BlackBerry | CYLANCE

CylancePROTECT®

Continuous Threat Prevention Powered by Artificial Intelligence

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 by utilizing an automated, prevention-first approach. It is an 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.

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

Proactively identifies malicious use of memory (fileless attacks) with immediate automated prevention responses.

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:

- **AI-Driven Prevention** reduces the strain on the endpoint compared to traditional solutions
- **No signatures** mean less human effort to manage
- **No cloud or new hardware required** minimizes total cost of ownership

CYLANCE PROTECT

At the core of the BlackBerry Cylance malware identification capability is a revolutionary machine learning research platform that harnesses the power of algorithmic science and artificial intelligence (AI). The platform is backed with human intelligence consisting of a large data science team with multiple PhDs, patents, and a substantial R&D commitment to data science.

Within a matter of milliseconds, the BlackBerry Cylance 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, and zero-day attacks useless in real time at machine speed.

How It Works

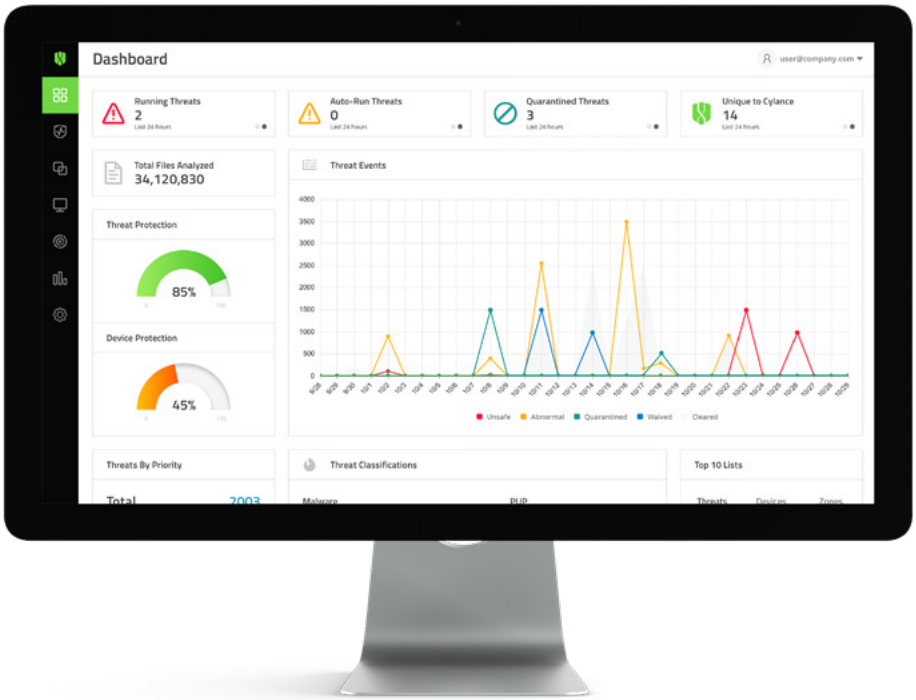
The algorithmic model utilized within CylancePROTECT means there are no signatures, patching, system scans, or slow endpoints due to the security solution running on them. Customers who have made the switch from reactive legacy, signature-based antivirus products see up to a 99% ROI, a 97% reduction in the re-imaging of machines, extended hardware and battery performance, and a 90% reduction in the number of full-time employees needed to manage the solution.[1]

The CylancePROTECT architecture consists of a lightweight single agent that is managed via BlackBerry Cylance's own SaaS-based cloud console. The cloud console easily integrates with existing software management systems and security tools. Hybrid and on-premises management options are available for air-gapped environments. The endpoint agent will detect and prevent malware on the host, independent of a cloud connection and without the need for continuous updates. CylancePROTECT is capable of detecting and quarantining malware in open, isolated, and virtual networks. BlackBerry Cylance's machine-learning-based approach stops the execution of harmful code regardless of having prior knowledge or employing an unknown obfuscation technique. CylancePROTECT is unique in the way it combines exceptional levels of efficacy and effectiveness with ease of use.

Common CylancePROTECT Use Cases

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

- Identify and block malicious executables without the need for constant updates or a cloud connection
- Control 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



Capabilities

Device Usage Policy Enforcement

- Control use of USB mass storage devices
- Prevent data theft via removable media

Role-Based Access Controls (RBAC)

- Minimize risk with more granular role management with custom RBAC
- Improve restrictions to network access based on roles of individual users
- Limit employee access rights to only the information they need to do their jobs
- Benefit from no impact on existing users

Application Control

- Lock down fixed-function devices
- Prevent bad binaries or modification of a binary
- Lock down specified systems and restrict any changes

Memory Protection

- Proactively identify and stop malicious use of memory
- Prevent memory-only attacks such as privilege escalation
- Benefit from granular exclusions and enhanced troubleshooting and reporting

Script Control

- Stop unauthorized scripts from running
- Benefit from granular whitelisting and safelist capabilities
- Support macOS®, Microsoft®, and Linux® operating systems
- Prevent execution of PowerShell one-liners

1 https://www.cylance.com/en-us/company/about-us/our-customers/2019-forrester-tei-report.html#form-anchor

axient

Axient Pty Ltd
Level 6, 28 Clarke Street
CROWS NEST NSW 2065
+61 2 8338 3444
www.axient.com.au

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

MKTG 19-2855-20200220