CYLANCE®

CylanceOPTICS™ Prevention-First EDR

What's New in CylanceOPTICS

What's New in CylanceOPTICS

CylanceOPTICS is an endpoint detection and response (EDR) solution designed to extend the threat prevention delivered by CylancePROTECT® by eradicating current threats and safeguarding against future ones.

CylanceOPTICS provides:

- Distributed search and collection
- AI root cause analysis
- Smart threat hunting
- Automated detection and response capabilities

Version 2.2 extends the capabilities of the solution with these enhancements.

Consistent Cross-Platform Visibility

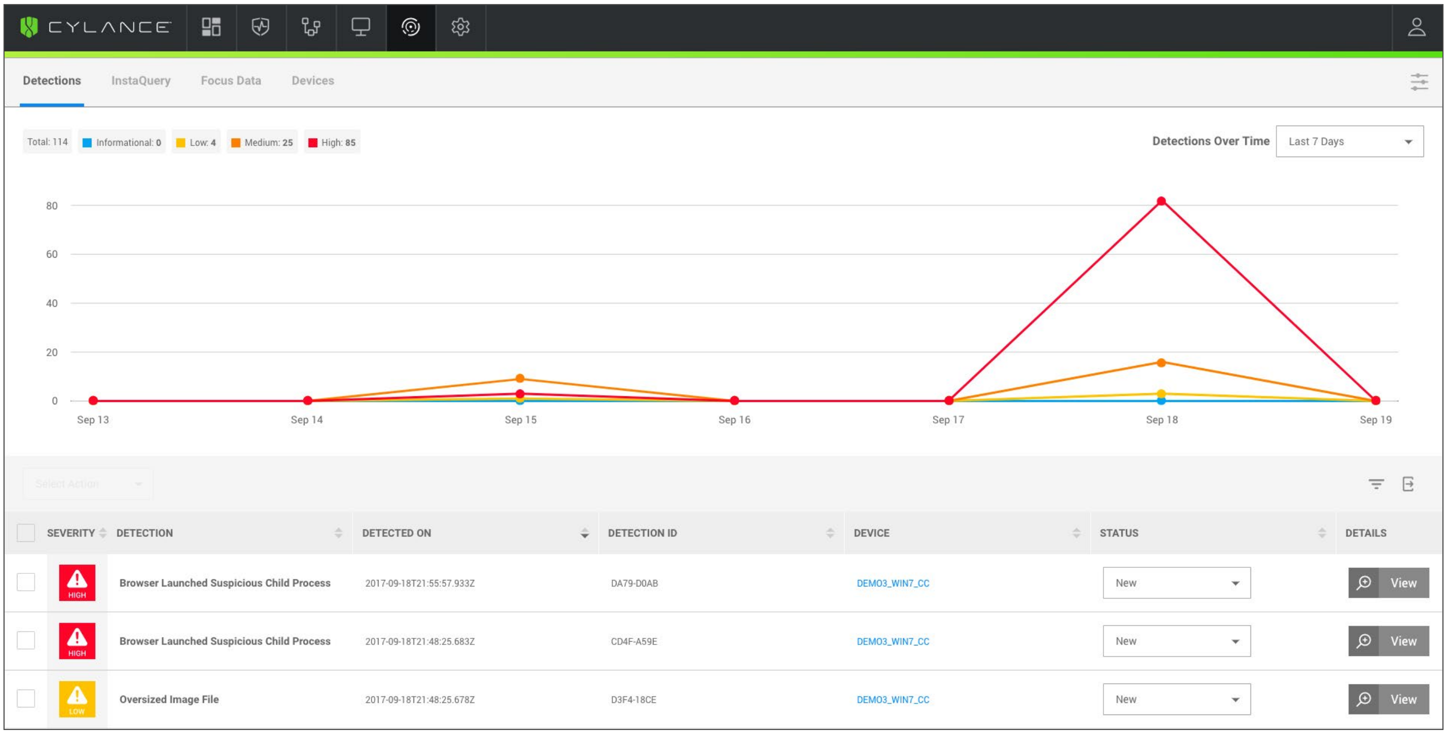
With support for Microsoft Windows endpoint and server machines, as well as MacOS endpoints, organizations can maintain situational awareness across their entire environment with one solution.

Custom Rules for Threat Detection

Users can now edit the Cylance-curated rules and create their own rules to meet their security needs. Adjust the parameters of existing rules or create new ones that minimize false positives and provide security analysts with high-fidelity alerts to investigate.

Significant Performance Gains

Users can take advantage of faster performance with disk I/O decreased by over 60% compared to previous versions of CylanceOPTICS. Additionally, users can now exclude processes (whitelist) to further boost performance.



□	SEVERITY	DETECTION	DETECTED ON	DETECTION ID	DEVICE	STATUS	DETAILS
□	HIGH	Browser Launched Suspicious Child Process	2017-09-18T21:55:57.933Z	DA79-D0AB	DEMO3_WIN7_CC	New	View
□	HIGH	Browser Launched Suspicious Child Process	2017-09-18T21:48:25.683Z	CD4F-A59E	DEMO3_WIN7_CC	New	View
□	LOW	Oversized Image File	2017-09-18T21:48:25.678Z	D3F4-18CE	DEMO3_WIN7_CC	New	View

Detections tab displays event trends over time with access to detailed threat information.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

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 120 '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
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612