Application Control—Key to Reducing Application Attack Surface

App Control Reimagined

WHITE PAPER

November 16, 2018

Authors: Praneeta Paradkar, Sheetal Venkatesh
Contributors: Mark Gentile

Contents

The Application Economy—An Application for Everything

The threat landscape is constantly evolving, with attackers developing new techniques to evade detection and increase the efficacy of their attacks. In their quest, they are constantly look for new ways to compromise endpoint devices – in today's "App Economy," applications simultaneously propel organizations forward and provide attackers a way in.

Corporate endpoints are interesting to criminals because of the wealth of information they store and their connection to the corporate network, which has even more valuable assets. With a single flip of a switch on the command-and-control (C2) server, all sensitive and valuable corporate information on an endpoint can be in the hands of an attacker in the blink of an eye. The price of this information can vary, from mere cents to many millions of dollars, in the cybercrime world.

As a result, attackers look for any opportunity to exploit the endpoint, and apps provide the perfect entry point. In the business world today, there is an app for practically everything. All businesses, regardless of what industry they cater to, are in the business of building software (read apps) to enable their core offerings. For example, retail, banking, insurance, healthcare, manufacturing, airlines, all use apps to transact and expand their core products and services.

Typically, when thinking of apps, all the apps on smartphones and mobile devices come to mind. However, apps are everywhere, running on desktops, within sensitive research and development (R&D) centers, and supply chain systems, as well as on ATMs, retail point of sale (POS) machines, kiosks, and healthcare stations.[1]

App prevalence is creating a variety of challenges to an organization's security strategy.

Supply-chain Attacks

The App Economy is responsible for another trend in the business world today - that of rapid app development (RAD), where app vendors increasingly use Open Source Software (OSS) or third-party software components for faster time-to-market. This trend presents a new juicy target for attackers because OSS does not typically go through the same rigorous security testing that licensed software is subject to, so they will try to inject it with vulnerabilities.

Sophisticated attackers manipulate software supply chains to infiltrate even the most well-guarded networks. One of the reasons why attackers have chosen to hijack software updates is that it is getting increasingly difficult, if not impossible, to find exploitable zero-day vulnerabilities. Apps based on OSS or third-party software are highly susceptible to attacks and increase the organization's attack surface manifold.[5]

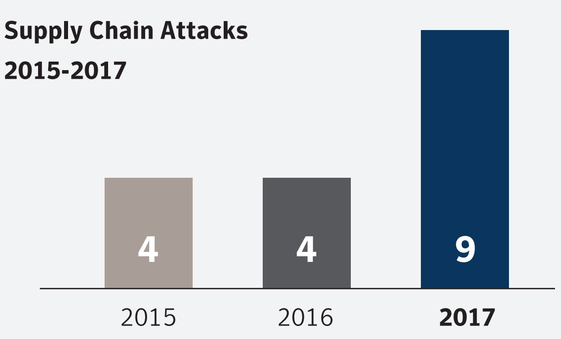


Figure 1: There was at least one large software update supply chain attack reported every month in 2017[2]

Kiosks—Evolution to Revolution

Another fallout of the App Economy is the use of Kiosks. Organizations in various industries are adopting self-service kiosks to increase customer reach and improve the consumer experience – all in a bid to drive the bottom line. The kiosk is now a fixture in day-to-day life – not only in banking and retail, with ATMs or point of sale (POS) machines, but also as in other industries, such as healthcare, travel, apparel and fashion, food and hospitality, et al.

These kiosks are vastly increasing an organization's attack surface, particularly as the form and function of these special devices expands, going beyond low-level routine tasks, such as dispensing, to high-level functions, such as preliminary screening of patient's vitals before a medical appointment.

[1] "Enabling Health and Healthcare Through ICT." Google Books. https://books.google.com/books?id=uuZNnyYWK2EC&pg
[2] "Internet Security Threat Report", Volume 23, 2018 Symantec. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Such advanced multi-function kiosks are more connected to the corporate network and store more valuable information than ever before, so they need a significantly higher degree of protection.

User Behavior in the "Shadows"

User behavior further complicates the threat landscape, expanding the attack surface by making it harder to manage apps and endpoints. Unauthorized downloads and usage of apps on endpoints in company networks, popularly known as Shadow IT, increase the likelihood of exploits that can compromise entire networks. For instance, when a user downloads an app that is not part of the standard operating environment (SOE) of the organization, it may simplify their day-to-day tasks and increase their productivity, but it also creates an unmanaged opening for attackers. Shadow IT can be anything, such as performance speed-up utilities, registry cleaners, disk defragmenters, YouTube downloaders, miscellaneous productivity software, entertainment, gaming apps, and so on.

By 2020, a third of successful attacks experienced by enterprises will be on their shadow it resources.[3]

These unauthorized apps, when allowed to run, use the same privileges as that of known "approved" apps. Often these apps have critical vulnerabilities, due to insecure coding practices and a lack of patching – weaknesses attackers will gladly exploit to gain control over the app. Once the app is compromised, the attacker gains access to entire OS, which means they can move laterally, and destroy, steal, data, or hold data ransom.

Newer Money Minting Cyber Crimes

App-based threats are not limited to supply chain attacks or attacks on fixed- or multi-function devices. Ransomware, crypto miners, DDOS-botnets, advanced persistent threats (APTs), targeted attacks, and most other attack techniques end up using apps at some point in their kill chain.

