Symantec™ Endpoint Protection 12.1.6

Data Sheet: Endpoint Security

Overview

Last year, we saw 317 million new malware variants, while targeted attacks and zero-day threats were at an all-time high[1]. The threat environment is evolving quickly and given the size and complexity of today's networks, organizations are struggling to keep up. Symantec™ Endpoint Protection is designed to address these challenges with a layered approach to security at the endpoint. It goes beyond traditional antivirus to include firewall, Intrusion Prevention System (IPS) and advanced protection technologies powered by the world's largest civilian threat intelligence network. Symantec Insight™ technology blocks rapidly-mutating malware and enables faster scan times, while SONAR™ stops zero-day threats by monitoring file behavior and blocking suspicious files while they execute. Granular policy settings such as application control and external media control provide an added layer of security. With a single management console and high-powered agent, Symantec Endpoint Protection delivers powerful protection at the endpoint without compromising performance.

Unrivaled Security

Stops targeted attacks and advanced persistent threats with intelligent security and layered protection

- Symantec Endpoint Protection leverages the world's largest civilian threat intelligence network to deliver advanced protection at the endpoint. This network consists of telemetry data coming from 175 million endpoints and 57 million attack sensors in 175 countries, providing unique visibility into the latest security threats.
- Derived from this intelligence network, our unique Insight™ technology identifies file reputation by analyzing key file attributes such as how often a file has been downloaded, how long a file has been there, and where it is being downloaded from. This information allows us to block more threats and defend against new, mutating malware.
- SONAR™ technology, also powered by this intelligence network, monitors application behavior in real-time and stops targeted attacks and zero-day threats
- Network Threat Protection analyzes incoming data streams and blocks threats while they travel through the network before hitting endpoints
- Symantec™ Endpoint Protection detects and removes threats more accurately[2], repeatedly scoring a AAA rating, the highest score, by Dennis Labs Real World A/V Test

Blazing Performance

Performance so fast your users won't know it is there

- Insight™ reputation technology accurately identifies file reputation so only at-risk files are scanned, effectively eliminating up to 70 percent of scan overhead compared to traditional solutions
- Symantec™ Endpoint Protection outperforms all products in its class in terms of scan speed and total performance impact[3]

[1.] Symantec Internet Security Threat Report 2015
[2.] AV-Test, Product Review, Corporate Solutions for Windows 7, April 2015
[3.] PassMark Software, "Enterprise Endpoint Security Performance Benchmarks", 2014

✓ Symantec™

- Optimizes content delivery for faster distribution and lower storage requirements. Virus definition sets require 90% less disk space on Symantec™ Endpoint Protection Manager.
- Supports embedded systems and Virtual Desktop Infrastructures (VDI) with smaller client size for reduced memory footprint
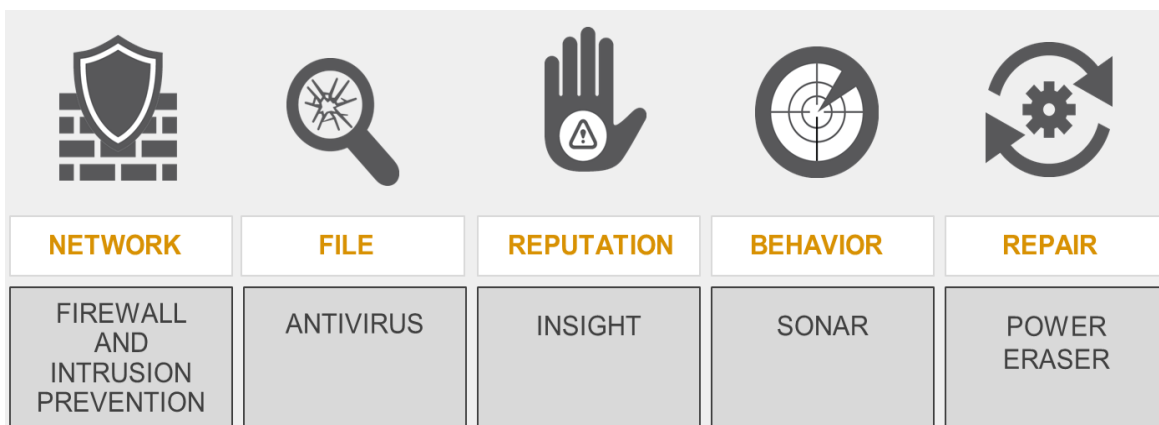
Smarter Management

