



 **BlackBerry** | Cybersecurity

BLACKBERRY CYBER SUITE

Bridging the Gap Between Zero Trust and Zero Touch

SOLUTION BRIEF

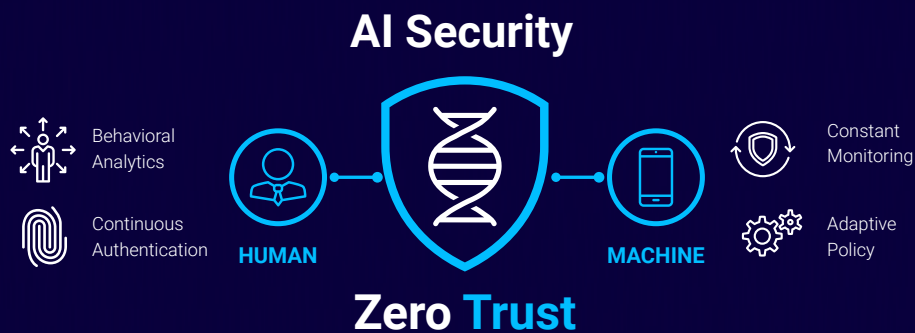


The challenge of securing and protecting data and endpoints is not a new requirement, but today it is more important than ever. With a rapidly expanding attack surface created by the proliferation of new types of endpoints ranging from mobile to the Internet of things (IoT) coupled with a wave of remote global workers, you've got a perfect storm. The concept and implementation of a Zero Trust framework has never been more important as securing and protecting endpoints and data goes hand in hand with Zero Trust.

Zero Trust was created to address de-perimeterization, or the erosion of the corporate network perimeter. With the consumerization of technology and the rise of cloud-based apps, CISOs had to change their approach to assume that no traffic within an organization's network was any more trustworthy than traffic coming in from the outside. Zero Trust is all about establishing trust and limiting access. It is about ensuring you have a trusted user on a trusted device while limiting access to the data and apps needed for that person to do their job. Balancing the requirements

of Zero Trust and worker productivity was hard enough before March 2020 when organizations moved their global workforce to a work-from-home model overnight. In turn, it has prioritized Zero Trust and business continuity to the top of the list of challenges that must be solved.

The components of BlackBerry Cyber Suite work in concert as a foundation for a Zero Trust enterprise security architecture.







HOW BLACKBERRY ADDRESSES THESE ISSUES:

The BlackBerry® Cyber Suite is a purposefully designed set of security controls offering a Zero Trust framework that is a minimally invasive (Zero Touch) user experience. The BlackBerry Cyber Suite is an integrated set of state-of-the-art security controls and processes that provide a foundation for a Zero Trust security architecture with security controls that span from traditional endpoints to mobile to IoT devices.

The components of BlackBerry Cyber Suite work in concert as a foundation for a Zero Trust enterprise security architecture. Advanced Zero Trust practitioners across all segments have found that adopting this architecture has resulted in several benefits, including:

- Improved security posture with enhanced visibility and greater control, providing superior risk mitigation
- Securing and managing all attack surfaces from laptops and servers to mobile to IoT devices
- Save time and money with a unified platform that is easy to deploy and easy to manage
- BlackBerry Cyber Suite results in accelerated speed and agility for the security team while providing better visibility across a diverse IT infrastructure

BLACKBERRY CYBER SUITE

COMPONENT	DESCRIPTION
 <p>Endpoint Protection</p>	Leveraging artificial intelligence (AI) and machine learning capabilities, CylancePROTECT® provides automated malware prevention, application and script control, memory protection, and device policy enforcement. It predicts and prevents cyberattacks with unparalleled effectiveness, ease of use, and minimal system impact.
 <p>Endpoint Detection and Response</p>	CylanceOPTICS® extends the threat prevention delivered by CylancePROTECT by using artificial intelligence to prevent security incidents. It provides true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities.
 <p>Mobile Threat Defense</p>	CylancePROTECT® MOBILE detects advanced malicious threats at the device and application levels. It leverages advanced AI-driven threat protection to stop malicious cyberattacks across mobile devices.
 <p>User & Entity Behavior Analytics</p>	CylancePERSONA™ creates trust based on biometrics, app usage, and network and process invocation patterns. It uses adaptive risk scoring and dynamic policy adaption across mobile devices to provide continuous authentication.



Endpoint Protection

CylancePROTECT uses an automated, prevention-first approach to stop malware from executing on an organization's endpoints. It prevents breaches including polymorphic ransomware, zero-day attacks, and other malware including the safeguards to prevent script-based, file-less, memory, and external device-based attacks. CylancePROTECT does this without user or admin intervention, a cloud connection, signatures, heuristics, or sandboxes.

CAPABILITIES

Malware Execution Controls

- The core protection technology that leverages artificial intelligence and machine learning to detect and prevent malware
- Protect Microsoft® Windows®, macOS®, and Linux® environments

Device Usage Policy Enforcement

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

Application Control

- Lock down fixed-function devices and restrict changes
- Prevent the addition of new applications

Memory Protection

- Proactively identify and stop memory-based attacks
- Allow for granular exclusions and enhanced troubleshooting and reporting

Script Control

- Stop unauthorized scripts from running
- Greater admin control with granular whitelisting and safelist capabilities
- Includes parenting controls that allow you to block a script like PowerShell unless it is run in a specific application.



