DATA SHEET

Symantec Endpoint Application Control

Minimize the endpoint attack surface

At a Glance

Comprehensive Application Discovery and Risk Assessment

- Gain a complete inventory of all endpoint applications and respective vulnerabilities
- Gain actionable insight with recommendations on how to manage new applications

Optimized Endpoint Hardening

- Deliver fixed-function device lockdown by enforcing default-deny to apps and restricting updates to defined trusted updaters
- Offer continuous monitoring to detect and alert on any application drift

Easy Deployment and Management

- Utilizes the same single Symantec Endpoint Protection agent and cloud console to reduce overhead
- Minimize effort with smart auto-generation of allow and block rules

Introduction

With the constant evolving nature of today's IT environment, attackers are using more sophisticated attacks to infiltrate networks. This trend is highlighted by Symantec's 2018 ISTR report that states a 46% increase in ransomware variants and a 92% increase in downloader variants. Endpoints are especially vulnerable due to their large attack surface and the endpoint represents the last line of defense. Attackers use ransomware, crytpojacking, and an assortment of sophisticated attacks to gain a foothold onto the endpoint to compromise the corporate environment. Attackers gain entry to conduct reconnaissance and ultimately to execute an attack.

Now given the above security concerns and the broad use of Shadow IT, i.e. applications not sanctioned by centralized IT, the security team needs to properly limit downloadable and allowed applications. So, how do IT teams balance security with employee productivity as end users want to fully browse the Internet and download any useful utility? In addition, how can IT teams address the shortage of security resources and expertise in light of the 7+ security technologies (agents) that are normally deployed onto endpoints. In the battle against advanced malware, IT security needs a solution that will keep employees productive and reduce the attack surface without adding undue burden to an already overworked team.

Symantec Endpoint Application Control

Symantec Endpoint Application Control minimizes the attack surface and delivers advanced application defenses. It provides comprehensive application visibility by discovering and classifying application risk levels. It uses this information, in combination with SEP, to offer unprecedented efficacy against malware and suspicious applications. It delivers value quickly by using the same SEP single agent. There is no need for deploying an additional agent. In addition, Application Control helps maintain high employee productivity by fully supporting standard employee workflows. See figure 1 for how Application Control fits into the Symantec single agent solution.

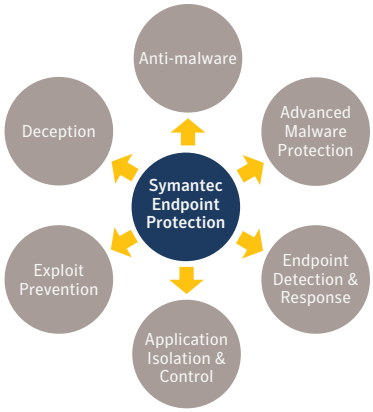

Figure 1. How Application Control fits into the Symantec Endpoint Protection Framework.

Application Visibility

Symantec Endpoint Application Control relies on a robust discovery engine that uncovers all the applications operating in the environment. It discovers every installed application and its associated files on the endpoint. It also automatically assesses each application's vulnerabilities, reputation, and prevalence to generate a risk score. And with this score, Symantec Endpoint Application Control delivers a risk assessment, actionable insight, and smart recommendations for blocking or allowing the application.

So, with Symantec, there are no more blind spots. As a result, organizations can specify only the apps they want allowed to run to block dangerous and unnecessary apps.

Smart Application Control

Stopping unwanted apps from running

Symantec Endpoint Application Control prevents unauthorized apps from running with control policies based on a broad range of parameters including static application attributes such as: application name, path, hash, publisher, user, and user group. User-based policy rules specify that only prescribed users can have access to the application, thus ensuring 'just-enough' privileges. Rules can also be created based on dynamic attributes such as reputation. Symantec Global Intelligence Network (GIN) lookup provides the latest information on the reputation of an application or file and tells an administrator whether the app is trending good or trending bad. To deliver the most effective application security, hybrid rules combine static and dynamic app attributes to offer real-time protection against emerging threats from malware, APTs, ransomware, crypto-miners, DDOS botnet malware, zero-days, and supply-chain attacks. Please see figure 2 for how application control works.

