Endpoint Protection

Identify and stop targeted attacks just as they are beginning.

Download the Datasheet

Cylance

Features

MALWARE EXECUTION CONTROL

- Machine learning with predictive analysis
- Automated static code analysis
- Memory Control Script Control
- Application Control
- Pre-execution prevention in <100ms
- No signatures |
- No prior knowledge needed No Internet required
- No daily scans Rejects potentially unwanted programs (PUPs)

Description

Cylance applies artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end users proactively solve the world's most difficult security problems. Using predictive analysis, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated math and machine learning with a unique understanding of a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats.

Specification

Windows Agent Requirements Supported Operating Systems (32-bit and 64-bit)

Windows XP SP3 (with KB 968730) through Windows 10 (excluding Windows RT)

Windows XP Embedded OS and newer

Windows Server 2003 SP2 (with KB 968730) through Windows Server 2012R2 ? System Memory and Local Storage

2 GB+ RAM

Approximately 500 MB of local disk storage not including quarantined items Additional Requirements

.NET Framework 3.5 (SP1) or higher is required on all Windows versions , Internet browser, Internet connection to register product, local administrative rights to install software.

Server 2003 SP2 also requires .NET 3.5 SP1 and the patch referenced in KB2868626 to update crypt32.dll. Up-to-date root certificates. ? Mac Agent Requirements Supported Operating Systems

OS X 10.9 Mavericks / OS X 10.10 Yosemite / OS X 10.11 El Capitan System Memory & Local Storage

2+ GB RAM

500 MB of local disk storage not including any items that may have been quarantined

Links

Data Sheet

Math vs. Malware

Fidelis

Features

- Detect attacks other solutions miss.
- Identify and stop targeted attacks just as they are beginning.
- Correlate seemingly unrelated network activity and behavior.
- Reduce time to detect and resolve incidents.
- Discover unmanaged devices on your network.

Description

Accelerate Triage and Validate Suspected Incidents

Automatically harvest rich system information from endpoints and correlate it against threat reputation services, advanced threat detectors and threat intelligence to confirm when endpoints are compromised.

Automate Incident Response Workflows

Easily create and customize response workflows specific to the organization. Automatically kick off

remediation or perform forensic analysis by defining trigger rules and actions with the alert response workflow engine.

Eliminate Blind Spots

Identify and validate threats on your endpoints anywhere in your environment – on or off your network.

Respond Immediately

Integrate with SIEMs, next-generation firewalls and alerting tools to accelerate your response and trace alerts to compromised endpoints.

Identify Compromised Endpoints

Automatically sweep all endpoints for signs of the compromise once an Indicator of Compromise (IOC) has been validated.

Proactively Hunt for Threats

Apply network- or host-based intelligence in any format, to rapidly identify compromised endpoints and automatically take action.

Know What Happened Using Playback

Protect your systems by recording key events (e.g. files accessed, running processes, registry changes, and network and DNS activity) and receiving a detailed timeline related to a suspected incident along with prioritized alerts.

Stop Data Theft and Remediate Endpoints

Halt data exfiltration and lateral movement by isolating endpoints, halting processes, wiping files, and kicking off a script to initiate an anti-virus scan.

Links

Datasheet
Gartner Review

McAfee

Features

Endpoint Protection – delivers advanced antivirus, anti-malware, host intrusion prevention, device control, host-based firewall, and application control to protect PCs, Macs, Linux systems, servers, virtual systems, smartphones, and tablets from online threats.

Description

A combination of AV, Firewall, web security (SiteAdvisor). Traditional Windows, Mac, and Linux systems need essential security to block advanced malware, control data loss and compliance risks caused by removable media, and provide safe access to critical email and web applications. McAfee Endpoint Protection Suite integrates these core functions into a single, manageable, multiplatform environment ideal for safeguarding traditional desktops that have limited exposure to Internet threats.

This proven enterprise and small business endpoint security solution delivers operational efficiencies and cost savings with the convenience of a single suite. It includes real-time anti-malware and antivirus protection, proactive email and web security, desktop firewall, comprehensive device control, and unrivalled centralized management.

Links

Data Sheet
Solution Brief
Product Guide
Installation Guide
Independent Review
ExpertCenter

Sweden
Cognosec Nordic AB
Birger Jarlsgatan 12
114 34 Stockholm
Sweden
Tel +46 (0)8 400 170 00
sales.se@cognosec.com

UK & Ireland
Cognosec Limited
3rd Floor
The News Building
3 London Bridge Street
London SE1 9SG
UK
Tel +44 (0)20 3870 1539
sales.uk@cognosec.com

Germany
Cognosec GmbH
An der Welle 4
60322 Frankfurt
Germany
Tel +49 (0)69 7593 8490
sales.de@cognosec.com

Austria
Cognosec GmbH
Castellezgasse 16/2
1020 Vienna
Austria
Tel +43 (0)1 212 2020
sales.at@cognosec.com

UAE
Cognosec DMCC
2202 Indigo Icon Tower
Cluster F
Jumeirah Lakes Towers, Dubai
UAE
Tel +971 (0)4 451 1552
sales.dxb@cognosec.com

Copyright © 2017 Cognosec Limited. All rights reserved.