BlackBerry Intelligent Security. Everywhere.

BLACKBERRY GUARD

Solution Brief

BUSINESS CHALLENGE

While cloud and mobile technologies provide significant opportunities for digital transformation, they also dramatically expand the attack surface, leaving coverage gaps for adversaries to exploit. To reduce these risks, organizations invest in security tools they hope will thwart cyberattacks and eradicate breaches. Some organizations deploy as many as 50 different tools[1] to manage their security environment. Unfortunately, despite these investments, breaches still occur every day, as adversaries hone their techniques to exploit new gaps in the security architecture.

Deriving actionable threat intelligence from these disparate tools is a major challenge for SecOps teams. Every device, network, user, and application generate huge quantities of telemetry data that must be continuously collected, correlated, contextualized, and analyzed to detect the subtle signals of a multi-pronged stealthy attack. Every tool generates alerts, many of them false positives, which must still be triaged, investigated, and resolved.

The alert management problem is compounded by the global IT security skills shortage, which has resulted in more than four million unfilled positions[2] and high burnout rates among CISOs and over-taxed security professionals[3]. Cisco reports[4] that 48% of alerts are never even investigated.

The solution is to augment an organization's internal resources by engaging a managed extended detection and response (XDR) service to proactively prevent threats and contain security incidents by correlating and analyzing alert and telemetry data from across an organization's entire digital environment.

[1] https://www.ibm.com/downloads/cas/VR9E8AKM

[2] https://www.hdi.global/infocenter/insights/2020/cyber-skills-gap/

[3] https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf?hsCtaTracking=db3c3c15-5a23-4caa-850f-7151d1c761f5%7C6b711f53-6181-45c4-b382-df76ff824ff9

[4] https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-ciso-benchmark-cybersecurity-series-feb-2020.pdf

THE BLACKBERRY GUARD APPROACH

BlackBerry® Guard provides the technology, processes, and support needed to investigate multi-pronged stealthy attacks, in which an attacker's footprint touches endpoints, users, networks, cloud, apps, and more. It is a subscription-based managed XDR solution that provides robust protection while eliminating the challenges organizations face managing threat detection and response across all of their internal security and business tools. Customers receive a cloud deployment of fully-integrated BlackBerry® security solutions, extended integration with third-party vendors, Cylance® AI-powered threat prevention, and 24x7x365 detection and response services, all in a single package. A subscription provides everything a client needs to safeguard onboarding, configuration, monitoring, threat hunting, incident handling, and remediation.

BlackBerry Guard provides critical cybersecurity services such as:

- ***Threat Prevention*** – BlackBerry Guard leverages advanced artificial intelligence (AI) and machine learning (ML) to detect and mitigate malware, fileless, and user-based threats.
- ***Threat Hunting*** – Cylance AI-powered security agents and human analysts work together to detect and trace attacks from initial compromise through to actions on objectives.
- ***Incident Management*** – Advanced orchestration, playbooks, triage, and filtering methods are custom tailored for each client.
- ***Event Response*** – BlackBerry Guard quickly disrupts cyberattacks and contains security breaches, then notifies account holders for maximum transparency.
- ***Enterprise-Wide Threat Intelligence*** – The BlackBerry Guard XDR platform ingests alert and telemetry data from across the enterprise, where it's correlated, contextualized, and analyzed, providing unprecedented visibility and insight into the organization's security environment.

Figure 1. BlackBerry Guard provides critical cybersecurity services.

TOOLS FOR SUCCESS

BlackBerry Guard consolidates alert and telemetry data from users, desktops, servers, mobile devices, and networks through its seamless integration with BlackBerry® Protect, BlackBerry® Optics, BlackBerry® Persona, and BlackBerry® Gateway.

THIRD-PARTY INTEGRATIONS

BlackBerry Guard also includes pre-built integrations with data from selected third-party tools, as well as service options to integrate additional tools as needed. For example, BlackBerry Guard analysts can further enrich and contextualize BlackBerry Guard threat intelligence by using Cylance AI to analyze log data aggregated by a SIEM application, or by correlating BlackBerry Guard alerts with alerts triggered by SIEM rulesets.

The BlackBerry Guard portal makes it easy for customers to consult with BlackBerry security experts as needed, including holidays, when coordinated attacks often occur.

ENDPOINT PROTECTION

BlackBerry Protect prevents endpoints from being compromised by malware, script-based, fileless, memory, and external device attacks. Sophisticated AI models trained for years on tens of millions of safe and malicious files recognize and prevent the execution of known malware and zero-day attacks. All threat prevention capabilities are applied automatically at the endpoint, without user or admin intervention.

MOBILE THREAT DEFENSE

Mobile threat defense is essential for organizations supporting a remote or mobile workforce. BlackBerry® Protect Mobile extends the predictive advantage capabilities of Cylance AI to prevent mobile threats from malware, outdated/unpatched software, URL phishing/smishing attacks, and unsafe network connections.

ENDPOINT DETECTION AND RESPONSE

BlackBerry Optics uses on-device mathematical threat models to perform root cause analysis, smart threat hunting, and automated detection, response, and remediation. While BlackBerry Protect is adept at preventing malware execution, BlackBerry Optics excels at discovering more subtle intrusions, such as those associated with enterprise resource abuse. Each endpoint can use a context analysis engine (CAE) to determine if suspicious activity warrants an automated response or intervention from a security analyst. Like BlackBerry Protect, BlackBerry Optics enables each endpoint to function as its own virtual security operations center, without any requirement for continuous access to cloud resources or additional investments in on-premises infrastructure.

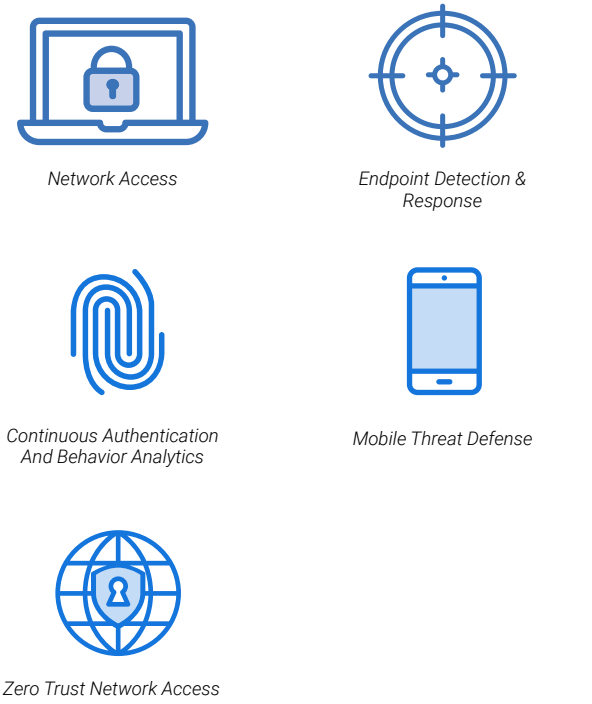

Figure 2. BlackBerry Guard leverages the BlackBerry® Cyber Suite, a portfolio of AI-powered prevention-first security solutions.

ZERO TRUST NETWORK ACCESS

BlackBerry Gateway is a Zero Trust Network Access (ZTNA) solution that secures all organizational device and network communication regardless of location. The Zero Trust framework is particularly effective at mitigating risks arising from supporting mobile and remote workers. Unlike VPNs, BlackBerry Gateway grants permissions for users to access secure and verified apps, not the entire network. It features full/split tunnel capabilities, allowing organizations to easily separate secure business activity from personal or other open communications. The BlackBerry Gateway IP security layer is optimized for mobile devices and supports SaaS identification to ensure critical business services never error out. The BlackBerry Gateway IP reputation features protect employees by keeping devices from accessing malicious domains and sites. The BlackBerry Gateway source IP pinning improves secure SaaS communications by allowing approved devices to access apps without relying on techniques that can compromise security.

CONTINUOUS AUTHENTICATION AND ADAPTIVE SECURITY POLICIES

BlackBerry Persona is an AI-driven continuous authentication and behavior analytics solution that has the unique ability to grant access and issue authentication challenges based on real-time risk analysis. If a user's risk score exceeds an admin-defined threshold, BlackBerry Persona can dynamically adapt the user's security and policy posture and apply remediation when needed. If risk scores remain low, access to resources can be streamlined, providing a Zero Touch experience that enhances user productivity. BlackBerry Persona allows the user experience and security/policy posture to be mutually and dynamically optimized, versus in conflict.

EXTENDED INTEGRATION WITH THIRD-PARTY VENDORS

BlackBerry software components directly feed integrated data from desktops, mobile devices, servers, users, and networks to the BlackBerry Guard XDR platform. There, it is correlated and contextualized with third-party data, enabling analysts to conduct cross-tool threat hunting from a single unified console.

EXPECTED BENEFITS

BlackBerry Guard helps organizations adopt a prevention-first, managed XDR approach to security that encompasses every device, user, network, and application in their IT infrastructure. Benefits include:

- 24x7x365 managed XDR services by a world-class team of BlackBerry incident response and threat hunting experts.
- A customized cloud-deployment of BlackBerry AI-powered endpoint security solutions.
- Deep enterprise-wide visibility and contextualization of security events generated by self-monitoring endpoints and telemetry from pre-integrated security tools. Subscribers can also retain optional BlackBerry Guard services for integrating additional third-party telemetry.
- Best practice security processes that reduce cyber-risks for employees, customers, and supply chain partners.
- Utilizes MITRE ATT&CK® Framework tactics, techniques, and procedures to classify threats, profile threat actors, and enrich threat intelligence.

- Enables cross-tool threat hunting from a single unified console to accelerate detection, tracing, and containment of multi-pronged stealthy attacks as they traverse the entire digital environment.
- Enhanced security with reduced total cost of ownership.
- Eliminates recurring costs to recruit, hire, and retain hard-to-find senior security analysts.
- Closes gaps in the security infrastructure without capital expenditures.
- Significantly shortens the time spent detecting and responding to threats, and the resulting remediation and recovery costs.
- Streamlines security administration, enabling internal resources to focus on digital transformation and other mission-critical projects.
- A multi-regional architecture that facilitates compliance with GDPR and other regulatory requirements.
- A choice of BlackBerry Guard packages to meet the business needs of organizations of all sizes.

TO LEARN MORE

BlackBerry has more than three decades of experience providing world-class security for electronic and mobile devices. Whatever security challenge organizations may be facing, a BlackBerry team of experts can help. For more information about BlackBerry Guard offerings, please visit the BlackBerry Guard web page or call +1-877-973-3336.

BlackBerry also offers a portfolio of security suites that deliver on our commitment to provide intelligent security, everywhere.

Discover our:

BlackBerry Spark® Suite

BlackBerry Cyber Suite

BlackBerry Spark® Unified Endpoint Management Suite

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**.*