Symantec™ Endpoint Protection 14

Data Sheet: Endpoint Security

Overview

Last year, we saw 431 million new malware variants, ransomware attacks diversified, and zero-day threats had more than doubled[1]. The threat environment is evolving quickly and given the size and complexity of today's networks, organizations are struggling to keep up. There are many vendors and startups trying to thwart malware infections with alternative methods and point solutions that offer limited protection. Everyone agrees that endpoint security remains critical, but delivering an effective solution is even more challenging than ever.

To protect against today's sophisticated threat landscape, customers need to stop threats regardless of how their endpoints are attacked. Accomplishing this requires certain capabilities:

- Advanced technologies to detect unknown threats and prevent zero day attacks including ransomware
- Memory exploit prevention for popular applications and operating systems
- Access to the richest global threat intelligence to protect against threats in real-time
- Orchestrated response to stop threats quickly
- Proven protection across all devices without compromising performance

Symantec Endpoint Protection 14 is designed to address today's threat landscape with a comprehensive approach that spans the attack chain and provides defense in depth. By utilizing the world's largest civilian threat intelligence network, Symantec Endpoint Protection 14 can effectively stop advanced threats with next generation technologies that apply multi-dimensional machine-learning, reputation analysis, and real-time behavioral monitoring. In addition to essential prevention technologies that are equally important to an organizations overall protection. With a single management console and lightweight agent that can integrate with other products in the security infrastructure to quickly respond to threats, Symantec Endpoint Protection 14 provides the best protection[2] in its class at the endpoint without compromising performance.

Comprehensive Protection across the Attack Chain

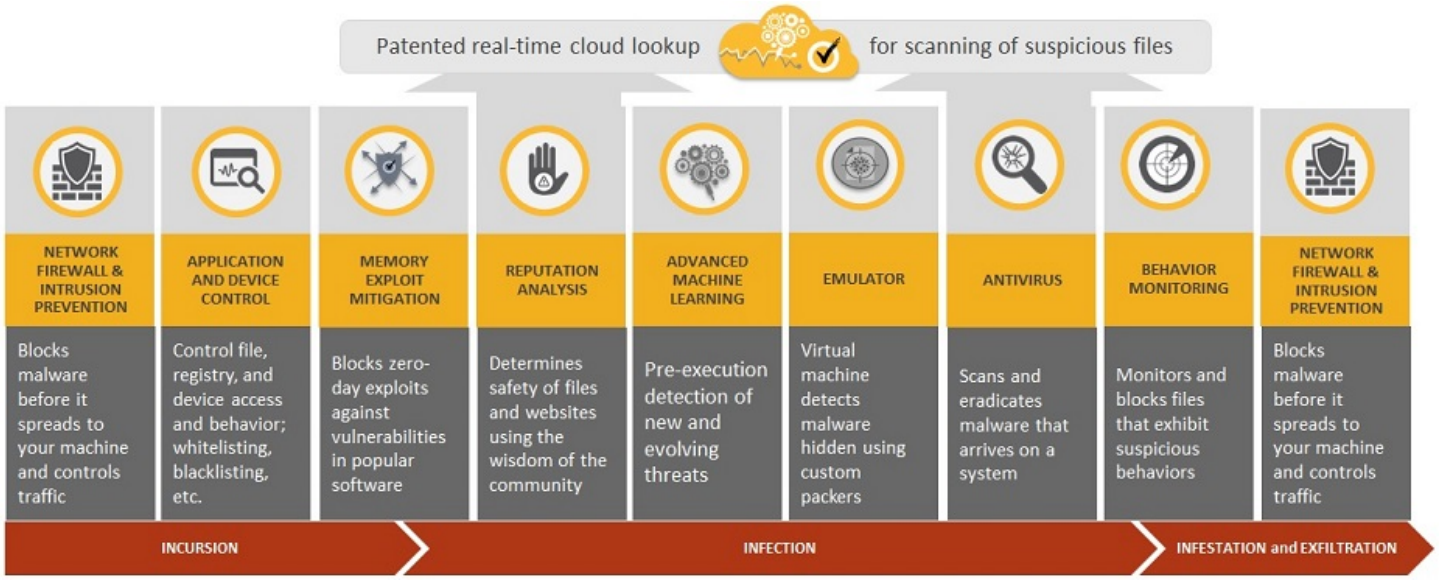
A combination of next generation and essential technologies stop advanced threats and rapidly-mutating malware regardless of how they attack your endpoint - all in a high-performance, lightweight agent.

Incursion:

- ***Network Intrusion Prevention, URL and Firewall Policies***: Symantec's network threat protection technology analyzes incoming and outgoing data and blocks threats while they travel through the network before hitting endpoints. Rules-based firewall and browser protection are available to protect against web-based attacks. In general, with strong network protection, over half of threats can be detected before delivery to the endpoint.
- ***Application Behavioral Control:*** Controls file and registry access and how processes are allowed to run.

1. Symantec Internet Security Threat Report 2016
2. Best Protection Award 2016 from AV-TEST.Org

- ***Device Control:*** 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.
- ***Exploit Prevention:*** Neutralizes zero-day exploits like Heap Spray, SEHOP overwrite, and Java exploits in popular software that have not been patched by the vendor. This signatureless technology works regardless of the flaw, bug, or vulnerability.



Infection:

- ***Exploit Prevention:*** Also plays a role in detecting malware to prevent infection.
- ***Reputation Analysis:*** Symantec's unique reputation analysis utilizes our intelligence network to correlate tens of billions of linkages between users, files, and websites to proactively block more threats and defend against rapidly mutating malware. 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, we can accurately identify whether a file is good or bad and assign a reputation score all before the file arrives at the endpoint. By utilizing file reputation only at-risk files are scanned, effectively eliminating a significant amount of scan overhead.
- ***Machine Learning***: Multi-dimensional machine learning on the endpoint stops new and unknown threats reducing our dependence on signatures. Using the trillions of samples of good and bad files in the global intelligence network to training the machine learning results in a very low false positive rate.
- *Emulation:* The high-speed emulator detects malware hidden using polymorphic custom packers. The static data scanner runs each file in milliseconds in a lightweight virtual machine to cause threats to reveal themselves, improving not only our detection rates but performance.
- ***Anti-virus File Protection***: 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
- ***Behavioral Monitoring***: Behavioral monitoring within Symantec Endpoint Protection is very effective, even though few threats make it to this point undetected. It leverages machine learning to provide zero-day protection, effectively stopping new and unknown threats by monitoring nearly 1,400 file behaviors while they execute in real-time to determine file risk.

Infestation and Exfiltration:

- ***Behavioral Monitoring***: Behavioral monitoring also plays a role in stopping the spread of infection.
- ***Network Intrusion Prevention, URL and Firewall Policies***: Both incoming and outgoing data is analyzed to blocks threats while they travel through the network.

Global Threat Intelligence: Our next-gen technologies take advantage of patented real-time cloud lookup techniques that provide rapid access to the world's largest civilian threat intelligence network. This enhances our machine learning with a deep understanding of the latest threat techniques to provide maximum protection across all endpoints; using our cloud algorithms updated in real-time. Data collected from 175 million endpoints and 57 million attack sensors in 157 countries is analyzed by over a thousand highly skilled threat researchers, providing unique visibility and developing cutting edge security innovations to combat threats.

Advanced Capabilities Deliver High-Performance

Although Symantec Endpoint Protection includes a wide breadth of technologies, it has been optimized so as not to slow down the network or the user; and consistently performs at the top of third party tests in terms of performance.

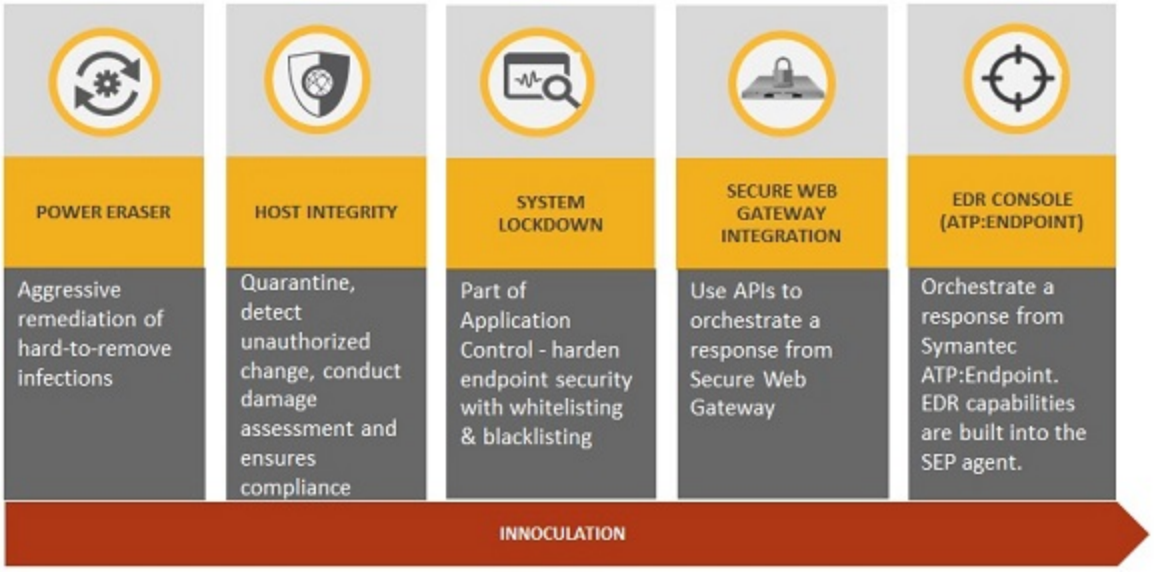
- Intelligent Threat Cloud's rapid scan capabilities using advanced techniques such as pipelining, trust propagation, and batched queries has made it unnecessary to download all signature definitions to the endpoint to maintain a high level of effectiveness. Therefore, only the newest threat information is downloaded, reducing the size of signature definition files by up to 70%, which in turn reduces bandwidth usage.
- With the additional effectiveness provided by Advanced Machine Learning on the endpoint not only has the frequency of downloads been reduced, but there is a minimum of disruption due to false positives to impact productivity.
- The single lightweight agent combines technologies and capabilities normally only obtained through multiple agents: machine learning, exploit mitigation, Endpoint Detection and Response (EDR), and antimalware. This presents the organization with the opportunity to reduce the number of managed agents on their endpoints for possible performance increases; while reducing the burden on IT and lowering total cost of ownership.

