CYLANCE

CylanceOPTICS

Endpoint Detection and Response Designed for CylancePROTECT® Endpoints

Benefits

- Identify and mitigate previously exploited attack vectors, **reducing the attack surface**
- **Find threats hiding** on your endpoints with smart threat hunting capabilities
- **Take immediate action** to reduce dwell time, improve efficiency, and decrease business impact of any security risk

Features

- **Root Cause Analysis:** Web-based, on-demand, root cause analysis of attacks blocked by CylancePROTECT
- **Smart Threat Hunting with InstaQuery:** Search endpoint data instantly for potential threats hiding on endpoints
- **Dynamic Threat Detection and Alerting:** Instant notification when suspicious activity is detected on any endpoint
- **Fast Incident Response:** Take incident response actions fast, quarantining, acquiring suspicious files, and/or isolating compromised endpoints from the network
- **Built for Scale:** High performance architecture built for scalability

The Endpoint Security Challenge

Endpoint security teams are inundated with data from the security products deployed across their network. Due to the need to maintain business continuity above all else, however, these teams have little time to perform any proactive threat hunting or strategic security improvements, leaving critical threats unidentified and their security infrastructure at risk. Compounded by the scarcity of skilled security resources on the market, many organizations must rely on their security tools to provide them the insights they need to identify, detect, and respond to security incidents. Unfortunately, many of these tools are not equipped to handle today's threats.

While 100% detection and prevention of all threats is not possible, it is important that organizations begin their path to total endpoint security with a strong *prevention* strategy. By doing all they reasonably can to prevent threats from impacting their business, organizations can then turn their attention to layering on technology and processes aimed at *detecting and responding* to the hard-to-prevent threats targeting their business.

A New Approach To Endpoint Detection and Response

CylanceOPTICS is an artificial intelligence (AI) driven endpoint detection and response (EDR) solution designed to extend the prevention delivered by Cylance's award-winning product, CylancePROTECT, through AI driven root cause analysis, scalable threat hunting, and immediate response with consistent visibility into threats against endpoints.

Unlike other EDR solutions built around porous antivirus products, CylanceOPTICS builds off the over 99% endpoint attack prevention rate delivered by CylancePROTECT, providing the consistent endpoint visibility that security analysts need to hone in on critical security issues that pose a threat to their business.

CylanceOPTICS allows security professionals to dissect any attack detected and blocked by CylancePROTECT to determine root cause and improve their overall security framework with ease. Additionally, CylanceOPTICS provides smart threat hunting capabilities with its dynamic endpoint data interrogation and visualization layer, InstaQuery (IQ).

Security professionals can use CylanceOPTICS to perform on-demand enterprise-wide threat hunts, searching for files, executables, and indicators of compromise, then use IQ to provide instant access to threat hunt results so analysts can quickly determine if any endpoint is at risk, minimizing available attack and dwell time to reduce the attack surface and speed incident response.

Using built-in response capabilities, analysts can remediate threats across the enterprise immediately, stopping attackers in their tracks and reducing the risk of a widespread compromise.

Effective Threat Detection Starts With Superior Threat Prevention

The combination of CylancePROTECT and CylanceOPTICS delivers the prevention, detection, and response capabilities needed for total endpoint security. With these powerful technologies in place, organizations can protect their sensitive data, reduce their risk of widespread compromises, and improve their overall security posture.

Reduce the Attack Surface

Evolve the organization's security framework, mitigating attack vectors and reducing risk of a breach.

Eliminate Hidden Threats

Find threats attempting to evade detection with smart threat hunting capabilities.

Take Immediate Action

Stop attackers in their tracks with integrated response, reducing dwell time and potential business impact.

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
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

CYLANCE™