BlackBerry. Intelligent Security. Everywhere.

MITIGATING INCIDENTS IN MILLISECONDS

with AI-Powered Endpoint Detection and Response.

SOLUTION BRIEF

INTRODUCTION

The days when an organization could fortify its network perimeter to reduce cyber risks are over. The proliferation of mobile and IoT devices that share data and connect to multiple networks has created an exponentially expanding attack surface.

In this new threat environment, priority one is to prevent adversaries from infecting these far-flung devices with malware. The BlackBerry® endpoint protection platform, BlackBerry® Protect, accomplishes this with artificial intelligence (AI) and machine learning (ML) technologies that prevent both known and unknown forms of malware from detonating.

As Verizon has noted however[1], "Malware has been on a consistent and steady decline as a percentage of breaches over the last five years." This doesn't mean that malware is fading away as an attack vector, only that adversaries are increasingly utilizing tactics, techniques and procedures (TTPs) that don't require the use of portable executables to compromise an endpoint. For example, they are using phishing to steal user credentials, exploiting widely-known vulnerabilities in external-facing network services, such as RDP, and embedding backdoors in widely-used applications, as in the SolarWinds attacks.

These tactics often involve a sequence of seemingly benign activities that only in combination reveal their malicious intent. A single data point may only be significant based on the context in which it appears and its correlation with other security events. This kind of contextual analysis

[1] 2020 Data Breach Investigations Report

is well-suited to endpoint detection and response (EDR) solutions.

Thus, EDR has the potential to play two crucial roles in cyber defense. First, it can alert security operations center (SOC) analysts when it detects early signs of a security breach so that containment responses can be initiated quickly enough to minimize damage. Reducing response time is not only essential for operational resilience, it also benefits the bottom line. Organizations that resolve incidents in less than 200 days realize an average costs savings of $1.12 million[2].

The second role is to arm analysts with the data they need to proactively hunt for threats and perform post-incident root cause analysis. However, given the proliferation of endpoint devices, and the huge volumes of telemetry and event data they generate, how is an analyst to distinguish the subtle signal of a threat from the random noise of routine activity?

In this solution brief, we'll consider how BlackBerry's AI-driven EDR solution, BlackBerry® Optics excels at helping customers achieve both objectives. For example, after deploying BlackBerry Protect and BlackBerry Optics, one customer[3]:

- **Reduced lost time by 95%** via faster investigation and remediation: Fewer end-users were compromised. Accelerated threat investigation and remediation allowed end-users to quickly resume productive work.
- **Reduced machine re-imaging by 97%**: This enabled the customer to re-allocate IT resources to more productive projects.
- **Saved $8.4 million** (net present value) by decommissioning the firm's legacy endpoint security solutions.

BLACKBERRY'S APPROACH TO EDR

BlackBerry's next-gen approach to EDR is based on three pillars:

- **Cloud-Enabled Architecture**: BlackBerry Optics applies all detection and response logic at the endpoint, and stores the resulting telemetry, alert, and forensic data in the cloud for off-line analysis.
- **Intelligent Edge AI**: AI-powered and context-driven threat detection rules identify security breaches and trigger automated responses that reduce mean time to detection (MTTD) and mean time to remediation (MTTR).
- **Deep Insight**: BlackBerry Optics facilitates threat hunting and root cause analysis by providing analysts with a consolidated, correlated, AI-driven, and enterprise-wide view of historical endpoint activity.

CLOUD-ENABLED ARCHITECTURE

Unlike other EDR products, BlackBerry Optics deploys all threat detection and response logic on the endpoint. In effect, each endpoint functions as a self-contained SOC, detecting and responding to threats in near real-time without any reliance on cloud connectivity. This eliminates the response latency that allows a minor security event to escalate into a major security incident.

Alert, event, and telemetry data for all protected endpoints is automatically collected, correlated, and stored in the cloud for off-line analysis. Out of the box, clients receive 30 days of cloud storage. BlackBerry also offers 90-day and 365-day retention package options for customers in highly regulated industries that need additional historical data to demonstrate compliance. This hybrid cloud approach eliminates physical storage limitations on the endpoint while ensuring maximum flexibility for threat hunting and post-incident analysis.

[2] IBM Security Cost of a Data Breach Report 2020
[3] Forrester Total Economic Impact™ Study

EDGE AI

The term Edge AI refers to BlackBerry's practice of deploying sophisticated AI and ML technologies at the endpoint to reduce cyber risks. Edge AI is found in BlackBerry Protect, BlackBerry Optics, and BlackBerry® Persona.

Detecting Threats with the Context Analysis Engine

The BlackBerry Optics Context Analysis Engine (CAE) is incorporated at each endpoint, monitoring events at machine speed to identify malicious and suspicious activities. The CAE comes with a prepackaged set of BlackBerry-curated detection logic that can trigger a myriad of ad-hoc and automated responses. The CAE includes rules:

- Based on industry threat intelligence feeds and management reports.
- Derived from real-world attacks investigated and resolved in the field by BlackBerry incident response teams, and threats deconstructed and documented by BlackBerry researchers. For example, the BlackBerry Threat Research team has authored custom rules that protect customers from Hafnium attacks on vulnerable Microsoft Exchange servers, and others that tag and mitigate Ryuk ransomware malware variants.
- Created by SOC analysts that reflect environment-specific security policies. For example, an analyst can define a rule that triggers an alert and forensic data collection whenever an end-user attempts to access a restricted resource or escalate their account privileges.
- Mapped to the MITRE ATT&CK® Framework, a global knowledge base of threat actor tactics and techniques drawn from real-world cyber attacks.
- That leverage unique CPU telemetry from Intel® Threat Detection Technology to detect and mitigate cryptojacking on Windows® 10 operating systems. The cryptojacking rules can easily be configured and impose virtually no processor impact on protected systems.

