Symantec Endpoint Protection 14

The Most Complete Endpoint Security Solution for the Cloud Generation

At-a-Glance

Protect endpoints from all attack vectors at industry leading efficacy with a single agent architecture

- Defend against ransomware and other emerging threats with multilayered protection that fuses signatureless technologies like advanced machine learning, behavior analysis and exploit prevention with proven protection capabilities like intrusion prevention, reputation analysis and more
- Gain enhanced visibility into suspicious files via tunable protection to make better policy decisions
- Use deception techniques to expose hidden adversaries and determine their intent to improve security posture
- Shield commonly used applications against vulnerability exploits and isolate suspicious applications from malicious activity

Realize integrated cyber defense at scale

- Detect threats anywhere and respond with SEP by integrating with network security infrastructure such as web and email gateways
- Integrate with EDR for incident investigation and response leveraging the same SEP agent
- Integrate with existing IT infrastructure for automation and orchestration with open-APIs

Enable business with a high-performance, lightweight solution

- Optimize content update frequency for endpoints with network bandwidth constraints without compromising security efficacy
- Boost performance with a lightweight agent and virus definition sets that require minimal network bandwidth usage (70% less compared to SEP12)
- Speed detection with advanced design techniques and patented real-time cloud lookup that delivers faster scanning times (15% faster compared to SEP12)

Introduction

With the constant evolving nature of today's IT environment, attackers are using more sophisticated attacks to infiltrate networks and the endpoint represents the last line of defense. Organizations are more concerned about cyber damage and disruption as ransomware attacks are trending upward as was evident with the WannaCry and Petya outbreaks. In addition, the attackers' expanding use of file-less and stealthy attacks combined with "living off the land" (leveraging common IT tools for attacks) threatens the confidentiality, integrity, and availability of endpoint assets.

So what can security teams do to address cyber attacks? Managing multiple point products and technologies is overwhelming and challenges mount when managing security across multiple geographies with diverse operation systems and platforms. With limited resources and limited budgets, security teams want easy-to-manage technologies that can integrate with each other to improve overall security. They do not need "just another point product." See Figure 1.

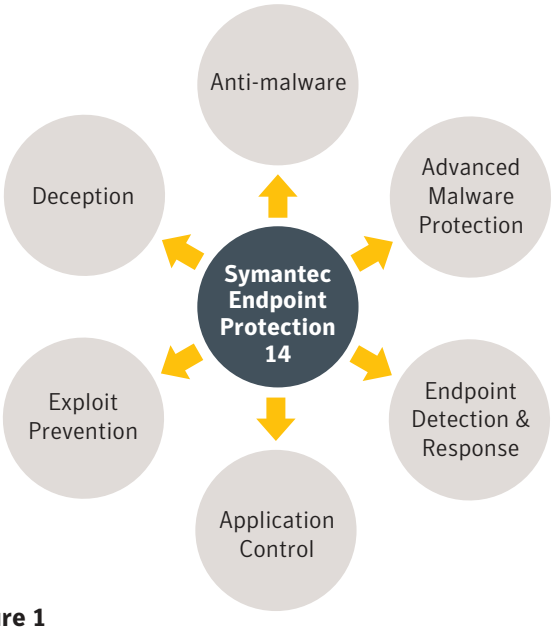

Figure 1

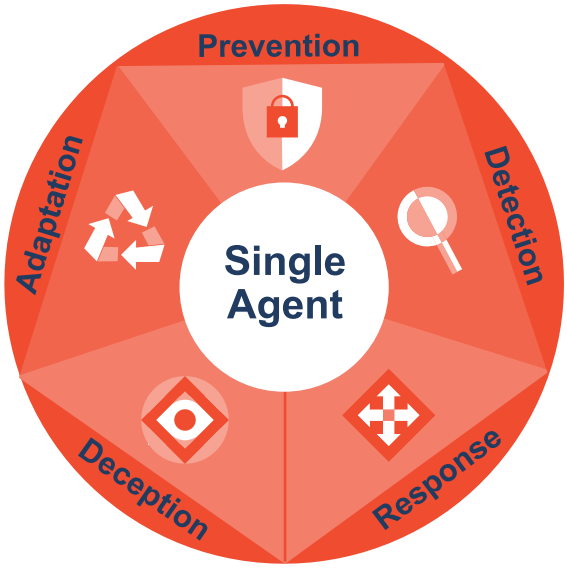

Figure 2. The SEP Security Framework

Symantec Endpoint Protection (SEP) delivers superior, multilayer protection to stop threats regardless of how they attack your endpoints. SEP integrates with existing security infrastructure to provide orchestrated responses to address threats quickly. The single, lightweight SEP agent offers high performance without compromising end-user productivity, so that you can focus on your business. SEP enables security personnel to execute on many security use cases as outlined by the security framework in Figure 2.