Ransomware remains a significant threat that is financially motivated. Despite the commoditization of ransomware, the number of ransomware variants grew by 46% indicating that this attack type cannot be ignored.[2] A meteoric crypto currency market in 2018 triggered a gold rush for cyber criminals. Detections of coin miners on endpoint computers increased by 8,500 percent in 2017, with Symantec logging 1.7 million in December of 2017 alone.[2]

Dynamicity of App Reputation and Protecting Vulnerable Apps

There are no guarantees that an app with a good reputation today will remain good tomorrow. Newer vulnerabilities and threats cause constant shifts in app reputation. Apps, therefore, must be constantly patched and updated using trusted channels. Some of the most widely used apps, such as Google Chrome and Adobe Reader, are also the most exploited. While all these apps and their proliferation are good for simplifying business transactions and processes, they need to be constantly monitored and secured to ensure they don't introduce risks.

[3] "Panetta, Kasey. "Gartner's Top 10 Security Predictions 2016." Gartner IT Glossary. https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016

App Control—Reimagined

For security to keep pace with the rate in which apps are proliferating and the risks they pose, traditional app control must be turned on its head. The traditional, old approach of managing legacy systems in lockdown mode is no longer sufficient for the modern use cases and challenges we face today. Symantec Endpoint App Control delivers a revolutionary approach, capable of applying intelligent controls that effectively address and minimize the threats opened up by all of today's apps and use cases.

How Symantec Endpoint App Control Works

Symantec Endpoint App Control significantly reduces the app attack surface of an organization by controlling the launch of every app or process to ensure only approved apps are allowed to run, and all unsafe or unapproved apps are blocked. Symantec Endpoint App Control enables organizations to configure a "default deny' security posture, so an app cannot be run unless it is on the allowed list. In other words, any app that is not on the allowed list is blocked; it's denied by default.

As mentioned earlier, apps in themselves are good for simplifying business and processes, but only if the apps can be trusted. Symantec Endpoint App Control enables trust in apps, based on a variety of app attributes, allowing or blocking apps based on one or a combination of any number of static (e.g. hash, path, publisher and certificate) and dynamic (e.g. risk and reputation score) attributes.

Symantec Endpoint App Control is used in Symantec Endpoint Security Complete, as part of a layered defense strategy. Together, Symantec Endpoint Security will detect and convict every file, script or process that is malicious, while App Control will limit all apps that can run on an endpoint to only those contained on the organization's global whitelist. The global whitelist can be based on what's discovered, a baseline, or a gold image. Finally, App isolation and Memory Exploit Mitigation policies will be used to restrict all running apps to good behavior. Any unauthorized tampering to the operating system (OS), critical data, or other running apps will be prevented.

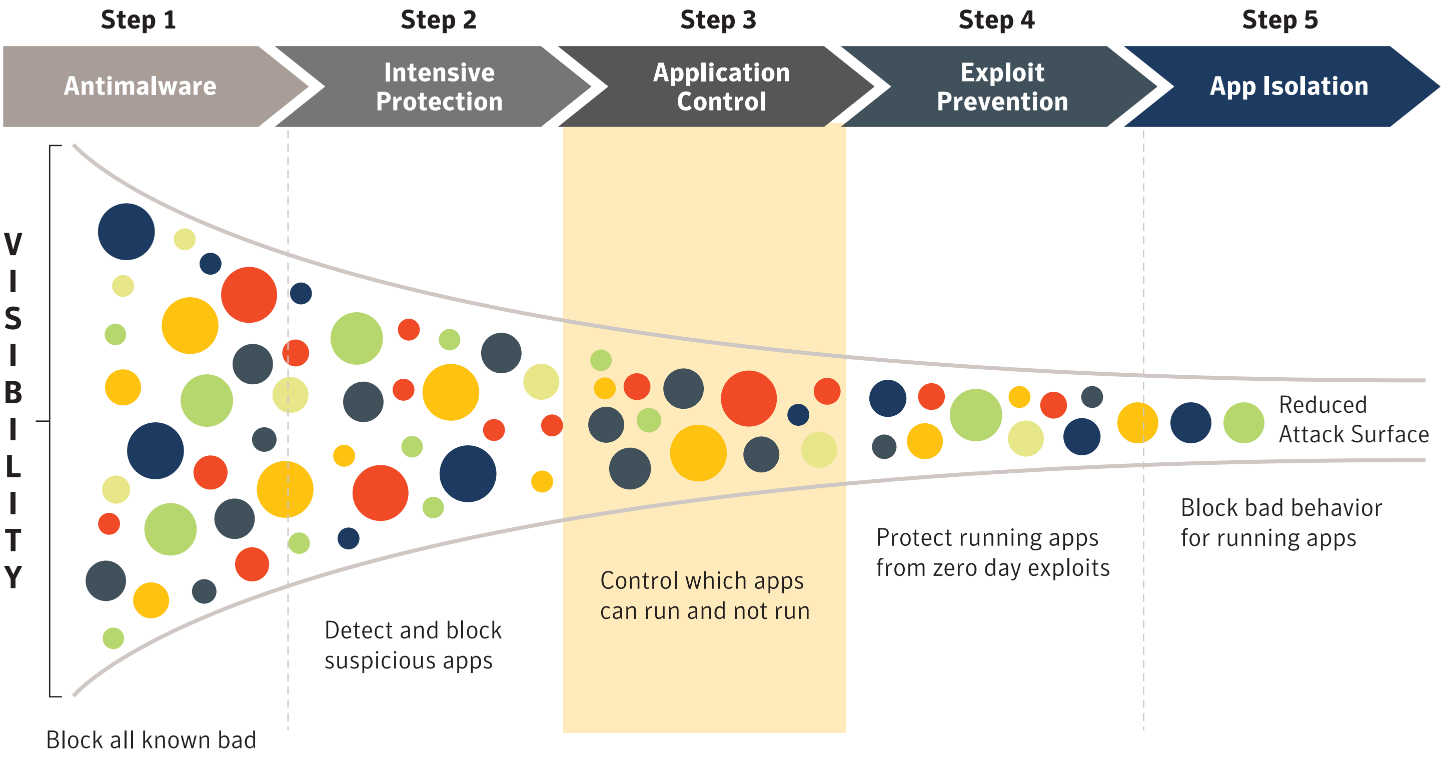


Figure 2: The Symantec layered defenses approach systematically reduces the endpoint attack surface.

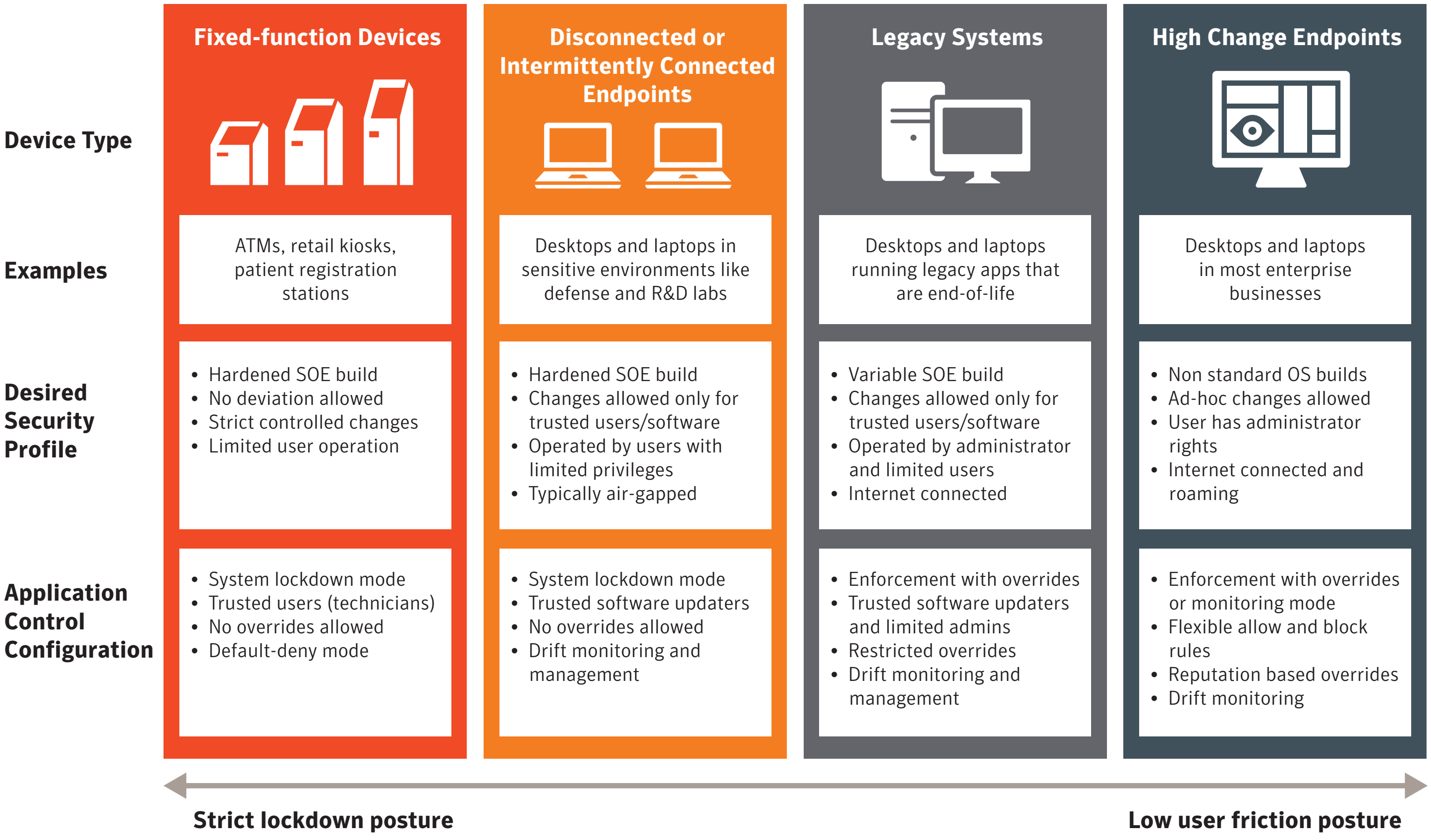
For more information about Symantec Endpoint App Isolation, check out this white paper to see how to apply a zero-trust model using Symantec Endpoint App Isolation.[4]

Top Symantec Endpoint App Control Use Cases

A typical organization runs a wide range of devices, varying from fixed-function to high-change endpoints, that each need to be appropriately protected. Symantec Endpoint App Control can protect them all:

- Fixed-function devices, such as ATMs, POS, and self-service kiosks that are mainly for customer use
- Disconnected or intermittently connected endpoints, such as endpoints in research and development (R&D) labs that contain substantial intellectual property (e.g. patents in process, test results, unique code, etc.)
- Legacy systems, such as desktops and laptops that run a combination of new and end-of-life'd apps
- High-change endpoints, such as desktops and laptops used by most users within most organizations

Depending on the device type, data sensitivity, and the desired security profile (e.g. locked down or open), Symantec Endpoint App Control can be configured to achieve different postures within the same environment. Figure 3 illustrates how different endpoints having different security posture requirements and different appetite levels for risk, all of which can be managed with Symantec Endpoint App Control.



