BlackBerry
Intelligent Security. Everywhere.

Solution Brief

Replacing Legacy AV

Legacy antivirus solutions rely on malware detection methods that range from byte-matching signatures to post-execution behavioral analysis. In response, threat actors have introduced increasingly sophisticated tactics, techniques, and procedures that are explicitly designed to evade them. For example, attackers now utilize polymorphic, single-use, and fileless attacks that cannot be detected by byte-matching. Since ransomware can encrypt enterprise data in a matter of minutes, post-execution behavioral analysis is no longer a viable defense strategy.

Organizations have been encouraged to address these drawbacks by adopting a defense-in-depth approach, 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.

On average, organizations have ten security agents running on their endpoints[1], consuming processor and memory resources that can degrade system performance and cause contention issues that create security gaps. Each control must be configured and re-configured repeatedly to reflect business needs and changes to the IT environment. Signatures must be continually updated and audited, a significant challenge for under-staffed security teams managing large fleets of geographically dispersed endpoints.

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 acknowledge their cybersecurity analysts are overwhelmed by the volume of endpoint and cloud data, and Cisco[3] has reported that 48% of alerts are never even investigated.

An excessive number of security controls can even have the unintended effect of reducing, rather than enhancing, an organization's cyber resilience. According to an IBM Security report[4], nearly 30% of the organizations surveyed have 50 or more tools deployed to manage their security environments. Compared to peers using fewer tools, these organizations ranked 8% lower in their ability to detect attacks and 7% lower in their capabilities for incident response.

BlackBerry's Prevention-First Approach To Cyber Defense

Unlike traditional AV products, BlackBerry® Cyber Suite prevents malware from executing on the endpoint via artificial intelligence (AI) and machine learning (ML) models that thwart attacker attempts to evade detection. BlackBerry data scientists build these models using an immense crowdsourced dataset of known safe and unsafe executable files in Windows®, macOS®, Linux®, iOS®, and Android™ frameworks. A statistically valid sample of these files is selected and then disassembled by algorithms into their constituent building blocks, known as features. These include such attributes as file size, signing attributes, string data, icon, imports, permissions in a data section, packers, compiler type and language, headers, directories, and millions more. Any static element that can be pulled from memory or from disc into memory can be analyzed.

---

[1] 3 Myths Debunked in the 2019 Endpoint Security Trends Report

[2] Reinventing Cybersecurity with Artificial Intelligence

[3] Cisco Cybersecurity CISO Benchmark Study, Securing What's Now and What's Next

[4] Cyber Resilient Organization Report 2020

Once optimized and deployed, the model examines each incoming file, assesses its features, and then generates a confidence score that predicts with 99% accuracy[5] whether the file is malicious or benign. The entire process takes milliseconds to complete and executes locally on the endpoint. BlackBerry Cyber Suite is equally effective at detecting and stopping fileless attacks and insider threats.

Today, BlackBerry Cyber Suite includes:

- **BlackBerry® Protect**, an endpoint protection solution that utilizes AI and ML to prevent the execution of malware on Microsoft® Windows®, macOS®, and Linux® systems. The solution also protects endpoints with advanced script and application control, memory protection, and device control features. All protection is applied at the endpoint automatically, without any reliance on cloud lookups or a network connection.
- **BlackBerry® Protect Mobile**, a mobile threat defense solution that provides iOS and Android users with advanced AI-driven threat protection at the device and application levels.
- **BlackBerry® Optics**, an endpoint detection and response solution that augments BlackBerry Protect by utilizing AI, context analysis, and MITRE ATT&CK framework rules to detect advanced threats and automate the incident investigation and response processes with playbook-driven workflows.
- **BlackBerry® Persona**, a continuous authentication solution that utilizes behavioral analytic models at the endpoint to compute trust scores and control user access to enterprise assets.

Benefits for Customers

By preventing malware from executing, BlackBerry Cyber Suite dramatically reduces the potential downstream consequences of an attack along with the resulting efforts to trace, contain, and remediate the damage. The security stack can now be simplified, reducing the administrative burden on security operations center staff besieged by alerts from dozens of downstream point solutions. Stopping malware at the exploitation stage is an important first step in increasing security resilience, reducing infrastructure complexity, and streamlining security management.

A Forrester Total Economic Impact™ Study[6] assessed the return on investment a multi-national manufacturer realized by decommissioning its legacy AV and deploying BlackBerry endpoint protection, detection, and response solutions. After other findings, the authors cited the following risk-adjusted present value (PV) quantified benefits:*

- **$8.4 million savings** from decommissioning a legacy on-premises endpoint security product after deploying BlackBerry software-as-a-service (SaaS) solutions.

---

[5] NSS Cylance Security Value Map™ (SVM)

[6] The Total Economic Impact™ Of CylancePROTECT® And CylanceOPTICS™

* *BlackBerry completed its acquisition of Cylance on February 21, 2019 and is currently selling the CylancePROTECT® and CylanceOPTICS® solutions under the newly rebranded names BlackBerry® Protect and BlackBerry® Optics. All references to the Cylance organization and its branded products and services in this document utilize BlackBerry branding.*

- **10% improvement** in cybersecurity team productivity. The cybersecurity team now proactively focuses on threat hunting rather than troubleshooting and maintaining the legacy AV product.
- **25% reduction** in the expected cost of a major security breach with more effective malware detection and protection.
- **95% reduction** in lost time via faster investigation and remediation. Fewer end-users are compromised. Faster threat investigation and remediation allow end-users to quickly resume productive work.
- **97% reduction** in time spent re-imaging machines. The organization takes fewer machines offline for re-imaging. Less re-imaging and less end-user downtime mean more IT resources are available for reallocation.
- **Eliminated manual software audits**. The security team receives an alert whenever an employee downloads software that could be malicious. The software is blocked, and the employee must ask for approval before using it. This eliminates the need for manual software audits.

The customer has not experienced any major malware or ransomware attacks since upgrading its endpoint defenses.

Switch To Smarter Endpoint Security Today

Organizations relying on traditional AV are being outpaced by modern threat actors. Powered by AI, ML, and automation, BlackBerry Cyber Suite enables organizations to safeguard their desktop, server, and mobile devices with unparalleled effectiveness, ease of use, and minimal system impact. Working together, they provide the unified threat prevention and policy management capabilities organizations need to optimize their resilience and enhance their productivity.

Visit our website for more information on how and why you should replace your legacy AV products.

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 over 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.

BlackBerry. Intelligent Security. Everywhere.

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

BlackBerry
Intelligent Security. Everywhere.