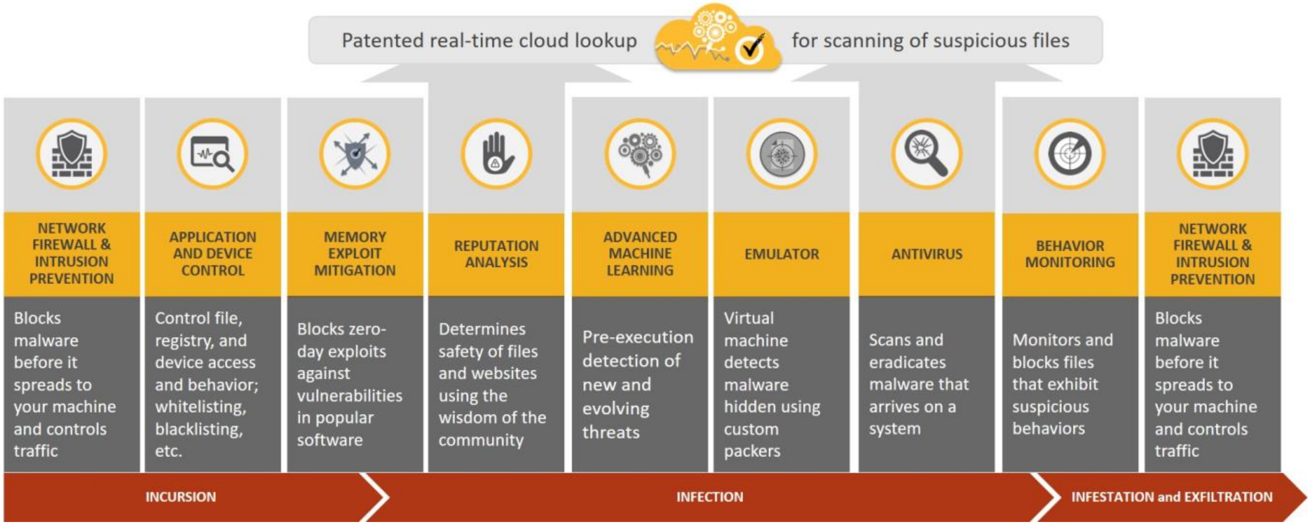
Fix 5 Common Misconfigurations to Dramatically Improve Effectiveness

Symantec™ Endpoint Protection

Overview

Symantec Endpoint Protection is a powerful yet flexible product made up of several protection engines. It is that flexibility, designed to meet the needs of any type of organization, which can lead to misconfigurations that reduces its effectiveness in your environment.



Patented real-time cloud lookup
for scanning of suspicious files
NETWORK FIREWALL & INTRUSION PREVENTION
Blocks malware before it spreads to your machine and controls traffic
APPLICATION AND DEVICE CONTROL
Control file, registry, and device access and behavior; whitelisting, blacklisting, etc.
MEMORY EXPLOIT MITIGATION
Blocks zero-day exploits against vulnerabilities in popular software
REPUTATION ANALYSIS
Determines safety of files and websites using the wisdom of the community
ADVANCED MACHINE LEARNING
Pre-execution detection of new and evolving threats
EMULATOR
Virtual machine detects malware hidden using custom packers
ANTIVIRUS
Scans and eradicates malware that arrives on a system
BEHAVIOR MONITORING
Monitors and blocks files that exhibit suspicious behaviors
NETWORK FIREWALL & INTRUSION PREVENTION
Blocks malware before it spreads to your machine and controls traffic
INCURSION
INFECTION
INFESTATION and EXFILTRATION

Figure 1: The variety of protection engines in Symantec Endpoint Protection across the attack chain

