bitdefender GravityZone Elite HD je přesně takovým pokročilým nástrojem. Obsahuje pokročilé strojové učení, behaviorální analýzy, antiexploit a integrovaný cloudový sandbox. S vysokou přesností a navíc velice rychle dokáže reagovat na jakékoliv hrozby, které mohou koncové body ohrozit.

HyperDetect™

Naprostá novinka na poli antimalwarové ochrany koncových bodů. Obsahuje lokální modely strojového učení a pokročilou heuristiku k rozpoznání sofistikovaných hackerských útoků, exploitů a technik obfuskace (ztížení analýzy škodlivého kódu útočnickem) malwaru. Speciálně navržené agresivní algoritmy dokážou detekovat exploity, ransomware a grayware, ale také bezsouborové útoky, cílené útoky a škodlivý síťový provoz. Hrozby zachycené systémem HyperDetect™ je možné automatickou akcí zablokovat, nebo pouze reportovat, nicméně ve velice granulární podobě blížící se EDR systémům.

Sandbox Analyzer

Je moderní obdobou klasického sandboxu s tím rozdílem, že analýza neprobíhá na koncových bodech, nýbrž na serverech Bitdefender Cloud Services. Nevytěžuje tedy prostředky koncového bodu a umožní uživateli bez zpomalení a omezení pokračovat v práci. Poté, co je soubor odeslán k analýze, je detonován v cloudovém sandboxu a následně pomocí pokročilých algoritmů strojového učení, behaviorálních analýz a forenzní analýzy je určen verdikt, který je odeslán zpět koncovému bodu. Do sandboxu je možné soubory odesílat jak automaticky, tak ručně.

Process Inspector

Je vysoce účinnou zbraní proti bezsouborovým útokům. Jakožto součást modulu aktivní ochrany před hrozbami (ATC – Active Threat Control) neustále monitoruje procesy a pátrá po jakékoliv škodlivé aktivitě všech procesů na koncovém bodu a jejich abnormálním chování. V případě nalezené hrozby je připraven ihned zasáhnout, proces okamžitě terminovat a vrátit vše do původního stavu.

Dejte sbohem falešným poplachům a průnikům hrozeb

Endpoint Security HD je jediná platforma ochrany koncového bodu, která může odkrýt podezřelé soubory a aktivity, jež na koncovém bodu zanechal útočník (bez ohledu na nastavení úrovně blokování), stejně jako poskytne detailní vhled do infrastruktury a velice přesné indikátory prvních úrovní útoku.

Novinky pro stávající uživatele

Full Disk Encryption: Data jsou nejdůležitějším artiklem digitální ekonomiky. Velkému riziku ztráty nebo krádeže jsou vystaveni především zaměstnanci s přenosným počítačem, ve kterém jsou uloženy informace o společnosti (např. během dovolené nebo služební cesty). Zatímco zařízení je možné vyměnit za relativně nízkou cenu, ztráta dat může vést k úbytku zákazníků, poškození pověsti nebo značným finančním ztrátám. Vyhnete se riziku ztráty dat a vynutíte předpisy pomocí úplného šifrování pevného disku vašich koncových bodů.

GravityZone FDE chrání data celého disku koncového bodu vynucením šifrovacího mechanismu Windows (BitLocker) a Mac (FileVault). Je potřeba nativní pod-

pora ze strany zařízení, aby byla zajištěna plná kompatibilita a maximalizován výkon. GZ FDE je plně integrován do konzole a agenta GravityZone bez nutnosti jakéhokoliv dalšího agenta nebo instalace serveru. Využití existující infrastruktury koncových bodů ke správě šifrování celého disku umožní plně centralizované nasazení s minimálním úsilím. Šifrování disků je dostupné jako add-on licence, dostupná k jakémukoliv původnímu řešení, ať už on-premise nebo cloud.

Patch management: V dosavadním prostředí kybernetické bezpečnosti se patching OS a aplikací stal pro IT administrátory vysokou prioritou v oblasti zabezpečení. GravityZone patch management umožňuje ověřit aktualizace celé firmy s cílem vynutit dodržování zásad zabezpečení.

Neaktualizované systémy zanechávají v infrastruktuře organizace volný prostor k malwarovým incidentům, hackerským útokům a únikům dat. Veškeré aktualizace máte plně pod kontrolou napříč ohromným spektrem aplikací na systému Windows pro pracovní stanice, fyzické servery a virtuální servery. Patch management je plně integrován do konzole GravityZone, nemusíte tedy řešit správu z více míst, konzole poskytuje ucelený vhled o stavu kritických i nekritických aktualizací v konzoli, kterou znáte, navíc s velice jednoduchou správou.

Patch management je stejně jako šifrování disků add-on licencí dostupnou k jakémukoliv existujícímu řešení Bitdefender GravityZone. Modul je samozřejmě spravován přímo z původní konzole.

GravityZone je nyní jediná sjednocená platforma ochrany koncových bodů nejen pro ochranu vašich koncových bodů před pokročilými útoky, ale také pro reakci na incidenty a správu aktualizací. Integrace, jednoduchost a snadná správa umožní IT administrátorům efektivněji pracovat. Navíc Bitdefender poskytuje i českou lokalizaci a českou podporu skrze lokální zastoupení pro ČR a SK.

Autor pracuje jako Security solution architect