

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

CylanceOPTICS provides:

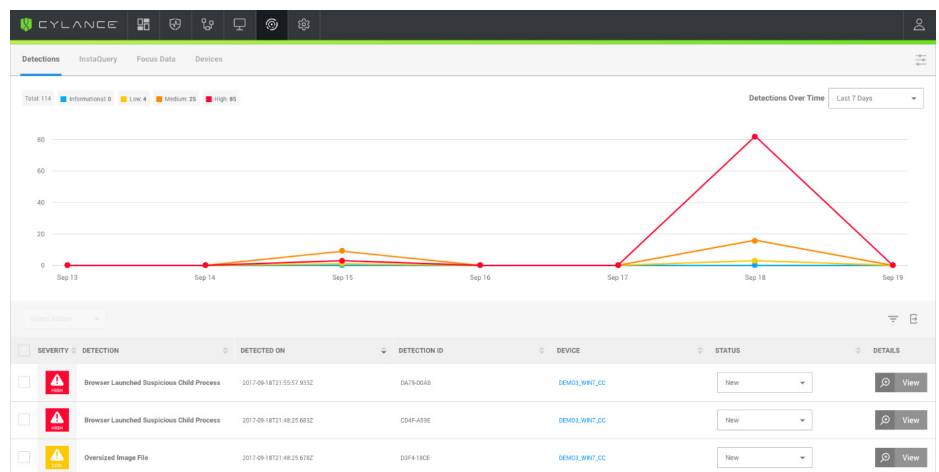
- AI-driven incident prevention
- Context-driven threat detection
- Machine learning threat identification
- Root cause analysis
- Smart threat hunting
- Automated remote investigations
- Dynamic playbook-driven response capabilities

Prevention-First EDR

Prevention products that rely on signatures cannot keep pace with today's fast-changing attacks, leaving security teams wading through a sea of alerts daily. Finding the critical security issues is near impossible, leaving attackers to run rampant across the business.

Prevention-first security can significantly reduce the number of alerts generated by the security stack, decreasing the burden and frustration associated with endless alert investigations that lead nowhere.

With CylancePROTECT preventing malware, malicious scripts, rogue applications, and fileless attacks from harming the business, CylanceOPTICS provides the artificial intelligence (AI) powered EDR capabilities required to keep data and businesses secure.



CylanceOPTICS is an EDR solution designed to extend the threat prevention delivered by CylancePROTECT by using AI to identify and prevent widespread security incidents.

Unlike other EDR products that are difficult to deploy, hard to maintain, and even harder to use, CylanceOPTICS:

- Can be installed on any endpoint in minutes with no hardware or expensive data streaming required
- Enables zero-latency detection and response by storing and analyzing data locally on the endpoint without needing constant updates
- Delivers self-contained, automated, machine learning threat detection modules designed to uncover threats that would be difficult to find with static behavior rules

CylanceOPTICS, working with CylancePROTECT, delivers the detection and prevention capabilities needed to stay ahead of the attackers, keeping the business secure.

Benefits

- Reduce dwell time and the impacts of potential breaches
- Drive consistent levels of security no matter the security staff skill-level
- Save significant time and money associated with recovering from a successful attack

CylanceOPTICS EDR Solution

Enterprise Ready	<ul style="list-style-type: none">▪ Distributed Search and Collection▪ Cross-Platform Visibility▪ API Accessibility▪ Syslog Integration
Detection	<ul style="list-style-type: none">▪ Context-Driven Detection▪ Machine Learning Modules▪ MITRE ATT&CK Framework
Investigation and Response	<ul style="list-style-type: none">▪ Root Cause Analysis▪ Remote Investigations▪ Threat Hunting▪ Playbooks▪ Containment and Remediation

Common Use Cases

- **Prevent Malicious Activity:** CylancePROTECT, which provides the foundation for CylanceOPTICS, is designed to specifically prevent successful attacks aimed at endpoints. This includes:
 - Identifying and blocking malicious executable and file identification using AI
 - Controlling where, how, and who can execute scripts
 - Managing the use of USB devices, prohibiting unauthorized devices
 - Eliminating the ability for attackers to use fileless malware attack techniques
 - Preventing malicious email attachments from detonating their payloads
- **Investigate Attack and Alert Data:** Users can investigate alerts from other security controls, including CylancePROTECT, with easy to understand visualizations of all activities associated with the alert, retrieving useful information from the endpoint.
- **Hunt for Threats Across the Enterprise:** Users can quickly search for files, executables, hash values, and other IOCs across the entirety of their network endpoints to uncover hidden threats.
- **Endpoint Threat Detection:** Suspicious behaviors and other indicators of potential compromise on endpoints will be uncovered automatically.
- **Rapid, Automated Playbook-Driven Incident Response:** Users can retrieve critical forensic information from impacted endpoints automatically, as well as take response actions automatically when a harmful endpoint is discovered.