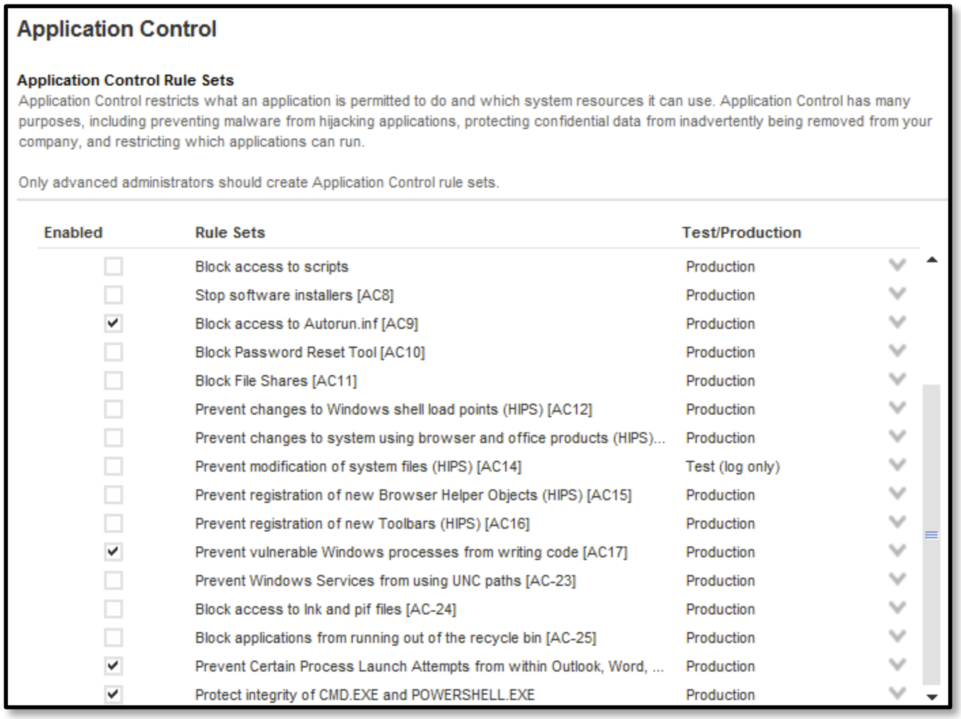
Although you have no doubt been using Symantec Endpoint Protection successfully for some time, we have found that the following 5 misconfigurations are very common. Although they may seem in some cases straightforward, they can result in a dramatic improvement in effectiveness.

Misconfiguration #1: Advanced technologies are disabled

Advanced protection technologies such as Symantec Online Network for Advanced Response (SONAR™), Symantec Insight™, and IPS (Intrusion Prevention System) are sometimes disabled due to false positives. Out-of-the-box Application Control policies are often not reviewed and applied where they can significantly reduce the endpoint attack surface. These signature-less technologies are used to protect endpoints against modern threats like ransomware and script-based attacks.

Recommendation: Enable all engines on workstations. Evaluate false positives on a case-by-case basis and remediate them using whitelisting, code signing, or reporting them to Symantec.

Review the Application Control policies and apply (in test mode initially, then in production mode) any of the out of the box policies that will help reduce the attack surface of your endpoints.



Application Control

Application Control Rule Sets

Application Control restricts what an application is permitted to do and which system resources it can use. Application Control has many purposes, including preventing malware from hijacking applications, protecting confidential data from inadvertently being removed from your company, and restricting which applications can run.

Only advanced administrators should create Application Control rule sets.

Enabled	Rule Sets	Test/Production
□	Block access to scripts	Production
□	Stop software installers [AC8]	Production
☑	Block access to Autorun.inf [AC9]	Production
□	Block Password Reset Tool [AC10]	Production
□	Block File Shares [AC11]	Production
□	Prevent changes to Windows shell load points (HIPS) [AC12]	Production
□	Prevent changes to system using browser and office products (HIPS)...	Production
□	Prevent modification of system files (HIPS) [AC14]	Test (log only)
□	Prevent registration of new Browser Helper Objects (HIPS) [AC15]	Production
□	Prevent registration of new Toolbars (HIPS) [AC16]	Production
☑	Prevent vulnerable Windows processes from writing code [AC17]	Production
□	Prevent Windows Services from using UNC paths [AC-23]	Production
□	Block access to lnk and pif files [AC-24]	Production
□	Block applications from running out of the recycle bin [AC-25]	Production
☑	Prevent Certain Process Launch Attempts from within Outlook, Word, ...	Production
☑	Protect integrity of CMD.EXE and POWERSHELL.EXE	Production

Figure 2: Application Control policy settings can help harden you endpoint

Misconfiguration #2: Out of Date Clients

Clients need to be kept up to date to remain effective and secure. Symantec Endpoint Protection has the potential to affect every client and server in a customer's environment. Similar to Microsoft patches, you should have a plan to distribute Symantec Endpoint Protection's critical patches in an acceptable time. Symantec Endpoint Protection Manager has the ability to deliver delta packages to ensure patches are as small as possible so as not to affect performance.

Maintaining software currency for your Symantec Endpoint Protection estate means you can maximize the benefit of new protection capabilities available for it and minimize your organizations risk exposure.