Single management console across physical and virtual platforms with granular policy control

- Delivers intelligent security technologies and policy lockdown features in a single high performance agent with a single management console across Windows®, Mac®, Linux®, virtual machines, and embedded systems
- Provides granular policy control with the flexibility to customize policies depending on users and their location
- Supports remote deployment and client management for both Windows® and Mac® systems making it easier to keep remote endpoints up-to-date
- Expands traditional reporting by incorporating multi-dimensional analysis and robust graphical reporting in an easy-to-use dashboard
- Reduces network overhead and decreases the time it takes to get updates by allowing one client to send updates to another (Group Update Provider). This also facilitates more effective updates in remote locations.

Five Layers of Protection

Symantec™ Endpoint Protection 12.1.6 provides five layers of protection in one high performance agent all managed through a single console.

NETWORK	FILE	REPUTATION	BEHAVIOR	REPAIR
FIREWALL AND INTRUSION PREVENTION	ANTIVIRUS	INSIGHT	SONAR	POWER ERASER

1) Network: Symantec's network threat protection technology analyzes incoming data and blocks threats while they travel through the network before hitting endpoints. Rules-based firewall and browser protection are also included to protect against web-based attacks.

2) File: Signature-based antivirus and advanced file heuristics look for and eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits

✓Symantec.™

3) Reputation: Symantec's unique Insight™ correlates tens of billions of linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, Insight™ can accurately identify whether a file is good or bad and assign a reputation score, effectively protecting against targeted attacks while reducing scan overhead by up to 70 percent.

4) Behavior: SONAR™ leverages artificial intelligence to provide zero-day protection. It effectively stops new and unknown threats by monitoring nearly 1,400 file behaviors while they execute in real-time to determine file risk.

5) Repair: Power Eraser™ aggressively scans infected endpoints to locate advanced persistent threats and remove tenacious malware. Remote support enables the administrator to trigger the Power Eraser scan and remedy the infection remotely from the Symantec™ Endpoint Protection management console.

Extended Policy Control Features

In addition to core protection technologies, Symantec™ Endpoint Protection 12.1.6 also provides granular policy controls, including:

| APPLICATION CONTROL | EXTERNAL MEDIA CONTROL | HOST INTEGRITY |
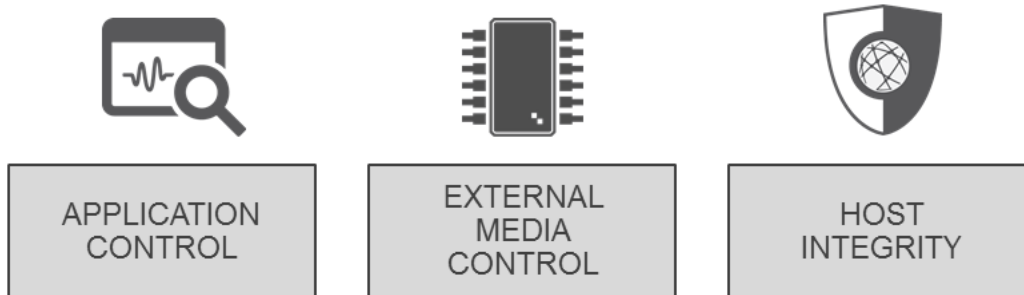
1) Application Control: Allows you to control file and registry access and how processes are allowed to run. It also includes advanced system lockdown features, only allowing whitelisted applications (known to be good) to run, or blocking blacklisted applications (known to be bad) from running.

2) External Media Control: Allows you to restrict access to select hardware and control what types of devices can upload or download information. External media control can be combined with application control to offer more flexible control policies.

