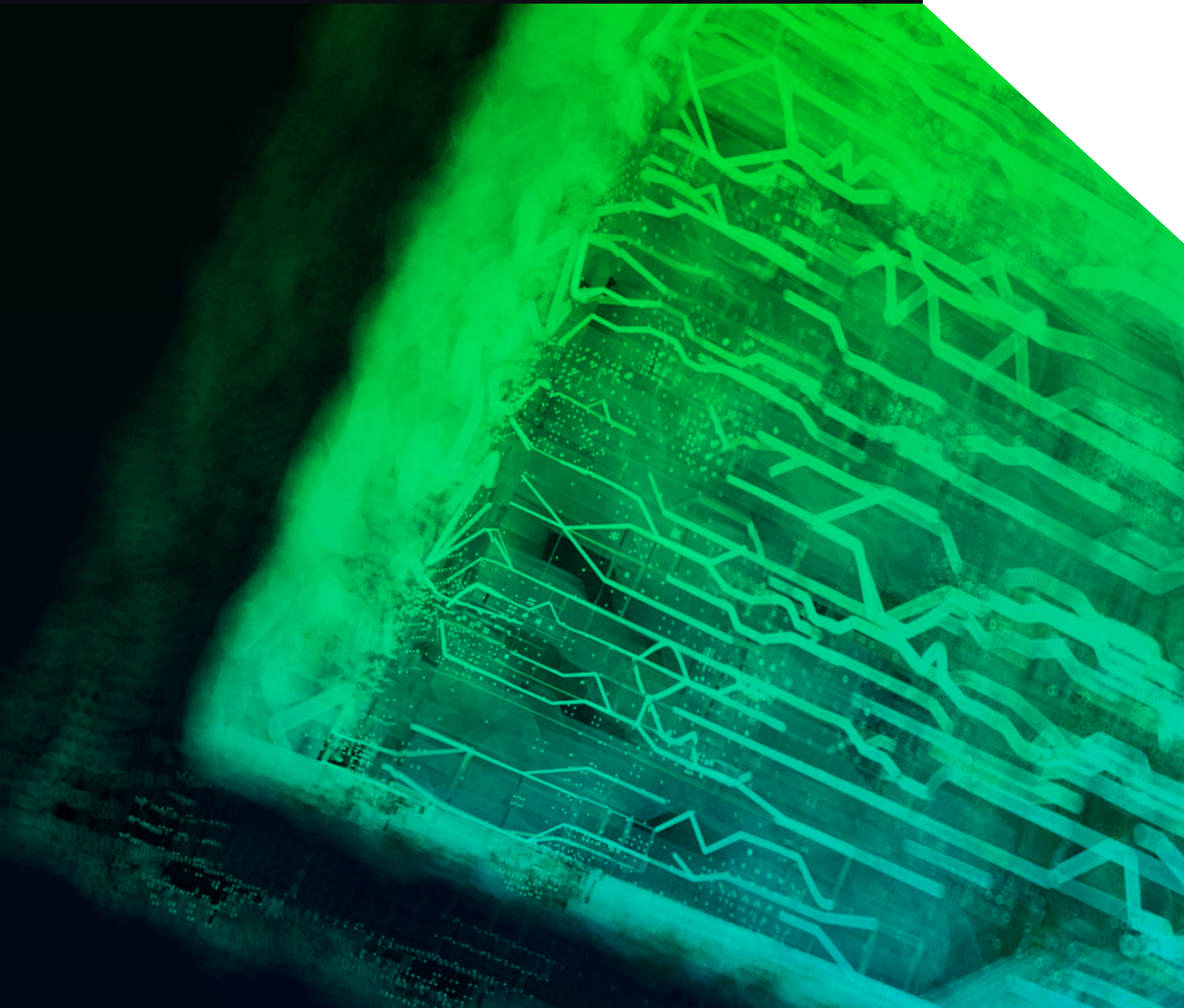
BlackBerry | CYLANCE

AI-Driven Threat and Incident Prevention, Detection, and Response

SOLUTION BRIEF



Modern threat landscape organizations must address the over 350,000 new variants of malware created every day.

