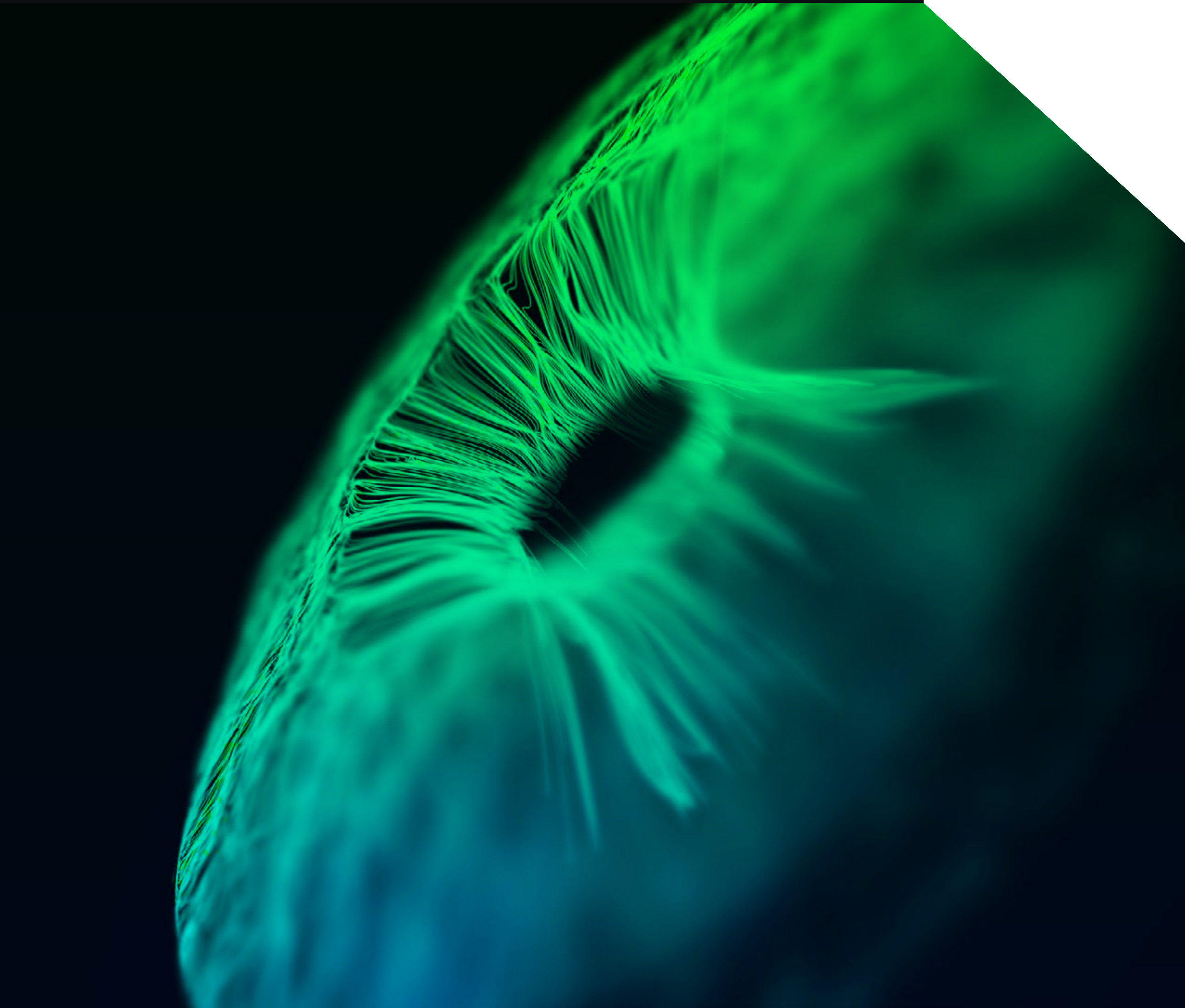
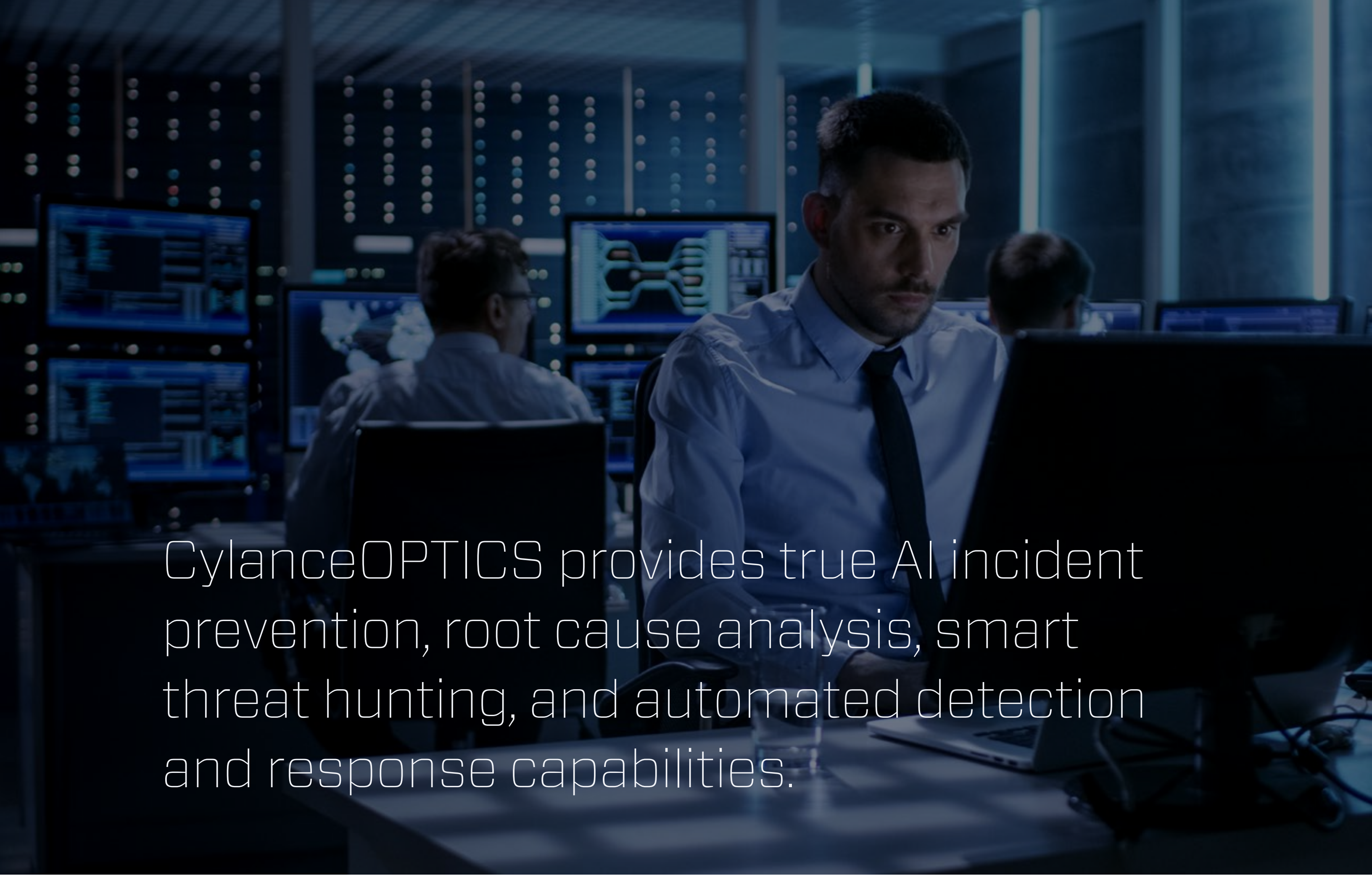
CylanceOPTICS™

