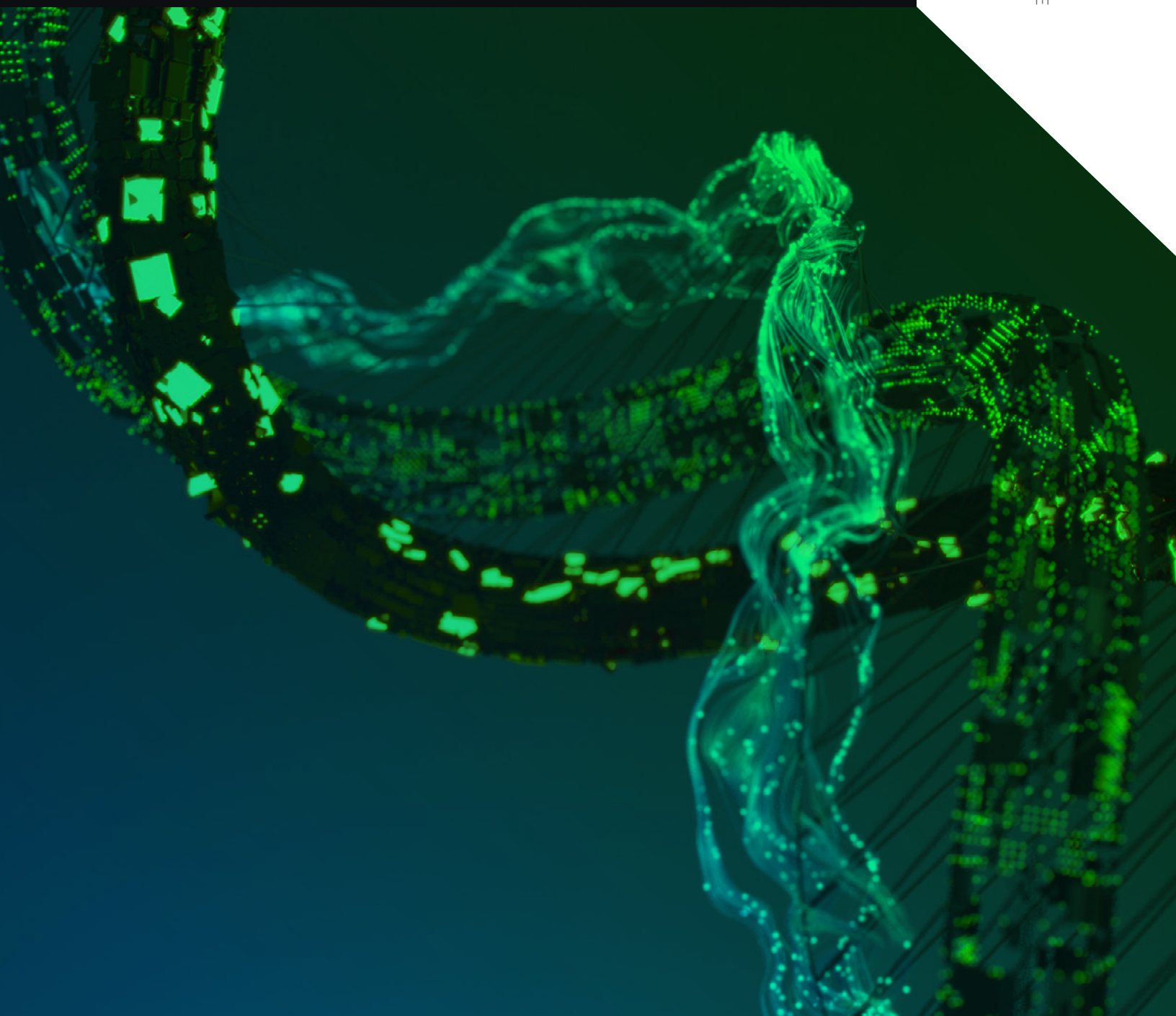


BlackBerry® Cylance® Products and Services

Prevent Cyber Attacks with Artificial Intelligence

OVERVIEW BROCHURE



CylancePROTECT®

Continuous Threat Prevention Powered by AI

Future-Proof Endpoint Security

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.

