BlackBerry Unified Endpoint Security (UES)

Запобігання загрозам, їх визначення та реагування на них за допомогою єдиної платформи

BlackBerry Cyber Solutions (UES)

CylancePROTECT (EPP)

Забезпечує автоматичний захист від шкідливого програмного забезпечення, керування програмами та скриптами, захист пам'яті та контроль пристроїв, що під'єднуються до кінцевої точки.

CylanceOPTICS (EDR)

Розширює можливості запобігання загрозам, які забезпечує CylancePROTECT. Компонент EDR функціонує завдяки використанню ML для визначення та автоматичної реакції на інциденти.

CylanceGATEWAY (ZTNA)

CylanceGATEWAY забезпечує керований штучним інтелектом доступ до мережі з нульовою довірою (ZTNA) для захисту приватних програм, розміщених локально або у хмарі.

CylancePROTECT Mobile (MTD)

Рішення для захисту мобільних кінцевих точок на основі штучного інтелекту, яке зупиняє шкідливі програми, не вимагаючи втручання людини, хмарних підключень, сигнатур, евристиків або пісочниць.

CylanceINTELLIGENCE

Запобігайте складним загрозам, відстежуйте їх та реагуйте на них за допомогою контекстної та дієвої служби розвідки кіберзагроз (CTI) від BlackBerry.

BlackBerry пропонує уніфікований захист кінцевих точок в єдиній консолі з розширеним інтелектом аналізу аномалій, машинним навчанням та автоматизацією.

Актуальність запобігання загрозам

Рівень блокування загроз та аномалій на кінцевих точках не змінюється зі зміною середовища: головний офіс, віддалені співробітники, ізольовані департаменти, серверне чи виробниче обладнання.

Швидкість управління та рольова модель

BlackBerry UES пропонує контроль усіх пристроїв, розслідування інцидентів та моніторинг аномалій з єдиної консолі адміністратора*, дотримуючись принципу зручного функціонального інтерфейсу та рольової моделі адміністрування

Безперебійність бізнес-процесів

Архітектура агента не дозволяє рішенню навантажувати кінцеву точку та дестабілізувати звичний робочий день співробітника

*Cloud, Hybrid або On-Prem

Основні можливості

Широке розгортання

Агент системи (CylancePROTECT) доступний для встановлення на такі ОС: Windows desktop/server, linux, macOS, iOS, Android

Захист на рівні ядра агента

Немає залежності від наявності інтенет-з'єднання, регулярних оновлень та підзавантаження сигнатур

Оновлення алгоритму

Модернізація алгоритму відбувається приблизно раз на 12 місяців інженерами BlackBerry, що забезпечує 24/7/365 актуальність технології та роботу в ізольованому середовищі або на ізольованих пристроях

Розслідування та реакція на інциденти ІБ

Рішення може бути укомплектоване Endpoint Detection and Response (EDR)-компонентом (CylanceOPTICS) для надання повної видимості в контексті активності файлів та процесів на кінцевій точці

Альтернатива небезпечному VPN на основі технології Zero Trust

Рішення може бути укомплектоване ZTNA-компонентом (CylanceGATEWAY) для запобігання несанкціонованого доступу до бізнес-мереж компанії. Cylance AI запам'ятовує поведінку конкретної людини в системі і автоматично зупиняє відомі загрози або загрози нульового дня від зламу мереж, пристроїв або ідетичностей користувачів.

blackberry.bakotech.com

blackberry@bakotech.com