Protect Endpoints from all Attack Vectors at Industry Leading Efficacy with a Single Agent Architecture

PREVENTION

SEP protects endpoints regardless of where attackers strike on the attack chain as show in Figure 3. SEP's security efficacy leads the industry as validated by third parties. This level

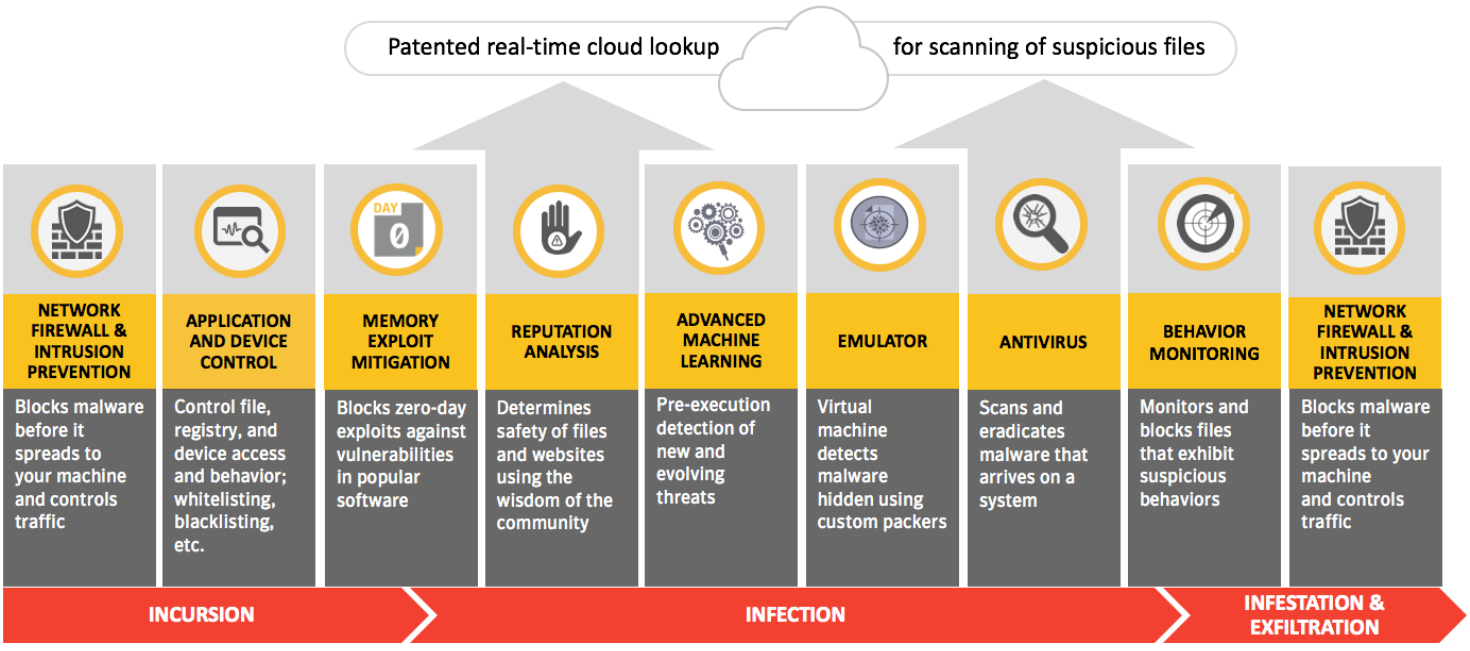

Figure 3.

of prevention is only possible with a combination of core technologies and new, leading-edge technologies.

SIGNATURELESS TECHNOLOGIES

- **Advanced Machine Language (AML)** – detects new and evolving threats, pre-execution.
- **Memory Exploit Mitigation** – blocks zero-day exploits against vulnerabilities in popular software.
- **Behavior Monitoring** – monitors and blocks file that exhibit suspicious behaviors.

ADVANCED CAPABILITIES

- **Global Intelligence Network (GIN)** – the world's largest civilian threat intelligence network informed by 175 million endpoints and 57 million attacks sensors across 157 countries. The data collected is analyzed by more than a thousand highly skilled threat researchers to provide unique visibility and cutting edge security innovations against threats.
- **Reputation Analysis** – determines safety of files and websites using artificial intelligence techniques in the cloud and powered by the GIN.
- **Emulator** – Uses a lite-sandbox to detect polymorphic malware hidden by custom packers.
- **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.
- **Secure Web Gateway Integration** – New programmable REST APIs make integration possible with existing security infrastructure including Secure Web Gateway, orchestrating a response at the endpoint to quickly stop the spread of infection.

