SOPHOS

simple + secure

Using application control to reduce risk with endpoint security

Unwanted applications, like games, result in productivity loss. This is often the primary consideration when applying application control. But unauthorized applications also increase your company's risks of malware infection and data loss. This paper details how endpoint security solutions that incorporate application control provide the most efficient, comprehensive defense against unauthorized applications.

By Dan Kirtley, Product Manager, Sophos

A Sophos whitepaper - June 2011

Why you need application control

Virtually every company recognizes the need to protect its systems against "bad" software. Businesses use antivirus software routinely to defend against malware, keyloggers, adware, fake antivirus software, and other malicious code.

But application control requires more than keeping bad applications off your network. You must also control the use of some legitimate applications—whether they are downloaded over the internet or copied from personal flash drives.

Savvy employees often install these applications to help them communicate, share files, and work collaboratively. They typically include:

- Web browsers, such as Google Chrome™ or Flock
- IM (instant messaging) software, such as AIM® or Windows Live® Messenger
- P2P (peer-to-peer) file-sharing applications, such as uTorrent™ or Azureus®
- Online storage applications, such as Dropbox or MobileMe℠
- Remote management tools, such as GoToMyPC™ and LogMeIn®

These applications may appear innocent enough. But their usage, particularly when the applications are untested, can increase your company's exposure to a host of vulnerabilities, including infection from malicious code and unintentional sharing of corporate data. In its Yearly Report 2010[1], Secunia found that products from 14 software vendors, including giants such as Apple, Google, Microsoft, IBM, Cisco, and Adobe, accounted for half of the known software vulnerabilities in the previous two-year period. The report goes on to say that from an attacker's perspective, the targeting of third-party programs from popular vendors is unlikely to abate any time soon.

> It's easier than ever for users to download and use web- or cloud-based applications, but the risks associated with these applications can't be ignored. The 2011 Verizon Data Breach Investigations report states that "remote access and desktop services are once again at the number one spot in the list of attack pathways. A whopping 71% of all attacks in the Hacking category were conducted through this vector."[2]

Cybercriminals and their nefarious exploits represent just one of the threats from the unfettered use of unauthorized applications. P2P file sharing of movies or music can also expose your company to legal liability due to licensing issues.

[1] Secunia Yearly Report 2010. © 2010 Secunia. All rights reserved.
[2] Verizon Data Breach Investigations Report © 2011 Verizon. All rights reserved.

"I bet there are millions of bosses out there who hate me. If I had a penny for every hour that has been wasted playing Solitaire in the office, I could hire Bill Gates as my golf caddie."

Wes Cherry,
Author of Microsoft Windows Solitaire

These issues are all too prevalent. In February 2010, the Federal Trade Commission notified nearly 100 organizations that sensitive data had been shared from their computer networks and was available on P2P file-sharing networks. This vulnerable customer and employee information could be easily used for identify theft or fraud.[3]

Games and other unwelcome applications can also impact your business with their drain on employee productivity. Social media tools, such as TweetDeck, which are meant to aid productivity, can also be a distraction.

Common approaches to application control

There are a variety of application control measures that can be used to reduce the risks associated with malware and unauthorized applications. Each of these methods has its advantages and disadvantages. These methods include:

- Using antivirus and HIPS (host intrusion protection systems) capabilities
- Using application allow lists (also known as "whitelists")
- Restricting administration rights
- Using client firewalls
- Using application block lists

Antivirus and HIPS capabilities

Antivirus detection and HIPS capabilities are the most commonly used techniques for blocking malware and known bad applications. Antivirus software is mandated by many regulations such as PCI DSS and is deployed as part of an endpoint security solution.

HIPS, also included in advanced endpoint security solutions, analyzes applications for suspicious behaviors. These behaviors may include registry modifications, suspicious files being written to the file system, or processes that start in a suspicious or unusual way. Antivirus and HIPS capabilities are effective at blocking malicious code. However, they don't control the use of legitimate but unwanted applications.

[3] FTC notifies almost 100 organizations of P2P data leaks: http://www.sophos.com/blogs/gc/g/2010/02/23/ftc-issues-p2p-data-leak-warning-organisations/

Application allow lists or "whitelists"

Application allow listing lets you identify specific applications and versions that are allowed to run on your systems. This "default deny" approach will block any application that has not been explicitly authorized.

Dedicated allow listing applications are typically too time consuming and inefficient to implement for general business use. These applications require ongoing research, evaluation, and administration to constantly update the list of allowable applications. Also, the longer the allow list—and it may need to be fairly long for general purpose computing—the less effective the security. When you increase the number of allowable applications, you increase the "surface area" on your systems that is vulnerable to attack.

Allow lists may make sense for specialized computing environments, such as point-of-sale systems, where the allowable list of applications is likely to be limited. However, for general businesses with wide-ranging user needs, this approach can significantly increase IT overhead and degrade end-user productivity.

Restrictive administration rights

You should limit administrative rights access within your organization. This approach will significantly reduce the volume of unauthorized applications within your environment.

