CylancePROTECT® and CylanceOPTICS™:

Your AI Driven Threat Prevention, Detection, and Response Solution



CYLANCE™

Simplifying your endpoint security stack while maintaining a secure environment can make your security team's work easier, and their efforts far more efficient. The combined solution of CylancePROTECT and CylanceOPTICS, built on the Cylance Artificial Intelligence (AI) platform, helps you consolidate and distill the security tools your team uses down to a manageable set, in turn reducing redundancies, eliminating high infrastructure expenses, and improving your team's ability to more proactively secure your endpoints.

With CylancePROTECT and CylanceOPTICS, you get *real-time predictive threat prevention* combined with *prevention based detection and incident response*. Built from the ground up to easily scale with your business, the solution delivers the following security functionality:

CylancePROTECT	CylanceOPTICS
AI driven malware prevention	Consistent endpoint visibility
Real-time memory protection	Root cause analysis
Integrated script and application control	Threat hunting capabilities
Device usage policy enforcement	Integrated incident response

Meeting Your Security Requirements — Use Case Summary

The following are examples of common security use cases that CylancePROTECT and CylanceOPTICS help to address and resolve:

Stopping Malicious Activity

Prevent endpoints from executing malicious executables

The best way to protect your endpoints from attackers is to identify and stop the attack before it ever starts. CylancePROTECT uses field proven AI to inspect any application attempting to execute 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 blocked from running, thwarting the attacker's attempt to compromise the endpoint. With over 99% efficacy, CylancePROTECT is the industry's best AI driven malware prevention solution.

Prevent endpoints from executing unauthorized scripts

Scripts are quickly becoming the 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 some security products to detect, as there are many non-threat uses for scripts. With CylancePROTECT, you get built-in script protection, meaning you maintain full control of when and where scripts are run in your environment, reducing the chances that an attacker can use this attack vector to cause harm to your business.

Protect memory from being used by fileless malware

Memory based attacks are on the rise as attackers realize the ease with which memory can be exploited to achieve their goals. Many security products have no ability to prevent these types of attacks, but with CylancePROTECT, memory protection is included. When an attacker attempts to escalate privileges, undertake process injection, or make use of an endpoint's memory inappropriately by other means, CylancePROTECT will identify and prevent it immediately.

Prevent endpoints from executing malicious email attachments

Phishing attacks are still one of the most effective ways attackers gain access to an endpoint and your business. Employees unwittingly open malicious attachments, thinking they are legitimate, and enable attackers to undertake any number of malevolent actions. With CylancePROTECT, 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 your environment.

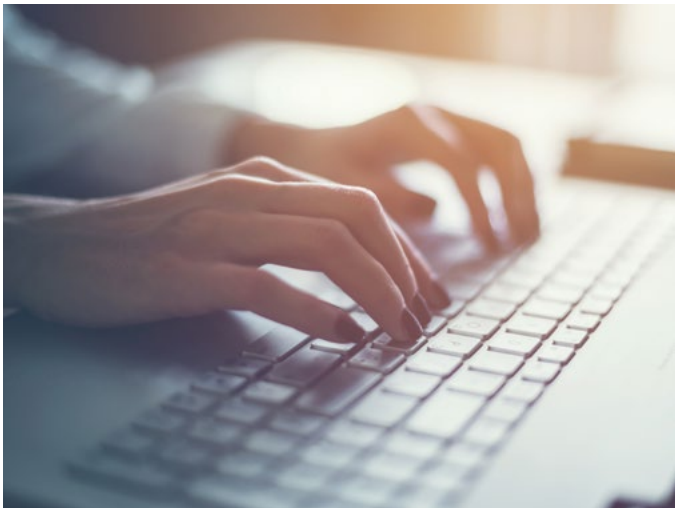


Prevent endpoints from accessing devices identified as malicious

USB devices are littered across your business. 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 your environment if they are loaded with malicious malware or are used to transfer sensitive data outside of your business. To combat this attack vector, CylancePROTECT has built-in device usage policy enforcement. This capability allows you to control which devices can be used in your environment. This ultimate control means that you can limit the chance that a USB device enables an attacker to successfully execute an attack or exfiltrate data.

