BlackBerry® | Cybersecurity

CylancePROTECT

Future-Proof Endpoint Security

DATA SHEET

For years, endpoint security products' primary threat protection was based on signatures, created after patient zeros were impacted and the damage already done. Assuming all attacks had been seen before, using signatures made sense. Today, malware mutates daily, even hourly, making signature-based prevention tools obsolete, and creating the need for a stronger prevention-based approach to endpoint security.

BlackBerry has redefined what an endpoint protection solution can and should do for organizations by utilizing an automated, prevention-first approach. It is an accurate, efficient, and effective solution for preventing advanced persistent threats and malware from executing on an organization's endpoints. CylancePROTECT® prevents breaches and provides additional security controls to safeguard against script-based, fileless, memory, and external device-based attacks. CylancePROTECT does this without user or admin intervention, a cloud connection, signatures, heuristics, or sandboxes.

Capabilities

Device Usage Policy Enforcement

- Control use of USB mass storage devices
- Prevent data theft via removable media

Role-Based Access Controls (RBAC)

- Minimize risk with more granular role management with custom RBAC
- Improve restrictions to network access based on the roles of individual users
- Limit employee access rights to only the information they need to do their jobs
- Benefit from no impact on existing users

Application Control

- Lock down fixed-function devices
- Prevent bad binaries or modification of a binary
- Lock down specified systems and restrict any changes

CylancePROTECT FOR DESKTOP

The algorithmic model utilized within CylancePROTECT means there are no signatures, patching, system scans, or slow endpoints due to the security solution running on them. Customers who have made the switch from reactive legacy, signature-based antivirus products have seen up to a 99% ROI, a 97% reduction in the re-imaging of machines, extended hardware and battery performance, and a 90% reduction in staff hours required to manage the solution.[1]

The CylancePROTECT architecture consists of a lightweight single agent that is managed via the BlackBerry® SaaS-based cloud console. The cloud console easily integrates with existing software management systems and security tools. Hybrid and on-premises management options are available for air-gapped environments. The endpoint agent will detect and prevent malware on the host, independent of a cloud connection and without the need for continuous updates. CylancePROTECT is capable of detecting and quarantining malware in open, isolated, and virtual networks. The BlackBerry machine-learning-based approach stops the execution of harmful code regardless of having prior knowledge or employing an unknown obfuscation technique. No other anti-malware product compares to the accuracy, ease of management, and effectiveness of CylancePROTECT.

The CylancePROTECT architecture consists of a lightweight single agent that is managed via the BlackBerry SaaS-based cloud console.

Capabilities

Memory Protection

- Proactively identify and stop malicious use of memory
- Prevent memory-only attacks such as privilege escalation
- Benefit from granular exclusions and enhanced troubleshooting and reporting

Script Control

- Stop unauthorized scripts from running
- Benefit from granular whitelisting and safelist capabilities
- Support MacOS®, Microsoft®, and Linux®
- Prevent execution of PowerShell one-liners

IOS® Sideloaded Application Detection

- Sideload applications are immediately scanned and detected

CylancePROTECT FEATURES

True Zero-Day Prevention

Resilient AI model prevents zero-day payloads from executing.

Device Usage Policy Enforcement

Controls which devices can be used in the environment, eliminating external devices as a possible attack vector.

AI-Driven Malware Prevention

Field-proven AI inspects any application attempting to execute on an endpoint before it executes.

Memory Exploitation Detection and Prevention

Proactively identifies malicious use of memory (fileless attacks) with immediate automated prevention responses.

Script Management

Maintains full control of when and where scripts are run in the environment.

Application Control for Fixed-Function Devices

Ensures fixed-function devices are in a pristine state continuously, eliminating the drift that occurs with unmanaged devices.

Capabilities

- Android™ Malware Scanning

UEM App Store Android and APK Malware Scanning

- Scans all applications in the BlackBerry® UEM app store, including customer and custom partner applications, protecting against malware

Phishing and Malicious URL Detection

- Leverages AI to automatically detect and stop malicious URLs, including those with embedded phishing elements

Secure Application Creation

- Enables partners and companies to build custom, secure applications for enterprise-accessible devices

IOS® App Integrity Checking for BlackBerry Dynamics SDK Apps

- Assures integrity of applications built on the BlackBerry® Dynamics™ SDK platform
- Allows only secure apps to be loaded onto devices and prevents any tampering of BlackBerry applications

CylancePROTECT MOBILE

Now more than ever, organizations are using mobile devices to compete in an agile, evolving market and keep their employees connected. For the first time, more than half of all devices connected to the Internet are mobile[2]. At the same time, mobile malware is more prevalent than ever, with attacks rising 50% in the last year alone[3]. While the focus of enterprise security solutions has historically been on desktop devices, more businesses are discovering the growing threat of malware phishing attacks aimed at mobile devices, especially within applications.

The damage from these attacks can be significant, with personally identifiable information (PII) and other critical data being leaked at higher rates than ever before.

This is leading more organizations to adopt deep packet inspection (DPI) and other capabilities to protect against malicious attacks.

It is no surprise, therefore, that the mobile threat defense (MTD) market is growing rapidly. MTD offers an extra layer of security by preventing, detecting, remediating, and improving overall security hygiene for all different levels within an organization's mobile fleet and applications.

The BlackBerry MTD solution, CylancePROTECT® MOBILE, augments the security baseline provided by BlackBerry UEM by addressing advanced malicious threats on mobile devices. CylancePROTECT MOBILE monitors attacks at the device and application levels and goes beyond the security of basic application containers.

- At the device level, CylancePROTECT MOBILE devices identifies security vulnerabilities and potential malicious activities by monitoring OS updates, system parameters, device configurations, and system libraries.
- At the application level, CylancePROTECT MOBILE devices uses application sandboxing and code analysis, as well as app-security testing, to identify malware and grayware.

In addition, CylancePROTECT MOBILE devices identifies any malware that might come in through sideloaded applications, unique signature-based malware, or simulations, adding an extra layer of security to the BlackBerry Dynamics SDK platform. This allows partners and companies to build customized, secure applications that can be loaded onto enterprise-accessible devices.

COMMON CylancePROTECT USE CASES

CylancePROTECT provides full-spectrum threat prevention that stops endpoint breaches by solving the following use cases:

- Identify and block malicious executables without the need for constant updates or a cloud connection
- Identify security vulnerabilities and potential malicious activities by monitoring OS updates, system parameters, device configurations, and system libraries
- Control where, how, and who can execute scripts
- Manage USB device usage and prevent unauthorized devices from being used
- Stop fileless malware attacks
- Lock down fixed-function devices such as kiosks, POS terminals, etc.
- Prevent zero-day and ransomware attacks
- Stop memory-based attacks and exploitations
- Use application sandboxing and code analysis as well as app-security testing to identify malware and grayware
- Identify any malware that might come in through sideloaded applications, unique signature-based malware, or simulations
- Protection for endpoints when users are online or offline

LEARN MORE

CylancePROTECT is just one of a wide range of world-class security solutions that BlackBerry offers. Learn more about our full selection of security suites that can provide your organization with intelligent security, everywhere.

Discover our:

BlackBerry Spark® Suite

BlackBerry Spark®
Unified Endpoint Security Suite

BlackBerry Spark®
Unified Endpoint Management Suite

[1] https://www.cylance.com/en-us/company/about-us/our-customers/2019-forrester-tei-report.html#form-anchor

[2] https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

[3] https://research.checkpoint.com/cyber-attack-trends-2019-mid-year-report/

Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 195M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

*For more information, visit **BlackBerry.com** and follow **@BlackBerry**.*