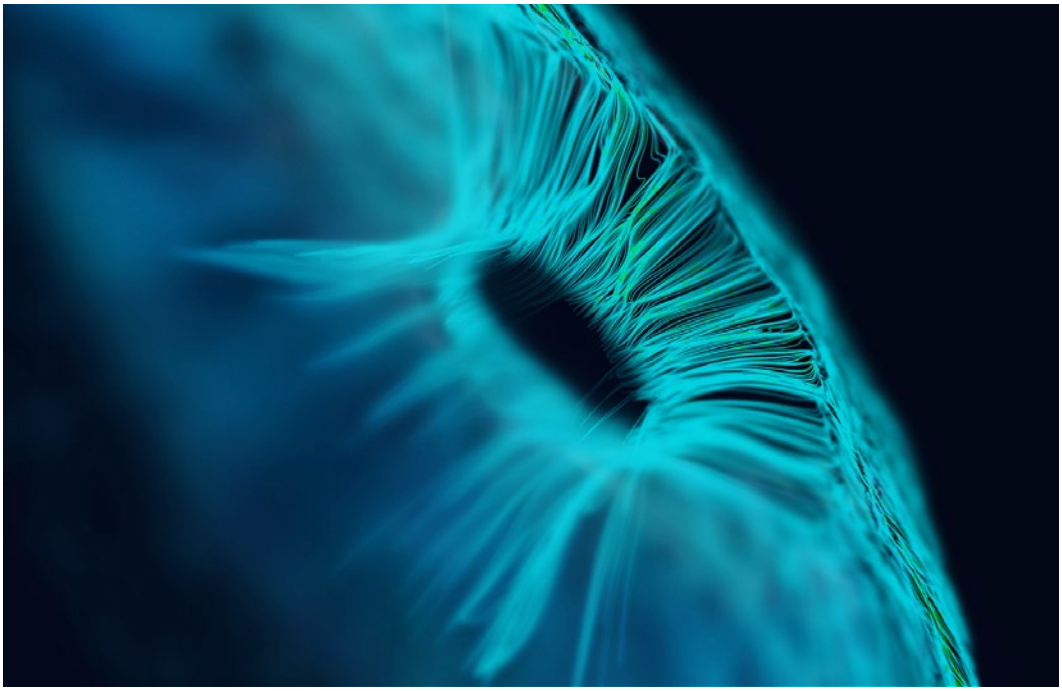
BlackBerry
Intelligent Security. Everywhere.

Data Sheet

BlackBerry Optics

AI-Powered Endpoint Detection and Response



Prevention-First EDR

Prevention products that rely on signatures cannot keep pace with today's fast-changing attacks, leaving security teams wading through a sea of alerts daily. Finding critical security issues is near impossible, leaving attackers to run rampant across the business.

Prevention-first security can significantly reduce the number of alerts generated by the security stack, decreasing the burden and frustration associated with endless alert investigations that lead nowhere.

With BlackBerry® Protect preventing malware, malicious scripts, rogue applications, and fileless attacks from harming the business, BlackBerry® Optics provides the AI-powered EDR capabilities required to keep data and businesses secure.

BlackBerry Optics is an endpoint detection and response (EDR) solution designed to extend the threat prevention delivered by BlackBerry Protect by using AI to identify and prevent widespread security incidents.

Using AI

BlackBerry Optics is an EDR solution that extends the threat prevention delivered by BlackBerry Protect using AI to identify and prevent widespread security incidents.

BlackBerry Optics provides:

- AI-driven incident prevention
- Context-driven threat detection
- Machine learning threat identification
- Root cause analysis
- Smart threat hunting
- Automated remote investigations
- Dynamic playbook-driven response capabilities

Benefits

- Reduce dwell time and the impacts of potential breaches
- Drive consistent levels of security no matter the security staff skill-level
- Save significant time and money associated with recovering from a successful attack

BlackBerry. Optics

Unlike other EDR products that are difficult to deploy, hard to maintain, and even harder to use, BlackBerry Optics:

- Can be installed on any endpoint in minutes with no hardware or expensive data streaming required
- Enables zero-latency detection and response by storing and analyzing data locally on the endpoint without needing constant updates
- Delivers self-contained, automated, machine learning threat detection modules designed to uncover threats that would be difficult to find with static behavior rules

BlackBerry Optics, working with BlackBerry Protect, delivers the detection and prevention capabilities needed to stay ahead of the attackers, keeping the business secure.

The 2.4 release of the BlackBerry EDR solution offers several enhancements to the InstaQuery, FocusView, and Context Analysis Engine (CAE) logic of BlackBerry Optics to provide greater visibility capabilities. These enhancement vectors include:

- Registry Introspection Enhancements
- DNS Visibility
- Windows® Logon Event Visibility
- RFC 1918 Address Space Visibility
- Enhanced WMI Introspection Via Windows API
- Enhanced PowerShell Introspection Via Windows API

The 2.4 release of BlackBerry Optics brings several product enhancements to aid in both the breadth and depth of EDR search parameters. These enhancements, which are built on the foundational AI-based protection of BlackBerry Protect and locally stored intelligence, offer real-time confidence to investigate, triage, and remediate when a CAE rule trigger occurs. This gives security professionals the ability to search and remediate at the speed of the threat landscape, and not be delayed by cloud queries, protracted forensic analysis, and other time-wasting processes. The security incident response team can understand all the artifacts that have occurred before and after the triggering event. This results in:

- Increased search parameter flexibility within InstaQuery, FocusView, and CAE rules
- Faster incident response
- Alignment with the MITRE ATT&CK framework
- Expanded automated response via CAE rules

BlackBerry Optics EDR Solution

Enterprise Ready	Detection	Investigation and Response
• Distributed Search and Collection • Cross-Platform Visibility • API Accessibility • Syslog Integration	• Context-Driven Detection • Machine Learning Modules • MITRE ATT&CK Framework	• Second Generation • Cloud-Enhanced Models

BlackBerry Optics, working with BlackBerry Protect, delivers the detection and prevention capabilities needed to stay ahead of the attackers, keeping the business secure.

Common Endpoint Detection and Response Use Cases

- **Prevent Malicious Activity:** BlackBerry Protect, which provides the foundation for BlackBerry Optics, is designed to specifically prevent successful attacks aimed at endpoints. This includes:
  - Identifying and blocking malicious executable and file identification using AI
  - Controlling where, how, and who can execute scripts
  - Managing the use of USB devices, prohibiting unauthorized devices
  - Eliminating the ability for attackers to use fileless malware attack techniques
  - Preventing malicious email attachments from detonating their payloads
- **Investigate Attack and Alert Data:** Users can investigate alerts from other security controls, including BlackBerry Protect, with easy to understand visualizations of all activities associated with the alert, retrieving useful information from the endpoint.
- **Hunt for Threats Across the Enterprise:** Users can quickly search for files, executables, hash values, and other IOCs across the entirety of their network endpoints to uncover hidden threats.
- **Endpoint Threat Detection:** Suspicious behaviors and other indicators of potential compromise on endpoints will be uncovered automatically.
- **Rapid, Automated Playbook-Driven Incident Response:** Users can retrieve critical forensic information from impacted endpoints automatically, as well as take response actions automatically when a harmful endpoint is discovered.

Learn More

BlackBerry Optics is just one of a wide range of world-class security solutions that BlackBerry offers. Learn more about our full selection of security suites that can provide your organization with intelligent security, everywhere.

Discover our:

- BlackBerry® Spark® Suite:
- BlackBerry® Unified Endpoint Security Suite
- BlackBerry® Unified Endpoint Management Suite

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 150M 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.

CONTACT US