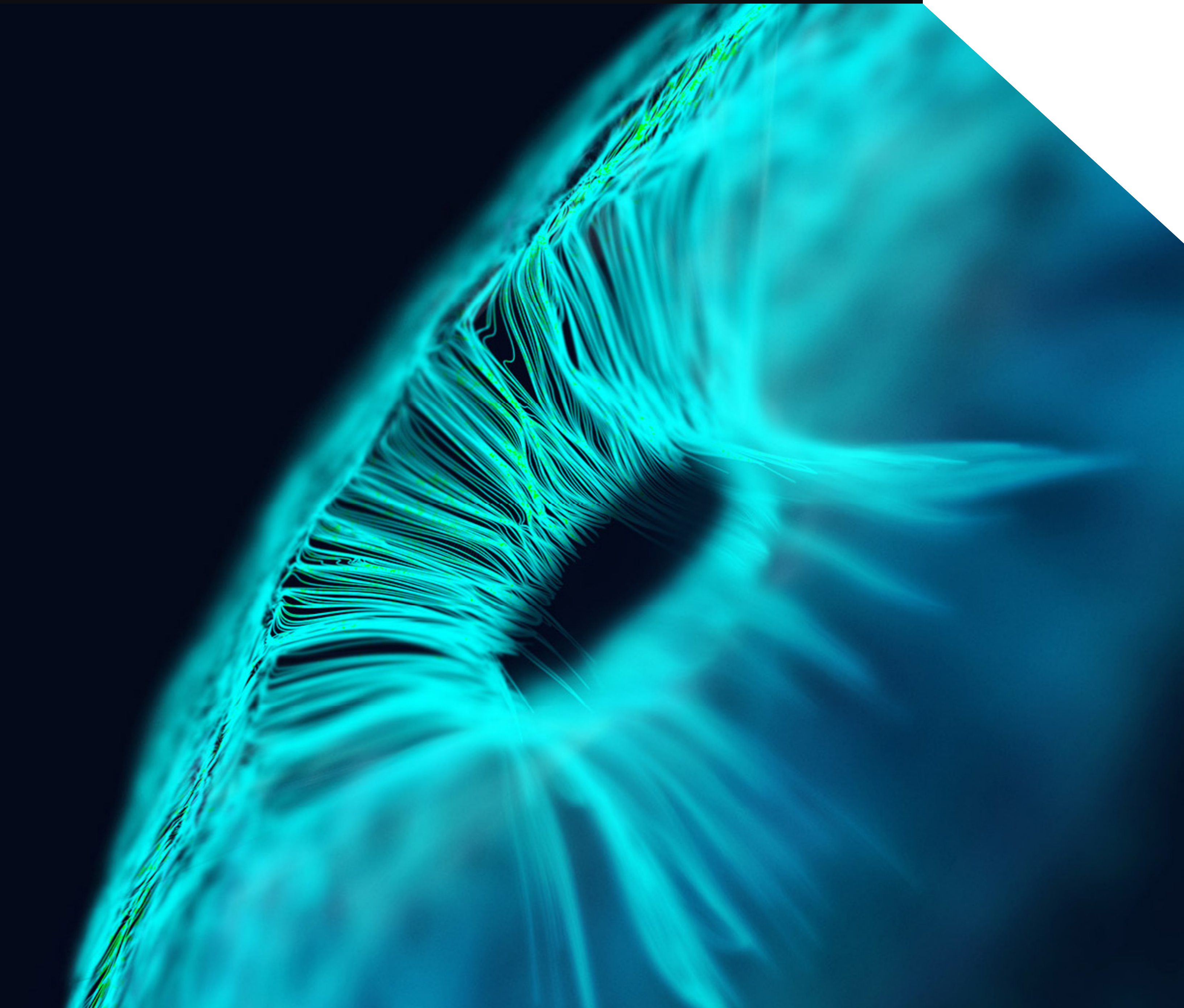