Easy Integration for an Orchestrated Response at the Endpoint

Symantec Endpoint Protection includes a single console and agent that offers protection across operating systems, platforms, and businesses of any size.

- **Power Eraser:** An aggressive tool, which can be triggered remotely, to locate advanced persistent threats and remedy tenacious malware.
- **Host Integrity:** 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. Use with threat detection products to orchestrate a response to quarantine an infected endpoint to quickly stop the spread of infection until you can remediate or reimage the endpoint.
- **System Lockdown**: Allow whitelisted applications (known to be good) to run, or blocking blacklisted applications (known to be bad) from running. Symantec Advanced Threat Protection (ATP) and Secure Web Gateway can use the programmable APIs to communicate with the SEP Management (SEPM) Console and orchestrate a response to blacklist newly discovered malicious applications using Application Control. Runs across Windows®, Mac®, Linux®, virtual machines, and embedded systems

- **Secure Web Gateway Integration**: New programmable REST APIs make integration possible with third-party products including Secure Web Gateway, orchestrating a response at the endpoint to quickly stop the spread of infection



- **EDR Console (ATP:Endpoint) Integration**: Symantec Endpoint Protection is integrated with Symantec EDR Console (Advanced Threat Protection (ATP:Endpoint)) designed to detect, respond and block targeted attacks and advanced persistent threats faster by prioritizing attacks. EDR (Endpoint Detection and Response) capability is built into Symantec Endpoint Protection making it unnecessary to deploy additional agents.

Protection, Performance, and Response

Symantec Endpoint Protection is a consistent leader in endpoint protection:

- Repeatedly scoring a AAA rating (the highest score) from SE Labs[3]
- A/V Test[4], 18 months with 100% protection for zero-day attacks
- A leader in the Gartner Magic Quadrant[5] for the last 14 years

3. SE Labs at https://selabs.uk/en/reports/enterprise
4. AV Test at https://www.av-test.org/en/antivirus/business-windows-client/
5. Gartner Magic Quadrant Feb 2016

Client Workstation and Server System Requirements*	
Windows Operating Systems	**Virtual Environments**
Windows Vista (32-bit, 64-bit)	Microsoft Azure
Windows 7 (32-bit, 64-bit, RTM and SP1)	Amazon WorkSpaces
Windows 7 Embedded Standard	VMware WS 5.0, GSX 3.2, ESX 2.5 or later
Windows 8 (32-bit, 64-bit)	VMware ESXi 4.1 - 5.5
Windows 8 Embedded (32 bit)	VMware ESX 6.0
Windows 8.1	Microsoft Virtual Server 2005
Windows 10	Microsoft Enterprise Desktop Virtualization (MED-V)
Windows Server 2008 (32-bit, 64-bit, including R2)	Microsoft Windows Server 2008, 2012, and 2012 R2 Hyper-V
Windows Essential Business Server 2008 (64-bit)	Citrix XenServer 5.6 or later
Windows Small Business Server 2011 (64-bit)	Virtual Box by Oracle
Windows Server 2012 (64-bit, including R2)	**Linux Operating Systems (32-bit and 64-bit versions)**
Windows Server 2016	Red Hat Enterprise Linux
Windows Hardware Requirements	SuSE Linux Enterprise (server/desktop)
1GHz CPU or higher	Oracle Linux (OEL)
512 MB of RAM (1 GB recommended)	CentOS
1.5 GB of free space on the hard disk	Ubuntu
Macintosh Operating Systems	Debian
Mac OS X 10.9, 10.10, 10.11, Mac OS 10.12	Fedora
Mac Hardware Requirements	**Linux Hardware Requirements**
64 - Bit Intel Core 2 Duo or later	Intel Pentium 4 (2 GHz CPU or higher)
2 GB of RAM	1 GB of RAM
500 MB of free space on the hard disk	7 GB of free space on the hard disk

Manager System Requirements	
Windows Operating Systems	**Hardware**
Windows Server 2008 (64-bit, including R2)	Intel Pentium Dual-Core or equivalent minimum
Windows Server 2012 (R2)	2 GB of RAM (8 GB recommended)
Windows Server 2016	8 GB or more free space on the hard drive
Web Browser	**Database**
Microsoft Internet Explorer	Embedded database included or choose from the following:
Mozilla Firefox	SQL Server 2008 R2, SP3, SP4
Google Chrome	SQL Server 2012, RTM - SP1; SP2
Microsoft Edge	SQL Server 2014, RTM and SP1
	SQL Server 2016

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

**Support added in Symantec™ Endpoint Protection 12.1.6 MP1a

Note: Symantec™ Endpoint Protection 12.1.6 MP2 supports Mac OS X10.11

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 or http://go.symantec.com/sep

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 towww.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

21320633-6 10/16