

# BLACKBERRY POC ALEBO LEPŠIE RAZ SKÚSIŤ, AKO X-KRÁT POČUŤ

Máte svoje zabehnuté bezpečnostné riešenia, ale ako v skutočnosti vyzerá vaše prostredie? Je naozaj bezpečné a pripravené na dennodenný boj s novými hrozbami? Ak áno, koľko úsilia a zdrojov na to míňate? Dá sa niečo vylepšiť alebo potvrdiť spoľahlivosť? Ako znížiť náklady na prostredie a pritom zostať mesiace chránený bez nutnosti pripojenia na internet? Máte rovnakú ochranu aj keď ste offline alebo dlhšie bez aktualizácií?

Vyskúšajte si produkty z portfólia BlackBerry vo svojom prostredí, podľa seba

**CylancePROTECT Desktop** blokuje ransomvér a iný malvér. Windows, macOS a Linux zariadenia využívajúce matematický prístup k identifikácii malvéru. Používa techniky strojového učenia namiesto reaktívnych podpisov, systémov založených na dôvere alebo karantény na poskytovanie detekcie a reakcie koncových bodov, vďaka čomu sú nový ransomvér, malvér, vírusy, roboty a budúce varianty zbytočné. CylancePROTECT Desktop analyzuje potenciálne spúšťanie súborov na ransomvér a iný malvér v OS a pamäťových vrstvách, aby zabránil doručovaniu a spúšťaniu škodlivých dát.

**CylanceOPTICS** monitoruje váš Windows, macOS a Linux zariadenia a dá vám vedieť, kedy môže byť vaša organizácia napadnutá. CylanceOPTICS zhromažďuje informácie zo zariadení a agreguje ich pomocou cloudových služieb na sledovanie, upozorňovanie a reagovanie na škodlivé udalosti hneď, ako k nim dôjde. CylanceOPTICS dokáže zastaviť útoky pred ich vykonaním a automatizovať vyšetrovanie a reakciu na útoky.

**CylancePROTECT Mobile** poskytuje mobilnú obranu proti hrozbám pre iOS, Android a ChromeOS zariadenia. Okrem identifikácie škodlivého softvéru CylancePROTECT Mobile tiež detekuje aplikácie, ktoré sú načítané bokom, škodlivé adresy URL v textových správach a ďalšie bezpečnostné riziká a odporúča konkrétne akcie na odstránenie hrozby.

**CylanceGATEWAY** poskytuje vašim používateľom prístup k sieti Zero Trust Network Access (ZTNA) iOS, Android, Windows, a macOS zariadenia na zabezpečenie prístupu používateľov k rozšírenému perimetru siete a jej ochranu pred hrozbami. CylanceGATEWAY chráni zariadenia tým, že vám umožňuje blokovat' pripojenia k internetovým cieľom, ku ktorým nechcete aby zariadenia pristupovali aj keď zariadenie nie je pripojené k vašej sieti. CylanceGATEWAY chráni vašu súkromnú sieť a cloudové služby tým, že umožňuje prístup iba oprávneným používateľom.

**CylanceAVERT (DLP)** identifikuje a kategorizuje citlivé údaje na Windows zariadení v prostredí vašej organizácie, aby ste vytvorili inventár citlivých súborov a upozornili špecifikovaných používateľov, keď sú citlivé údaje zapojené do exfiltrácie. CylanceAVERT dokáže skenovať súbory, ktoré sú skopírované na zariadenie USB, odovzdané do umiestnenia prehliadača alebo na sieťovú jednotku, alebo v obsahu tela alebo v prílohách e-mailových správ a odporučiť nápravu.

Mnohé riešenia sú postavené na pokojné časy a nie na krízové časy. Fungujú v systémoch, ktoré sú moderné, výkonné, nové a vždy pripojené na internet. Zabezpečte si ochranu bez kompromisov pre všetky aj staršie systémy BlackBerry POC alebo lepšie raz skúsiť, ako x-krát počuť.

## POC v skratke

### Čo potrebujem na POC?

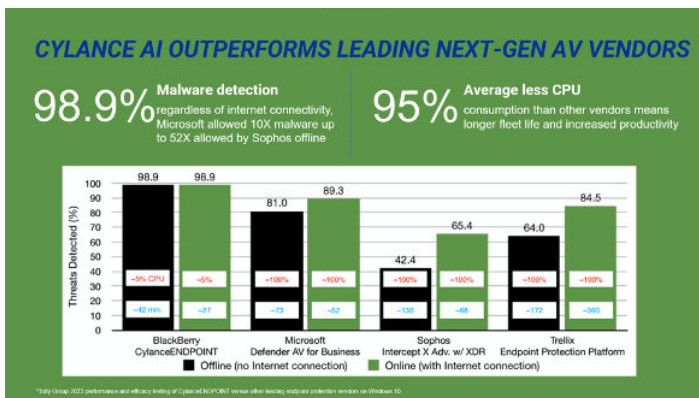
- Poslať email na [blackberry@sectec.sk](mailto:blackberry@sectec.sk) a uviesť
  - emailovú adresu na ktorú bude vytvorený prístup
  - produkty o ktoré sa zaujímate
  - preferované dátumy na online workshop

### Kol'ko stojí POC?

Licencie na POC ako aj workshopy sú **bezplatné**.  
**Tak na čo čakať?**

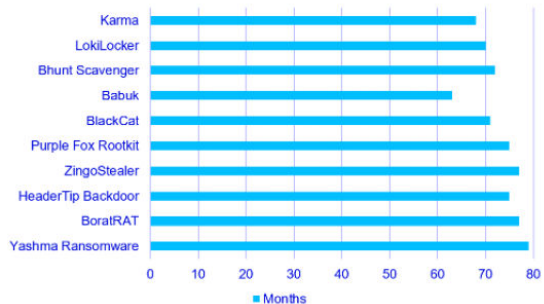
## Ako prebieha POC?

Po odoslaní emailu obratom vytvoríme pre vás POC tenanta s plnou funkcionalitou. Počas workshopu vám predstavíme daný produkt, architektúru, základné nastavenia a integrácie, licencovanie a samozrejme vaše konkrétne nasadenie. Workshop trvá medzi 2-4 hodinami v závislosti od produktu. POC môžete spravidla využívať 2 mesiace. Po skončení POC je možné priradiť licencie a bez nutnosti meniť zabehnutý POC pokračovať v užívaní.



## SELF-DEFENDING AI

CONSISTENTLY STOP ATTACKS EARLIER WITH LESS DAMAGE



## Cylance Endpoint Security architecture

