STOP ATTACKS AND MITIGATE RISK WITH APPLICATION AND DEVICE CONTROL

Overview

Stop Attacks and Mitigate Risk with Application and Device Control

Harden endpoints using advanced security features available within Symantec™ Endpoint Protection.

Symantec™

You're tasked with protecting your organization from cyberthreats, but malware and potentially uninformed users make it difficult to prevent attacks on your endpoints. Now there is a way to be more proactive and effective in safeguarding your organization from malicious attacks and advanced threats. By restricting the applications and devices that can be run in your environment, you can mitigate the risk of breach and enforce company policies and compliance with industry regulations.

Application Control and Device Control (also known as External Media Control) are advanced security capabilities in Symantec™ Endpoint Protection that allow you to take action ahead of time, to plan and to implement controls that support the needs of your users and organization. These advanced features not only improve incident response but also provide reliability for IT administrators to prepare for what their ecosystems need.

Mitigate risks and prevent attacks

The Application Control capability in Symantec Endpoint Protection controls what an application is permitted to do and which system resources it can use on client computers. It allows you to restrict unauthorized access by whitelisting and blacklisting, to prevent the execution of unapproved programs and devices. Device Control is another important capability to defend endpoints. It prevents threats from entering the network through unintentional or malicious individual actions and is often used for compliance requirements. These features improve endpoint security by

- Protecting good applications and devices within your environment
- Keeping bad applications and devices out of your ecosystem
- Preventing both known and unknown applications from behaving maliciously

Improve security with Application and Device Control

Here are some ways you can take advantage of the Application Control and Device Control features in Symantec Endpoint Protection.

Use whitelisting and blacklisting to harden endpoints

Application Control can enhance protection for business-critical systems by only allowing whitelisted (known to be good) applications to run. It can also block blacklisted applications (known to be bad) or any application not included within the master corporate image from running. For instance, you can blacklist applications such as peer-to-peer (P2P) software, which distributes music, games, and other files, as well as easily hidden malware. You can also block access to scripts and modifications to host files.

Recommended by security experts

Application control and device control features are two of the top tools for preventing cyberattacks according to Center for Internet Security (CIS) Controls, which was originally created by

- U.S. National Security Agency
- U.S. Department of Energy National Laboratories
- Law enforcement organizations
- Top forensic and incident response organizations

Learn more about CIS Controls at www.cisecurity.org/critical-controls.cfm.

Customize your security policies with granular policy control

Maximize flexibility of your security policies with customized rules for multiple user groups, different locations, and application behaviors. For instance, you can grant or deny access to certain registry keys, files, folders, applications, and dynamic link libraries. You can also set policies to stop software installers and terminate applications launched through an irregular process. Application Control detects certain errors such as registry keys being written and automatically notifies administrators or blocks applications from writing to sensitive files.

Prevent threats from entering via external media

You can block employees or others from using USB devices or only allow approved external devices to prevent threats like the Conficker computer worm, for example, from entering the network through external media. You can prevent unauthorized entry of files and prevent users from inadvertently removing confidential data from your organization via external storage devices.

"Symantec Endpoint Protection has allowed us to take more of a governance approach to our applications. We're able to lock them down more effectively … and stop them from being used in certain instances."

– Frank McGinnis, Vice President of IT, Broadridge Financial Solutions

See how Broadridge uses Symantec Endpoint Protection: www.symantec.com/tv/products/details.jsp?vid=1854266189001.

Strengthen your endpoint defense

Symantec Endpoint Protection delivers unrivaled security against advanced threats, blazing performance, and smarter management. Its advanced security features such as Application Control and Device Control allow you to customize and enforce security policies that reduce your attack surface and mitigate the risk of cyberthreats.

When you take advantage of Application Control and Device Control, you gain the following:

- Improved endpoint security and reduced risk of breach
- Improved compliance with corporate rules and industry regulations
- Time-savings and improved incident response when there is an active threat by automatically blocking applications and actions

Find out more about Symantec Endpoint Protection at http://go.symantec.com/sep12.

Symantec™

21363187