BlackBerry Intelligent Security. Everywhere.

BLACKBERRY OPTICS.

AI-Empowered Endpoint Detection and Response That's Cloud-Enabled, Not Cloud-Dependent.

DATA SHEET

In a perfect world, endpoints would be impregnable, users would be immune to phishing scams, and vulnerable systems would always be patched promptly. In the real world, however, prudent organizations prepare for the near-certainty of a breach by deploying BlackBerry® Optics, the BlackBerry® Cyber Suite solution for next-gen endpoint detection and response (EDR).

BlackBerry Optics enables security operations center (SOC) analysts to detect early signs of a breach so that containment responses can be initiated quickly 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[1]. BlackBerry Optics also arms analysts with the threat hunting and root cause analysis tools they need to distinguish the subtle signals of a threat from the random noise of routine activity.

[1] IBM Security Cost of a Data Breach Report 2020

BLACKBERRY'S NEXT-GEN APPROACH TO EDR

BlackBerry's EDR approach 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**: Artificial intelligence (AI), machine learning (ML), 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 seamless access to correlated and contextualized endpoint data.

CLOUD-ENABLED ARCHITECTURE

Unlike other EDR products, BlackBerry Optics deploys all threat detection and response logic on the endpoint. Alert, event, and telemetry data for protected endpoints

are 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 packages for customers in highly regulated industries that need additional historical data to demonstrate compliance.

DETECTING THREATS WITH EDGE AI AND CONTEXTUAL ANALYSIS

The BlackBerry Optics Context Analysis Engine (CAE) monitors endpoint 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 threat researchers.
- Mapped to the MITRE ATT&CK® Framework.
- That leverage unique CPU telemetry from Intel® Threat Detection Technology to detect and mitigate cryptojacking on Windows®10 operating systems.

BlackBerry Optics also includes ML threat detection modules developed by BlackBerry's data science team that continuously analyze endpoint activity to detect zero-day attacks and advanced persistent threats (APTs). SOC analysts can also create custom rules that reflect their organization's environment-specific security policies.

NEXT-GEN PROTECTION

BlackBerry Optics utilizes AI, ML, and contextual analysis for:

- Threat detection
- Threat hunting
- Root cause analysis
- Triggering automated containment and remediation responses

BENEFITS

- Utilizes multiple techniques to detect early-stage attacks.
- Deploys detection and response logic at the endpoint to minimize response latency. Eliminates dependence on cloud lookups and connectivity.
- Out of the box, provides 30 days of endpoint data cloud storage. Longer retention packages available.
- Automated playbooks accelerate incident response, remediation, and recovery.
- Advanced InstaQuery searches facilitate threat hunting and root cause analysis.
- Extensive cross platform support, including Linux®.

RESPONDING TO THREATS WITH ON-DEMAND PACKAGES AND AUTOMATED PLAYBOOKS

BlackBerry Optics provides for both on-demand and automated responses whenever a detection rule is triggered.

- **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. Packages can be deployed on-demand 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 that run automatically whenever a detection rule is triggered. For example, an analyst could create a playbook that automatically collects PowerShell logs, browser history files, and memory dump data whenever an endpoint runs a PowerShell command to download a file.

HUNTING FOR INDICATORS OF COMPROMISE WITH ADVANCED INSTAQUERY SEARCHES

BlackBerry Optics streamlines threat hunting 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. 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?

COMMON BLACKBERRY OPTICS USE CASES

BlackBerry Optics is the right fit for organizations that want to:

- Reduce MTTD and MTTR by containing threats with on-demand packages and automated playbooks.
- Remediate threats by rapidly restoring compromised systems to a pristine state.
- Search endpoint data for files, executables, MITRE ATT&CK objects, and other indicators of compromise.
- Protect endpoints without imposing performance bottlenecks.
- Quickly identify the signals of an attack hidden within masses of endpoint data.
- Increase their resilience by streamlining threat hunting and root cause analysis.

FOR MORE INFORMATION

Learn more about BlackBerry Optics and the BlackBerry Cyber Suite.