

BlackBerry Unified Endpoint Security (UES)

Предотвращение угроз, их определение и реагирование на них с помощью единой платформы

BlackBerry Cyber Solutions (UES)



CylancePROTECT (EPP)

Обеспечивает автоматическую защиту от вредоносного программного обеспечения, управление приложениями и скриптами, защиту памяти и контроль устройств, подключаемых к конечной точке.



CylanceOPTICS (EDR)

Расширяет возможности предотвращения угроз, которые обеспечивает CylancePROTECT. Компонент EDR работает благодаря использованию ML для определения и автоматической реакции на инциденты.



CylanceGATEWAY (ZTNA)

CylanceGATEWAY обеспечивает управляемый искусственным интеллектом доступ к сети с нулевым доверием (ZTNA) для защиты частных программ, размещенных локально или в облаке.



CylancePROTECT Mobile (MTD)

Решение для защиты мобильных конечных точек на основе искусственного интеллекта, которое останавливает вредоносные программы, не требуя вмешательства человека, облачных подключений, сигнатур, эвристик или песочниц.



CylanceINTELLIGENCE

Предотвращайте сложные угрозы, отслеживайте их и реагируйте на них с помощью контекстной и эффективной службы разведки киберугроз (CTI) от BlackBerry.

BlackBerry предлагает унифицированную защиту конечных точек в единой консоли с расширенным интеллектом анализа аномалий, машинным обучением и автоматизацией.



Актуальность предотвращения угроз

Уровень блокировки угроз и аномалий на конечных точках не меняется с изменением среды: главный офис, удаленные сотрудники, изолированные департаменты, серверное или производственное оборудование.



Скорость управления и ролевая модель

BlackBerry UES предлагает контроль всех устройств, расследование инцидентов и мониторинг аномалий с единой консоли администратора*, придерживаясь принципа удобного функционального интерфейса и ролевой модели администрирования.



Бесперебойность бизнес-процессов

Архитектура агента не позволяет решению нагружать конечную точку и дестабилизировать обычный рабочий день сотрудника.

*Cloud, Hybrid або On-Prem

Основные возможности

■ Широкое развертывание

Агент системы (CylancePROTECT) доступен для установки на такие ОС: Windows desktop/server, linux, macOS, iOS, Android

■ Защита на уровне ядра агента

Нет зависимости от наличия интернет-соединения, регулярных обновлений и загрузки сигнатур

■ Обновление алгоритма

Модернизация алгоритма проводится примерно раз в 12 месяцев инженерами BlackBerry, обеспечивая 24/7/365 актуальность технологии и работу в изолированной среде или на изолированных устройствах

■ Расследование инцидентов ИБ и реакция на них

Решение может быть укомплектовано Endpoint Detection and Response (EDR)-компонентом (CylanceOPTICS) для предоставления полной видимости в контексте активности файлов и процессов на конечной точке

■ Альтернатива небезопасному VPN на основе технологии Zero Trust

Решение может быть укомплектовано ZTNA-компонентом (CylanceGATEWAY) для предотвращения несанкционированного доступа к бизнес-сети компании. Cylance AI запоминает поведение конкретного человека в системе и автоматически останавливает известные угрозы или угрозы нулевого дня, препятствуя взлому сетей, устройств или идентичностей пользователей.