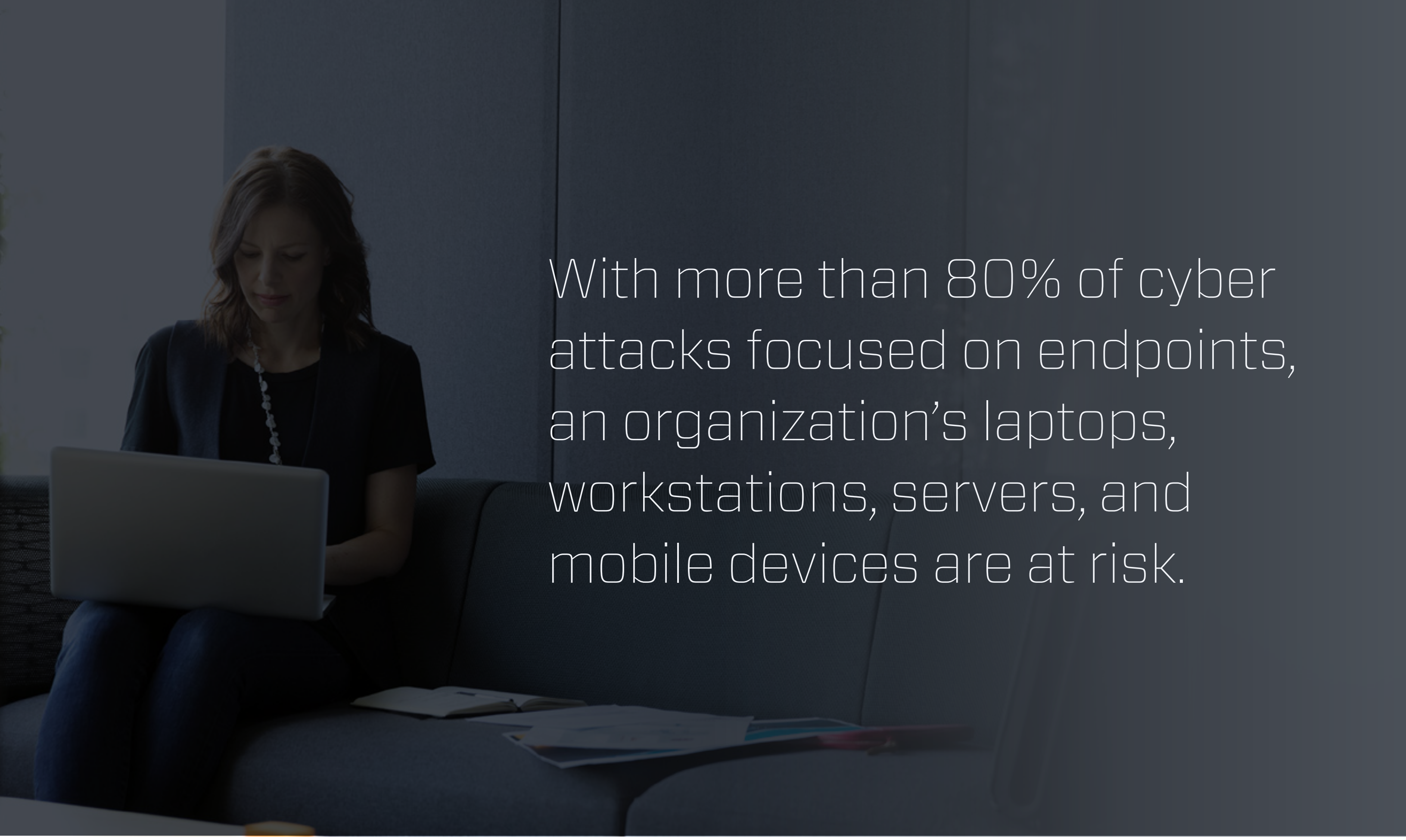
SOLUTION BRIEF