Introduction

Traditional cybersecurity approaches suffer from two glaring weaknesses. First, they rely on the digital signatures of known malware in order to identify threats. This approach leaves systems vulnerable to new and non-cataloged malware. Second, they are reactive in nature, ascribing to the “it’s not a matter of if, but when” mentality and often responding to the damage caused by zero-day threats only after they execute. Guarding against known threats is important, but in the modern threat landscape organizations must also address the over 350,000 new variants of malware created every day[1].

Many cybersecurity companies attempt to stop evolving threats by building new layers of security on top of existing solutions. This approach often creates additional noise within the security stack, making it harder for analysts to quickly identify and respond to threats. The benefits of new security layers are quickly offset by their demand for more system resources and alert fatigue.

The BlackBerry Cylance Approach

BlackBerry Cylance avoids the weaknesses of traditional AV by using highly trained artificial intelligence (AI) to detect threats. Our cybersecurity AI trains on over a billion safe and malicious files. This process allows our security agents to reference and evaluate over a million file features before determining if a program should execute. The threat profiling capabilities of CylancePROTECT® gives our clients a proven predictive advantage[2] of up to 33 months over known, unknown, and zero-day malware.

[1] https://www.av-test.org/en/statistics/malware/
[2] https://threatvector.cylance.com/en_us/home/cylance-vs-future-threats-the-predictive-advantage.html

Our endpoint detection and response (EDR) solution, CylanceOPTICS™, deploys trained threat behavior models directly on the endpoint. This empowers protected devices to function as self-contained security operations centers (SOC), independent of cloud connectivity. CylanceOPTICS includes a configurable context analysis engine (CAE) that monitors endpoint events in near real time. The CAE identifies suspicious behavior, as defined by the device policies and detection rules set by your in-house security team. For example, your endpoints may send alerts or engage automated responses based on how PowerShell is called and where it is invoked.

Meeting Your Security Requirements — Use Case Summary

The following use cases demonstrate the benefits of BlackBerry Cylance's prevention-first approach to cybersecurity:

Malware (Ransomware, Trojans, Adware, Etc.)

BlackBerry® Cylance® solutions use highly trained AI to evaluate portable executable files before they map to memory space and execute. The machine learning model running on the endpoint determines if a file is malicious or safe within milliseconds. If malicious, the executable is prevented from running, thwarting the attacker's attempt to compromise the endpoint.

Fileless Malware

Fileless attacks are on the rise[3] as attackers increasingly rely on hijacking legitimate system resources to breach organizations. Security products that rely on identifying malicious executable files cannot prevent these types of attacks. BlackBerry Cylance solutions prevent fileless attacks several ways, including through memory exploit prevention, script management, and fileless threat detection modules. When an attacker attempts to escalate privileges, undertake process injection, or inappropriately use system memory, BlackBerry Cylance solutions quickly detect and prevent the attack.

Our advanced EDR solution offers introspection tools that uncover threats in the Windows Registry where fileless attacks typically create persistence mechanisms. It empowers endpoints to sense, analyze, and record Windows Management Instrumentation (WMI) events, a vital component of living-off-the-land attacks. Protected endpoints also monitor and catalog the usage of PowerShell, a critical tool leveraged by threat actors to rapidly automate system tasks and processes.

Malicious Scripts

Scripts are extremely popular with threat actors for several reasons. First, for novice attackers, malicious scripts capable of performing any number of system operations are readily available in the cyber crime underworld. Additionally, scripts are often difficult for security products to detect as they serve many legitimate uses. With BlackBerry Cylance solutions, organizations can leverage built-in script management. Security professionals can maintain full control over when and where scripts run. This allows the legitimate use of scripts to continue while severely limiting attackers attempts to misuse them.