But don't be solely dependent on this approach. Many applications, such as the Google Chrome web browser, do not require administrative rights for installation. Users may also download portable versions of software from removable storage devices regardless of usage rights.

Pros and cons of common application control approaches

Approach	Advantage	Limitation
Antivirus and HIPS	Detects and blocks malware	Cannot block legitimate, but unwanted, applications
Application allow lists	Blocks any application that is not specifically allowed to run	Increases IT overhead in most business situations and can still leave systems vulnerable to attack
Restrictive administration rights	Reduces the volume of unauthorized applications	Cannot block applications that require no administrative rights
Client firewalls	Controls access to network or internet resources	Cannot prevent native applications from being run and offers no protection when using a system offsite
Application block list	Blocks or tracks applications that you want to control	Can increase IT overhead by requiring the creation of unique signatures for each application and version you want to control

Client firewalls

A client firewall can help limit the use of unauthorized applications by controlling access to network or internet resources. For example, a client firewall can look for and block IM traffic. However, a client firewall can't prevent native applications from being run. Some applications, such as Skype, can outsmart a client firewall using camouflage techniques. These applications find ways to hide their traffic by rapidly identifying and moving through a range of innocent ports, making them difficult to detect and stop.

Adding to the problem is the large number of users who work outside a company's firewall, using unsecured networks at internet cafes, hotels, and home offices. Only the more sophisticated location-aware client firewall on a laptop or endpoint PC can enforce tighter security when connected to a non-trusted network.

Application block lists

Application block listing enables you to monitor or prevent the use of applications that you want to control. It is useful for blocking applications outright. It can also be used to silently track high-risk user behaviors and provide information to inform your security policy.

Most block-list solutions require the IT administrator to create unique signatures for each application they want to control. They often do this using a checksum identifier, which requires upfront configuration as well as ongoing maintenance to identify subsequent versions of the software.

A more practical approach to block listing involves using vendor-provided detection data that covers a broad range of application categories. For example, you could block the use of file sharing applications completely and restrict the use of software from commonly attacked vendors. This approach requires much less upfront configuration and maintenance since the vendor is responsible for updating application detection criteria when new software is released.

Application control as part of an endpoint security solution

As with many security technologies, application control works best as part of a broader endpoint security solution. Using this approach, the whole is greater than the sum of its parts. A complete endpoint security solution allows you to easily combine a variety of security capabilities, such as antivirus detection, HIPS, block listing, and client firewalls, to offer the most rigorous and comprehensive application control.

With a complete endpoint security solution, you can:

- Stop malware from running
- Reduce risk of data loss
- Limit employee distractions from unauthorized applications
- Reduce liability exposure from the downloading of music or movies

Endpoint security solutions offer complete, cost-effective application control

A fully integrated endpoint security solution provides comprehensive defense against unauthorized applications. It offers a single security solution that is easy to deploy and manage. It also delivers a seamless set of security capabilities that work intelligently and efficiently in the background environment.

By using application control as part of an endpoint security solution, you can:

- Keep IT overhead costs low and decrease maintenance time with vendor-provided detection data
- Give IT administrators greater visibility into high-risk user behavior to help set policy
- Make the most efficient use of computing resources so users can stay productive

How application control works within an endpoint security solution

Endpoint security feature	Application control offered	Protects against
Antivirus detection	When a user attempts to download or use an application, antivirus software scans the application for known malware. If no viruses are found, HIPS functionality kicks in.	Protects against: Known malware or fake antivirus tools (e.g., W32.Stuxnet or Trojan.Win32.FakeAV.cogs)
HIPS	HIPS functionality analyzes whether the application exhibits any suspicious behaviors. If suspicious behavior is detected, the application is blocked or a notice is sent to the administrator. If no suspicious behaviors are found, then the application control checklist is used.	Protects against: New malware that exhibits suspicious behaviors, often including zero-day attacks
Application control list	The application is checked against a prepared control list. If a match is found, the specific policy setting is followed. The application may be blocked or it may be allowed to run with a notification alert sent to the administrator.	Protects against: File sharing tools, games, remote management tools, and other unwanted applications
Location-aware client firewall	When a user is connected outside of the corporate network, tighter security can be automatically triggered. Client firewalls, particularly when combined with HIPS technology, are used to help block suspicious applications from downloading and executing.	Protects against: Traffic from unauthorized applications not blocked by application control

Sophos Application Control: Take control of what your users install

We help you control the applications that could cause security or legal problems, like P2P or instant messaging. And you'll get a handle on the unwanted applications that clog your network. With our Application Control—part of Sophos Endpoint Security and Data protection—you can monitor and control what your employees are installing without interfering with their work.

How does it work?

- We've built application control into our antivirus engine, so you don't have to deploy or manage a separate product
- We provide you with detection for a wide range of applications that our experts keep up to date with new versions and new applications
- You simply set policies for the whole company or specific groups to block or allow particular applications
- Use application control to switch off VoIP but allow remote users to use it. Or standardize on a single Internet browser

Try it now for free

Get a free 30 day trial of Sophos Endpoint Security and Data Protection

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK