CYLANCE

Cylance **Continuous Threat Prevention**

Company Overview

Cylance uses cloud trained machine learning models that are then deployed on-device to detect and prevent malicious executable files from running in milliseconds, pre-execution, without the use of signatures, cloud look-ups, or sand-boxing. **Get everything you need in one spot when you buy Cylance directly from ConnectWise.**

Prevent Cyberattacks with Artificial Intelligence

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, file-less malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

Category Information

Security

Solutions Include

- **CylancePROTECT®:** Continuous Threat Prevention Powered by Artificial Intelligence
- **CylanceOPTICS™:** Incident Prevention EDR for CylancePROTECT® Environments

CylancePROTECT:

For years, prevention products' primary threat protection was based on signatures. Assuming all attacks at a business had been seen before, using signatures made sense. Today, malware mutates daily, even hourly, making signature-based prevention tools obsolete. It is time to think beyond traditional antivirus. Think CylancePROTECT.

Integration Information

- Autodeploy for Cylance agent install or uninstall
- Cylance identified threats
- Assign Cylance policies
- Assign computers to Cylance zones

Features & Benefits

Features:

- **True Zero-Day Prevention:** Resilient AI model prevents zero-day payloads from executing
- **AI-Driven Malware Prevention:** Field-proven AI inspects any application attempting to execute on an endpoint before it executes
- **Script Management:** Maintains full control of when and where scripts are run in the environment
- **Device Usage Policy Enforcement:** Controls which devices can be used in the environment, eliminating external devices as a possible attack vector
- **Memory Exploitation Detection & Prevention:** Proactively identifies malicious use of memory (file-less attacks) with immediate automated prevention responses
- **Application Control for Fixed-Function Devices:** Ensures fixed-function devices are in a pristine state continuously, eliminating the drift that occurs with unmanaged devices

Benefits:

- AI-driven prevention reduces the strain on the endpoint compared to traditional solutions
- No signatures mean less human effort to manage
- No cloud or new hardware required minimizes total cost of ownership
- Uses AI, not signatures, to identify and block known and unknown malware from running on endpoints

Strengthen Your Security with **CYLANCE**

- Delivers prevention against common and unknown (zero-day) threats without a cloud connection
- Continuously protects the endpoint without disrupting the end-user

System Requirements/Technical Specifications

Microsoft Windows (32-bit or 64-bit):

Windows XP SP3
Windows Vista
Windows 7
Windows 8 and 8.1
Windows 10
Windows Server 2003 SP2
Windows Server 2008/2008 R2
Windows Server 2012/2012 R2
Windows Server 2016

Requirements:

2GB Memory
500MB available disk space
Microsoft .NET Framework 3.5 SP1
Internet browser
Internet connection to register product
Local admin rights to install software

Mac OS:

Mac OS X 10.9 (Mavericks)*
Mac OS X 10.10 (Yosemite)*
Mac OS X 10.11 (El Capitan)*
Mac OS X 10.12 (Sierra)*

** Complements Apple's built-in XProtect*

Requirements:

2GB Memory
500MB available disk space
Internet browser
Internet connection to register product
Local admin rights to install software

Linux:

Red Hat Enterprise Linux / CentOS 6.6 – 32-bit and 64-bit
Red Hat Enterprise Linux / CentOS 6.7 – 32-bit and 64-bit
Red Hat Enterprise Linux / CentOS 6.8 – 32-bit and 64-bit
Red Hat Enterprise Linux / CentOS 7.0 – 64-bit
Red Hat Enterprise Linux / CentOS 7.1 – 64-bit
Red Hat Enterprise Linux / CentOS 7.2 – 64-bit
Red Hat Enterprise Linux / CentOS 7.3 – 64-bit

Requirements:

2GB Memory
500MB available disk space
Internet browser
Internet connection to register product
Local admin rights to install software

CylanceOPTICS:

With CylancePROTECT preventing malware, malicious scripts, rogue applications, and file-less 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.

Features & Benefits

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

Strengthen Your Security with **CYLANCE**

- **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

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