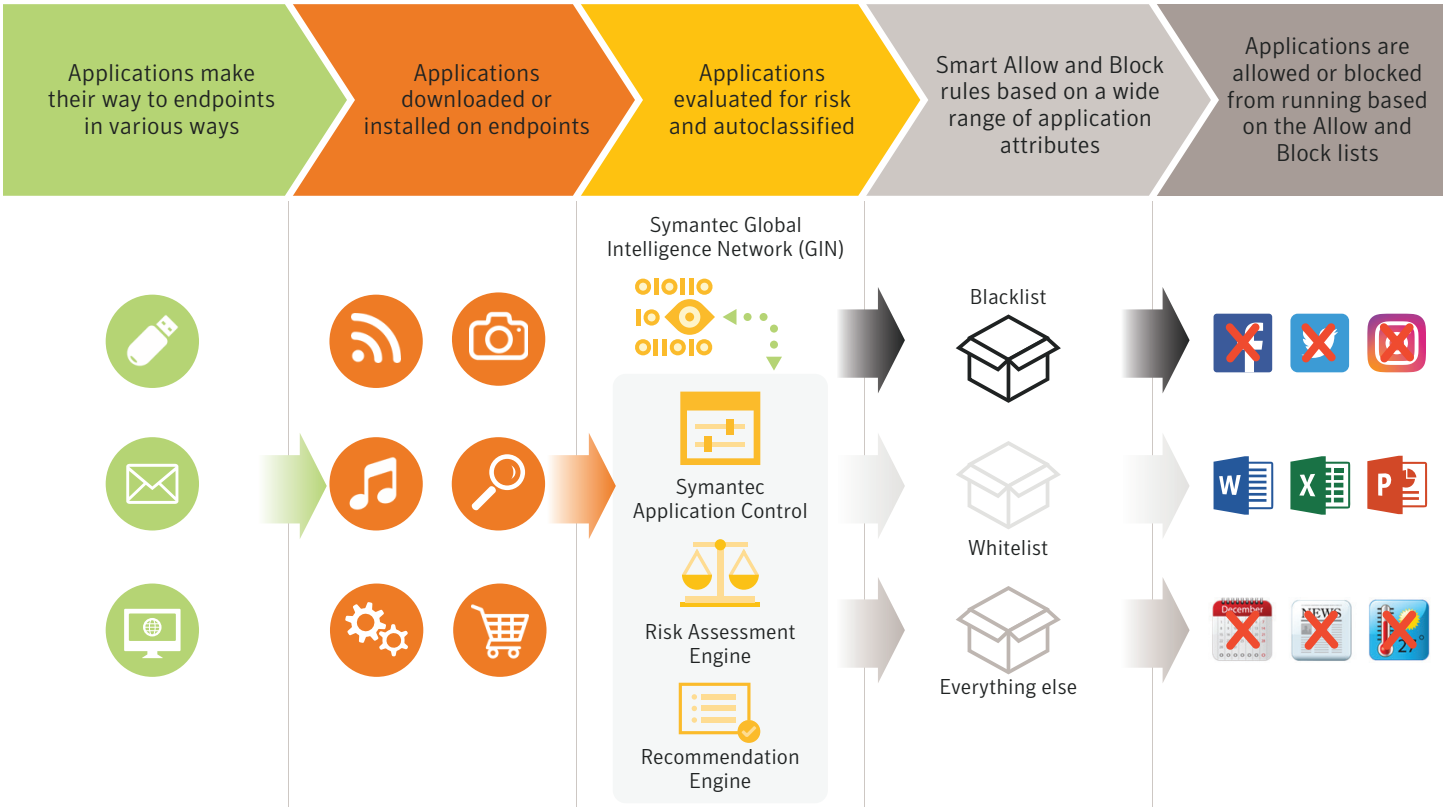

Figure 2. How application control works?

Utilizing trusted updaters

For most endpoints, software updates are desired and required. Symantec Endpoint Application Control enables administrators to define trusted updaters — apps, files, users, user groups — that can install new software or applications on endpoints to patch vulnerabilities and roll out the latest version of software for enhanced functionality. These trusted updaters are granted a fixed set of privileges which allow them to carry out routine tasks in the course of updating or installing new software such as laying down new files on the file system, modifying the file system or registry, and more.

