Data Sheet

Symantec Endpoint Protection Family of Security Products

In 2016, ransomware incidents tripled: more than 1 million new malware variants appeared every day, and the average ransom payment more than doubled to $1,077. Having effective endpoint security is critical for protecting complex networks from these numerous and ever-mutating external threats. This means you need complete endpoint security specifically designed to protect, detect, and respond to a rapidly shifting security environment.

Protecting your endpoints in this sophisticated threat landscape requires access to real-time global threat intelligence; advanced technologies to detect unknown threats, prevent zero-day attacks, and stop memory exploits; and an orchestrated response to stop threats quickly.

On-premises or in the cloud

The Symantec™ Endpoint Protection family of security products spans the attack chain and provides defense in depth. With the world's largest civilian threat intelligence network, Symantec Endpoint Protection 14, Symantec Endpoint Protection Small Business Edition, and Symantec Endpoint Protection Cloud options all effectively use machine learning, file reputation analysis, and real-time behavioral monitoring to stop advanced threats. Using either a single cloud or on-premises management console and lightweight agent, the Endpoint Protection family of products provides security without compromising performance.

Whether you need cloud or on-premises management, simplified setup with security policy controls already set, or fine-grained policy control, Symantec's portfolio of endpoint protection options meets your specific business requirements.

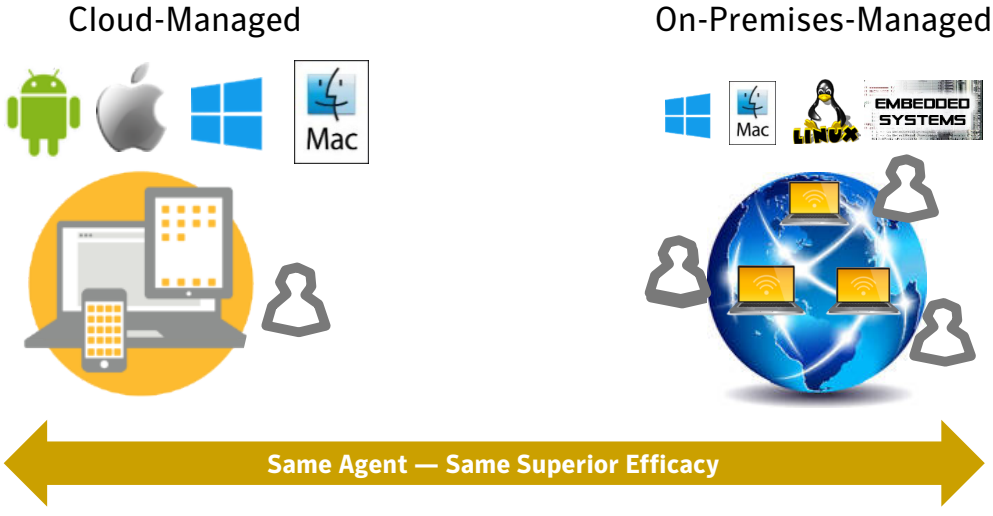

Figure 1 Cloud or on-premises endpoint protection options meet your specific business requirements.

Symantec™

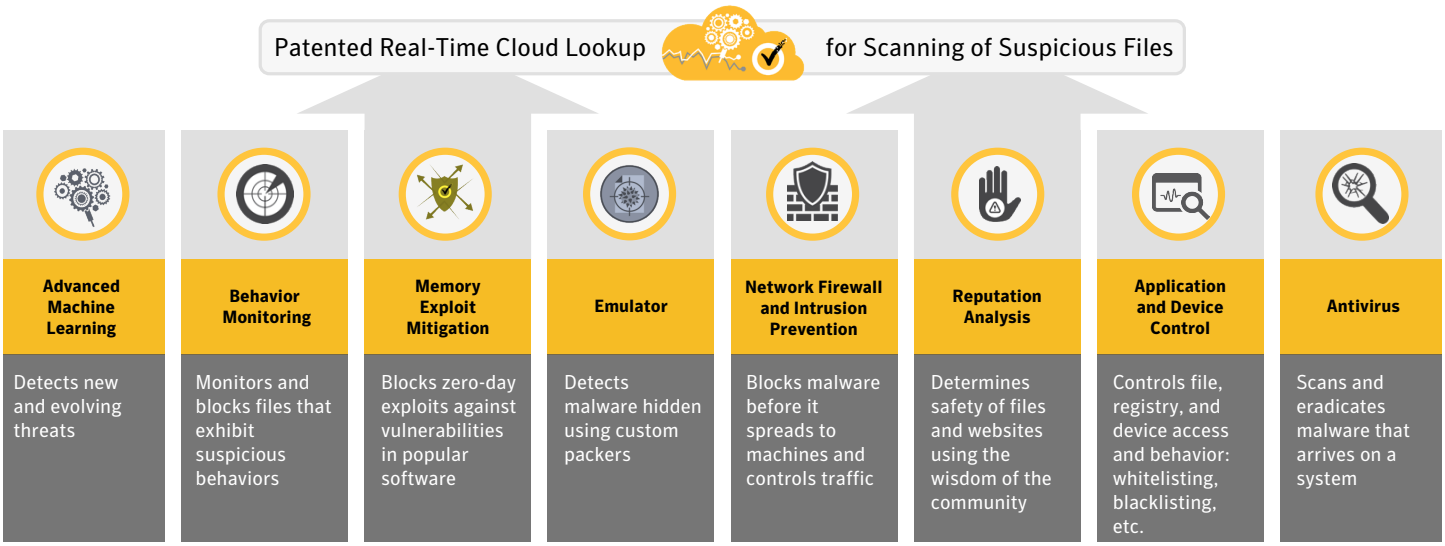

Figure 2 Combination of Symantec technologies protects across the attack chain.

Protection across the attack chain

A combination of technologies works together to stop advanced threats and rapidly mutating malware regardless of how they attack your endpoints:

- **Advanced machine learning:** Stop new and unknown threats while reducing dependence on signatures, using the trillions of samples of good and bad files in the Symantec Global Intelligence Network to train the machine-learning results in a very low false-positive rate.
- **Behavior monitoring:** Effectively stop new and unknown threats by monitoring nearly 1,400 file behaviors while they execute in real time to determine file risk.
- **Memory exploit mitigation:** Signatureless technology works regardless of flaw, bug, or vulnerability to neutralize zero-day exploits like heap spraying and attacks on Structured Exception Handler Overwrite Protection (SEHOP) and Java™ exploits in popular software that has not been patched by the vendor.
- **Emulation:** 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 force threats to reveal themselves, improving both detection rates and performance.
- **Network firewall and intrusion prevention:** Network threat protection technology analyzes incoming and outgoing traffic and blocks threats while they travel through the network before hitting endpoints. A rules-based firewall and browser protection are available to protect against web-based attacks. With strong network protection, you can detect most threats before they reach endpoints.
- **File reputation analysis:** Symantec Global Intelligence Network correlates tens of billions of linkages between users, files, and websites to block more threats and defend against rapidly mutating malware. By analyzing key attributes such as how often a file has been downloaded, how long it has existed, and where it is being downloaded from, it can accurately identify whether a file is good or bad and assign a reputation score—all before the file arrives at the endpoint. File reputations eliminate a significant amount of scan overhead by limiting scans to at-risk files.
- **Application and device control:** Limit file and registry access and determine how processes are allowed to run. Restrict access to certain hardware, and control what types of devices can upload or download information. Combine external media control with application control for more flexible control policies.
- **Antivirus file protection:** Signature-based antivirus and advanced file heuristics look for and eradicate malware on systems to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.