	Fixed-function Devices	Disconnected or Intermittently Connected Endpoints	Legacy Systems	High Change Endpoints
Device Type				
Examples	ATMs, retail kiosks, patient registration stations	Desktops and laptops in sensitive environments like defense and R&D labs	Desktops and laptops running legacy apps that are end-of-life	Desktops and laptops in most enterprise businesses
Desired Security Profile	• Hardened SOE build • No deviation allowed • Strict controlled changes • Limited user operation	• Hardened SOE build • Changes allowed only for trusted users/software • Operated by users with limited privileges • Typically air-gapped	• Variable SOE build • Changes allowed only for trusted users/software • Operated by administrator and limited users • Internet connected	• Non standard OS builds • Ad-hoc changes allowed • User has administrator rights • Internet connected and roaming
Application Control Configuration	• System lockdown mode • Trusted users (technicians) • No overrides allowed • Default-deny mode	• System lockdown mode • Trusted software updaters • No overrides allowed • Drift monitoring and management	• Enforcement with overrides • Trusted software updaters and limited admins • Restricted overrides • Drift monitoring and management	• Enforcement with overrides or monitoring mode • Flexible allow and block rules • Reputation based overrides • Drift monitoring

Strict lockdown posture **Low user friction posture**

Figure 3: The Top Symantec Endpoint App Control Use Cases Within an Organization—Postures & Configurations

[4] https://www.symantec.com/content/dam/symantec/docs/white-papers/delivering-zero-day-defenses-with-endpoint-protection-en.pdf

What Sets Symantec Endpoint App Control Apart

There are a number of path-breaking features that differentiate Symantec Endpoint App Control from all other solutions on the market.

Simplified Onboarding with Journey Line

Symantec makes it easy to make the most of the solution in the shortest possible time with the product Journey Line, on the App Control Dashboard. The Journey Line significantly reduces the learning curve, guiding organizations through the essential steps required to get App Control up and running, so it can start protecting their endpoints (see Figure 4). Once a step has been performed, it is marked as complete and can be collapsed to hide it from view, helping organizations focus on what comes next.

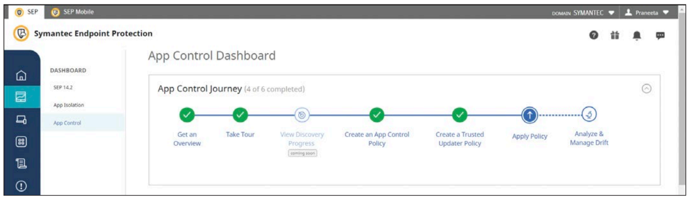
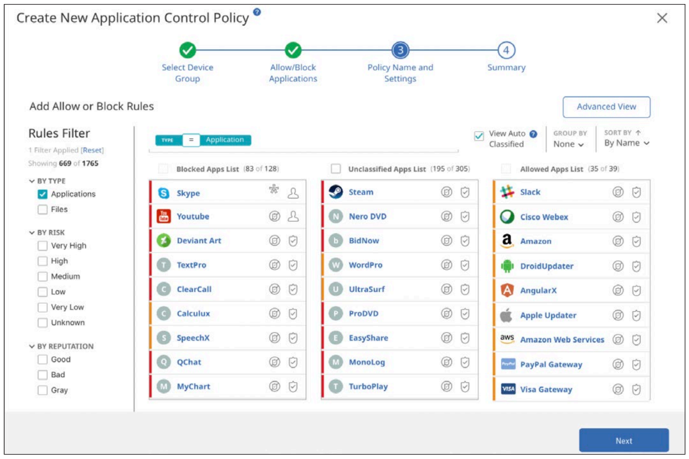


Figure 4: App Control Journey Line—Faster Time to Value.

Easy Policy Creation with Drag-and-Drop Logical View

To further simplify the involved process of policy creation, Symantec Endpoint App Control makes it easy for administrators to drag-and-drop apps across the a three-pane paradigm on the user interface (see Figure 5). The admin can slice-and-dice in this view - filtering, sorting, grouping information to generate a smaller dataset for analysis. The admin can also toggle between the logical view and the advanced view, which shows the granular attribute-based rules that power the logical view.



Blocked Apps List (83 of 128)	Unclassified Apps List (195 of 305)	Allowed Apps List (35 of 39)
Skype	Steam	Slack
Youtube	Nero DVD	Cisco Webex
Deviant Art	BidNow	Amazon
TextPro	WordPro	DroidUpdater
ClearCall	UltraSurf	AngularX
Calculux	ProDVD	Apple Updater
SpeechX	EasyShare	Amazon Web Services
QChat	MonoLog	PayPal Gateway
MyChart	TurboPlay	Visa Gateway

Figure 5: User-friendly drag-and-drop interface makes it easy to create policies.

Smart Rules and Broad Range of Parameters for Policy Creation

The majority of the app control products available today offer only limited attributes an organization can use to create policies, namely app name, path, and hash (and maybe publisher). Fewer attributes available for rule creation means less flexibility, more rigid rules, and therefore more end-user disruption.

Also, most apps are not perfect and have one or more attributes missing, which means that an admin must have more latitude in rule creation to account for various scenarios using varied combinations of parameters. Also, using static attributes are limiting and ineffective because the app risk posture is typically dynamic, varying based on the vulnerabilities that are constantly being discovered or exploits that are continuously being crafted.

Symantec Endpoint App Control enables policy rule creation on a broad range of parameters that include app name, path, and hash, reputation, publisher, user, user group, and command line parameters (see Figure 6). Symantec Global Intelligence Network (GIN) lookup provides the latest information on the reputation of an app or file. Creating rules based on users ensures only prescribed users have access to an app, with 'just-enough' privileges.

