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

AI Driven Threat and Incident Prevention, Detection, and Response

CYLANCE

Prevention-First Security with CylancePROTECT and CylanceOPTICS

Simplifying the endpoint security stack, without sacrificing security, can make any security team's work easier, and their efforts far more efficient.

Cylance helps maximize the return on security stack investments by delivering prevention-first endpoint security solutions designed to eliminate successful attacks across environments, dramatically reducing the number of relevant alerts generated by the security stack.

With CylancePROTECT and CylanceOPTICS, organizations get *real-time artificial intelligence (AI) driven threat and incident prevention*. Built from the ground up to easily scale with the business, Cylance's solution delivers the following security functionality:

CylancePROTECT	CylanceOPTICS
AI driven malware prevention	AI based incident prevention
Memory exploitation prevention	On-demand root cause analysis
Device and script management	Enterprise-wide threat hunting
Application control for fixed-function devices	Automated threat detection and response

Meeting Your Security Requirements — Use Case Summary

The following are examples of common security use cases that the Cylance Prevention Platform™ addresses:

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. Cylance 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

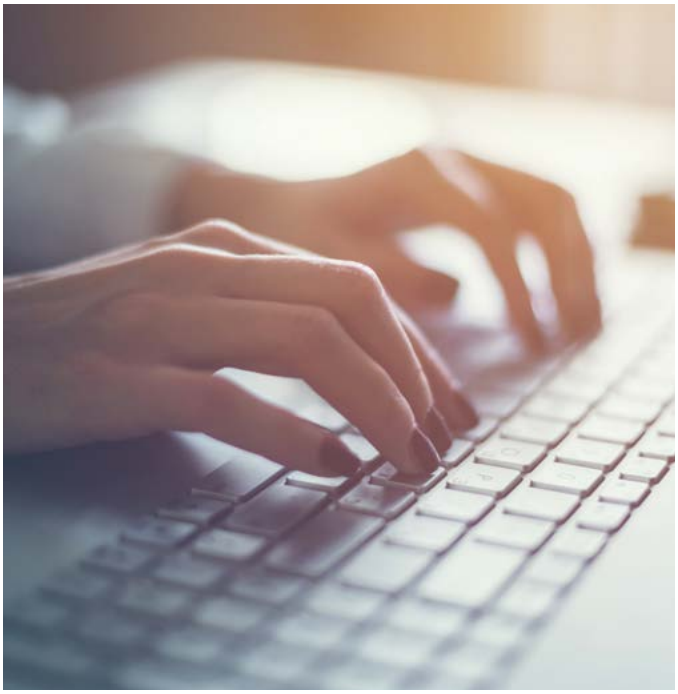
Fileless attacks are on the rise as attackers realize the ease with which legitimate admin tools and memory can be used to compromise a system without writing any files to the disk. Many security products have no ability to prevent these types of attacks, but with Cylance, memory exploit prevention, 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, Cylance will detect and *prevent* it immediately.

Malicious Scripts

Scripts are a favorite tool of choice for many attackers for several reasons. First, for novice attackers, malicious scripts are readily available in the cybercrime 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 Cylance, 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 Cylance, 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, Cylance 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 Forensic 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. Cylance 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, forensic 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. Cylance 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 Cylance, delivering access to both current and historical endpoint data. Unlike other tools that store every piece of data from an endpoint, Cylance stores only the forensically relevant data, meaning security teams won't have to spend time sifting through mountains of irrelevant information to find threats.

Dynamic Threat Detection

Static Rule and Artificial Intelligence Based Detection

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.

Cylance includes a rule based engine deployed on every endpoint, called the Context Analysis Engine (CAE), to identify potential threats automatically. The CAE is a high-performance analysis and correlation engine that monitors events as they occur on an endpoint in near real time to identify malicious or suspicious activities. This 24x7 monitoring occurs with no need for a cloud connection. The CAE includes a set of curated rules provided by Cylance as well as the ability to create customized rules.

While detection rule engines are necessary, it is difficult to model all potential attack behaviors. To that end, Cylance includes AI based incident prevention. Powered by machine learning threat detection modules for the endpoint, Cylance continuously analyzes changes occurring on each endpoint to uncover threats that would be difficult, if not impossible, for a human analyst to uncover in a reasonable amount of time.

When a potential threat is identified, CylanceOPTICS can take decisive actions, in real time, to stop the attack and avoid the cost, risk, and long-term impacts that come with a widespread security incident. The combination of these threat detection capabilities provides broad protection against attacks.

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 Cylance, enterprises get fully-integrated automated incident response capabilities. 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 Cylance, 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 Cylance, enterprises get the best of both worlds in one solution, 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
400 Spectrum Center Drive, Suite 900, Irvine, CA 92618

20180628-1087