Recommendation: Ensure that client updates are enabled and review Symantec Endpoint Protection reports showing out of date clients. Review the compensating control capabilities (such as Application & Device control or Host Integrity policies) to increase the protection levels on any categories of clients that cannot, for operational reasons, keep track with the latest releases.

Fix 5 Common Misconfigurations to Dramatically Improve Effectiveness

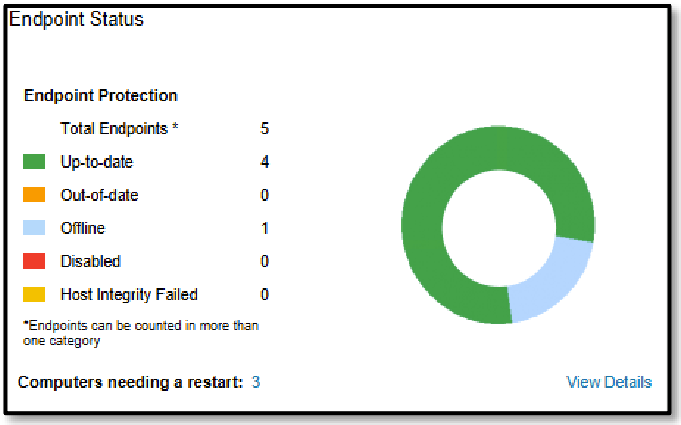
SymantecTM Endpoint Protection

Misconfiguration #3: Outdated Exceptions

Exceptions are often created to address false positives, but they are sometimes too broad and are easily forgotten. These exceptions can add up over time and create holes in your endpoint defense for malware to take advantage of. When impacted applications are upgraded, legacy exceptions are often “orphaned” and can provide an unnecessary attack vector for a well-planned malicious incursion.

Recommendation: Review existing exceptions and determine if they are still needed or if they are overly broad.

Include the review of Symantec Endpoint Protection exceptions as part of a regular change control board process to ensure that the requirement for such exceptions are still current.



Endpoint Status

Endpoint Protection

	Total Endpoints *	5
🟩	Up-to-date	4
🟧	Out-of-date	0
🟦	Offline	1
🟥	Disabled	0
🟨	Host Integrity Failed	0

*Endpoints can be counted in more than one category

Computers needing a restart: 3

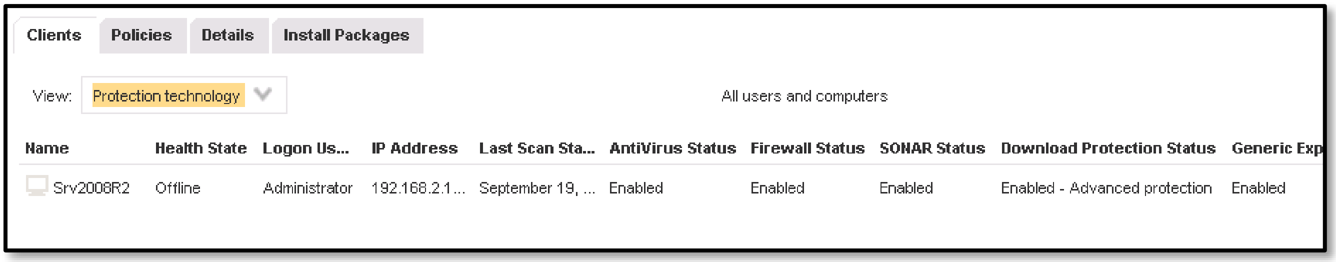
Figure 3: Review Out of Date clients regularly

Misconfiguration #4: Users Can Change Client Settings

Symantec Endpoint Protection has very strong tamper protection, but if users are able to add exceptions and disable protection engines, they can unintentionally weaken your endpoint security.

Recommendation: Review all of your Symantec Endpoint Protection policies and configure client policies to restrict users from modifying any security settings your organization considers mandatory.

Review the Symantec Endpoint Protection Mangement console client status (Protection Technology view) or run a “Computer Status” Log Monitor job using the “compliance options” filters and investigate any clients where the status of protection engines is non-compliant with your corporate policy. Learn how to block a user’s ability to disable Symantec Endpoint Protection on clients in this technology brief.



