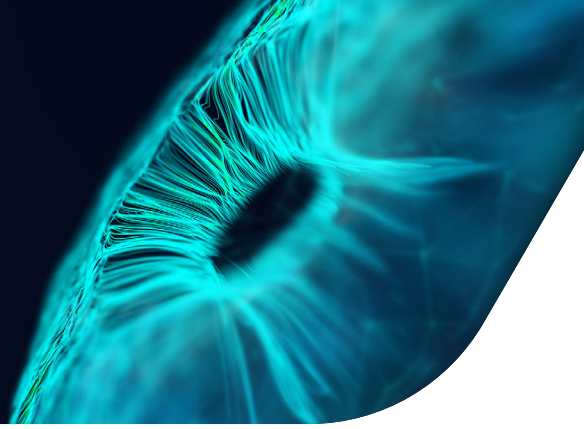
BlackBerry | CYLANCE

CylanceOPTICS™

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

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

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

- 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

CylanceOPTICS, working with CylancePROTECT, delivers the detection and prevention capabilities needed to stay ahead of the attackers, keeping the business secure.

The 2.4 release of the BlackBerry Cylance EDR solution offers several enhancements to the InstaQuery, FocusView, and Context Analysis Engine (CAE) logic of CylanceOPTICS 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

Using AI

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

CylanceOPTICS 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

CYLANCE OPTICS

The 2.4 release of CylanceOPTICS 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 CylancePROTECT and locally stored intelligence, offer real-time confidence to investigate, triage, and remediate when a CAE rule trigger occurs. This gives EDR practitioners 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 EDR 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

CylanceOPTICS EDR Solution

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

Common Use Cases

- **Prevent Malicious Activity:** CylancePROTECT, which provides the foundation for CylanceOPTICS, is designed to specifically prevent successful attacks aimed at endpoints. This includes:
  - Identifying and blocking malicious executables and files 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 CylancePROTECT, 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.

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 19-0436-20191016