2.4 Release

FEATURE FOCUS





CylanceOPTICS provides true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities.

Executive Summary

CylanceOPTICS is an endpoint detection and response (EDR) solution designed to extend the threat prevention delivered by CylancePROTECT® by using artificial intelligence (AI) to identify and prevent security incidents. CylanceOPTICS provides true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities that are fully integrated with CylancePROTECT. 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 even 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

New Features Detail

Feature	Description	Benefit
Registry Introspection Enhancements	Increased visibility into common Windows Registry persistence points, including memory attacks via Focus View, InstaQuery, or CAE detection logic.	This enhancement extends the visibility that CylanceOPTICS has into the Windows Registry. The Windows Registry is commonly used by malicious actors to store malware settings, change system configurations, or establish persistence on a system. To more efficiently surface high fidelity, actionable information, CylanceOPTICS records registry keys and values that are commonly associated with malware or techniques of malicious actors. These enhancements can be used with Focus View, InstaQuery, or CAE. This is useful in monitoring for fileless attacks, lateral movement, living off the land attacks, etc.
DNS Visibility	Enables the endpoint agent to sense and record what has instigated a DNS query, by which IP address and domain it was initiated, when it was initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAE detection logic.	This enhancement gives standard names to Internet connections (if available), providing visibility into DNS cache compromises, rogue DNS servers, DNS-based data exfiltration, and connections to web addresses rather than just IP addresses.
Windows Logon Event Visibility	This feature enables the endpoint agent to sense and record what has instigated a Windows Logon event, the user that logged on, by which IP address and domain it was initiated, when it was initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAE detection logic.	This new feature enables monitoring of a specific user if they access multiple systems and is helpful in detecting and mitigating potential insider threats. Further, this provides visibility to observe where the attacker went and what he did when moving laterally through the network.
Private Address (RFC 1918 / RFC 4193) Space Visibility	Enables the endpoint agent to sense, analyze, and record an event originating from a private Internet address on a TCP/IP network via Focus View, InstaQuery, or CAE detection logic.	This feature this is extremely valuable when looking for lateral movement attacks. Previous versions could only view movement through a public network space.
Enhanced WMI Introspection	Enables the endpoint agent to sense, analyze, and record an MS Windows Management Instrumentation event via Focus View, InstaQuery, or CAE detection logic.	This is useful in monitoring for fileless attacks and lateral movement, including living off the land attacks.
Enhanced PowerShell Introspection	Enables the endpoint agent to sense, analyze, and record a PowerShell event via Focus View, InstaQuery, or CAE detection logic.	This enhancement extends the visibility CylanceOPTICS has into PowerShell events, which are commonly used to rapidly automate tasks that manage operating systems and processes.

The 2.4 release of CylanceOPTICS enhances both the breadth and depth of EDR search parameters. Built on the foundational AI-based protection of CylancePROTECT and stored locally in real time, this solution bolsters the confidence to investigate, triage, and remediate when a CAE rule trigger occurs. EDR practitioners now have the ability to search and remediate at the speed of the threat landscape, and not be delayed by cloud query, protracted forensic analysis, and other time-wasting processes. The EDR team can then 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

Identifying a potential security issue in any environment is important, however, to protect from the fallout of a widespread incident, organizations need the ability and agility to investigate and respond to an attack with speed and certainty. With CylanceOPTICS 2.4, organizations get several new product enhancements to accelerate incident investigation and response options that enable them to gather relevant information about an incident and act fast, either in an automated or customizable fashion.

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