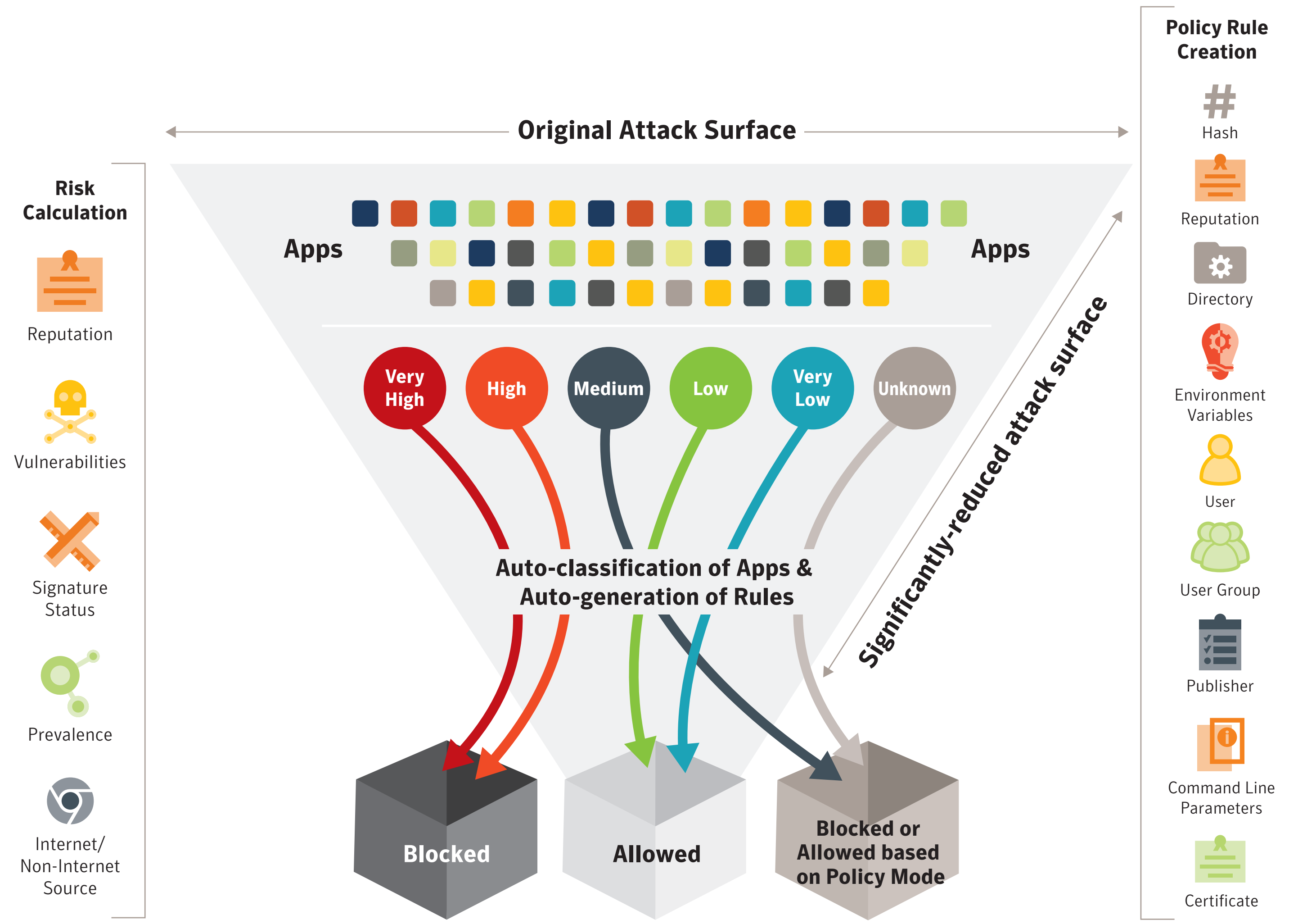
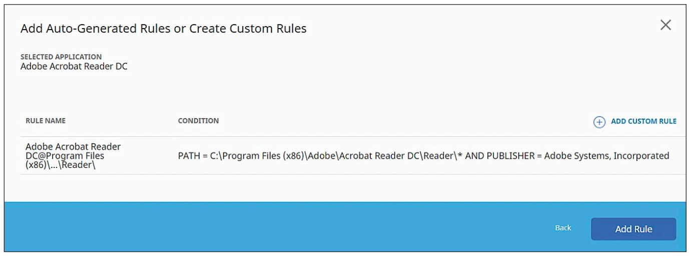


Figure 6: Significant reduction in attack surface with smart rules & the autoclassification of apps.

Rules can be based on static app attributes, such as the ones mentioned above, which can be collected via discovery, or dynamic attributes, such as reputation, which tell admins whether the app is trending good or bad. If rules are based on dynamic attributes, an app that is allowed today may end up falling off the allowed list tomorrow because of a change in attributes. This offers enhanced security that keeps up with current conditions, as an app's risk posture is rarely static, thanks to a variety of factors(see Figure 6).

Symantec Endpoint App Control auto-generates rules based on app risk computation (see Figure 7), further simplifying the process of allowing or blocking apps, and enabling the faster deployment of App Control throughout large organizations.