CORE CAPABILITIES

- **Antivirus** – scans and eradicates malware that arrives on a system.
- **Firewall and Intrusion Prevention** – blocks malware before it spreads to the machine and controls traffic.
- **Application and Device Control** – controls file, registry, and device access and behavior; also offers whitelisting and blacklisting.
- **Power Eraser** – an aggressive tool, which can be triggered remotely, to address 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.
- **System Lockdown** – allows whitelisted applications (known to be good) to run, or block blacklisted applications (known to be bad) from running.

In addition, only SEP allows IT security teams to tune the level of detection and blocking to optimize protection and gain enhanced visibility into suspicious files for each customer environment as shown in Figure 4. This tunable security called Intensive Protection is made available with a new cloud console that integrates automatically with the on-premises SEP Manager and provides an easy workflow to blacklist suspicious files or whitelist any false positives.

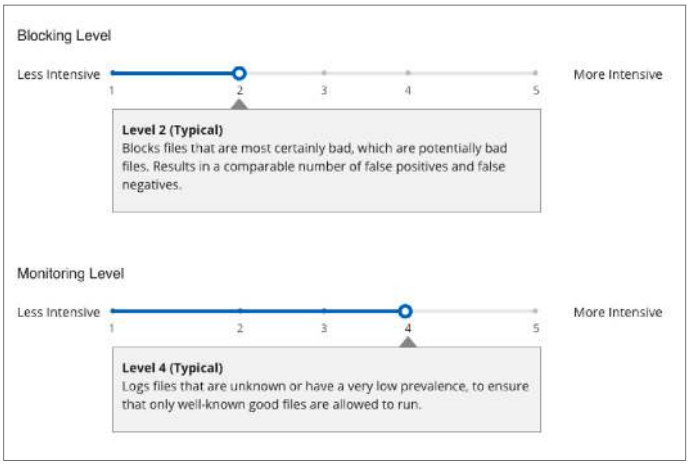

Figure 4. Tunable monitoring and blocking is available via Intensive Protection.

Symantec's single agent architecture enables IT security teams to add innovative security technology with simplified deployment, meaning no new agents are needed.

DETECTION AND RESPONSE (EDR)

Symantec Advanced Threat Protection: Endpoint provides incident investigation and response utilizing the integrated EDR capabilities in SEP. It can be deployed within an hour to expose advanced attacks with precision machine learning, behavioral analytics and threat intelligence minimizing false

positives and helps ensure high levels of productivity for security teams. Symantec's EDR capabilities allow incident responders to quickly search, identify and contain all impacted endpoints while investigating threats using on-premises and cloud-based sandboxing. In addition, continuous recording of system activity supports full endpoint visibility and real-time queries.

Symantec EDR:

- **Detects and Exposes** – Reduce time to breach discovery and quickly expose scope.
- **Investigates and Contains** – Increase incident responder productivity and ensure threat containment.
- **Resolves** – Rapidly fix endpoints and ensure threat does not return.
- **Enhances Security Investments** – Pre-built integrations and public API's.

DECEPTION

SEP Deception[1] plants deceptors (i.e. baits) to expose hidden adversaries and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture. SEP Deception features accurate and insightful detection while delivering fast time to value. Joint Symantec Endpoint Protection and Symantec Managed Security Services customers benefit from 24x7 real-time SEP Deception monitoring and response by a global team of experts. Symantec is the only endpoint protection platform vendor offering deception.

SEP Deception:

- Uses lures and baits for proactive security to expose and delay attackers.
- Determines attacker intent to improve security posture.
- Delivers deception at scale to simplify deployment and management.

ADAPTATION

SEP Hardening is a cloud delivered advanced application defense solution that provides comprehensive protection for applications by isolating suspicious apps and shielding trusted ones. Unlike point products from other application isolation vendors, SEP Hardening, in combination with SEP, delivers unprecedented efficacy against malware and suspicious applications. In addition, SEP Hardening maintains high employee productivity by fully supporting standard employee workflows.

SEP Hardening:

- Comprehensive application security by minimizing the attack surface.
- Unprecedented visibility by discovering and categorizing all endpoint applications.
- Fastest speed to value by leveraging SEP's single agent architecture.

