CylanceOPTICS™
Winter 2019 Release

CYLANCE

Combining AI, Automation, and Security Expertise

Matthiew Morin
Senior Product Manager

Agenda

- CylanceOPTICS Overview / Refresher
- CylanceOPTICS Winter 2019 Release Overview
- Package Playbooks Demo

The Problem

Too many alerts, not enough time

Inconsistent visibility across the environment

Not enough security expertise

The Cylance Security Solution

Cylance Security Solution:
All Paths Lead to Prevention

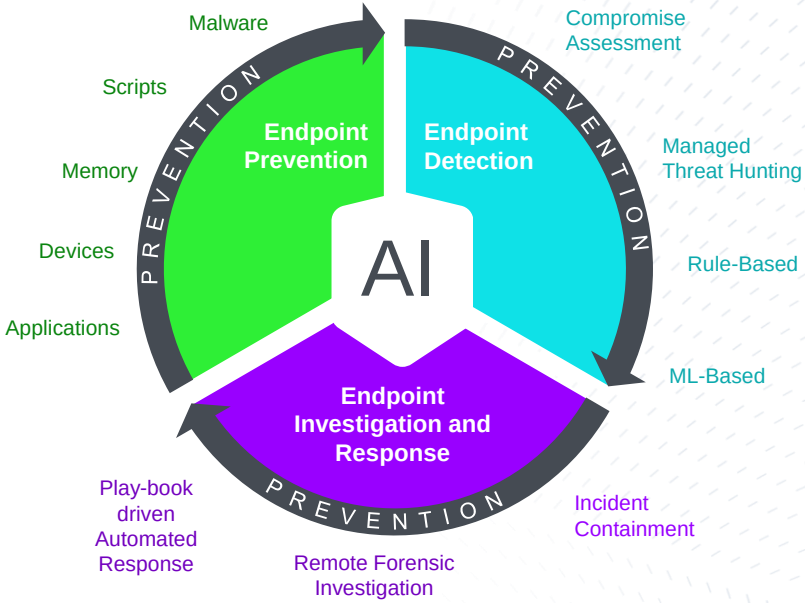
Endpoint Prevention

+

Predictive EDR

+

24x7 Services to IR Prevention



SECURITY FOUNDATION

Data Science Threat Research Human Security Expertise

CYLANCE

Milliseconds Matter

especially in cybersecurity

CylanceOPTICS EDR:

1. Makes **automated** decisions **locally** at the endpoint immediately
2. Eliminates the response latency that can cause a minor security event to grow into a widespread, uncontrolled security incident.

Key Differentiator: Local Decisions

Other EDR Products

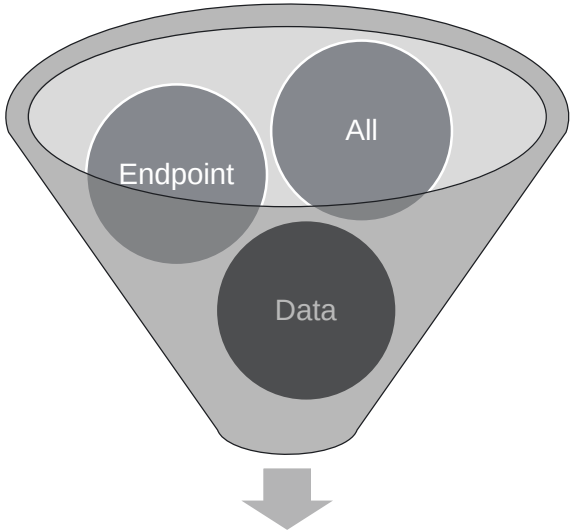
Dedicated Hardware and
Continuous Data Streaming

CYLANCE OPTICS

Zero Latency
Detection and Response

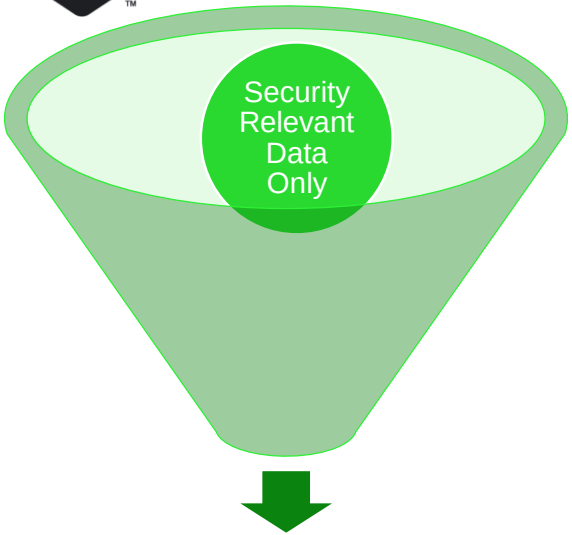
Key Differentiator: Relevant Data Only

Other EDR Products



Alert Avalanche

CYLANCE OPTICS



High-Fidelity Security Events

CylanceOPTICS EDR Solution

Enterprise Ready

- Distributed Search and Collection
- Cross-Platform Visibility
- API Accessibility
- Syslog Integration