Add Auto-Generated Rules or Create Custom Rules

SELECTED APPLICATION
Adobe Acrobat Reader DC

RULE NAME	CONDITION
Adobe Acrobat Reader DC@Program Files (x86)\...\Reader\	PATH = C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\* AND PUBLISHER = Adobe Systems, Incorporated

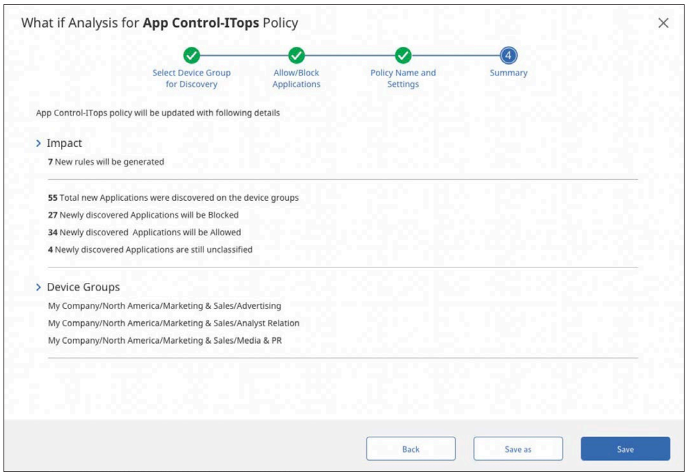
Figure 7: Auto-generation of App Control Rules.

Hybrid rules, based on a combination of static and dynamic app attributes, can also be created to ensure real-time protection against emerging threats.

What-if Analysis

Symantec Endpoint App Control policies can be enforced in “monitor only” mode to help admins understand how it will be implemented before deploying it in their production environment. Essentially, this mode allows admins to take the policy for a test drive and record the observations, without blocking anything.

This also gives admins an opportunity to perform “what-if” analysis, so they can iteratively change the policy, based how a policy impacts a group of endpoints, before ever having to apply the policy. This allows admins to use a policy for an existing device group and see what it does to very similar or completely different device group, so they can quickly and easily evaluate the suitability of the policy and make any necessary adjustments for maximum effectiveness. The “what-if” analysis is summarized in easy-to-understand, simple terms, with detailed information about all the apps that will be allowed to run, all the apps that will be blocked, and all the apps that fall in the gray list (see Figure 8).


What if Analysis for **App Control-ITops** Policy

App Control-ITops policy will be updated with following details

› Impact

7 New rules will be generated

55 Total new Applications were discovered on the device groups
27 Newly discovered Applications will be Blocked
34 Newly discovered Applications will be Allowed
4 Newly discovered Applications are still unclassified

› Device Groups

My Company/North America/Marketing & Sales/Advertising
My Company/North America/Marketing & Sales/Analyst Relation
My Company/North America/Marketing & Sales/Media & PR

Figure 8: What-if Analysis—a powerful tool to shorten app control deployments

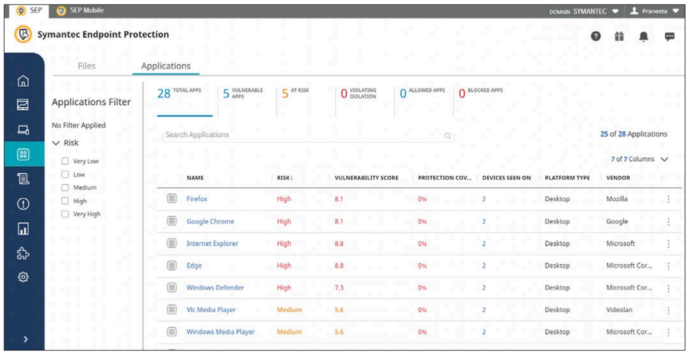
This type of analysis is a powerful tool in the hands of an admin, helping them drastically shorten the time between creating and finalizing a policy, so they have a full understanding of its consequences before they ever apply it.

Simplified, Powerful Drift Management

Drift is introduced by users downloading various apps on the endpoint that are not allowed by a policy. Drift makes endpoints prone to risk and needs to be actively managed. Failure to do so can result in undesirable apps running on endpoints that can be exploited for information or identity theft. Minimizing drift actively minimizes the gray list and helps the administrator gain tighter control of their environment. Symantec Endpoint App Control helps admins manage drift smartly and painlessly to reduce the app attack surface. With an easy drag-and-drop interface, similar to policy creation (see Figure 5), and recommendations, based on the auto-classification of which apps should be allowed to run and which need to be blocked, drift management is a breeze.

Comprehensive Discovery and Inventory

Symantec Endpoint App Control presents organizations with all apps and files discovered in their environment, (see Figure 9). With a robust discovery engine, App Control scans and inventories all the apps and files collected from all the endpoints in the environment. A “Discovered Items” view provides detailed information about each app and file, including the name, risk, publisher, reputation, number of devices it is seen on, and so on.



Applications Filter

No Filter Applied

Risk
□ Very Low
□ Low
□ Medium
□ High
□ Very High

28 TOTAL APPS | 5 VULNERABLE APPS | 5 AT RISK | 0 VIOLATING ISOLATION | 0 ALLOWED APPS | 0 BLOCKED APPS

Search Applications

25 of 28 Applications

7 of 7 Columns

NAME	RISK	VULNERABILITY SCORE	PROTECTION COV...	DEVICES SEEN ON	PLATFORM TYPE	VENDOR
Firefox	High	8.1	0%	2	Desktop	Mozilla
Google Chrome	High	8.1	0%	2	Desktop	Google
Internet Explorer	High	8.8	0%	2	Desktop	Microsoft
Edge	High	8.8	0%	2	Desktop	Microsoft Cor...
Windows Defender	High	7.3	0%	2	Desktop	Microsoft Cor...
Vlc Media Player	Medium	5.6	0%	2	Desktop	Videolan
Windows Media Player	Medium	5.6	0%	2	Desktop	Microsoft Cor...

