BlackBerry | Kybernetická bezpečnost

BLACKBERRY CYBER SUITE

Propojení přístupů Zero Trust a Zero Touch

POPIS ŘEŠENÍ

Zabezpečení dat a ochrana koncových bodů nejsou novinkou, přesto nikdy nebyly důležitější než dnes. S neustále se rozšiřujícím spektrem útoků, stálým nárustem koncových bodů od mobilních zařízení až po Internet věcí (IoT), a v kombinaci s globálním trendem práce na dálku, narůstá tlak na zajištění kybernetické bezpečnosti. Koncepty a implementace rámce s tzv. Zero Trust nabývají na klíčovém významu, protože zabezpečení dat a ochrana koncových bodů jdou ruku.v ruce právě s tímto přístupem.

Princip tzv. Zero Trust byl vytvořen s cílem řešit deperimetrizaci neboli narušení tradičních hranic podnikových sítí. Zároveň se zvýšeným přístupem uživatelů k technologiím a nárůstem cloudových aplikací museli ředitelé pro informační bezpečnost změnit svůj přístup a začít předpokládat, že žádný provoz uvnitř sítě organizace není důvěryhodnější než provoz přicházející zvenčí. Princip tzv. Zero Trust spočívá v posouzení důvěryhodnosti a omezení přístupu. Jeho cílem je zajistit, že uživatel i zařízení jsou důvěryhodné, a zároveň omezit přístup pouze na data a aplikace nezbytné k výkonu jejich práce.

Vyvážení požadavků na Zero Trust a zachování produktivity zaměstnanců bylo vždy výzvou. Nicméně ještě před březnem 2020, kdy organizace ze dne na den přesunuly své globální pracovníky do režimu práce z domova, se princip Zero Trust a kontinuita podnikání rychle staly prioritou, kterou bylo nutné řešit.

Vyvážení požadavků na Zero Trust a zachování produktivity zaměstnanců bylo vždy výzvou. Nicméně ještě před březnem 2020, kdy organizace ze dne na den přesunuly své globální pracovníky do režimu práce z domova, se princip Zero Trust a kontinuita podnikání rychle staly prioritou, kterou bylo nutné řešit.

Komponenty BlackBerry Cyber Suite společně tvoří základ pro podnikovou bezpečnostní architekturu založenou na principu Zero Trust.

JAK BLACKBERRY ŘEŠÍ TYTO VÝZVY:

BlackBerry® Cyber Suite je speciálně navržená sada bezpečnostních prvků, která nabízí kombinaci rámce s nulovou důvěrou (Zero Trust) a uživatelského prostředí s minimálními zásahy (Zero Touch). Tyto prvky pokrývají tradiční koncové body, mobilní zařízení i IoT zařízení. BlackBerry Cyber Suite zahrnuje nejmodernější bezpečnostní kontroly a procesy tvořící základ pro bezpečnostní architekturu založenou na principu Zero Trust.

Experti v kybernetické bezpečnosti, kteří využívají zabezpečení na principu Zero Trust napříč odvětvími, zjistili, že přijetí této architektury přináší řadu výhod, jako například:

- Vylepšená bezpečnostní strategie, která nabízí rozšířený přehled a větší kontrolu pro efektivní minimalizaci rizik
- Zabezpečení a správa všech potenciálních zdrojů útoku od notebooků a serverů, přes mobilní zařízení až po zařízení IoT
- Úspora času a finančních prostředků díky jednotné platformě, která nabízí snadné nasazení a následnou správu
- Použití BlackBerry Cyber Suite vede ke zrychlení a zvýšení agility bezpečnostního týmu při zajištění lepšího přehledu napříč různorodou IT infrastrukturou

BLACKBERRY CYBER SUITE

SOUČÁST	POPIS
 **Ochrana koncového bodu**	Řešení CylancePROTECT® využívá strojové učení a umělou inteligenci (AI) k poskytování automatizované ochrany před malwarem, kontrole aplikací a skriptů, ochraně paměti a vynucování bezpečnostních zásad. Vysoká efektivita, snadné použití s minimálním dopadem na provoz umožňují předvídat kybernetické útoky a bránit jim.
 **Detekce a reakce na koncových bodech**	Řešení CylanceOPTICS® rozšiřuje prevenci hrozeb poskytovanou nástrojem CylancePROTECT, díky využití umělé inteligence k předcházení bezpečnostních incidentů. Poskytuje skutečnou prevenci incidentů pomocí AI, analýzu příčin, inteligentní vyhledávání hrozeb a automatickou detekci a reakci.
 **Mobilní ochrana před hrozbami**	Řešení CylancePROTECT® MOBILE detekuje pokročilé škodlivé hrozby na úrovni zařízení a aplikací. Využívá pokročilou ochranu před hrozbami, založenou na umělé inteligenci. Účinně tak zabraňuje škodlivým kybernetickým útokům napříč mobilními zařízeními.
 **Behaviorální analýza uživatelů a subjektů**	Řešení CylancePERSONA vytváří důvěru na základě biometrických údajů, sledování používání aplikací a analýzy vzorců volání procesů a aktivity na síti. Využívá adaptivní systém hodnocení rizik a dynamické uplatňování pravidel napříč mobilními zařízeními pro neustálé ověřování.