Malicious Email Attachments

Phishing attacks are one of the most effective ways attackers gain access to an endpoint. Employees open malicious attachments thinking they are legitimate and unwittingly allow attackers to perform malicious actions. With BlackBerry Cylance solutions, weaponized

[3] https://threatpost.com/threatlist-ransomware-attacks-down-fileless-malware-up-in-2018/136962/

BlackBerry Cylance Solutions	Organization Benefit
AI **identifies and blocks malicious applications**, even those never seen before, from executing on endpoints	Organizations dramatically decrease the likelihood that business is impacted by a **zero-day attack**
Static, machine learning, and custom rules **identify and block advanced threats**	Organizations **reduce dwell time** and the impacts of potential breaches
Playbook-driven workflows automate investigation and response, ensuring appropriate actions are always taken	Organizations drive **consistent levels of security** no matter the security staff skill-level
An AI-driven **prevention-first approach to EDR** thwarts most attacks before they have an opportunity to execute	Organizations **save significant time and money** associated with recovering from a successful attack
An advanced toolset **detects and mitigates insider threats,** fileless attacks, and suspicious lateral network movement	Organizations quickly **detect, prevent, and investigate threats to gain profound insight** into the methods and motivations of attackers

Information is a key asset for protecting infrastructure and preventing breaches. Analysts who understand the tactics, techniques, and procedures (TTPs) of cyber attacks are better prepared to stop them.

attachments are identified and blocked automatically. For example, if an attached document includes a VBA macro our solutions deem risky, it will be blocked from executing.

External Devices

USB storage devices are widely used by many organizations. However, they pose significant risks to environments when infected with malware or misused to transfer sensitive data outside of the business. To combat this risk, BlackBerry Cylance solutions have built-in device usage policy enforcement. We limit the dangers posed by USB and other portable data storage by allowing administrators to control which devices connect to their environment.

System admins can investigate and mitigate a potential breach by insider threats by using our Windows logon event visibility feature. This feature enables each endpoint to detect and record details related to Windows logon events, including IP addresses, domains, and time signatures. Security admins can analyze logon information to streamline their permission processes, monitor users across multiple systems, or track suspicious activity.

Uncover Hidden Threats

Detecting malicious activity is key to preventing a breach. This task becomes difficult when threat actors mimic the behaviors of legitimate users by accessing the same tools and resources. Many cybersecurity solutions rely on alerting system admins when suspicious activity occurs. If the threshold for triggering an alert is set too low, the IT staff is quickly overwhelmed by false alarms. If the threshold is set too high, security analysts risk missing an impending attack altogether.

BlackBerry Cylance solutions streamline the investigation process by providing immediate access to forensically relevant data stored on the endpoint. Security analysts can gather the critical information related to an alert and quickly determine whether an incident is serious or benign. For in-depth investigation, our tools allow endpoints to record how DNS queries occurred, including the time, domain, and IP address of the requestor. We also provide features like RFC 1918 address space visibility to facilitate the tracking of lateral movement across networks.

Investigate Attack and Alert Data

Information is a key asset for protecting infrastructure and preventing breaches. Analysts who understand the tactics, techniques, and procedures (TTPs) of cyber attacks are better prepared to stop them. BlackBerry Cylance security solutions uncover hidden threats by capturing the critical forensic data attackers leave behind. For example, the Focus View feature in CylanceOPTICS generates a timeline of system activity leading up to an attack. Collecting individual endpoint data offers additional context of suspicious activity and provides a broader overview of an incident. Your security team can analyze collected data to discover how your environment was exploited and fix any outstanding vulnerabilities.

SEVERITY	DETECTION	DETECTED ON	DETECTION ID	DEVICE	STATUS	DETAILS
Low	Process Without Common Executable Extension	2019-02-01 20:39:14 Z	D0F4-541C	MSEDGEWIN10	New	View
Low	Process Without Common Executable Extension	2019-02-01 20:39:14 Z	1384-4416	MSEDGEWIN10	New	View
Low	One-Liner ML Module	2019-02-01 18:07:12 Z	56E5-86CF	MN-PS-CLT8W62	New	View
Low	Process Without Common Executable Extension	2019-02-01 20:39:14 Z	D0F4-541C	MSEDGEWIN10	New	View
Low	Process Without Common Executable Extension	2019-02-01 20:39:14 Z	1384-4416	MSEDGEWIN10	New	View
Low	One-Liner ML Module	2019-02-01 18:07:12 Z	56E5-86CF	MN-PS-CLT8W62	New	View

CylanceOPTICS automates the critical task of searching for suspicious artifacts across endpoints and enterprises.