Advanced capabilities for high performance

Although Symantec Endpoint Protection includes a wide variety of technologies, it has been optimized to work without slowing down the network or the user, consistently performing at the top of third-party benchmarks:

- Rapid scan capabilities use advanced techniques such as pipelining, trust propagation, and batched queries to avoid downloading all signature definitions to the endpoint. Downloading only the latest signature definitions reduces the size of definition files by up to 70 percent, which reduces bandwidth usage.
- Advanced machine learning on the endpoint reduces download frequency and minimizes user disruption due to a low rate of false positives.
- Single lightweight agent that combines technologies and capabilities normally only obtained through multiple agents—exploit mitigation, endpoint detection and response, and antimalware—reduces IT management overhead and increases overall endpoint performance.

Symantec named consistent leader in endpoint protection

- **18 months with 100 percent protection for zero-day attacks, AV-TEST**
- **Gartner Magic Quadrant leader for past 15 years**
- **Five-star rating and recommendation, SC Magazine, August 2016**
- **Overall highest endpoint security score, PassMark Software, Enterprise Endpoint Security, Performance Benchmarks, February 2017**

Symantec Global Threat Intelligence Network

Our patented real-time cloud lookup techniques provide rapid access to the world's largest civilian threat intelligence network. More than 1,000 highly skilled threat researchers analyze data collected from 175 million endpoints and 57 million attack sensors in 157 countries. Our machine-learning algorithms are updated in real time, with a deep understanding of the latest threat techniques, and provide maximum protection across all endpoints.

Easy integration for orchestrated response at the endpoint

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

- **Symantec Power Eraser:** Aggressive tool can be triggered remotely to address advanced persistent threats and remove tenacious malware.
- **Host Integrity:** Endpoints remain 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. You can use Host Integrity with threat detection products to orchestrate a quarantine of an infected endpoint to quickly stop the spread of infection until you can remediate or reimage it.
- **System Lockdown:** You can allow whitelisted applications (which are known to be good) to run, or block blacklisted applications (known to be bad) from running. Symantec Advanced Threat Protection and Symantec Secure Web Gateway can use the programmable APIs to communicate with the Symantec Endpoint Protection Manager console to blacklist newly discovered malicious applications using the Application Control feature.
- **Secure web gateway integration:** Programmable REST APIs allow integration with existing security infrastructure including the secure web gateway, allowing you to orchestrate endpoint responses to quickly stop the spread of infection.

Features	Symantec Endpoint Protection Cloud	Symantec Endpoint Protection Small Business Edition	Symantec Endpoint Protection 14
Protection and Performance			
Advanced machine learning	√	√	√
Memory exploit mitigation	√	√	√
Behavioral monitoring	√	√	√
Emulator	√	√	√
Intrusion prevention	√	√	√
File reputation analysis	√	√	√
Antivirus	√	√	√
Password protection and OS device controls	√		
Granular device controls	√	√	√
Wi-Fi and email access	√		
Host Integrity			√
Application rules		√	√
Platform Support			
Client OS	Windows®, Mac®	Windows, Mac	Windows, Mac, Linux®
Mobile OS	Android®, iOS®		
Windows Server®	√	√	√
Orchestration, Usability, and Scale			
On-premises deployment/cloud hosted service	Cloud hosted	Cloud hosted	On-premises
Cross-platform user-based policies	√		
Reporting capabilities	√	√	√
Regional update distribution		√	√
Identity provider integration	Azure® Active Directory®, Symantec VIP Access Manager, Okta	Active Directory	Active Directory, LDAP

Feature Table: Symantec Endpoint Protection family of security products

Learn more about **Symantec Endpoint Protection Cloud, Symantec Endpoint Protection Small Business Edition, and Symantec Endpoint Protection 14**.

To speak with a product specialist in the United States, call (800) 745-6054 toll-free. For other countries, visit our website for **contact information**.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec Corporation World Headquarters | 350 Ellis Street, Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com