Ochrana koncových bodů

Řešení CylancePROTECT se zaměřuje na prevenci a automaticky brání spuštění malwaru na koncových bodech v organizaci. Účinně chrání před různými typy hrozeb, včetně polymorfního ransomwaru, útoků zero-day a dalšího malwaru. Zahrnuje ochranná opatření, která zabraňují útokům založeným na skriptech, útokům bez souborů i útokům, které využívají paměť a externí zařízení.

To vše provádí CylancePROTECT automaticky, bez zásahu uživatele nebo správce, nutnosti připojení ke cloudu a použití podpisů, heuristiky nebo sandboxů.

SCHOPNOSTI

Ovládání spuštění malwaru

- Základní technologie ochrany, která využívá umělou inteligenci a strojové učení k detekci a prevenci malwaru
- Poskytuje ochranu pro operační systémy Microsoft® Windows®, macOS® a Linux®

Vynucování zásad použití zařízení

- Kontrola používání velkokapacitních paměťových zařízení USB
- Prevence úniku dat prostřednictvím vyměnitelných médií

Kontrola aplikací

- Uzamčení zařízení na funkce s pevně danými omezeními změn
- Prevence instalace nových aplikací

Ochrana paměti

- Proaktivní identifikace a zastavení útoků využívajících paměť zařízení
- Možnost podrobného nastavení výjimek a vylepšeného hlášení problémů a jejich řešení

Kontrola skriptů

- Blokování spouštění neoprávněných skriptů
- Lepší kontrola pro administrátora s možností detailního nastavení povolených a bezpečných položek
- Kontrola umožňující zablokování skriptu, jako je například PowerShell, pokud nejsou spouštěny v konkrétní aplikaci.

Detekce a reakce na koncových bodech

CylanceOPTICS® představuje EDR řešení, které rozšiřuje ochranu před hrozbami poskytované řešením CylancePROTECT, díky využívání umělé inteligence k prevenci bezpečnostních incidentů.

CylanceOPTICS nabízí skutečnou prevenci incidentů pomocí AI, analýzy příčin, inteligentního vyhledávání hrozeb a automatické detekce, reakce a nápravy.

Na rozdíl od jiných produktů EDR nevyžaduje CylanceOPTICS významné investice do firemní infrastruktury. K provozu není třeba nepřetržité streamování dat do cloudového prostředí pro ukládání a analýzu, ani technických znalostí. Architektura a funkce prevence incidentů s využitím skutečné umělé inteligence jsou navrženy tak, aby běžely přímo na koncovém bodě.

Tato jednoduchá architektura umožňuje organizacím osvojit si funkce EDR za přijatelnou cenu s intuitivním uživatelským rozraním, automatizovanou reakcí a nápravou.

SCHOPNOSTI

Distribuované vyhledávání a sběr

Unikátní přístup ke sběru dat optimalizuje proces jejich získávání, vyhledávání a analýzy.

Konzistentní přehled napříč platformami

Přehled o situaci v celém firemním prostředí s použitím jediného řešení, díky podpoře koncových bodů se systémy Microsoft Windows, macOS a Linux.

Analýza příčin

Webová analýza příčin útoků blokovaných řešením CylancePROTECT a dalších důležitých artefaktů identifikovaných na koncových bodech na vyžádání.

Vyhledávání hrozeb v rámci celého podniku

Okamžitá kontrola dat na koncových bodech pro odhalení skrytých potenciálních hrozeb.

Rychlá reakce na incidenty

Rychlé provádění kroků v reakci na incidenty, získávání podezřelých souborů a jejich umístění do karantény a izolace napadených koncových bodů od sítě.

Dynamická detekce hrozeb

Automatizované odhalování potenciálních hrozeb v reálném čase pomocí vlastních i předpřipravených pravidel detekce.

S využitím cloudu, avšak nezávisle na cloudu

Poskytování lokální inteligence v každém koncovém bodě bez nutnosti připojení do cloudu nebo lidského zásahu.

Vzdálená reakce

Poskytnutí rozhraní pro intuitivní a interaktivní spouštění skriptů a tradičních nebo nativních příkazů na systémech pro rychlé třídění a zobrazení výsledků téměř v reálném čase.

Automatizovaná reakce

Automatická náprava škodlivých událostí napříč celou infrastrukturou.

Přizpůsobená reakce

Přizpůsobení akcí automatizované reakce na základě sady pravidel s eliminací prodlev.