View: Protection technology

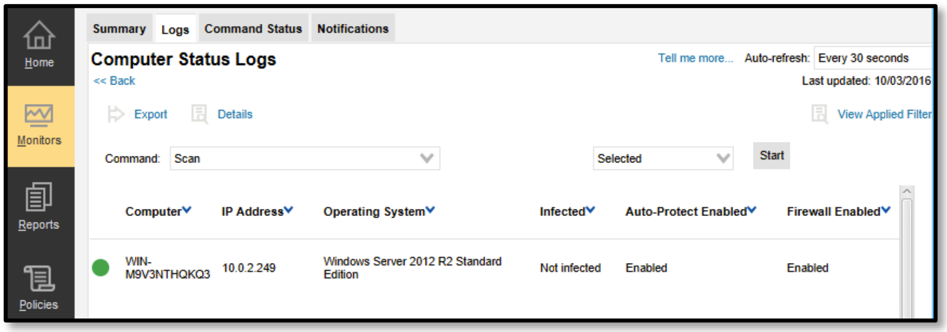
All users and computers

Name	Health State	Logon Us...	IP Address	Last Scan Sta...	AntiVirus Status	Firewall Status	SONAR Status	Download Protection Status	Generic Exp
Srv2008R2	Offline	Administrator	192.168.2.1...	September 19, ...	Enabled	Enabled	Enabled	Enabled - Advanced protection	Enabled

Figure 4: Review Symantec Endpoint Protection Manager Console client status

Fix 5 Common Misconfigurations to Dramatically Improve Effectiveness

Symantec™ Endpoint Protection



Computer Status Logs

<< Back

Tell me more... Auto-refresh: Every 30 seconds

Last updated: 10/03/2016

Export Details View Applied Filter

Command: Scan Selected Start

Computer	IP Address	Operating System	Infected	Auto-Protect Enabled	Firewall Enabled
● WIN-M9V3NTHQKQ3	10.0.2.249	Windows Server 2012 R2 Standard Edition	Not infected	Enabled	Enabled

Figure 5: Check compliance by running a Computer Status Log monitor job

Misconfiguration #5: External Communication

Symantec Endpoint Protection uses Insight to perform reputation lookups of files, URLs, and code signers in conjunction with its other engines. If the External Communication policy is misconfigured or if Insight is disabled, this lookup will fail and Symantec Endpoint Protection will be less effective at detecting malware.

Recommendation: Ensure Symantec Endpoint Protection clients can perform Insight lookups by reviewing client logs in the Symantec Endpoint Protection Manager

Conclusion

Symantec Endpoint Protection provides powerful protection capabilities. Ensure they're working for you as effectively as possible by addressing any misconfigurations that exists in your environment.

Stay safe with Symantec Endpoint Protection. Get the broadest array of overlapping protection engines consisting of both next-gen and essential technologies to deliver the protection you need against advanced threats. The high-speed, lightweight single agent also provides capabilities to orchestrate a response using programmable APIs through the Symantec Endpoint Protection management console, quarantining or blocking threats to quickly stop the spread of infection. While additional next-gen capabilities ensure advanced features do not impact performance or the end-user.

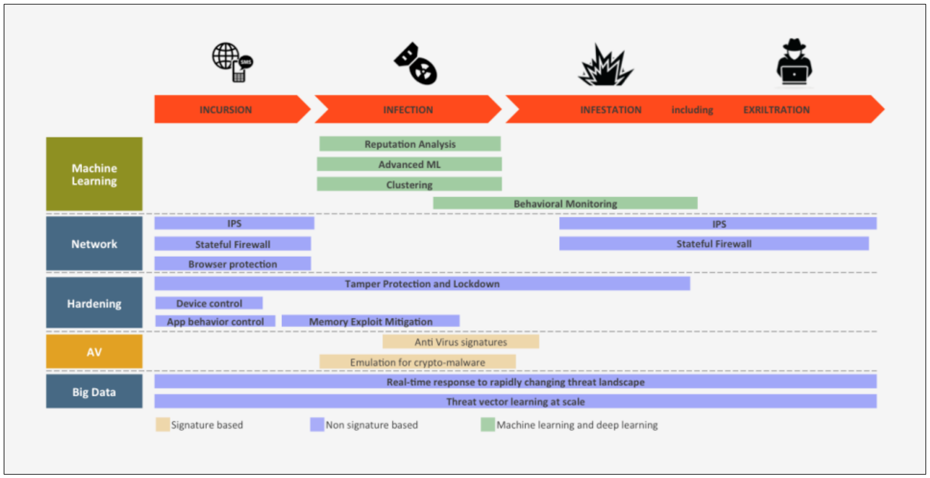


Figure 6: Overlapping technologies provide superior protection

Learn more about what's new in Symantec Endpoint Protection 14 at go.symantec.com/sep.