BlackBerry Unified Endpoint Security (UES)

Prevent, identify, and respond to threats with a single platform

BlackBerry Cyber Solutions (UES)

CylancePROTECT (EPP)

Provides automatic malware protection, application and script management, memory protection, and control of devices connected to the endpoint.

CylanceOPTICS (EDR)

Expands the threat prevention capabilities provided by CylancePROTECT. The EDR component functions due to ML using to identify and automatically respond to incidents.

CylanceGATEWAY (ZTNA)

CylanceGATEWAY Provides AI-driven Zero Trust Network Access (ZTNA) to protect private programs hosted on-premises or in the cloud.

CylancePROTECT Mobile (MTD)

An AI-powered mobile endpoint protection solution that stops malware without requiring human intervention, cloud connections, signatures, heuristics or sandboxes.

CylanceINTELLIGENCE

Prevent, track, and respond to advanced threats with BlackBerry's contextual, actionable Cyber Threat Intelligence (CTI) service.

BlackBerry offers unified endpoint protection in a single console with advanced anomaly analytics intelligence, machine learning and automation.

Relevance of Threat Prevention

The level of blocking of threats and anomalies at endpoints does not change as the environment changes: head office, remote workers, isolated departments, server or production equipment.

Control Speed and Role Model

BlackBerry UES offers all-device control, incident investigation, and anomaly monitoring from a single admin console*, with a seamless user experience and role-based administration model.

Continuity of Business Processes

The agent architecture prevents the solution from burdening the endpoint and disrupting the employee's normal workday.

*Cloud, Hybrid a6o On-Prem

Key Features

Wide Deployment

System agent (CylancePROTECT) is available for installation on the following operating systems: Windows desktop/server, linux, macOS, iOS, Android

Agent Kernel-Level Security

There is no dependence on the availability of an Internet connection, regular updates and signatures loading

Algorithm Update

Algorithm upgrades are carried out approximately every 12 months by BlackBerry engineers, ensuring 24/7/365 technology up-to-date and working in an isolated environment or on isolated devices

Investigation of Information Security Incidents and Response to Them

The solution can be equipped with an Endpoint Detection and Response (EDR) component (CylanceOPTICS) to provide complete visibility into the context of file and process activity on the endpoint

Alternative to an Insecure VPN Based on Zero Trust Technology

The solution can be equipped with a ZTNA component (CylanceGATEWAY) to prevent unauthorized access to the company's business network. Cylance AI learns the behavior of a specific person on the system and automatically stops known threats or zero-day threats, preventing networks, devices or user identities from being compromised

blackberry.bakotech.com

blackberry@bakotech.com