Ochrana mobilních zařízení před hrozbami

CylancePROTECT MOBILE je řešení určené k ochraně mobilních zařízení (MTD), které rozšiřuje základní úroveň zabezpečení poskytovanou řešením BlackBerry® UEM. Toto řešení předchází škodlivým hrozbám, dokáže je detekovat a řešit přímo na úrovni zařízení a aplikací. Kombinuje funkce správy mobilních koncových bodů řešení BlackBerry UEM s pokročilou ochranou před hrozbami, které využívají umělou inteligenci.

Díky řešení CylancePROTECT MOBILE jsou mobilní zařízení schopná udržet si náskok před škodlivými kybernetickými útoky v prostředí postaveném na Zero Trust principu.

SCHOPNOSTI

Detekce neoficiálně nainstalovaných aplikací v iOS®

Okamžitá detekce a skenování aplikací nainstalovaných z neoficiálních zdrojů.

Skenování malwaru v systému Android™

Obchod s aplikacemi BlackBerry UEM provádí skenování malwaru v systému Android a v souborech APK

Všechny aplikace v obchodě, včetně přizpůsobených aplikací partnerů a zákazníků, jsou skenovány a chráněny před malwarem.

Detekce phishingu a škodlivých URL adres

Umělá inteligence řešení CylancePROTECT se neustále učí rozpoznávat malware nebo škodlivé URL adresy, které mohou obsahovat prvky phishingu.

Offline ochrana pro systémy Android a iOS

Kontrola integrity aplikací iOS pro aplikace BlackBerry® Dynamics™ SDK:

Řešení CylancePROTECT zajišťuje integritu aplikací založených na platformě BlackBerry Dynamics SDK a zaručuje, že se do zařízení nainstalují pouze bezpečné aplikace. Zároveň zabraňuje v neoprávněné manipulaci s aplikacemi společnosti BlackBerry®.

Integrované vykazování na kontrolním panelu

Monitorování a upozorňování koncových uživatelů prostřednictvím panelu BlackBerry UEM a oznámení analytikům umožňuje rychlou reagovat na škodlivý software a hackerské události v reálném čase.

Ochrana mobilních zařízení před hrozbami

Řešení CylancePERSONA nabízí nepřetržité ověřování pomocí strojového učení a prediktivní umělé inteligence, která se dynamicky přizpůsobuje zásadám zabezpečení v závislosti na aktuální poloze uživatele, zařízení a dalších faktorech.

Díky adaptivnímu hodnocení rizik a dynamickému uplatňování zásad napříč mobilními zařízeními zajišťuje CylancePERSONA neustálé ověřování uživatelů. Tímto způsobem chrání prostředí před lidskými chybami a pokusy o obejití pravidel s neškodnými úmysly.

SCHOPNOSTI

Adaptivní hodnocení rizik

- **Behaviorální poloha:** Analýza frekvence a vzorců uživatelské aktivity na základě anonymizovaných údajů o poloze. To umožňuje určit rizikové skóre v závislosti na aktuální poloze.
- **Důvěryhodnost sítě:** Hodnotí četnost používání sítě a na základě příslušného profilu dynamicky upravuje zabezpečení. Například při připojení k nové veřejné Wi-Fi síti se upraví skóre rizika.
- **Časové a uživatelské anomálie:** Hladká integrace s dalšími poskytovateli a identifikačními systémy. Osvědčená bezpečnostní infrastruktura společnosti BlackBerry umožňuje bezpečné a snadné sdílení všech dat.
- **DNA zařízení a aplikace:** Umožňuje zjistit, zda jsou zařízení a aplikace kompatibilní a aktuální. Řešení CylancePERSONA dokáže upravit zásady zabezpečení na základě profilu DNA zařízení a aplikací.

Dynamické přijímání zásad

- Udělení přístupu
- Přijetí zásady
- Odeslání výzvy k ověření
- Vydání výstrahy a provedení nápravy

Průběžné ověřování

- Využívá pasivní biometrické údaje a další vzory založené na chování uživatele, aby neustále a nenápadně ověřoval identitu uživatele.
- V případě zaznamenání anomálního chování automaticky blokuje přístup k aplikacím.
- Zvyšuje úroveň zabezpečení a zároveň zlepšuje uživatelský zážitek, přičemž eliminuje statické expirace relací.

BlackBerry. Intelligent Security. Everywhere.

Společnost BlackBerry (NYSE: BB; TSX: BB) poskytuje inteligentní bezpečnostní software a služby pro podniky a vládní organizace na celém světě. Společnost spravuje zabezpečení více než 500 milionů koncových bodů, včetně více než 195 milionů vozidel. Sídlí ve Waterloo ve státě Ontario a využívá umělou inteligenci a strojové učení k poskytování inovativních řešení v oblasti kybernetické bezpečnosti, zabezpečení a ochrany osobních údajů. Je lídrem v oblasti zabezpečení a správy koncových bodů, šifrování a vestavěných systémů. Vize společnosti BlackBerry je jasná – zajistit propojenou budoucnost, které můžete důvěřovat.

BlackBerry. Intelligent Security. Everywhere.

Další informace najdete na stránkách BlackBerry.com a při sledování účtu @BlackBerry.

BB23 | 220622