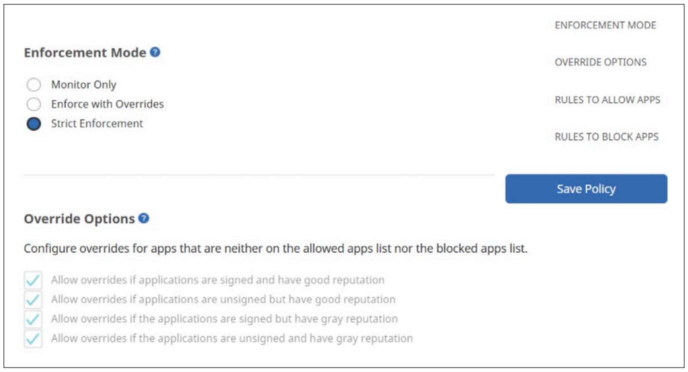
Figure 9: Comprehensive Discovery and Inventory

Risk Computation

Symantec Endpoint App Control computes risk for both an app and a file. The risk computation considers various attributes collected via discovery, such as vulnerabilities (CVSS), Internet or non-Internet download source, prevalence, reputation, and signature status (see Figure 6).

Flexible Policy Enforcement Modes for Different Scenarios

Apps with medium or unknown risk are allowed, based on the desired or configured risk posture of the organization. For example, if the policy is configured to allow end users to override restrictions, the end-users can run the app, and an operational event is created to record the occurrence. If the policy is configured in a strict mode, users cannot run apps that are discovered to pose a medium or unknown risk. In this scenario, apps with medium or unknown risk are treated like apps on the blocked list. App Control can be configured in three convenient modes of operation to suit the needs of the environment, the exposure of the environment to risk, and the preferred security posture (see Figure 10).



Enforcement Mode

○ Monitor Only
○ Enforce with Overrides
● Strict Enforcement

Override Options

Configure overrides for apps that are neither on the allowed apps list nor the blocked apps list.

☑ Allow overrides if applications are signed and have good reputation
☑ Allow overrides if applications are unsigned but have good reputation
☑ Allow overrides if the applications are signed but have gray reputation
☑ Allow overrides if the applications are unsigned and have gray reputation

Figure 10: Flexible policy enforcement modes for different scenarios

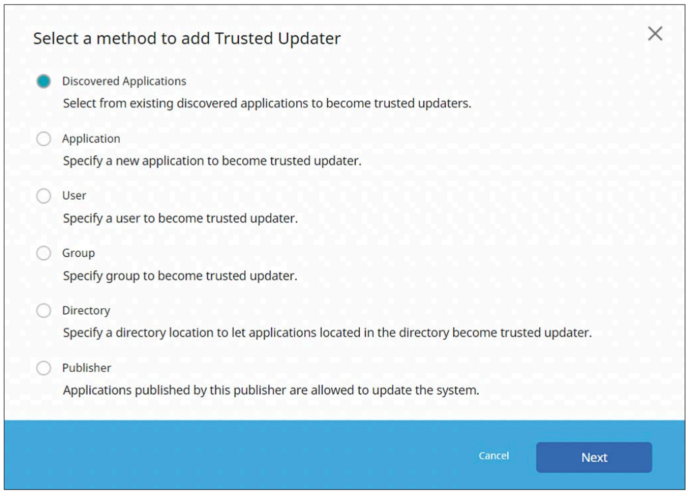
- In the “Monitor-only” mode, end users can run all apps without enforcing app control. This mode enables admins to take the App Control policy for a test-drive, so the effects of enforcing the policy are known and well understood before implemented. This helps admins minimize end-user disruption, by ensuring legitimate apps required for day-today business use are allowed. Admins can keep refining policies iteratively till a “golden mean,” between security, manageability, and end-user productivity is reached.

- In the “Enforce with Overrides” mode, end users can run apps that are neither on the allow list, nor on the block list. Users will initially be prevented from running new apps, however, they can override the block and use it. This will trigger the app to be tagged as ‘drift,’ so it can be analyzed and managed appropriately by admins. If App Isolation is enabled in combination with App Control, all drift apps will be subject to varying levels of isolation to ensure “drift” apps are restricted to good behavior.

- In the ‘Strict” mode, end users can only run a predefined set of apps and those that are installed via trusted updaters.

Trusted Updaters Ensure Security, Flexibility, and Overhead Reduction

Most general-purpose devices require software updates from time to time to patch vulnerabilities or roll out enhanced functionality for optimal performance. Symantec Endpoint App Control enables administrators to define trusted updaters — which can be apps, files, users, user groups — that can install or update software on the endpoints (see Figure 11). These trusted updaters are granted a fixed set of privileges, which allow them to carry out tasks that are routine or normal 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 so on.



Select a method to add Trusted Updater

● Discovered Applications
Select from existing discovered applications to become trusted updaters.

○ Application
Specify a new application to become trusted updater.

○ User
Specify a user to become trusted updater.

○ Group
Specify group to become trusted updater.

○ Directory
Specify a directory location to let applications located in the directory become trusted updater.

○ Publisher
Applications published by this publisher are allowed to update the system.

Figure 11: Numerous trusted channels available for configuration

Trusted Updaters offer much required flexibility, allowing users to run apps without an admin's intervention. This eliminates administrative overhead and helpdesk calls, so admins can focus on other IT concerns of strategic importance.

