Symantec™ Endpoint Protection 12.1.5 Datasheet

Data Sheet: Endpoint Security

Overview

Malware has evolved from large-scale massive attacks to include Targeted Attacks and Advanced Persistent Threats that cannot be stopped by antivirus alone. It's time to move beyond antivirus. Symantec's unique ability to provide intelligent security leverages the collective wisdom of the world's largest Global Intelligence Network (GIN) that gathers data from millions of users and sensors. Derived from GIN, the exceptional Insight™ technology in Symantec™ Endpoint Protection blocks mutating threats and enables faster scan time by analyzing a file's reputation. Meanwhile, SONAR™ technology stops zero-day threats by monitoring file behavior in real-time. With a single high-powered agent that integrates intelligent security technologies with strong antivirus and policy lockdown, Symantec™ Endpoint Protection 12.1.5 allows you to focus on your business without compromising security or performance.

Unrivaled security

Stops targeted attacks and advanced persistent threats with intelligent security and layered protection that go beyond antivirus

- Leverages the world's largest Global Intelligence Network (GIN) made up of hundreds of millions of sensors that feed data into our proactive protection technologies
- Derived from GIN, the unique Insight™ technology identifies file reputation by analyzing key file attributes such as how often a file has been downloaded, how long has a file 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 GIN, monitors application behavior in real-time and stops targeted attacks and zero-day threats
- Network Threat Protection analyzes incoming data streams that arrive on a user's machine via network connections and blocks threats before they hit the system
- Symantec™ Endpoint Protection detects and removes more threats than any other solution in its class[1], repeatedly scoring 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.

- The Symantec Insight™ technology included in Endpoint Protection eliminates up to 70 percent of scan overhead compared to traditional solutions by accurately identifying file reputation so only at-risk files are scanned
- Allows hardware to run faster and last longer thanks to reduced system impact
- Reduces network load by providing flexible control over the number of connections and bandwidth
- Out performs all products in its class in scan speed and total performance impact[2]

1. AV-TEST, Product Review, Corporate Solutions for Windows 7, July/August 2013.
2. PassMark Software, "Enterprise Endpoint Security Performance Benchmarks", 2014.

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 PC, Mac, Linux and Virtual machines
- Provides granular policy control with the flexibility to customize policies depending on users and their location
- Supports remote deployment and client management for both PC and Mac 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
- Group Update Provider reduces network overhead and decreases the time it takes to get updates by enabling one client to send updates to another, enabling more effective updates in remote locations

5 Layers of Protection

Symantec™ Endpoint Protection 12.1.5 provides **5-layers of protection-** 1) network 2) file 3) reputation 4) behavior, and 5) repair:

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

2) File: Signature-based antivirus looks for and eradicates malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.

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 and assign a reputation score to each file, effectively protecting against targeted attacks while reducing scan overhead by up to 70%.

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

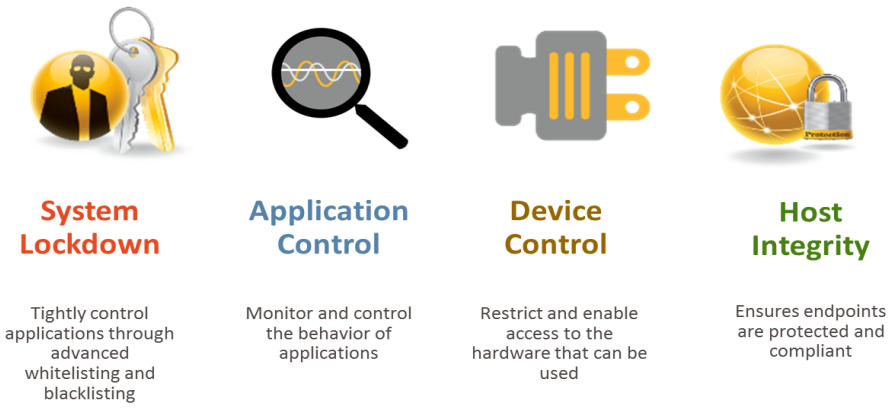
In addition to core protection technologies, Symantec™ Endpoint Protection 12.1.5 also provides granular policy controls, including:

1) System Lockdown: Enhances protection for business critical systems by only allowing whitelisted applications (known to be good) to run or by blocking blacklisted applications (known to be bad) from running

2) Application and Device Control: Helps prevent internal and external security breaches by monitoring application behavior and controlling file access, registry access, processes that are allowed to run, and devices information can be written to

3) Host Integrity Checking & Policy Enforcement: Allows users to run script on their endpoints to verify and report compliance; quarantine location and peer-to-peer enforcement lockdown and isolate a non-compliant or infected system

4) Location Awareness: Automatically detects what location a system is connecting from, such as a hotel, hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment



Virtual Optimization

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 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 virtual machine images.

7) Scan throttling for virtualization- Detects disk load and reduces scan speed to prevent utilization spikes