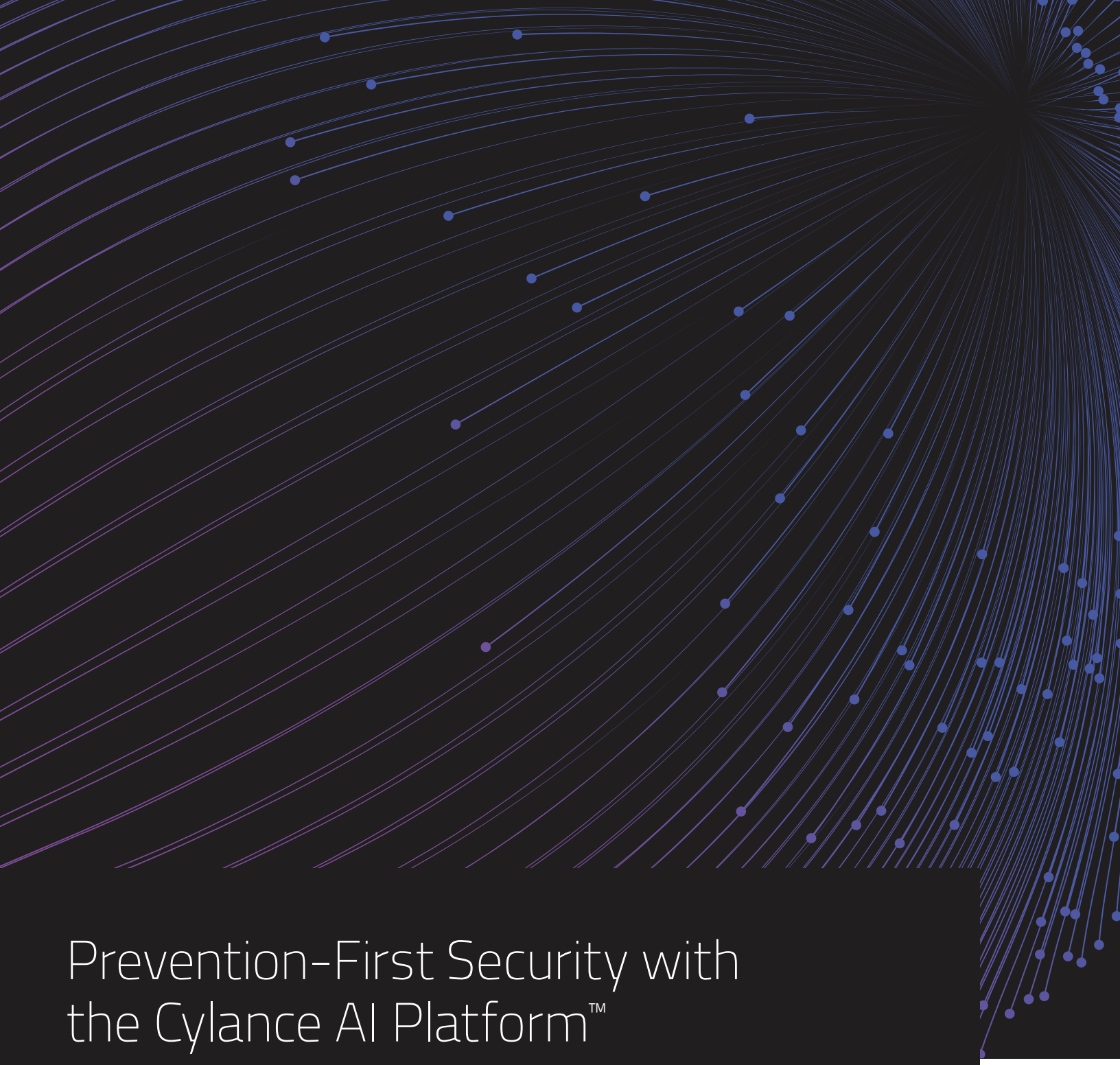

Prevention-First Security with the Cylance AI Platform™

A unified, AI-powered platform delivering threat prevention, endpoint detection, and response

CYLANCE®

Prevention-First Unified Security

Simplifying the endpoint security stack can make any security team's work easier and their efforts far more efficient. The challenge is figuring out a way to transition to a simpler approach without impacting the organization's security posture.

Cylance® helps organizations make this change by delivering a prevention-first endpoint security solution designed to prevent successful attacks while simultaneously reducing the noise generated by the entire security stack.

With the Cylance AI Platform, organizations get artificial-intelligence-driven threat prevention, detection, and response under one unified agent. Built from the ground up to easily implement new security technologies with the scale and needs of business, Cylance's unified solution provides innovative security that delivers real benefits to organizations.

Cylance Unified Solution	Organization Benefit
Use artificial intelligence (AI) to identify and block malicious applications and events, even those never seen before, from executing on endpoints	Organizations can 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	Organizations can reduce dwell time and the impacts of potential breaches
Automate investigation and response with playbook-driven workflows, ensuring appropriate actions are always taken	Organizations can 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	Organizations can save significant time and money while decreasing the time to remediation from an attack

Capabilities at a Glance

Anti-Malware / On-Device Execution	Machine Behavior / Threat Hunting / Response	User Behavior
AI-driven malware prevention	Static behavior rule threat detection and response	AI personal assurance
Memory exploitation prevention	On-demand root cause analysis	Account takeover prevention
Device policy enforcement	Enterprise-wide threat hunting	Persona conduct baselining
Script management	Automated ML-built playbook response	Proactive persona risk response
Application control for fixed-function devices	Remote investigation and remediation	Flexible two-factor authentication
	Aggressive containment	

Meeting Your Security Requirements—Use Case Summary

The following are examples of common security use cases that Cylance's prevention-first security solutions address:

Prevent Successful Attacks

Malware (Ransomware, Trojans, Adware, Etc.)

The best way to protect endpoints from attackers is to identify and stop the attack before it ever starts. The Cylance AI Platform uses field-proven AI to inspect portable executable files attempting to run on an endpoint before it executes. Within milliseconds, the machine learning model running on the endpoint determines if the executable is malicious or safe. 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 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 the Cylance AI Platform, 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, the Cylance AI Platform will detect and prevent it immediately.

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 the Cylance AI Platform, 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.

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 the Cylance AI Platform, 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, the Cylance AI Platform has 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.

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. The Cylance AI Platform delivers 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. The Cylance AI Platform provides immediate access to the forensically-relevant data stored on any 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/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 capable with the Cylance AI Platform, delivering access to both current and historical endpoint data. Unlike other tools that store every piece of data from an endpoint, the Cylance AI Platform stores 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. One way is for security analysts to 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 Cylance's endpoint detect and response (EDR) built into the Cylance AI Platform 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, the Cylance AI Platform 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 the Cylance AI Platform EDR threat detection and response, enables security analysts to choose from a wide variety of default detection rules developed by 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.

About Cylance

Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. 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, Cylance protects the endpoint without increasing staff workload or costs. We call it the Science of Safe.

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 the Cylance AI Platform, 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 the Cylance AI Platform, 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 the Cylance AI Platform, enterprises get the best of both worlds, maximizing the return on security stack investments, making analysts more efficient, and making the business more secure.

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

CYLANCE

20190225-0162