BlackBerry

Whitepaper

AI-DRIVEN SECURITY FOR A MOBILE WORLD

How BlackBerry Mobile Threat Defense uses AI-driven cybersecurity to protect mobile devices and simplify user experience

Ponder this fact: There are now more mobile devices in the world—over 7 billion—than there are people.[1] So it should come as no surprise that more than half of all devices connected to the Internet today are mobile.[2] Yes, there are now more Android™ connections to the Internet than Windows®.[3]

But the explosion of mobile devices has also spawned a parallel, more insidious, phenomenon: the rise of mobile malware and cyberattacks. A recent Verizon report indicates that one out of three enterprise attacks now involves a mobile device.[4] Moreover, the pace of attacks is quickening, with mobile malware incidents growing at double- and triple-digit rates in recent years.[5]

The impact of mobile attacks can be staggering, rivaling the cost of "traditional" cyberattacks that target servers and desktop computers. Industry analyst Aberdeen estimates that the annual business impact from mobile phishing attacks reaches more than $200 million, with a median cost of about $500,000.[6] The recent CopyCat attack, which infected 14 million Android devices, netted the hackers $1.5 million in stolen ad revenues in two months.[7]

The reality is that mobile devices present an especially attractive point of entry for all kinds of bad actors. Apps downloaded to cell phones, for example, can be easily exploited as a vector for malicious malware. Mobile networks can be compromised using man-in-the-middle techniques to intercept mobile traffic. It turns out that mobile endpoints are more than two-times more likely than servers to be successfully compromised.[8] Even more worrisome, users are often unaware of a mobile attack, with malware sometimes laying hidden on a device for more than a year, quietly stealing data and resources.[9]

Mobile Attacks by the Numbers

- **Over 42 million** mobile malware attacks take place every year[10]
- **63%** of grayware apps leak the device's phone number[11]
- **Nearly 1 in 5** business and industry apps leak personally identifiable information[12]
- Cyberattacks targeting smartphones have risen by **50%** in the first half of 2019 compared with 2018[13]
- **25%** of compromises go undetected for one to four years[14]

From Optional to Required

Given the very real and growing risk of attacks, enterprises are beefing up their protections against mobile threats. However, the increasing popularity of "bring your own device" (BYOD) programs at work has made it tougher for organizations to implement effective threat-reduction measures. Since the current generation of tech-savvy users now expect to use their devices for both personal and business uses, most enterprises no longer pursue the option of barring personal devices from the workplace. Similarly, attempts to implement a variety of controls to bring all mobile devices "under management" have proved largely unworkable.[15]

The answer for more and more enterprises is to embrace a rapidly emerging class of mobile security capabilities known as mobile threat defense (MTD). These solutions go beyond traditional enterprise mobile management (EMM) solutions, offering an extra layer of security by preventing, detecting, remediating, and improving overall security hygiene for an organization's entire mobile fleet and applications.

"The need for mobile threat defense…is clear for any enterprise taking its mobile transformation journey seriously," says Jason Koestenblatt, writing in *Enterprise Mobility Exchange*.[16] Gartner says that by 2020, 30% of organizations will have MTD in place, an increase from less than 15% in 2019.[17]

Zero Trust: The Foundation of Mobile Security

According to Aberdeen, the most effective mobile security solutions should incorporate the principle of "zero trust". Developed more than 15 years ago, the concept means that "access to enterprise resources is always conditional on establishing a level of assurance for devices, users, and normal behaviors and locations, both before and after the initial connection."[18]

Zero trust is the foundation for addressing the ever-present risks related to security, privacy, and regulatory compliance from the use of mobile devices. MTD solutions employing zero trust principles screen all mobile devices for threats and vulnerabilities *before* users are granted access to enterprise infrastructure and data—and then continuously monitor the security profile and health of all mobile devices, as well as user behavior, while connected.[19]

The best MTD solutions continuously defend against cyberattacks and enforce strict authentication in high risk situations ("Zero Trust"). Yet they also streamline access for users that are accessing systems under normal work scenarios and at locations proven to be secure ("Zero Touch").

As Aberdeen explains, the goal of MTD is not to slow your users down, but to help them go faster during normal low-risk use. Put another way: MTD solutions based on zero trust principles are great at protecting against the "bad"—the constellation of mobile threats that can wreak havoc in your organization—while also facilitating the "good"—all the benefits of productivity, convenience, and scalability that mobile devices are known to bring to the enterprise.[20]

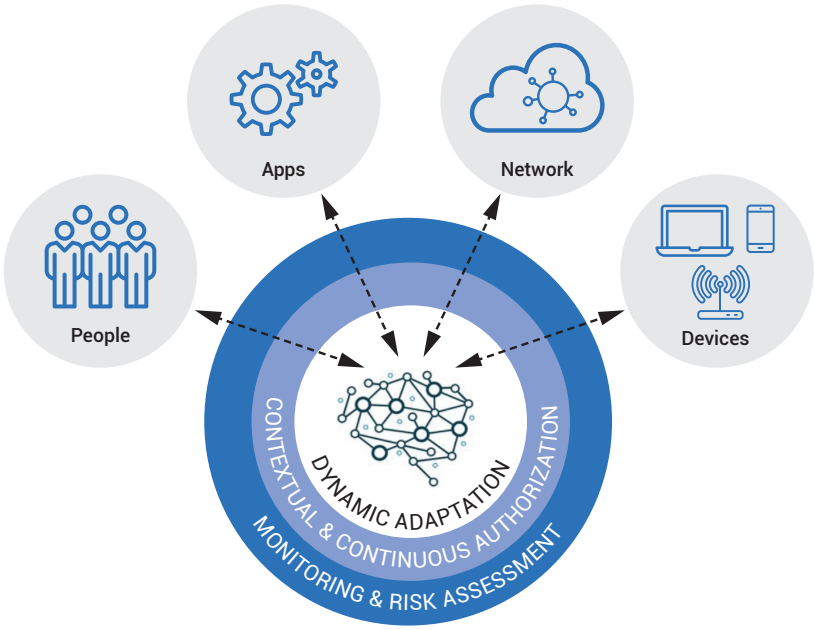
CylancePROTECT: Bridging the Gap Between Zero Trust and Zero Touch

The ability to integrate tight mobile security with smart policy adaptation is what BlackBerry calls "bridging the gap between zero trust and zero touch"—and it's a core capability of CylancePROTECT®, BlackBerry's next-generation MTD solution.

CylancePROTECT's AI-driven threat detection continuously works to protect all endpoints and mobile devices without disrupting end-users. It leverages the best of zero trust and zero touch architectures to automatically adjust policies and security levels based on the user's location, behavior, and device.

CylancePROTECT integrates with BlackBerry UEM to redefine endpoint protection, using the power of AI to protect your mobile endpoints from zero-day threats.

BlackBerry Zero Trust Architecture



Continuous Endpoint Protection

Today organizations are using CylancePROTECT to protect their mobile device fleets against advanced malicious threats, extending the security baseline provided by BlackBerry® Unified Endpoint Manager (UEM). The MTD solution monitors threats at both the device and application levels and goes beyond the security provided by BlackBerry's 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 uses AI and machine learning-based detection to identify any malware that might come in through sideloaded applications. This adds an extra layer of protection to the BlackBerry® Dynamics™ SDK platform, BlackBerry's advanced containerization solution for mobile apps. Enterprises and their partners are now able to build and customize a full range of secure applications that can be loaded onto enterprise-accessible devices.

Advanced Threat Protection

While there are many mobile threat solutions on the market, CylancePROTECT delivers a uniquely powerful set of capabilities.

CylancePROTECT can detect and prevent new, emerging cybersecurity threats, with an average predictive advantage of 25 months.

