CYLANCE

CylanceOPTICS™ Prevention-First EDR

What's New in Winter 2018-2019 Release

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

Due to the evolution of the threat landscape and the continuous expansion of the attack surface, organizations are challenged to maintain a situational awareness and a steady-state security posture. Advancements in security technology have helped make it more difficult for attackers to be successful, however, organizations face two challenges that show no signs of lessening:

- **Skilled security expert shortage:** With a shortage forecasted to be in the millions within the next five to 10 years, organizations will find it more difficult to add skilled resources to their team, not to mention maintain their current team makeup. Therefore, organizations are seeking out security solutions that combine advanced security capabilities with automation that allow them to mitigate the risk of this human resource shortage.
- **The need for security purchases to show positive return on investment (ROI):** Despite the increased visibility into debilitating outbreaks, security team management often find themselves fighting for security budget. Often security management must agree to demonstrate a reasonable ROI to have budget released. Therefore, now more than ever, organizations are seeking out security solutions that offer the opportunity for threat reduction while simultaneously providing demonstrable ROI.

The Winter release of CylanceOPTICS delivers new detection, investigation, response, and automation capabilities that enable organizations concerned with advanced threats, delivering ROI, and staffing issues to adopt an EDR solution with ease.

New Benefits at a Glance

- **Improved Threat Visibility though Syslog Integration:** CylanceOPTICS now outputs all detection events to the syslog, allowing users to make use of this critical threat data across their security and IT stack.
- **Programmatically integrate CylanceOPTICS into the security stack with new API support:** CylanceOPTICS is now fully accessible via APIs, allowing organizations to incorporate this AI-driven EDR solution into their existing management consoles without the need to use the CylanceOPTICS user interface.
- **MITRE ATT&CK Framework rules packages:** The Cylance Context Analysis Engine, the driving force behind threat detection and response, now comes with a pre-configured set of rules mapped to the MITRE ATT&CK Framework, improving threat detection capabilities.
- **Reduce dwell time and increase response time and consistency with playbook-driven response:** Initiate a set of discrete response tasks automatically if the rule is triggered. Playbook-driven response capabilities assist organizations in eliminating dwell time by ensuring threat responses are fast and consistent across the environment regardless of the skill-level of on-duty security personnel.
- **Complete suspicious device investigations faster with partial lockdown:** Extending current lockdown response capabilities in CylanceOPTICS, partial lockdown will enable a security analyst to maintain communication with a suspected compromised endpoint without risk of further environment contamination.

CylanceOPTICS Data Collection Approach

CylanceOPTICS takes a targeted approach to data collection, capturing changes to endpoints and servers that would indicate a potential security threat.

Unlike other products that stream all changes to the cloud continuously, CylanceOPTICS stores this security-relevant data locally on the endpoint to enable fast, local decisions, minimizing response latency.

Data Collected

Changes to:

- Files
- Process
- Network
- Registry
- User
- Removable Media

The Power of CylanceOPTICS

The power of CylanceOPTICS comes from the unique and efficient way threat detection and response capabilities are delivered. Unlike other EDR products that rely on cloud-based analysis to uncover threats and security analysts for response, CylanceOPTICS pushes all detection and response decisions down to the endpoint, eliminating response latency that can mean the difference between a minor security event and a widespread, uncontrolled security incident.

Each rule, whether default, custom, or machine learning, can be configured with a playbook that can initiate a set of discrete response tasks automatically if the rule is triggered. The playbook-driven response capabilities assist organizations in eliminating dwell time by ensuring threat responses are fast and consistent across the environment regardless of the skill-level of the on-duty security personnel.

CylanceOPTICS also includes remote investigation capabilities that make completing detailed incident analysis fast. Analysts can quickly deploy packages to endpoints to collect critical artifacts as well as complete other tasks, even using other tools remotely, drastically reducing the time to resolution.

CylanceOPTICS allows security analysts to dissect any CylancePROTECT-prevented attack to determine root cause to improve their overall security framework. CylanceOPTICS also provides enterprise-wide threat hunting capabilities powered by InstaQuery (IQ), enabling on-demand threat hunting with instant access to the results.

Finally, CylanceOPTICS is 100% API accessible, enabling security teams to gain the benefits of AI-driven EDR without learning a new user interface. With simple-to-configure API calls, analysts can do anything from consume threat data to perform system-wide threat hunts without ever touching the CylanceOPTICS user interface.

The threat detection, investigation, response, and automation delivered by CylanceOPTICS means organizations can maintain continuous situational awareness and strong security posture regardless of changes to the threat landscape, budget, or their security team.

Cylance Solution	Customer Benefit
Combine static, machine learning, and custom rules to **identify and block advanced threats**	Organizations can **reduce dwell time** and the impacts of potential breaches
Automate investigation and response with **playbook-driven workflows**, ensuring appropriate actions are always taken	Organizations can drive **consistent levels of security** no matter the security staff skill-level
Implement an AI-driven **prevention-first approach to EDR** through which most attacks are thwarted before they have an opportunity to execute	Organizations can **save significant time and money** associated with recovering from a successful attack

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE