

...patrolling endpoint security and productivity

top facts on the need for application control

The challenges posed by the installation of unauthorized applications on company computers are significant. While there are a number of solutions available that help IT administrators to manage the problem, many require additional investment and, for many organizations, they can be expensive, unwieldy and difficult to maintain. Harnessing the power of your anti-malware solution, however, will let you elevate application control right up to the first line of defense where it rightly belongs in today's business environment.

1 What's causing the problems?

The impact of Web 2.0

Web 2.0 is beginning to redefine how individuals interact with the internet, and the related technologies pose a range of new threats. Employees installing and using unauthorized applications like Instant Messaging, VoIP, games and peer-to-peer file-sharing applications cause many businesses serious concern. New vectors for threats include:

- Instant Messaging (IM)
- Peer-to-peer (P2P) file-sharing applications
- Voice over Internet Protocol (VoIP)
- Browser toolbars
- Games

The need for autonomy

A key part of the challenge is that many users have to be allowed to be local administrators, being given privileges necessary to download applications that they need to do their job, for example, downloading updated Adobe Acrobat software. However, this means that they can also download a variety of other software that they might want to install and use.

2 What exactly ARE the problems?

Legal, compliance and security breaches

Uncontrolled use of IM, for example, poses a severe legal and regulatory and security risk because the content of IM chat often includes attachments, jokes, gossip, rumors and disparaging remarks, confidential information about the company, employees and clients, and sexual references. In addition, IM-based malware attacks are growing exponentially and a similar security risk is posed by the increased use of P2P applications which are notorious vectors for malicious code such as remote command execution, remote file system exploration or file-borne viruses.

Extra IT support burden

If not properly tested and deployed by the company IT department, uncontrolled applications can cause stability or performance issues on company computers. Apart from the additional support headache that this unnecessary troubleshooting gives IT administrators, it also represents a significant waste of IT's most precious resource – time.

Network and system overhead

The corporate network bandwidth and computer processor power consumed by unauthorized applications can have a direct negative impact on network resources and availability. For example, distributed computing projects harness the "spare" processing power of millions of computers to help create models or simulations of scenarios such as climate change. VoIP also use such spare capacity.

Employee productivity issues

Although VoIP and IM can have business advantages, they can be a distraction if used inappropriately and in most cases this type of application is not required by end users for business purposes. A more significant reduction in productivity comes from employees playing games, sharing music and using other P2P applications.

3 What are businesses currently doing to fix the problems?

Locking down their computers and assigning only limited administrator rights

Pro It's relatively easy.

Con The inflexibility of the strategy means that countless policies need to be created. For example, many simple Windows functions, such as adding a printer driver that wasn't shipped with Windows, changing time zones and adjusting power management settings, are not allowed with a standard user account and therefore require constant changing of the assigned rights.

Using specialist application control products

Pro These products are designed specifically for controlling which applications can and cannot be run on a computer by validating usage against large databases of allowed and blocked applications.

Con They are yet another product that needs to be evaluated, purchased, installed and managed. In addition, while application control products can be effective in blocking execution of applications, it is more difficult to stop the initial installation – a drawback that has led to their failure to gain significant traction in the wider market.

“When I wrote Solitaire for Microsoft, I unleashed a monster of unproductivity onto the world. 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, speaking to Sophos in January 2007

Implementing corporate firewall rules and HIPS

Pro Firewalls and HIPS (Host-based Intrusion Prevention Systems) can play a role in limiting the use of unauthorized applications by controlling access to network or internet resources, for instance by looking for and blocking VoIP traffic

Con They are generally focused on blocking potentially malicious network traffic and looking for undesirable behavior as it unfolds, rather than simply stopping the code executing in the first place.

4 What should you do now to fix the problems?

Use your anti-virus solution to block applications – and see your ROI soar

Integrating the blocking of unauthorized applications into the existing management infrastructure for your anti-malware detection will save you time, money and system resources. Make sure you choose a solution where the vendor creates and automatically updates detection signatures in exactly the same way as it deals with virus, spyware and adware signatures (rather than making you create your own application signatures and maintain your own allow and block lists). After all, you have to have an anti-malware solution, so you might as well maximize the investment by simultaneously reducing the time spent by technical support staff sorting out computers that have been destabilized by the installation of unauthorized applications.

Sophos Anti-Virus, version 6 optionally includes Application Control and is part of Sophos's commitment to a complete security and control system that uses a single management console and universal client for all aspects of operational desktop management. To find out more about this and other Sophos products and how to evaluate them, please visit www.sophos.com

Sophos is a world leader in IT security and control. Sophos offers complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, policy abuse and uncontrolled network access. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries. Through over 20 years' experience and a global network of threat analysis centers, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, Mass., and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2007. Sophos Plc. All rights reserved. All trademarks are the property of their respective owners.

tt070222

SOPHOS
secured.