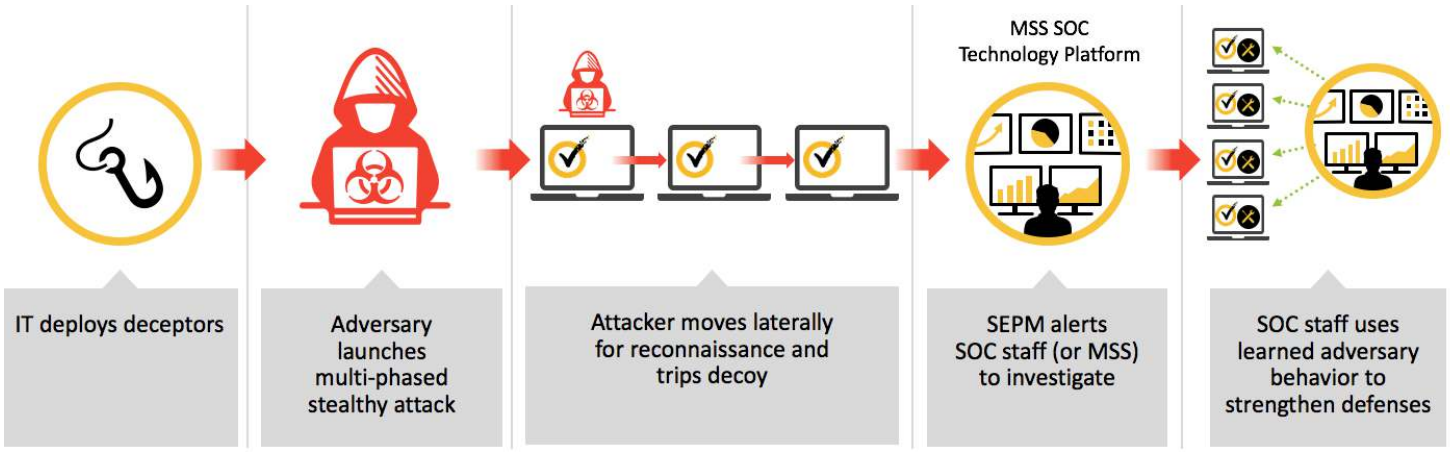

Figure 5. How SEP Deception works?

[1] Consulting services are required to configure and deploy the SEP Deception feature.

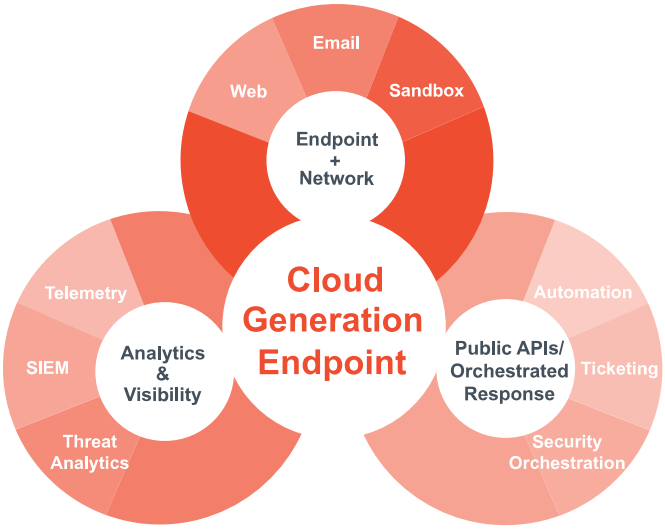

Figure 6.

Realize Integrated Cyber Defense at Scale

Most large organizations support global IT environments that are becoming increasingly complex. Many implemented solutions only do a very specific job. Therefore, organizations need an endpoint protection solution that provides greater value and better overall protection by integrating with other IT security solutions to share intelligence and defend the network together.

SEP 14 is a foundational product that facilitates integration so that IT security teams can detect threats anywhere in their network and address these threats with orchestrated responses. SEP 14 works alongside Symantec solutions (for example, as a key component of the Integrated Cyber Defense Platform and with 3rd party products (via published APIs) to strengthen security posture. Symantec's Integrated Cyber Defense Platform unifies cloud and on-premises security to protect users, information, messaging and the web, powered by unparalleled threat intelligence. No other vendor provides an integrated solution that orchestrates a response at the endpoint (blacklists and remediation) triggered by the detection of a threat at the network gateway (i.e. web and email security gateways).

Enable Business with a High-performance, Lightweight Solution

Large and/or frequent content updates take up bandwidth, reduce endpoint performance, and compromise productivity. Optimizing content updates and delivering better detection of threats is a win-win. These capabilities reduce the IT team's burden for scheduling frequent security updates. And end users do not have the hassle of security updates impacting productivity.