BlackBerry Cylance has redefined what an endpoint protection solution can and should do for organizations with an automated, prevention-first approach. It is the most accurate, efficient, and effective solution for preventing advanced persistent threats and malware from executing on an organization’s endpoints. CylancePROTECT prevents breaches and provides additional security controls to safeguard against script-based, fileless, memory, and external device-based attacks. CylancePROTECT does this without user or admin intervention, a cloud connection, signatures, heuristics, or sandboxes.

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 artificial intelligence (AI). 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 machine learning techniques versus reactive signatures and sandboxes. This innovative technique renders malware, ransomware, viruses, bots, or zero-day attacks useless in real time at machine speed.







Common CylancePROTECT Use Cases

CylancePROTECT provides full-spectrum threat prevention that stops endpoint breaches by solving these use cases:

- Identify and block malicious executables without the need for constant updates or a cloud connection
- Controlling where, how, and who can execute scripts
- Manage USB device usage and prevent unauthorized devices from being used
- Stop fileless malware attacks
- Lock down fixed-function devices such as kiosks, POS terminals, etc.
- Prevent zero-day and ransomware attacks
- Stop memory-based attacks and exploitations



CylancePROTECT Features

True Zero-Day Prevention  Resilient AI model prevents zero-day payloads from executing.	Device Usage Policy Enforcement  Controls which devices can be used in the environment, eliminating external devices as a possible attack vector.
AI-driven Malware Prevention  Field-proven AI inspects any application attempting to execute on an endpoint before it executes.	Memory Exploitation Detection and Prevention  Resilient AI model prevents zero-day payloads from executing.
Script Management  Maintains full control of when and where scripts are run in the environment.	Application Control for Fixed-Function Devices  Ensures fixed-function devices are in a pristine state continuously, eliminating the drift that occurs with unmanaged devices.

Benefits

- **Comprehensive Security**
Full-spectrum autonomous threat prevention simplifies the security stack
- **Smooth Business Operations**
Whisper-quiet prevention ensures business operations are not disrupted
- **Zero-Day Payload Prevention**
Eliminates the risk of an attack exploiting a zero-day from being successful



CylanceOPTICS™

AI-Powered Endpoint Detection and Response

The Case for Prevention-First Security

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 EDR solution designed to extend the threat prevention delivered by CylancePROTECT by using AI to identify and prevent 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.

Common CylanceOPTICS Use Cases

- **Prevent Malicious Activity:** CylancePROTECT, which provides the foundation for CylanceOPTICS, is designed to specifically prevent successful attacks aimed at endpoints.
- **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 indicators of compromise 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 Incident Response:** Users can retrieve critical forensic information from impacted endpoints, as well as take aggressive containment actions when a harmful endpoint is discovered. The solutions also can automatically trigger response actions if a pre-defined rule is triggered.



CylanceOPTICS Features

AI-Driven Incident Prevention  Uncover threats that would be difficult to identify with behavior rules using machine learning threat detection modules	Enterprise-Wide Threat Hunting  Easily search endpoint data for suspicious/malicious activity to uncover hidden threats
Consistent Cross-Platform Visibility  Detect and prevent incidents across Microsoft Windows® and Apple MacOS® platforms	Dynamic Threat Detection  Automate threat detection, in real time, using custom and curated behavior rules running on the endpoint
On-Demand Root Cause Analysis  Understand how attacks entered the environment so corrective actions can be taken, reducing the attack surface	Automated, Fast Response  Customize automated response actions to minimize the risk of a widespread incident

Benefits

- **Reduce Alert Volume**
Reduce security alert volume with full-spectrum threat and incident prevention, improving team efficiency
- **Gain Situational Awareness**
Understand the attack surface across the environment, eliminating potential weaknesses
- **Relieve the Strain on Security Teams**
Automate responses to identified threats 24x7, without disrupting the security team



Cylance Smart Antivirus™

The Protection of CylancePROTECT
Beyond the Corporate Firewall

Protect Employees at Home

The virtual borders of a corporate network are no longer defined by the corporate firewall. With the proliferation of work and personal devices at home, the distinction between the corporate network and employees' home networks has become blurred. CISOs and their security teams have a difficult time controlling their security risk and exposure from cybersecurity threats originating from employees' homes.

Have you considered:

- 67% of workers use their own personal devices while at work
- 37% of U.S. workers telecommute regularly
- Cloud-based solutions (Office365, DropBox, Box, Trello, Atlassian, etc.) allow employees to access corporate assets from personal devices
- Employees can connect USB thumb drives to personal devices infected with malware, then plug them into a company device
- Employees can access corporate email on personal devices
- Telecommuters can VPN into work from a personal device
- Cached credentials from employees logging into company assets from a personal device can be stolen by malware
- Webcam-enabling malware on a personal device can spy on and compromise employees

BlackBerry Cylance has redefined what antivirus can and should do by using artificial intelligence to predict and protect enterprise organizations against malware. With Cylance Smart Antivirus, that same groundbreaking enterprise technology is available for corporate employees to use at home to protect their family's personal devices.

Organizations offering Cylance Smart Antivirus to their employees to protect their personal Windows and Mac devices enable the company's security team to extend their perimeter protection and reduce their attack surface without infringing on an employee's privacy, or managing their personal devices.

Smart, Simple Security

Cylance Smart Antivirus:

- Is the first next-generation consumer security product that uses artificial intelligence to predict and block future, unknown variants of malware, offering better protection than any existing traditional antivirus solution
- Does not bog down systems with the bloated, system-slowing, noisy, and pop-up-riddled experience associated with traditional consumer security products
- Is easy to install, easy to manage and configure, updates itself automatically, and protects consumer devices for a set-it-and-forget-it security experience
- Empowers the technical expert in the family with the visibility and awareness of the security status of all devices in the family's environment
- Ensures the employee's family and/or remote loved ones' (elderly parents, college kids, etc.) devices are safe, secure, and protected



How It Works

Cylance Smart Antivirus uses BlackBerry Cylance's patented mathematical approach, utilizing machine learning techniques instead of reactive signatures and sandboxes to render malware, viruses, bots, and unknown future variants incapable of executing.

Corporate employees using Cylance Smart Antivirus will have access to their own personal cloud console where they will have visibility and the ability to manage protection for up to 10 devices for their family, extended family, and loved ones.

Unlike with traditional antivirus software, Cylance Smart Antivirus users do not need to worry about checking to see if they have the latest signature file updates multiple times per day. The product automatically updates itself with new features, eliminating the need to worry about outdated software, constant updates, and patches.

Compatible with Microsoft Windows and macOS

Cylance Smart Antivirus is compatible with the latest versions of Microsoft Windows and macOS laptops and desktops.


Windows 7
Windows 8 and 8.1
Windows 10

2GB Memory

500MB Available
Disk Space

REQUIRES
Microsoft .NET
Framework 3.5 SP1
Internet browser
Internet connection
to register product
Local admin rights
to install software


OS X Mavericks
OS X Yosemite
OS X El Capitan
macOS Sierra
macOS Catalina

2GB Memory

500MB Available
Disk Space

REQUIRES
Internet browser
Internet connection
to register product
Local admin rights
to install software



ThreatZERO™

Delivering Provable Prevention

Ensure Maximum Value

While implementing new security solutions can be exciting for a company, optimizing them for specific environments can put a stress on already limited IT resources. The need to protect, identify, and act on progressive threats can be challenging for even the most experienced security teams. Cylance Consulting's proven methodologies ensure maximum value and security are achieved as quickly as possible with little to no disruption to systems or vital processes.

ThreatZERO experts provide a refreshing mix of technological expertise and personalized white glove service to optimize CylancePROTECT and CylanceOPTICS and move environments into prevention while providing measurable results of progress throughout the process.

Cylance Consulting offers:

- **ThreatZERO (Foundational)** — Complete implementation and operationalization of CylancePROTECT and CylanceOPTICS
- **Managed Prevention** — Foundational ThreatZERO coupled with subscription-based monthly or quarterly maintenance to ensure environments stay in prevention

- **ThreatZERO + Compromise Assessment** — Foundational ThreatZERO coupled with a Compromise Assessment to reveal previous or potential indicators of compromise
- **ThreatZERO Resident Expert** — Dedicated, on-site staff augmentation resources help deploy, manage, and operationalize CylancePROTECT and CylanceOPTICS
- **ThreatZERO Training** — Best practices solution training for product administrators and users to optimize security, maintenance, and return on investment

“ThreatZERO was very useful. If you don’t understand a product, you end up only using 10% of its capabilities. We got the knowledge we needed to use all the products’ features to optimize our environment. Now our team can focus on other problems.”