Use Indicators of Compromise (IOCs) To Find Threats

Threat hunting, at its core, is hypothesis testing. Security analysts form a hypothesis then perform a series of investigations (using IOCs or other terms) to verify or debunk their theory. BlackBerry Cylance gathers both current and historical endpoint data, giving your analysts critical information for evaluating risks. Unlike other tools that store every piece of data from an endpoint, BlackBerry Cylance solutions preserve only forensically relevant data. This allows your security team to focus on actionable information and avoid sifting through mountains of irrelevant data.

Static, Machine Learning, and Custom Rules

CylanceOPTICS automates the critical task of searching for suspicious artifacts across endpoints and enterprises. It does this by deploying trained AI-models directly on the endpoint, empowering each device to perform detection and response activities. Allowing endpoints to function as independent SOCs eliminates threat response latency and prevents or reduces the impact of security breaches.

The context analysis engine (CAE) is a driving force behind CylanceOPTICS. It enables security analysts to create their own security rules or select pre-made ones, including those which map to the MITRE ATT&CK Framework. Security professionals can use the CAE to develop customized detection and response rules and then deploy them to endpoints within the environment.

Take Response Action

It is important for organizations to have effective threat response capabilities. Responding to the early phases of an attack can greatly minimize the impact of a security breach. With CylanceOPTICS, your security team can create automated playbooks of threat response actions that launch when specific conditions are met. Automated playbooks eliminate dwell time and ensure your organization maintains consistent, fast, and effective threat response across the environment.

For example, security analysts can isolate endpoints that trigger automated responses for further analysis. Investigating devices that report suspicious activity can offer insight into the TTPs of attackers or highlight hidden vulnerabilities in the environment. Focusing on relevant data while allowing the endpoints to handle first-wave threat response makes your security posture more efficient and effective.

The Benefits of BlackBerry Cylance Cybersecurity

Our AI-driven solutions will save your organization time and money by predicting and preventing zero-day threats, advanced attacks, and data breaches[4]. Fewer breaches mean lower costs for system remediation and fewer system re-images. Automating enterprise and endpoint security with our AI-driven solutions allows your IT and security staff to focus on other business needs.

[4] https://www.adapture.com/blog/cylance-forrester-report/

BlackBerry Cylance security tools are easy to deploy and deliver benefits that translate directly into financial gains. For example, one organization switched to BlackBerry Cylance and experienced[5]:

- **Improved cybersecurity team productivity:** One employee uses CylancePROTECT and CylanceOPTICS to monitor and respond to issues in the environment, a task that once required the entire team. Now, the cybersecurity team proactively focuses on threat hunting and addressing other business-critical needs.
- **Reduced lost time by 95% via faster investigation and remediation:** Fewer end-users are compromised. Faster threat investigation and remediation allows end-users to quickly resume productive work.
- **Reduced machine re-imaging by 97%:** The organization takes fewer machines offline for re-imaging. Less re-imaging and shorter end-user downtime mean more IT resources are available for reallocation.
- **Decommissioned legacy on-premises endpoint security solution, saving $8.4 million (present value):** The organization fully decommissioned its legacy on-premises endpoint security solution after deploying the BlackBerry Cylance software-as-a-service (SaaS) solution.

Switch To Smarter Security Today

BlackBerry Cylance can enhance existing solutions with AI-driven prevention technology or serve as a full cybersecurity replacement. Our expert consulting services simplify transitioning to BlackBerry Cylance solutions by assisting with deployment and implementation, optimization, or any of your security staff augmentation needs.

Let our AI-driven solutions move your organization to a prevention-first security posture and handle the repetitive tasks currently exhausting your IT and security resources and staff.

For more information, visit us at https://www.cylance.com/en-us/solutions/use-case/ai-driven-edr.html.

[5] https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/ForresterTEI-CylancePROTECTandCylanceOPTICS.pdf?kui=pz-UectBOAQ9D-bcsm1qPOQ

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.

BlackBerry
CYLANCE

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