BlackBerry® Cylance® Prevention-First Security with CylancePROTECT® and CylanceOPTICS®

AI-Powered Threat Prevention, Endpoint Detection, and Response





With more than 80% of cyber attacks focused on endpoints, an organization’s laptops, workstations, servers, and mobile devices are at risk.

Prevention-First Security

With more than 80% of cyber attacks focused on endpoints, an organization’s laptops, workstations, servers, and mobile devices are at risk. For years, endpoint security products’ primary threat protection was based on signatures, created after patient zeros were impacted and the damage already done. Assuming all attacks had been seen before, using signatures made sense. Today, malware mutates daily, even hourly, making signature-based prevention tools obsolete, and creating the need for a stronger prevention-based approach to endpoint security. This has given rise to the security in-depth approach provided by endpoint protection platforms (EPP). EPPs provide the depth of protection to stop breaches, and the visibility to detect malicious activities and quickly respond to stop the attack.

BlackBerry Cylance security solutions proactively reduce risk from cybersecurity threats through a predictive, native AI platform that delivers enterprise-ready products and services across the prevention, detection, and response spectrum. This EPP solution has a lightweight single agent and single installer, and is managed in a single window.

With BlackBerry Cylance, organizations get AI-driven automated threat prevention, detection, and response as part of the BlackBerry Spark® unified endpoint security platform that is built from the ground up to easily scale as organizations grow.

Meeting Security Requirements— Use Case Summary

The following are examples of common security use cases that BlackBerry Cylance prevention-first security solutions addresses:

Prevent Successful Attacks

Malware, zero-day, ransomware, script-based, fileless, memory, and external device-based attacks

The best way to protect endpoints from attackers is to identify and stop the attack before it ever starts. At the core of BlackBerry Cylance's unprecedented malware identification capability is a revolutionary machine learning research platform that harnesses the power of algorithmic science and AI, and is backed with human intelligence consisting of a large data science team with multiple Ph.D.s, patents, and a substantial R&D commitment to data science.

Within a matter of milliseconds, BlackBerry Cylance's prevention model analyzes and classifies millions of characteristics per file, breaking them down to an atomic level to discern whether an object is good or bad and preventing malware from executing on endpoints. BlackBerry Cylance's mathematical approach to malware identification utilizes the machine learning techniques versus reactive signatures and sandboxes. This innovative technique renders malware, ransomware, viruses, bots, and zero-day attacks useless in real time at machine speed.

Fileless Malware

Fileless attacks are on the rise as attackers realize the ease with which legitimate admin tools and memory can be used to compromise a system without writing any files to the disk. Many security products have no ability to prevent these types of attacks, but with BlackBerry Cylance solutions, memory-exploit prevention, script management, and the fileless-threat-detection modules block these attacks before they have a chance to impact the business. When an attacker attempts to escalate privileges, undertake process injection, or make use of an endpoint's memory inappropriately by other means, BlackBerry Cylance solutions can detect and prevent it immediately.

Capabilities at a Glance

CylancePROTECT®	CylanceOPTICS®
Advanced AI malware prevention	Context-driven threat detection
Memory exploitation prevention	On-demand root cause analysis
Device policy enforcement	Enterprise-wide threat huntivng
Safeguard against script-based attacks	Automated playbook-driven response
Application control for fixed-function devices	Remote investigation and remediation

Malicious Scripts

Scripts are a favorite choice for many attackers for several reasons. First, for novice attackers, malicious scripts are readily available in the cyber crime underworld, which makes it easy to find one that meets the attacker's needs. Additionally, scripts are often difficult for security products to detect, as there are many legitimate uses for scripts. With BlackBerry Cylance solutions, organizations get built-in script management, meaning security professionals maintain full control of when and where scripts are run in their environment, reducing the chances that an attacker can use this attack vector to cause harm to the business while still allowing their legitimate use.

A few operational enhancements include additional whitelisting capabilities that can block a script unless it is run in a specific application, the ability to cluster identical

BlackBerry Cylance Solutions	Organization Benefit
Use AI and ML to identify and **block malicious applications**, even those never seen before, from executing on endpoints	Dramatically decrease the likelihood that business is impacted by a **zero-day attack**
Combine static, machine learning, and custom rules to **identify and block advanced threats**	**Reduce dwell time** and the impacts of potential breaches
Automate investigation and response with playbook-driven workflows, ensuring appropriate actions are always taken	Drive **consistent levels of security** no matter the security staff skill-level
Thwart attacks before they have an opportunity to execute using an AI-driven **prevention-first approach to EDR**	**Save significant time and money** associated with recovering from a successful attack

malicious scripts, and an added counter, so now, when a malicious script runs, reporting will show the number of times that script has run. Coverage and visibility have also been expanded by adding script engine support for Python, Dotnet DLR (Iron Python), and JavaScript.

Malicious Email Attachments

Phishing attacks are one of the most effective ways attackers gain access to an endpoint. Employees unwittingly open malicious attachments, thinking they are legitimate and enable attackers to undertake any number of malicious actions. With BlackBerry Cylance solutions, weaponized attachments are identified and blocked automatically. If a document, for example, includes a VBA macro deemed to be risky, it will be blocked from executing. This protection adds an additional layer of security, protecting employees from becoming the victim of an attacker and introducing a compromise to the environment.

External Devices

USB devices are littered across most organizations. Most of these devices are useful tools, enabling employees to share files with others quickly and efficiently. However, these devices can cause significant damage to environments if they are loaded with malware or are used to transfer sensitive data outside of the business. To combat this risk, BlackBerry Cylance solutions have built-in device usage policy enforcement. This capability allows administrators to control which devices can be used in their environment. This ultimate control limits the chance that an external device enables an attacker to successfully execute an attack or exfiltrate data.