SEP 14 delivers better protection with better performance and lower bandwidth requirements. Symantec consistently scores at the top in 3rd party performance tests including Passmark Software's Enterprise Endpoint Security Performance Benchmark tests for Windows 7 and Windows 10. Visit the Symantec Performance Center for additional third-party validation symantec.com/products/performance-center.

Significant performance increases within SEP include:

- Reducing content update sizes by 70%[2]
- Delivering 15% faster detection scan times[2]

Compared to emerging vendors, SEP offers less endpoint complexity by bundling multiple capabilities in a single, lightweight agent. Attempting to match Symantec endpoint security capabilities would require multiple emerging vendors, multiple solutions, and certainly multiple agents.

[2] Gains from SEP 12 to SEP 14.

System Requirements

Client Workstation and Server System Requirements*

Windows® Operating Systems

- Windows Vista (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit; RTM and SP1)
- Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows Embedded 8 Standard (32-bit and 64-bit)
- Windows 8.1 (32-bit, 64-bit), including Windows To Go
- Windows 8.1 update for April 2014 (32-bit, 64-bit)
- Windows 8.1 update for August 2014 (32-bit, 64-bit)
- Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)
- Windows 10 November Update (2015) (32-bit, 64-bit)
- Windows 10 Anniversary Update (2016) (32-bit, 64-bit)
- Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2)
- Windows Small Business Server 2008 (64-bit)
- Windows Essential Business Server 2008 (64-bit)
- Windows Small Business Server 2011 (64-bit)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 update for April 2014
- Windows Server 2012 R2 update for August 2014
- Windows Server 2016

Windows Hardware Requirements

- 1.9 GHz CPU or higher
- 1 GB of RAM (2 GB recommended)
- 530 MB of free space on the hard disk

Macintosh® Operating Systems

- Mac OS X 10.10, 10.11, macOS 10.12, 10.13

Mac Hardware Requirements

- 64-bit Intel Core 2 Duo or later
- 2 GB of RAM
- 500 MB of free space on the hard disk

Virtual Environments

- Microsoft Azure
- Amazon WorkSpaces
- VMware WS 5.0, GSX 3.2, ESX 2.5 or later
- VMware ESXi 4.1 – 5.5
- VMware ESX 6.0
- 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
- Oracle Cloud
- Virtual Box by Oracle

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

- Amazon Linux
- CentOS 6U3, 6U4, 6U5, 6U6, 7, 7U1, 7U2, 7U3; 32-bit and 64-bit
- Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit
- Fedora 16, 17; 32-bit and 64-bit
- Oracle Linux (OEL) 6U2, 6U4, 6U5, 7, 7.1, 7.2, 7.3
- Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U8, 7 - 7.3
- SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP3; 32-bit and 64-bit; 12
- SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP3; 32-bit and 64-bit
- Ubuntu 12.04, 14.04, 16.04; 32-bit and 64-bit

Linux Hardware Requirements

- Intel Pentium 4 (2 GHz CPU or higher)
- 1 GB of RAM
- 7 GB of free space on the hard disk

Manager System Requirements

Windows® Operating Systems

- Windows Server 2008 (64 bit), including R2)
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2012 R2
- Windows Server 2016

Web Browser

- Microsoft Internet Explorer 11
- Mozilla Firefox 5.x through 55.x
- Google Chrome 61.x
- Microsoft Edge

Hardware

- Intel Pentium Dual-Core or equivalent minimum
- 2 GB of RAM (8 GB recommended)
- 8 GB or more free space on the hard disk

Database

Embedded database included or choose from the following:

- SQL Server 2008, SP4
- SQL Server 2008 R2, SP3
- SQL Server 2012, RTM – SP3
- SQL Server 2014, RTM – SP2
- SQL Server 2016, RTM, SP1

SEP Hardening Supports the Following Operating Systems:

- Windows 7 (64-bit; RTM and SP1)
- Windows Embedded 7 Standard, POSReady, and Enterprise (64-bit)
- Windows 8 (64-bit)
- Windows Embedded 8 Standard (64-bit)
- Windows 8.1 (64-bit), including Windows To Go
- Windows 8.1 update for April 2014 (64-bit)
- Windows 8.1 update for August 2014 (64-bit)
- Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (64-bit)
- Windows 10 (64-bit); Windows 10 November Update (2015) (64-bit)
- Windows 10 Anniversary Update (2016) (64-bit)
- Windows 10 Creators Update (2017) (64-bit)

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

Threatscape

To learn more, contact us via info@threatscape.com or on 0203 653 0000 (UK) or 01 901 7000 (Ireland) | www.threatscape.com

Symantec.

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

SYMC_DS_SEP14_CloudGeneration_EN_v1a