Using AI

CylanceOPTICS is an EDR solution that extends the threat prevention delivered by CylancePROTECT using 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

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
The 2.4 release of CylanceOPTICS brings several product enhancements to aid in both the breadth and depth of EDR search parameters. These enhancements, which are built on the foundational AI-based protection of CylancePROTECT and locally stored intelligence, offer real-time confidence to investigate, triage, and remediate when a CAE rule trigger occurs. This gives EDR practitioners the ability to search and remediate at the speed of the threat landscape, and not be delayed by cloud queries, protracted forensic analysis, and other time-wasting processes. The EDR team can understand all the artifacts that have occurred before and after the triggering event. This results in:

- Increased search parameter flexibility within InstaQuery, FocusView, and CAE rules
- Faster incident response
- Alignment with the MITRE ATT&CK framework
- Expanded automated response via CAE rules

### CylanceOPTICS EDR Solution

<table>
<thead>
<tr>
<th>Enterprise Ready</th>
<th>Detection</th>
<th>Investigation and Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Distributed Search and Collection</td>
<td>• Context-Driven Detection</td>
<td>• Second Generation</td>
</tr>
<tr>
<td>• Cross-Platform Visibility</td>
<td>• Machine Learning Modules</td>
<td>• Cloud-Enhanced Models</td>
</tr>
<tr>
<td>• API Accessibility</td>
<td>• MITRE ATT&amp;CK Framework</td>
<td></td>
</tr>
<tr>
<td>• Syslog Integration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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 executables and files 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.