BlackBerry
Intelligent Security. Everywhere.

Business Brief

The Evolution and Arrival of the Prevention-First Approach to Cybersecurity

A few years ago, a proactive prevention-based security posture was more an aspiration than a reality. The endpoint security tools of the day relied on signature hash matching and heuristics to detect malware. Often, they required a suspect file to execute on, and subsequently infect, one of its subscriber's endpoints before it could be judged malicious. Others required massive volumes of data to be sent to the cloud to be analyzed, introducing unacceptable delays in detection and response. All these approaches were inherently reactive.

The breakthrough came in 2012, when a group of security thought leaders and data scientists came together to launch Cylance®, introducing a brand-new approach to endpoint defense that leverages artificial intelligence (AI) and machine learning (ML). The endpoint security solution they built, now re-branded as BlackBerry® Protect, was uniquely capable of preventing the execution of never-before-seen malware at the endpoint without reliance on signatures or a cloud connection.

Today, this prevention-first security approach is both proven and practical. Yet, perhaps out of inertia, some organizations still cling to a reactive approach to cybersecurity that has long since passed its expiry date.

Defense-in-Depth Is No Defense At All

More than 350,000 new malware variants[1] are released into the wild each and every day. Adversaries are continually finding new ways to exploit fundamental flaws in the traditional defense-in-depth approach to cybersecurity, which holds that every type of attack should be countered with a tailored security control. The result is a multi-layered, multi-vendor security infrastructure that is both ineffective and unsustainable.

And since each security layer generates frequent, and often spurious, alerts, it has become difficult, if not impossible, for analysts to distinguish between the signal and the noise quickly enough to take corrective actions. According to a Capgemeni survey[2], 56% of the respondents acknowledged that their cybersecurity analysts were overwhelmed by the sheer volume of endpoint and cloud data. Cisco reports[3] that 48% of alerts are never even investigated.

As a result, it took an average of 280 days for organizations responding to a Ponemon Institute survey[4] to identify and contain a data breach caused by a malicious attack. Reducing that response time is not only essential for operational resilience; it also benefits the bottom line. Organizations that resolve incidents in fewer than 200 days realize an average costs savings of $1.12 million[4].

Staffing Up Is No Solution

These challenges are exacerbated by a global IT security skills shortage, which has resulted in more than four million unfilled positions[5] as well as high burnout rates among existing but over-taxed security professionals. As ESG senior principal analyst Jon Oltsik puts it[6], "With a revolution in digital transformation, IoT, and 'smart' infrastructure, the cybersecurity skills shortage should be seen as an existential threat, not a minor inconvenience."

Obviously, the industry needs to encourage more young people to enter the security field and offer ongoing opportunities for experienced professionals to learn new skills. However, even if that were possible, staffing up will not solve the problems we face today. There are simply too many ways for determined adversaries to break through traditional defenses, and there will always be too few experienced professionals to stop them utilizing reactive approaches. Organizations need endpoint defenses that stop attacks automatically so that security teams can focus on business continuity, digital transformation, and resilience-building projects. That means adopting a proactive unified endpoint security (UES) strategy based on AI, ML, and automation.

The Road to Prevention

A prevention-first security posture begins with neutralizing malware prior to the exploitation stage of the kill-chain. If malware cannot execute, then the downstream consequences, and the resulting efforts to trace, contain, and remediate the damage, are dramatically reduced. The security stack can be simplified, reducing the administrative burden on security operations center staff besieged by alerts from dozens of downstream point solutions. By stopping malware at the exploitation stage, BlackBerry® solutions help organizations increase their resilience, reduce infrastructure complexity, and streamline security management.

BlackBerry® Cyber Suite now encompasses the endpoint protection of BlackBerry Protect, the endpoint detection and response of BlackBerry® Optics, and the unique user behavior analytics of BlackBerry® Persona. Working together, these UES solutions provide analysts with a broad and richly contextualized view of threat activity, along with the policy enforcement tools they need to prevent adversaries from achieving their objectives.

There can no longer be any question about what constitutes a responsible approach to cyber defense. Organizations must lead with proactive prevention.

---

[1] AV-TEST Website

[2] Reinventing Cybersecurity with Artificial Intelligence

[3] Cisco Cybersecurity Report Series 2020: Securing What's Now and What's Next

[4] IBM Security Cost of a Data Breach Report

[5] CSO Magazine: The cybersecurity skills shortage is getting worse

[6] The Life and Times of Cybersecurity Professionals 2020

About BlackBerry

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 175M cars on the road today. 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 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.*

BlackBerry
Intelligent Security. Everywhere.

BB20-XXXX | 210414