Managing application drift

Drift is introduced when users download various applications on the endpoint that are not explicitly allowed. For example, Application Control checks if the policy allows the end user to override the block. If the app is neither on the whitelist nor the blacklist, and the policy is configured to allow user overrides, then the user is allowed to run the app, and it is reported as "drift." The administrator can then analyze the drift and choose to explicitly block or allow it to run in the environment in the future. Otherwise, failure to address (and stop) undesirable applications running on endpoints can lead to cyber attacks and information theft.

Two key use cases - dynamic workstations and fixed function devices

DYNAMIC WORKSTATIONS

"Restricted execution" for high-change end user workstations prevents unauthorized applications from executing by:

- Allowing a broad range of approved applications governed by flexible rules
- Extending users the flexibility to use unapproved applications when assessed to be safe
- Facilitating regular IT maintenance and upgrades with defined trusted updaters
- Alerting administrators when newly introduced applications (drift) pose a risk to the environment

FIXED FUNCTION DEVICES

Symantec Endpoint Application Control enables you to lock down fixed-function devices, e.g., ATMs, Kiosks, POS devices to a known baseline of applications by:

- Enforcing a default-deny mode where only an approved list of apps can run
- Restricting updates to defined trusted updater mechanisms
- Continuous monitoring to detect and alert on any drift

Easy Deployment and Management

Using the single agent/single console

By sharing the same agent and console as Symantec Endpoint Protection, Application Control is deployed without adding the complexity of an additional agent or console. The software infrastructure is already in place, just configure and deploy policy.

Managing smart rules

Symantec Endpoint Application Control makes policy creation easy through the generation of smart rules, which are based on the assessed risk of apps and other app attributes as discovered on the endpoints. High risk applications have narrow rules using more application attributes to provide tighter control, while low-risk applications have broader rules using fewer application attributes. Administrators can opt for easy policy creation, using simple drag-and-drop capabilities, or can go deeper to define granular rules based on various app attributes. The flexibility of applying policies in different enforcement modes makes it easy to test-drive policies and gradually increase strictness, as required.

Application Control and Application Isolation: Better Together

When Symantec Endpoint Application Control is purchased and implemented together with Symantec Endpoint Application Isolation, the result is a powerful combination that controls what apps can run (app control) and what apps can do (app isolation). Symantec Endpoint Application Isolation prevents applications from executing privileged operations such as downloading executables, writing to the registry, and more. It also shields trusted applications to prevent attacks from exploiting the applications' vulnerabilities.

Why Deploy Symantec Endpoint Application Control

- **Comprehensive visibility** – Discover all applications: running, installed or just on the hard drive as an executable. Also, assess the attack surface and determine the risk of existing vulnerabilities to score each application.
- **Recommendation driven drift management** – Use intelligence to manage and update security control policy for new applications and versions.
- **Reduced complexity with a single agent** – Application Control uses the same SEP agent to deliver better protection without adding an additional agent. Please see figure 3. Therefore, SEP offers operational ease endpoint by combining 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.

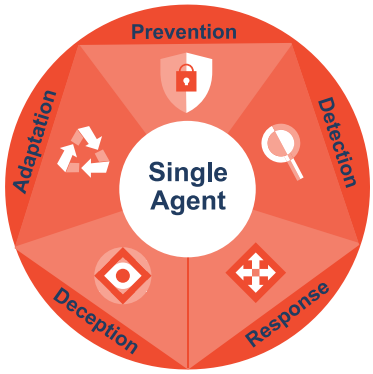

Figure 3. Symantec offers multilayered protection via a single agent for easy deployment and better performance

System Requirements

Client Workstation Requirements*

- Windows 7 (RTM and SP1), Professional Enterprise
- Windows 8, Professional, Enterprise
- Windows 8.1 (update for April 2014 and August 2014; Windows To Go), Professional, Enterprise
- Windows 10 (RTM), Professional, Enterprise
- Windows 10 November Update (version 1511), Professional, Enterprise
- Windows 10 Anniversary Update (version 1607), Professional, Enterprise
- Windows 10 Creators Update (version1703), Professional, Enterprise
- Windows Fall Creators Update (version1709), Professional, Enterprise
- Windows 10 April 2018 Update (version 1803), Professional, Enterprise (Version 14.2 only)

Version 14.0.1.x clients only support 64-bit operating systems. Version 14.2 and later clients support both 32-bit and 64-bit operating systems.

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

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

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

19C197753_ds_ApplicationControl_EN