CylanceOPTICS™ Prevention-First EDR

What's New in v2.3

CylanceOPTICS is an endpoint detection and response (EDR) solution that extends the threat prevention delivered by CylancePROTECT® by using artificial intelligence (AI) to identify and prevent security incidents.

CylanceOPTICS provides:

- AI driven incident prevention
- Machine learning assisted threat detection
- On-demand root cause analysis
- Smart threat hunting
- Remote investigation capabilities

What's New in v2.3

CylanceOPTICS Version 2.3 extends the capabilities of the solution with these enhancements:

- **AI Driven Incident Prevention:** Machine learning threat detection modules targeting fileless attacks, malicious/suspicious one-line commands, and malicious application behavior are now incorporated into the Context Analysis Engine, continuously monitoring changes on each endpoint to uncover threats that would be difficult to detect with behavior rules alone (see page 2 for more details).
- **Remote Forensic Data Collection:** Users can now interact with endpoints to retrieve advanced sets of forensic data, execute scripts, or applications to capture critical information related to any suspicious event or security incident.
- **Enhanced Detection Details and Device Lockdown:** Enhanced lockdown and detection details, including:
  - An improved Event Description section to better display the rule's logic in a 'natural language' form.
  - An improved Event Artifact section to include all Artifacts and Facets associated with an event.
  - The ability to select the Lockdown Duration and initiate the Lockdown from the current page/workflow.
- **Device Information Visibility:** Users now have easier access to important information about devices in their environment with the introduction of the Device Drawer, including:
  - The Device Name now being clickable to display quick information about the device via a slide-out drawer within the current page.
  - The ability to Lockdown the device or initiate a Package Deployment from the device drawer.
  - A link to the Device Details page for further CylancePROTECT-specific information.
- **Easy Exception Handling:** Users can now quickly create exceptions for detections generated by the Context Analysis Engine (CAE) that can address potential false positives and/or abnormal, but non-threat activity. These exceptions will reduce the volume of detections as well minimize the need for many custom rules. Now users can simply apply these exceptions to any existing rule and the CAE will ignore activity that matches the exception in the future.

Machine Learning Threat Detection Modules: A Closer Look

CylanceOPTICS v2.3 our first EDR solution that delivers AI/ML based threat detection and response running on the endpoint. Trained machine learning models are deployed directly to each endpoint with no requirement for streaming data to the cloud or dedicated on-premises hardware, enabling fast detection and response.

The first three CylanceOPTICS-based machine learning models are:

- **Fileless Attack Model:** So-called "fileless" attacks may be fileless in the sense that they do not rely on a malicious or suspicious binary; however, they will typically rely on other system-based artifacts that can be easily sensed and correlated with CylanceOPTICS. The Fileless Attack Model evaluates the context and parameters of system utility invocations to understand their intended outcomes.
- **Malicious One-Liner Commands:** Scripting engines like cmd, PowerShell, and wscript are the workhorses of IT operations, but they expose a significant amount of functionality that can be leveraged by malicious actors. The Malicious One-Liner Model evaluates the content of command line scripts with an emphasis on the language of the script and the command line context of the script.
- **Malicious Application Behavior:** An overwhelming number of attacks target a small, predictable number of trusted applications commonly found in enterprise environments. The Malicious Application Behavior Model learns legitimate interactions between common software and the operating system and blocks anything that veers too far off course.

ENDPOINT DATA COLLECTED

Event Type	Description of Events
CylancePROTECT	▪ Back tracing from a CylancePROTECT detect or quarantine event gives users a bread crumb trail leading up to the malware showing up on the device
File	▪ Capture file create, modify, delete, and rename events along with metadata and file attributes ▪ Correlate file to process relationships ▪ Identify alternate data streams ▪ Identify files from removable devices
Process	▪ Process create and exit ▪ Module loads ▪ Thread injections ▪ Correlation of processes with their owning user and image file ▪ Correlation of processes to all of their activity, including files, registry keys, network connections, etc.
Network	▪ IP address ▪ Layer 4 protocol ▪ Source and destination ports
Registry	▪ Capture, create, modify, and delete events for registry keys and values ▪ Identify multiple 'persistence points' that are used by malware to persist after system reboot ▪ Correlate registry keys/values with the process that created them ▪ Correlate persistent registry keys/values with the file trying to persist through a specialized parser
User	▪ Capture all users that have logged onto the device previously ▪ Associate users with the actions they perform, including create, modify, and delete events ▪ Correlate users with malicious activity
Removable Media	▪ Capture removable media insertion events along with files being copied to and from media, including files that execute ▪ Capture device details ▪ Identify processes that make changes to or copy files from removable media ▪ Identify whether the malware detected by CylancePROTECT originated from removable media

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

20180830-0648