– Robert Osten, IT Manager, Formel D



Benefits

- Accelerated pathway to prevention from cyber attacks
- Measurable prevention is demonstrated throughout the process
- Expert solution tuning for CylancePROTECT and CylanceOPTICS
- Reduced overhead through expert guidance and knowledge transfer to staff
- Separates the signal from the noise of commodity malware and adware
- Maintains prevention status through quarterly maintenance and remediation
- Advanced EDR tuning to provide visibility into TTPs and interesting artifacts



Consulting Services

Let Us Prove Prevention Is Possible

Delivering the Outcome of Prevention

Cylance Consulting is a world-class cybersecurity solutions provider to organizations around the globe. Cylance Consulting helps our clients address cybersecurity concerns and challenges of all types, working together to construct a strong and effective security posture utilizing Cylance Consulting's prevention-first methodologies. Cylance Consulting's industry-leading experts provide the technical expertise needed to effectively analyze cybersecurity requirements and to design comprehensive solutions to meet goals and objectives. Cylance Consulting's number one priority is to secure our clients as quickly as possible using advances in automation, including artificial intelligence and machine learning.

Cylance Consulting Services

Incident Response and Containment

Provide faster and more accurate results to quickly contain and remediate incidents using AI-driven products.

- Compromise Assessment
- Incident Containment and Retainers
- IR Tabletop Exercises
- Malware Analysis
- Disk and Memory Forensics

Red Team Services

Identify, prioritize, and manage risk through assessments and social engineering to secure environments.

- Attack Simulation Services
- IoT / Embedded Systems

Strategic Services

Align cybersecurity initiatives with the organization's business interests and operational needs.

- Incident Response Program Development
- vCISO Services
- Prevention Program Review
- Strategic Technology Assessment
- NIST CSF Gap Analysis

Education

Empower defenders and protectors with knowledge to find and respond to attackers.

- ENGAGE and ENABLE Solution Training
- Cylance Security Professional Accreditation
- Incident Response Technical Training
- ThreatZERO Knowledge Transfer
- A Guide To Threat Hunting Using ELK Stack and Machine Learning



Benefits

- Achieves prevention with measurable results of the progress
- Artificial intelligence incorporated into tools and methodologies
- Best-in-class consultants based around the world
- Prevention-first methodologies improve security posture and reduce costs
- Engagement managers are dedicated to lead every project

 **BlackBerry**
CYLANCE.

CylanceGUARD™

24x7 Advanced Threat Hunting

AI-Powered Threat Hunting

CylanceGUARD is a 24x7 threat hunting solution that provides actionable intelligence for customers to prevent threats quickly, while minimizing alert fatigue and reducing resource requirements. Through mobile alerts and interaction, companies will have proactive alerting at their fingertips, with delivered context to streamline investigations through interaction with BlackBerry Cylance to respond. Leveraging skilled threat hunting experts and using the visibility provided by CylancePROTECT and CylanceOPTICS gives organizations a comprehensive solution for prevention.

BlackBerry Cylance offers two levels of CylanceGUARD. CylanceGUARD provides a foundation that can be built upon to allow the immediate maturation of an organisation's security position. CylanceGUARD Advanced is a comprehensive solution delivered by BlackBerry Cylance that meets all the resource requirements an organisation needs for threat hunting. Both offerings leverage the pre-execution abilities of CylancePROTECT, the post-execution of monitoring and blocking associated with CylanceOPTICS, and the personalised, white glove onboarding and operationalisation of the security solution by BlackBerry Cylance experts through ThreatZERO.

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.

Benefits

- Prevention-first threat hunting using the power of AI
- BlackBerry Cylance community intelligence shared/leveraged to protect clients
- 24x7 model, leveraging automation and AI web and mobile user interaction
- Transparency into the triage and response actions taken by analysts



CYLANCE
GUARD

For more information on Cylance products, contact:

+1-844-CYLANCE
sales@cylance.com

For more information on Cylance Consulting Services, contact:

+1-877-973-3336
proservices@cylance.com