3) Host Integrity Checking & Policy Enforcement: Ensures endpoints are protected and compliant by enforcing policies, detecting unauthorized changes, and conducting damage assessments with the ability to isolate a managed system that does not meet your requirements

Optimization for Virtual Environments

Symantec™ Endpoint Protection protects your high-density virtual environment while maintaining performance levels superior to agentless solutions and providing end-to-end security visibility.

1) VMware vShield™ Integration: Allows higher virtual machine (VM) density and reduces I/O and CPU usage

2) Virtual Image Exception: Whitelists files from a standard virtual machine image to optimize scanning

3) Resource Leveling: Randomizes scan and update schedules to prevent resource utilization spikes

4) Shared Insight™ Cache: Scans files once, shares the results between clients, and de-duplicates file scanning to reduce bandwidth and latency

5) Virtual Client Tagging: Automatically detects and reports whether the client is running in a virtual environment, making it easier to set different policies for virtual machines

6) Offline Image Scanning: Finds threats in offline VM images

7) Scan Throttling for Virtualization: Detects disk load and reduces scan speed to prevent utilization spikes

Client Workstation and Server System Requirements*

Windows Operating Systems

- Windows XP (32-bit, SP3 or later; 64-bit)
- Windows XP Embedded (SP3 or later)
- Windows Vista (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit)
- Windows 7 Embedded
- Windows 8 (32-bit, 64-bit)
- Windows 8 Embedded
- Windows 8.1
- Windows 10**
- Windows Server 2003 (32-bit, 64-bit, R2 or SP1 or later)
- Windows Server 2008 (32-bit, 64-bit, including R2)
- Windows Server 2012 (64-bit, including R2)
- Windows Small Business Server 2011 (64-bit)
- Windows Essential Business Server 2008 (64-bit)

Macintosh Operating Systems

- Mac OS X 10.8, 10.9, 10.10

Linux Operating Systems (32-bit and 64-bit versions)

- Red Hat Enterprise Linux
- SUSE Linux Enterprise (server/desktop)
- Novell Open Enterprise Server
- Oracle Linux
- CentOS
- Ubuntu
- Debian
- Fedora

Virtual Environments

- Microsoft Azure
- Amazon WorkSpaces
- VMware WS 5.0, GSX 3.2, ESX 2.5 or later
- VMware ESXi 4.1–5.5
- Microsoft Virtual Server 2005
- Microsoft Enterprise Desktop Virtualization (MED-V)
- Microsoft Windows Server 2008, 2012, and 2012 R2 Hyper-V
- Citrix XenServer 5.6 or later
- Virtual Box by Oracle

Hardware Requirements

- 1 GHz CPU or higher
- 512 MB of RAM (1 GB recommended)
- 1.5 GB of free space on the hard disk

Manager System Requirements

Windows Operating Systems

- Windows XP (32-bit, SP3; 64-bit, all SPs)
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2003 (32-bit, 64-bit, R2, or SP1 or later)
- Windows Small Business Server 2003
- Windows Server 2008 (32-bit, 64-bit, including R2)
- Windows Small Business Server 2008 (64-bit)
- Windows Essential Business Server 2008 (64-bit)
- Windows Small Business Server 2011 (64-bit)
- Windows Server 2012 (64-bit, including R2)

Hardware

- Intel Pentium Dual-Core or equivalent minimum
- 2 GB of RAM (4 GB recommended)
- 16 GB or more of free space on the hard drive

Web Browser

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome

Database

- Embedded database included or chose from the following:
    - SQL Server 2005, SP4
    - SQL Server 2008, RTM - SP4
    - SQL Server 2008 R2, RTM - SP3
    - SQL Server 2012, RTM - SP1; SP2**
    - SQL Server 2014

* For a complete list of system requirements visit our support page

**Support added in Symantec™ Endpoint Protection 12.1.6 MP1a

More Information

Try it now for FREE

Try the leading solution in endpoint protection by downloading a free 60-day trial today:

http://www.symantec.com/endpoint-protection/trialware

Read third party reviews and find out why Gartner has ranked Symantec as a leader in the Endpoint Protection Platform Magic Quadrant:

http://www.symantec.com/endpoint-protection/news-reviews

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21320633-4 09/15

✓Symantec.™