BlackBerry Cylance AI Advantage

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

Mobile Suite Protection for All Managed and BYO Devices

When CylancePROTECT is integrated into the BlackBerry UEM platform, organizations can be assured their entire mobile fleet is protected without having to rely on employees to maintain third-party apps. Also, by avoiding the need to manually configure VPNs or VDIs, organizations can increase workforce productivity and decrease costs.

Single Pane of Glass

With CylancePROTECT, there is no separate product or console to set up and configure because it's tightly integrated into the BlackBerry UEM server and applications. This means security and management functionality are available in a single, convenient location.

Mobile Threat Defense to Protect Your Entire Mobile Fleet

- Protects mobile endpoints against malware and phishing attacks
- Scans mobile applications for existing malware
- Provides complete endpoint protection for all devices, including BYOD
- Embedded directly into BlackBerry® Dynamics™ apps and managed by BlackBerry UEM

BlackBerry Named a Leader in the IDC MarketScape on UEM, EMM, and EMM for Ruggedized/IoT Device Deployments

Once again, IDC has recognized BlackBerry as a leader in the enterprise mobility market segment in three recent IDC MarketScape studies. These findings continue to validate BlackBerry as a vendor of choice for enterprises and governments that need software and services to secure mobile devices, as well as embedded devices in the IoT space.

- A Leader — IDC MarketScape: Worldwide Unified Endpoint Management Software 2019–2020 Vendor Assessment (Doc #US45355119, Nov 2019)
- A Leader — IDC MarketScape: Worldwide Enterprise Mobility Management Software 2019–2020 Vendor Assessment (Doc #US45353719, Nov 2019)
- A Leader — IDC MarketScape: Worldwide EMM Software for Ruggedized/ IoT Device Deployments 2019–2020 Vendor Assessment (Doc #US45353819, Nov 2019)

Conclusion

Enterprises are confronting a tough challenge: the growing threat of malware attacks aimed at mobile devices, and especially the apps that run on them.

The consensus of industry security analysts is clear: enterprises must place greater emphasis on countering the rising tide of mobile threats, from malware phishing to data leakage, spyware, and more. Remember that mobile devices are two times more likely to be compromised than desktops and servers, and bad actors frequently use mobile endpoints as stepping stones to invade enterprise networks and the valuable assets they contain.

MTD solutions are the answer, and more enterprises are adding MTD to their security budgets. Yet not all solutions are the same. Using AI and machine learning, BlackBerry provides a unique mobile security solution that delivers the protective power of zero trust with the adaptive flexibility of zero touch to unleash the productive potential of mobile workforces.

Learn More

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

Endnotes

[1] "How Many Phones Are in the World?," Bankmycell.com.

[2] "Desktop vs. Mobile vs. Tablet Market Share Worldwide – November 2019," StatCounter.

[3] "Mobile Threat Defense Now a Necessity for Enterprises," Enterprise Mobility Exchange.

[4] "Mobile Security Index 2019," Verizon.

[5] "The Current State of Mobile Malware," Wandera.

[6] "'Zero Trust' For Enterprise Mobility: The Brakes that Help Your Users Go Faster," Aberdeen.

[7] "How the CopyCat malware infected Android devices around the world," Check Point Software Technologies.

[8] "'Zero Trust' For Enterprise Mobility: The Brakes that Help Your Users Go Faster," Aberdeen.

[9] Ibid.

[10] "Mobile malware evolution 2017," Kaspersky Lab.

[11] "2019 Internet Security Threat Report," Symantec.

[12] "2017 Mobile Leak Report," Wandera.

[13] "Mobile malware attacks are booming in 2019: These are the most common threats," ZDNet.

[14] "'Zero Trust' For Enterprise Mobility: The Brakes that Help Your Users Go Faster," Aberdeen.

[15] Ibid.

[16] "Mobile Threat Defense Now A Necessity For Enterprises," Enterprise Mobility Exchange.

[17] Gartner, Market Guide for Mobile Threat Defense, Nov. 2019.

[18] "'Zero Trust' For Enterprise Mobility: The Brakes that Help Your Users Go Faster," Aberdeen.

[19] Ibid.

[20] Ibid.

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.