BlackBerry Intelligent Security. Everywhere.

BLACKBERRY PROTECT MOBILE

Prevention-First Mobile Threat Defense Powered by Cylance AI

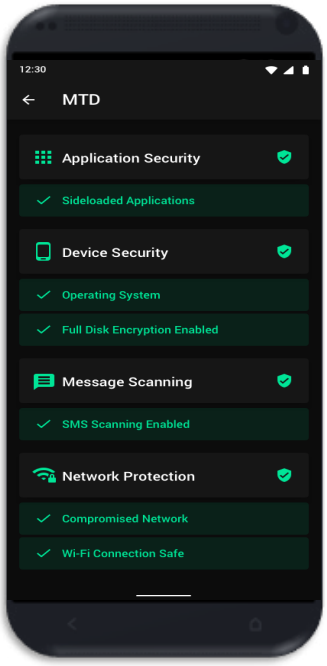
DATA SHEET

For the first time in computing history, more than half of all devices connected to the Internet are mobile.[1] Adversaries have been quick to exploit this expanding attack surface. Attacks on mobile devices spiked by 50% in the past year alone.[2] Organizations have responded by deploying mobile threat defense (MTD) solutions to protect their vulnerable endpoints.

Unfortunately, many legacy approaches to MTD lack the prevention, visualization, and management capabilities needed to efficiently incorporate mobile devices into the overall security architecture. Standalone products, for example, often furnish only a mobile-centric view of threat activity. Admins are tasked with ensuring mobile threat data is properly ingested and combined with telemetry from desktop and server systems. This consumes SecOps resources and may leave significant gaps in the security fabric. Other MTD products target only a subset of mobile attack vectors, e.g., phishing exploits.

In contrast, BlackBerry takes a unified endpoint security (UES) approach to MTD that encompasses every kind of security threat, device type, and ownership model.

" ...mobile malware is more prevalent than ever, with attacks rising 50% in the last year alone."



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

KEY CAPABILITIES

BlackBerry® Protect Mobile extends the Cylance® AI-powered security in BlackBerry® Protect to mobile devices. It's also a core component of the BlackBerry Spark® Zero Trust platform, preventing security incidents while delivering the productivity and user benefits of Zero Touch computing.

BlackBerry Protect Mobile:

- Monitors mobile threats at the device, network, and application layers, preventing malware infections without adding SecOps overhead.
- Identifies security vulnerabilities and potentially malicious activities by monitoring OS updates, system parameters, device configurations, and system libraries at the application level. For example, admins can restrict the use of sideloaded and other unauthorized applications that can leak data or provide adversaries with an entry point to the enterprise network.

PEERLESS PROTECTION FOR MOBILE DEVICES

- Malware detection and prevention powered by seventh-generation Cylance AI technology stops mobile malware, phishing attacks, and zero-day payload execution.
- Sideload detection restricts use of unapproved Android™ and iOS® apps from third-party app stores. Works equally well in both managed and BYO/unmanaged device deployment scenarios.
- URL scanning/anti-smishing controls neutralize social engineering attacks utilizing malicious SMS/MMS messages.
- Advanced detection of privilege escalation, and vulnerable device security configurations.
- Network defenses against vulnerable Wi-Fi connections and man-in-the middle (MITM) attacks. MITM detections include TLS connectivity checks, false/rogue base stations, SSL/TLS tripping protections, and insecure access points.

A PRODUCTIVITY MULTIPLIER FOR SECOPS

- All mobile threat activity is visualized and managed in the same familiar and trusted BlackBerry® security console used for desktop and server endpoints.
- Mobile threat data is automatically collected and correlated with telemetry from users, apps, and networks.

- Device vulnerability reports enable admins to easily visualize and export OS and vulnerability information from all managed devices.
- Streamlined user/group enrollment via Active Directory® searches. Convenient activation and synchronization for users via QR codes.

PROMOTES GOOD CYBER HYGIENE

- Users can easily monitor the status of all UES services and device health parameters in the intuitive BlackBerry Protect Mobile app dashboard.

WELCOME TO PREVENTION-FIRST MOBILE SECURITY

BlackBerry Protect Mobile leverages Cylance AI technology to defend mobile devices against malware, phishing attacks, OS vulnerabilities, insecure networks, and zero-day payload execution. Admins can now manage the security of every type of endpoint, with security and telemetry data seamlessly collected, contextualized, and displayed in the UES console. Users are encouraged to adhere to security policies and practice good cyber hygiene by an intuitive dashboard that displays the health and status of their mobile devices.

BlackBerry's unified approach to MTD paves the way for adopting a Zero Trust / Zero Touch security strategy that increases productivity while reducing security risks and costs.

Learn how BlackBerry Protect Mobile can benefit your organization.

ZERO TRUST

Zero Trust is what security teams want – No one gets or keeps access to anything until they prove and continue to prove who they are, that access is authorized, and they are not acting maliciously.

ZERO TOUCH

Zero Touch is what users want – immediate gratification with instant access to anything and everything they need to get the job done, without the hassle of passwords, timeouts, or intrusive requests for re-authentication.

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.

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