Restrict Network Access Based on the User's Role

Role-Based Access Control (RBAC)

RBAC improves operational efficiency, enhances compliance, improves an administrator's visibility and oversight into the business, reduces costs, and minimizes risk of a data breach. BlackBerry Cylance allows administrators to customize roles and permissions and easily add new employees with no impact to users. Quickly restrict access to only what employees need to access to do their jobs and nothing more.

Investigate Attack and Alert Data

Perform Root Cause Analysis and Data Collection To Determine the Origin of the Attack

Stopping a threat from impacting endpoints is critical to ensuring sensitive data remains secure. Going one step further, when a threat is thwarted, critical data is captured so security professionals can see how an attacker attempted to compromise the endpoint. BlackBerry Cylance solutions deliver this capability, not only for blocked attacks but for any potential threat that may be found on endpoints. With a simple click, the timeline of activities that led up to the threat, known as a Focus View, can be generated. Additionally, data can be remotely collected from the impacted endpoint to gain further insight into the attempted attack or suspicious activity. This provides an understanding of how the attacker attempted to exploit the environment, so steps can be taken to ensure any vulnerability or gap in security controls can be addressed.

Perform Targeted Threat Hunting

Uncover Hidden Threats

Some malicious activities are easy to identify, while others are anything but cut and dry. When a computer begins to behave irregularly, or it is determined that an endpoint may be at risk of compromise, it is critical that an organization's security toolkit gives it the visibility required to make definitive judgments. BlackBerry Cylance solutions provide immediate access to the forensically-relevant data stored on an endpoint. Within moments of a suspicious activity being identified, searches can be targeted to the exact threat being investigated.

Use Indicators of Compromise To Find Threats

Threat hunting can be described as the act of forming a hypothesis and then running a series of searches and investigations, using IOCs or other terms, to either prove or disprove that hypothesis. Having access to the right data is at the essential core of performing this skill effectively. Targeted threat hunting with refined results is possible with BlackBerry Cylance solutions, delivering access to both current and historical endpoint data. Unlike other tools that store every piece of data from an endpoint, BlackBerry Cylance solutions store only the forensically-relevant data, meaning security teams won't have to spend time sifting through mountains of irrelevant information to find threats.

Context-Driven Threat Detection

Static, Machine Learning, and Custom Rules

There are several ways to identify potential threats and compromises. First, security analysts can perform searches across endpoints to identify suspicious artifacts, and through manual investigation, determine that a threat exists. While there is tremendous value in this process, it simply does not scale across an enterprise. To root out threats hidden on endpoints, an automated approach to threat detection must be used.

The power of CylanceOPTICS comes from the unique and efficient way threat detection and response capabilities are delivered. Unlike other EDR products that rely on cloud-based analysis to uncover threats and security analysts for response, CylanceOPTICS pushes all detection and response decisions down to the endpoint, eliminating response latency that can mean the difference between a minor security event and a widespread, uncontrolled security incident.

The Context Analysis Engine, the driving force behind CylanceOPTICS threat detection and response, enables security analysts to choose from a wide variety of default detection rules developed by BlackBerry Cylance security specialists, including a package of rules that map to the MITRE ATT&CK Framework, or create their own custom rules that meet specific business needs. Analysts can also choose to deploy machine learning threat detection rules to the endpoints to uncover threats that would be difficult, if not impossible, to uncover with static rules.

Take Response Actions

Even with security controls in place, no business can guarantee that every single attack can be stopped. This means organizations must be prepared to respond when an attack is detected. With BlackBerry Cylance solutions, enterprises get fully integrated automated incident response capabilities.

Each rule, whether static, machine learning, or custom, can be configured with a playbook to initiate a set of discrete response tasks automatically if the rule is triggered. The playbook-driven response capabilities assist organizations in eliminating dwell-time by ensuring threat responses are fast and consistent across the environment regardless of the skill-level of the on-duty security personnel.

If an attack is detected, a response can be initiated automatically, with no human intervention. If further responses are required, the item in question can be quarantined and the endpoint can be locked down, disabling its ability to communicate with any other endpoints.

Forensic data from the impacted endpoint can be collected to gain further context about the incident. Identifying a security concern is important but having the ability to respond automatically is a necessity. With BlackBerry Cylance solutions, organizations have that ability.

True endpoint security does not come from prevention or detection. To combat today's attacks, organizations must have strong prevention and detection capabilities in place to keep pace with attackers. With BlackBerry Cylance solutions, enterprises get the best of both worlds, maximizing the return on security stack investments, making analysts more efficient, and making the business more secure.

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