Endpoint Detection and Response

CylanceOPTICS is an EDR solution that extends the threat prevention delivered by CylancePROTECT by using artificial intelligence to prevent security incidents. CylanceOPTICS provides true AI incident prevention, root cause analysis, smart threat hunting, and automated detection, response, and remediation capabilities. Unlike other EDR products, CylanceOPTICS requires no significant investment in on-premises infrastructure. It does not require streaming data continuously to a cloud environment for storage and analysis nor technical expertise to operate. CylanceOPTICS and its true AI incident prevention capabilities are designed to run on the endpoint. This lightweight architecture means organizations can adopt EDR capabilities affordably with a simple user interface and automated response and remediation.

CAPABILITIES

Distributed Search and Collection

Our unique approach to data collection optimizes data gathering, search, and analysis.

Consistent Cross-Platform Visibility

With support for Microsoft Windows, macOS, and Linux endpoints, organizations can maintain situational awareness across their entire environment with one solution.

Root Cause Analysis

Web-based, on-demand, root cause analysis of attacks blocked by CylancePROTECT as well as other interesting artifacts identified on endpoints.

Enterprise-Wide Threat Hunting

Search endpoint data instantly for potential threats hiding on endpoints.

Fast Incident Response

Quickly execute incident response actions, quarantining, acquiring suspicious files, and/or isolating compromised endpoints from the network.

Dynamic Threat Detection

Automate potential threat discovery, in real time, using custom and curated detection rules.

Cloud enabled but not cloud dependent

Provide local intelligence on each endpoint so you are not reliant on connectivity or human intervention.

Remote Response

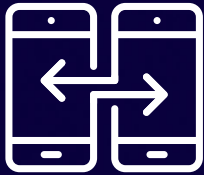
Provide an interface to intuitively and interactively execute scripts and run traditional or native commands on systems to quickly triage and see the results of those commands in near-real-time.

Automated Response

Automate remediation of malicious events across your infrastructure

Custom Response

Customize automated response actions associated with rule sets to eliminate dwell time.



Mobile Threat Defense

CylancePROTECT MOBILE is a mobile threat defense (MTD) solution that augments the security baseline provided by BlackBerry® UEM. It prevents, detects, and remediates malicious threats at the device and application levels. It combines the mobile endpoint management capabilities of BlackBerry UEM with advanced AI-driven threat protection. CylancePROTECT MOBILE allows mobile devices to stay in front of malicious cyberattacks in a Zero Trust environment.

CAPABILITIES

iOS® Sideloaded Application Detection

Sideloaded applications are immediately detected and scanned.

Android™ Malware Scanning

BlackBerry UEM App Store with Android and APK Malware Scanning

All applications in the BlackBerry UEM app store, including custom partner and customer applications, are scanned and protected against malware.

Phishing and Malicious URL Detection

CylancePROTECT's AI constantly works to understand what malware or malicious URLs look like and which might have embedded phishing elements.

Offline Protection for Android and iOS

iOS App Integrity Checking for

BlackBerry® Dynamics™ SDK Apps:

CylancePROTECT assures integrity of applications built on the BlackBerry Dynamics SDK platform, ensuring only secure apps are brought onto devices. It also prevents any tampering of BlackBerry® applications.

Integrated Dashboard Reporting

End-user monitoring and alerting through the BlackBerry UEM dashboard and notifications allows analysts to quickly remediate malware and hacking events in real time.



Mobile Threat Defense

CylancePERSONA provides continuous authentication with machine learning and predictive AI to dynamically adapt a security policy based on user location, device, and other factors. CylancePERSONA also uses adaptive risk scoring and dynamic policy adaption across mobile devices to provide continuous authentication for users. By improving the user verification experience, CylancePERSONA protects the environment against human mistakes and well-intentioned workarounds.

CAPABILITIES

Adaptive Risk Scoring

- Behavioral Location: Looks at the frequency and patterns of users, based on predictive analysis of anonymized location data to determine a location-based risk score.
- Network Trust: Determines the frequency of network use and adjusts security dynamically based on that profile. For example, accessing a public Wi-Fi for the first time would adjust the risk score accordingly.
- Time and Usage Anomalies: Integrates seamlessly with other identity providers and systems. The proven BlackBerry security infrastructure enables all data to be securely and easily shared.
- Device and App DNA: The ability to determine whether the device and apps are compliant and up to date. CylancePERSONA can adjust the security policy based on the device and app DNA profile.

Dynamic Policy Adoption

- Grant access
- Adopt a policy
- Issue an authentication challenge
- Alert and remediate

Continuous Authentication

- Leverages passive biometrics and other usage-based patterns to continuously verify user identity in an unobtrusive fashion.
- A malicious user is automatically blocked from accessing apps when they exhibit anomalous behavior.
- Enhances security posture and at the same time, improves end-user experience over having a static timeout.



 **BlackBerry** 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.

BlackBerry. Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow [@BlackBerry](https://twitter.com/BlackBerry).

© 2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, EMBLEM Design and CYLANCE are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. BlackBerry is not responsible for any third-party products or services.