Case Studies—Putting App Control to Work

Case Study 1: Unauthorized and Unwanted Apps—Fixed Function Devices

George works as a security administrator at Acme Healthcare, which recently installed patient kiosks at their facility. The patients use these kiosks as a two-way channel to provide information about their current conditions and learn how to improve their health. The kiosks administer tips and behavioral strategies, including but not limited to the patient's personal health goals. The kiosks also provide feedback about the patient's progress in various areas, such as mobility, bladder control, mood, sleep, and so on. The kiosks run different versions of Microsoft Windows operating systems.

Acme Security Operations is fully aware that attackers can exploit the kiosks to launch script editors, calculators and browsers that can ultimately grant them access to the file system. Once an attacker has access to the kiosk system, they can install network taps, malware or malicious apps to gain access to a host of personal information, including all the information retained on the kiosks or saved on servers and other network devices. This data needs to remain private and secure, according to the Health Insurance Portability and Accountability Act (HIPAA)—any compromise can have costly and damaging repercussions. In addition to stealing or holding the data ransom, attackers can engage in further clandestine activities, such as man-in-the-middle attacks and denial-of-service attacks.[5]

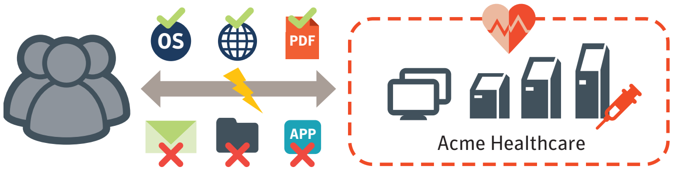


Figure 12: Flexible policy enforcement modes for different scenarios

George can rest easy because he pushed down a Symantec Endpoint App Control policy that allows only a predefined list of apps to run on the kiosks. Apps that are typically not used for collecting or displaying information are not allowed to run. Even if attackers gain access to the kiosk, they can't run any incursion, exfiltration or lateral movement tools, as these unauthorized processes would not be allowed to execute.

Benefits: App Control only allows approved and authorized software to run, protecting endpoints from being compromised by dangerous and unwanted apps.

Case Study 2: Balancing User Productivity with Security—High Change Endpoints

Nancy manages the security operations for a large multinational pharmaceutical company. Most of the assets in Nancy's network are desktops and laptops, grouped into different asset groups. Users in the Sales and Marketing group are constantly transacting business on-the-run, so they tend to download a lot of apps on their laptops.

To keep the workforce productive, Nancy has ensured policies for each asset group match the requirements and job roles of those users. To accommodate her Sales and Marketing team's needs, she has configured the Symantec Endpoint App Control policy to be enforced with user overrides allowed. There are also situations where Nancy approves the broader use of some apps when there is a valid business justification. In this way, she ensures uninterrupted service, so nothing impedes their ability to close deals for the company, while allowing her to monitor and protect against apps that pose a danger.

[5] "Takyi, H., Watzlaf, V., Matthews, J. T., Zhou, L., & Dealmeida, D. (2017). Privacy and Security in Multi-User Health Kiosks. International journal of telerehabilitation, 9(1), 3-14. doi:10.5195/ijt.2017.6217

The “drift” introduced by apps that are not explicitly covered by a policy is presented to Nancy, with a recommendation about how they should be handled, based on the risk assessment and reputation lookup. While the recommendations are powerful, Nancy is ultimately the one who makes the decisions about what to allow and block (see Figure 13).

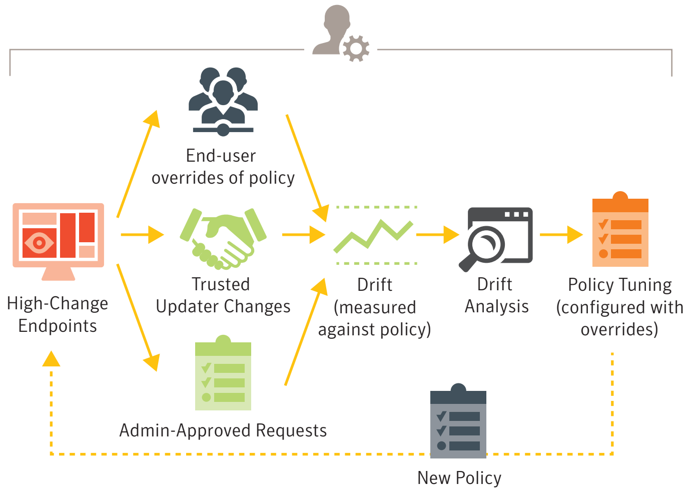

End-user overrides of policy
High-Change Endpoints
Trusted Updater Changes
Drift (measured against policy)
Drift Analysis
Policy Tuning (configured with overrides)
Admin-Approved Requests
New Policy

Figure 13: Drift analysis and policy tuning for high-change endpoints

Benefits: App Control enables smart drift management, making it easy to stay on top of suspicious apps or grayware within the company. It also supports active decision-making that reduces the uncertainty and attack surface created by new and unknown apps.

Conclusion

The risks posed by proliferating apps are exponentially increasing. Symantec’s comprehensive endpoint protection helps organizations harden their endpoints to reduce their attack surface and proactively defend the integrity of their resources. App Control effectively uncovers and then blocks unauthorized and unwanted apps, eliminating risks posed by supply-chain attacks and Shadow IT that exploit vulnerabilities in legitimate apps. In combination with Symantec Endpoint Security and App Isolation, App Control delivers unrivaled protection, keeping apps and endpoints safe from known and emerging threats.

To learn more about Symantec App Control, visit https://www.symantec.com/products/endpoint

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, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

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