Detection

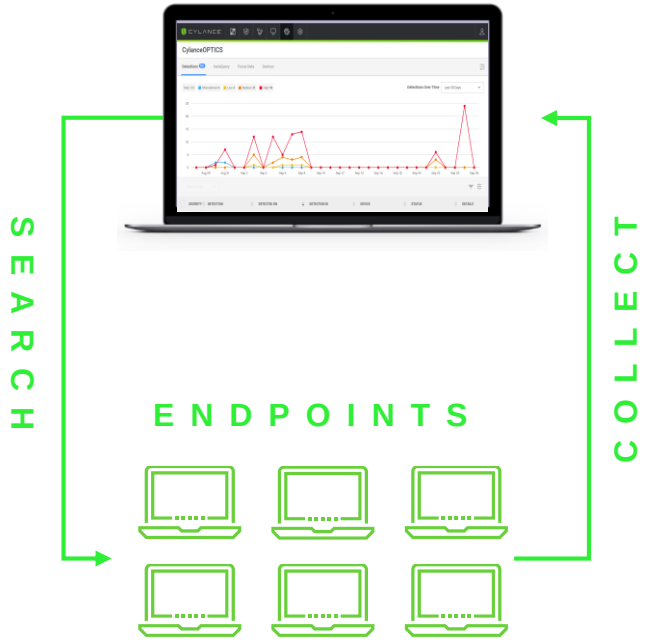
- Context-Driven Detection
- MITRE ATT&CK Framework

Investigation and Response

- Root Cause Analysis
- Remote Investigations
- Threat Hunting
- Playbooks
- Containment and Remediation

Eliminate Dedicated Hardware and/or Continuous Data Streaming

- Distributed search and collection avoids the over-collection and storage of irrelevant data
- Mitigates data privacy concerns
- Reduces the infrastructure costs associated with EDR



CylanceOPTICS Winter 2019 Release
Syslog Integration, APIs, and Playbooks

Improved Threat Visibility with Syslog Integration

- Users can now receive a feed of Context Analysis Engine detection events directly to their SIEM or logging platform
- The syslog integration allows users to continue to build automated workflows receiving, triaging, and respond to malicious or suspicious behavior detected by CylanceOPTICS.
- Cylance's official Splunk app supports the new inputs from CylanceOPTICS allowing users to easily visualize and drill into data.

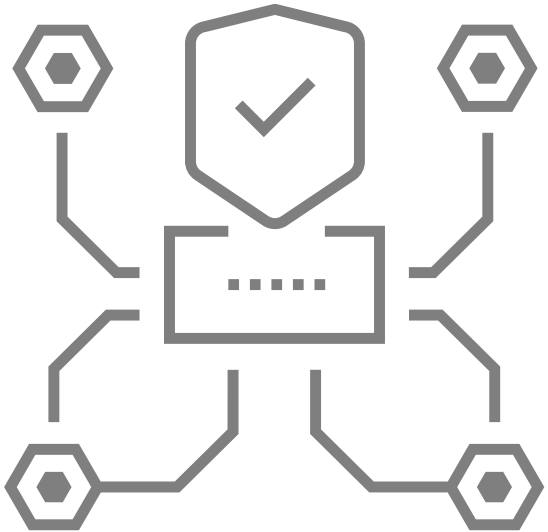
CYLANCE

+

splunk>

Integrate, Interact, and Automate with CylanceOPTICS via API

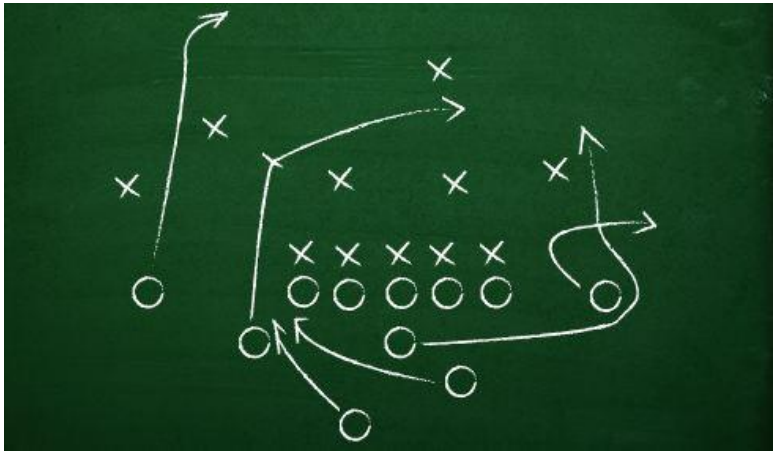
- Request an InstaQuery
- Request a Focus View
- Publish, update, and delete Context Analysis Engine rules and exceptions
- Create, update, and delete Detection Rule Set configurations
- Send Device Lockdown commands to endpoints
- Retrieve arbitrary files from endpoints
- Upload, remove, and deploy Packages to endpoint



Reduce Dwell Time, Speed Response Time & Improve Consistency with Playbook Driven Response

Automated Playbooks combine the near-zero latency response time of CylanceOPTICS with the power of CylanceOPTICS remote investigations allowing users to automatically:

- Collect high value forensic artifacts
- Execute in-house or 3rd party applications and scripts
- Take additional scripted response, remediation, or recovery actions




CYLANCE