While detection rules are necessary, they cannot model every kind of attack behavior. Therefore, BlackBerry Optics also includes ML threat detection modules developed by the BlackBerry Data Science team that continuously analyze endpoint activity to detect zero-day attacks and advanced persistent threats (APTs).

Responding to Threats with On-Demand Packages and Automated Playbooks

BlackBerry Optics provides for both on-demand and automated responses whenever a CAE or ML detection rule is triggered. Both are essential for minimizing dwell time and reducing the costs, risks, and long-term impacts that arise from a widespread security incident.

- **On-Demand Responses with Packages:** Analysts can utilize the advanced scripting engine in BlackBerry Optics to create and deploy packages. These are collections of scripts that execute on the endpoint to run applications, collect forensic data, take systems offline, and perform other investigation and remediation functions. BlackBerry Optics ships with a default set of packages for many routine tasks. Packages can be deployed on-demand and at scale to a single device, multiple devices, selected security zones, or enterprise-wide.
- **Automated Responses with Playbooks:** Packages can also be combined and configured as playbooks, complex collections of response actions that run automatically whenever a CAE or ML detection

is triggered. For example, an analyst could create a forensic data collection playbook that executes whenever an endpoint runs a PowerShell command to download a file. When the rule is triggered, the playbook could automatically collect PowerShell logs, browser history files, and data from a memory dump, thereby providing contextualized forensic information to the analyst without requiring a single keystroke.

DEEP INSIGHT

Once an incident is detected, it must be thoroughly investigated to ensure that all stages of the kill-chain are understood and accounted for during subsequent containment and recovery efforts. The term Deep Insight refers to the extensive set of manual and automated incident investigation and threat hunting tools that provide analysts with seamless access to endpoint data.

Hunting for Indicators of Compromise with InstaQuery Searches

Threat hunters utilize both intelligence and methodology-based processes to identify anomalous security events and patterns of activity that combine to indicate an attack may be underway. This has traditionally required elite analysts with specialized skills and extensive experience. Fortunately, BlackBerry Optics makes it possible for analysts of every skill level to hunt for threats easily and efficiently.

BlackBerry Optics simplifies the threat hunting process by enabling security teams to collect and analyze data using Advanced InstaQuery (IQ) searches. IQ is a lightweight tool that collects and aggregates relevant endpoint data and presents it in a format that is both contextualized and intuitive to analyze. IQ searches can collect artifacts associated with files, registry keys, processes, network connections, and much more. It enables analysts to answer such questions as:

- Has this hash value or file extension ever been seen on one of my endpoints before?
- Has this command line ever been executed on one of my systems?

BlackBerry Incident Response consultants recently utilized IQ to help a large enterprise investigate and remediate a ransomware outbreak. Within seconds, the team determined that the primary indicator of compromise, the ransomware's file extension, was only present in the United States. This enabled the client and BlackBerry teams to focus their investigation, remediation, and cleanup efforts there, rather than spending unproductive hours assessing the client's operating environments in Europe, Asia, and the South Pacific. BlackBerry consultants also assisted the client in preventing further infections by creating and distributing custom rules that ensured the ransomware would be detected instantly and promptly quarantined.

Optimizations for Linux Environments

BlackBerry Optics also offers enhanced protection for systems running Linux® operating system versions that include RHEL, Ubuntu, CentOS, and SUSE. Protecting Linux systems is essential, since APT groups are increasingly viewing Linux as a rich target of opportunity. In a recent report, the BlackBerry Research and Intelligence team noted that most security companies focus their engineering and marketing attention on products designed for the front office instead of the server rack. Defensive coverage for Linux is often sparse and immature. BlackBerry Optics addresses these security shortfalls with Linux-specific features that include:

- **A driverless architecture** that enhances security by eliminating kernel-level dependencies.
- **CAE rules for Linux** that automatically detect malware and malicious events.

- **Refract for Linux**, which automatically remediates malware and malicious events.
- **Device lockdown**, which facilitates incident remediation and recovery by isolating infected endpoints to stop malware from spreading.

These features enable administrators to detect and stop threats targeting data center servers, point of sale (POS) devices, automated teller machine (ATM) terminals, and Linux-based fixed-function devices. Linux is also ubiquitous on web servers, supercomputers, major websites, and cloud service providers that include Google, Yahoo, and Amazon.

EXPECTED BENEFITS

BlackBerry's AI-driven approach to EDR helps organizations reduce cyber risks by:

- **Containing threats with automated responses**. These include isolating devices, terminating processes, and taking other appropriate actions that prevent threat actors from stealing credentials, escalating privileges, moving laterally across the network, or otherwise pursuing their objectives.
- **Remediating threats by returning affected systems back to a previously pristine state**. This includes eliminating all traces of the attack, along with its persistence mechanisms and forensic artifacts.
- **Helping analysts identify the signals of an attack** hidden within the massive amounts of historical endpoint telemetry data and metadata stored in the cloud. This includes every file created, every process started, every change to registry keys, every network connection, etc. BlackBerry Optics accomplishes this with automated detection rules driven by AI and contextual analysis.
- **Streamlining the process of tracing attacks and identifying security gaps** by providing analysts with immediate access to the contextualized data they need for efficient threat hunting and root cause analysis.

FOR MORE INFORMATION

Learn more about BlackBerry Optics and the BlackBerry® Cyber 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 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**.*