CYLANCEPROTECT

Mobile Threat Defense Powered by AI and Integrated With BlackBerry UEM

Going Mobile Increases Risk

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.[1] At the same time, mobile malware is more prevalent than ever, with attacks rising 50% in the last year alone.[2] 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 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.

[1] https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet
[2] https://research.checkpoint.com/cyber-attack-trends-2019-mid-year-report/

CylancePROTECT: Continuous Mobile Endpoint Protection

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

Device level. Identifies security vulnerabilities and potential malicious activities by monitoring OS updates, system parameters, device configurations, and system libraries.

Application level. Uses application sandboxing and code analysis, as well as app-security testing, to identify malware and grayware.

In addition, CylancePROTECT 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.

Advanced Threat Protection

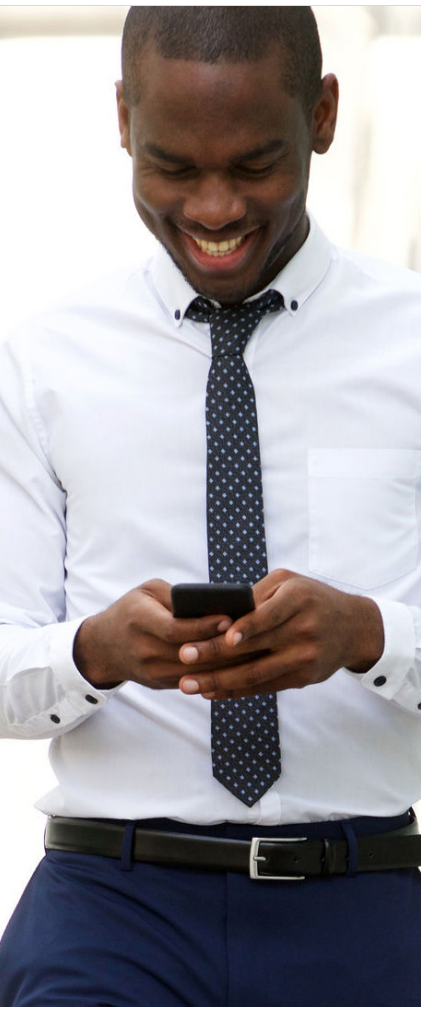
Although there are many mobile threat solutions on the market, CylancePROTECT delivers a uniquely powerful set of features that separates it from the competition.

BlackBerry Cylance AI Advantage

CylancePROTECT leverages AI technology embedded in BlackBerry® Cylance®, known for its advanced machine learning capabilities. BlackBerry Cylance's cybersecurity solution protects against known and unknown malware, fileless attacks, and zero-day payload execution.

Mobile Suite Protection for All Managed and BYO Devices

Since CylancePROTECT is built right into BlackBerry UEM apps, organizations can be assured that their entire mobile fleet is protected without having to rely on employees to maintain third-party apps. By avoiding the need to manually configure VPNs or VDIs, which is typically required by other MTD vendors, organizations can increase productivity and decrease costs.



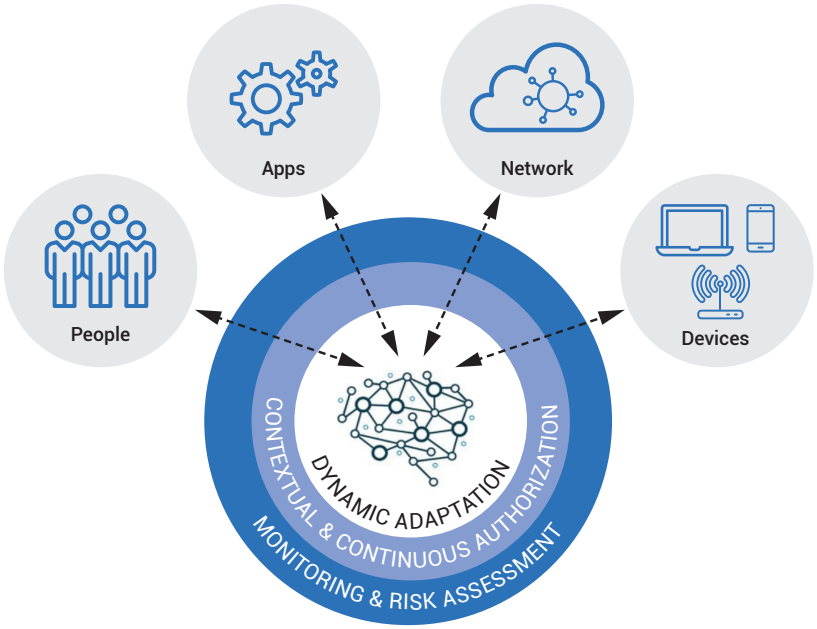
Single Pane of Glass

With CylancePROTECT, there is no separate product or console to set up and configure. It is all tightly integrated into the BlackBerry UEM server and applications, so security and management functionality are available in a single, convenient location.

Zero Trust to Zero Touch Architecture

While organizations today require highly secure environments, balancing the need for authentication with usability and productivity can be challenging. However, the typical static policy solutions available offer little toward addressing either issue. CylancePROTECT's AI-driven threat detection is different. It continuously works to protect all endpoints without disrupting end-users, leveraging the best of zero trust and zero touch architectures. Similar to BlackBerry® Intelligent Security, CylancePROTECT adjusts policies and security levels dynamically based on a user's location, behavior, and device, strengthening existing UEM policies.

Phase 1 BlackBerry Zero Trust Architecture



On average, BlackBerry Cylance blocks emerging threats 25 months before they are first detected, and BlackBerry Cylance solutions have been deployed by more than 3,400 organizations securing 14.5 million endpoints.*

Features

- **iOS® sideloaded application detection:** Sideloaded applications are immediately scanned and detected.
- **Android™ malware scanning**
- **UEM app store Android and APK malware scanning:** All applications in BlackBerry's UEM app store (including custom partner and customer applications) are scanned and protected against malware.
- **Phishing and malicious URL detection:** BlackBerry Cylance 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 and preventing any tampering of BlackBerry applications.
- **Integrated dashboard reporting:** End user monitoring and alerting through the BlackBerry UEM dashboard and notifications allows BlackBerry to quickly remediate malware and hacking events in real time.

Learn More

To learn more about CylancePROTECT, please visit www.blackberry.com/mtd.

* Source: BlackBerry Cylance

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.

© 2019 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.