Incident Response and Containment

No business, no matter what security controls are in place, can guarantee that an attack will never be successful. This means you must be prepared to respond if an attack is detected. With CylanceOPTICS, you get fully-integrated incident response capabilities. If an attack is identified, with just a few clicks, you can quarantine files, disabling their ability to be used anywhere in your environment. If you determine an endpoint is harmful, you can also take an aggressive containment move and lock down the endpoint, disabling its ability to communicate with any other endpoints. Identifying a security concern is important, but having the ability to respond is also critical, and with CylanceOPTICS, you now have that ability.



Suspicious Activity Validation

Malicious activity validation

Endpoints are continuously changing based on how they are being used. Generally, these changes are normal, however when a user, or a security control, indicates malicious activity on an endpoint, it is your team's job to validate. With CylanceOPTICS, you can quickly review identified files, processes, network activity, and more to determine if an endpoint has, in fact, been compromised. With InstaQuery, part of the CylanceOPTICS threat hunting capability, you can interrogate endpoints in seconds, reviewing potentially critical information to determine what steps, if any, should be undertaken to ensure your business remains secure.

Perform root cause analysis to determine the origin of the attack/threat

Stopping a threat from impacting your endpoints is critical to ensuring your sensitive data remains secure. Going one step further, when a threat is thwarted, critical data is captured and stored for future investigations, you can now see how an attacker attempted to compromise your endpoint. CylanceOPTICS delivers this capability, not only for blocked attacks, but for any threat you may find on your endpoint. With a simple click, you can create a Focus View, which generates a timeline of activities that led up to the threat. This means you can see where the attacker attempted to exploit your environment and takes steps to ensure any vulnerability or gap in your security controls is addressed.

Threat Hunting

Review activities that appear suspicious

Some malicious activities are easy to identify, while others are anything but cut and dry. When a computer begins to behave irregularly, or you determine an endpoint may be at risk of compromise through your threat hunting, it is critical that your security toolkit gives you the visibility required to make definitive judgments. With CylanceOPTICS, you have immediate access to the forensically-relevant data stored on any endpoint. Within moments of a suspicious activity being identified, you can hone your search and investigation to target the exact threat for which you are looking.

Incident Data Search and Investigations

Current and historical system state search (including Indicators of Compromise (IOC) searches)

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 what you will see with CylanceOPTICS, delivering access to both current and historical endpoint data. Unlike other tools that store every piece of data from an endpoint, CylanceOPTICS stores only the forensically relevant data, meaning your team won't have to spend time sifting through mountains of irrelevant information to find threats.

Suspicious Activity Detection

Rule based and threat 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, you must use an automated approach to threat detection. In upcoming releases, automated threat detection in CylanceOPTICS will be delivered in two phases:

First, a rule based engine will be incorporated into the solution to notify users, in real time, if an endpoint triggers a threat detection rule. While the solution will be delivered with a set of rules curated by the security experts at Cylance®, your team will also be able to create rules customized to your organization's needs.

For phase two, CylanceOPTICS threat detection will take a giant leap forward with the introduction of AI based threat detection designed to run on the endpoint. Unlike other security technologies that run a form of machine learning from a cloud environment requiring endpoint activity to be streaming to the cloud continuously, the CylanceOPTICS AI threat detection capability runs locally on the endpoint. This ensures that threat detection never stops, even when the endpoint is not connected to the corporate network or a cloud environment. This capability changes the face of threat detection, providing uninterrupted protection.

True endpoint security does not derive from prevention or detection. To face the constant and variable attacks presented by the modern threat landscape, organizations must have both capabilities in place and deeply integrated to keep pace with attackers. With CylancePROTECT and CylanceOPTICS, you get the best of both worlds in one solution, simplifying your security stack, making your analysts more efficient, and making your business more secure.



+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170511-1087