# CylanceOPTICS™

Incident Prevention EDR for CylancePROTECT® Environments

## Benefits

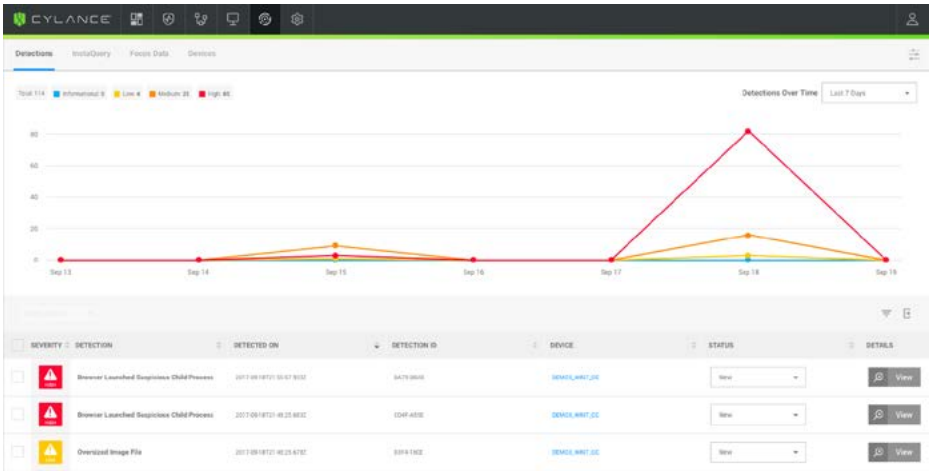
- **Reduce Alert Volume**
  Reduce security alert volume with full-spectrum threat and incident prevention, improving team efficiency
- **Gain Situational Awareness**
  Understand the attack surface across the environment, eliminating potential weaknesses
- **Relieve the Strain on Security Teams**
  Automate responses to identified threats 24x7, without disrupting the security team

## The Case for Prevention-First Security

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 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.

## Common Use Cases

- **Prevent Malicious Activity:** CylancePROTECT, which provides the foundation for CylanceOPTICS, is designed to specifically prevent successful attacks aimed at endpoints.
- **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 Incident Response:** Users can retrieve critical forensic information from impacted endpoints, as well as take aggressive containment actions when a harmful endpoint is discovered. The solutions also can automatically trigger response actions if a pre-defined rule is triggered.

## CylanceOPTICS Features

**AI Driven Incident Prevention**

Uncover threats that would be difficult to identify with behavior rules using machine learning threat detection modules

**Enterprise-wide Threat Hunting**

Easily search endpoint data for suspicious/malicious activity to uncover hidden threats

**Consistent Cross-Platform Visibility**

Detect and prevent incidents across Microsoft Windows and Apple MacOS platforms

**Dynamic Threat Detection**

Automate threat detection, in real time, using custom and curated behavior rules running on the endpoint

**On-Demand Root Cause Analysis**

Understand how attacks entered the environment so corrective actions can be taken, reducing the attack surface

**Automated, Fast Response**

Customize automated response actions to minimize the risk of a widespread incident

**Remote Forensic Data Collection**

Capture critical information related to any suspicious event or security incident fast

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



20180601-2793