SOPHOS

Instant Messaging, VoIP, P2P, and games in the workplace: How to take back control

Employees installing and using unauthorized applications like Instant Messaging, VoIP, games and peer-to-peer file-sharing applications cause many businesses serious concern. This paper looks at why it is important to control such applications, discusses the various approaches, and highlights how integrating this functionality into malware protection is the simplest and most cost-effective solution.

Instant Messaging, VoIP, P2P and games in the workplace: How to take back control

IT departments have long understood the need to prevent viruses, spyware and other malicious applications or activity from compromising security and disrupting business continuity.

Now the rapid emergence of Web 2.0 is beginning to redefine how individuals interact with the internet, and the related technologies pose a range of new threats. Web-savvy users who have local administration rights for their work computers are downloading applications such as Instant Messaging (IM), peer-to-peer (P2P) file-sharing applications and Voice over Internet Protocol (VoIP) services to help them communicate, share files and work collaboratively online – for both official and unofficial business.

In September 2006, a Sophos online poll asked IT administrators to evaluate what kind of software applications they would like to prevent their users from being able to access and use.[1] The results, shown in Figure 1, reveal that administrators have a clear desire to be able to exert more control and to prevent users from installing and using unwanted applications. For example, 86.1 percent of respondents said they would like the opportunity to block VoIP applications which allow internet telephony, with 62.8 percent going even further and indicating that blocking is essential.

The extent of the problem can also be seen in a recent report which discovered that 50 percent of workplace users download free IM tools from the internet with 26 percent of employers unaware of their actions.[2]
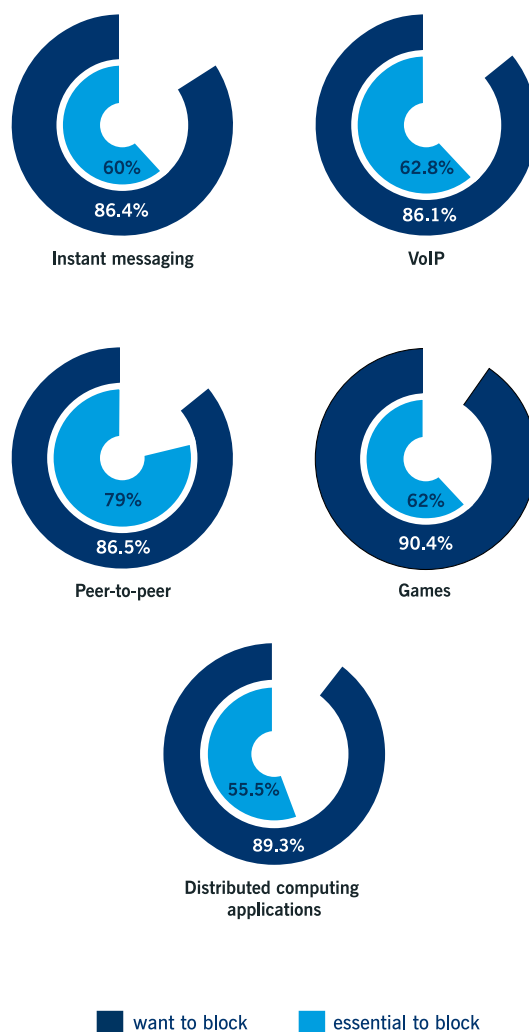

Instant messaging — 60% / 86.4%
VoIP — 62.8% / 86.1%
Peer-to-peer — 79% / 86.5%
Games — 62% / 90.4%
Distributed computing applications — 55.5% / 89.3%

■ want to block   ■ essential to block

Figure 1: Controlling applications a must for ITAdmins

The challenge of unauthorized software

Current business defenses inadequately protect against the new set of threats posed by this user behavior. The difficulties presented by some legitimate software applications raise particular challenges over and above "straightforward" protection against malware. To increase security and productivity IT departments need to restrict the rights to non-essential applications, and control the usage of those that are authorized for business purposes, but in practice this presents a significant challenge.

> "*4.1 You hereby acknowledge that the Skype Software may utilize the processor and bandwidth of the computer (or other applicable device). You are utilizing, for the limited purpose of facilitating the communication between Skype Software users.*"[3]

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. This makes life particularly difficult for the IT Administrator: malicious software would be blocked by anti-virus software but applications like IM are not malicious in any way. They are not being installed automatically by stealth and are not attempting to self-replicate or steal confidential information.

Nevertheless, the unauthorized or uncontrolled installation and use of such software by employees on business computers presents a real and growing threat in four major areas:

- Legal, compliance and security breaches
- Extra IT support burden
- Network and system overhead
- Employee productivity issues.

Legal, compliance and security breaches

Regulations such as the UK's Data Protection Act and the US's Sarbanes-Oxley Act and HIPAA (Health Insurance Portability and Accountability Act) place additional requirements on IT administrators to maintain and protect data integrity within their networks. So the installation of unauthorized applications can pose significant legal risk as well as security risks.

For example, uncontrolled use of IM poses a severe legal, regulatory and security risk because the content of IM chat often includes attachments, jokes, gossip, rumours and disparaging remarks, confidential information about the company, employees and clients, and sexual references.

In addition to the legal risk, IM poses a security risk with IM-based malware attacks growing exponentially. Similarly, P2P applications are on the increase and 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. In a business context, such activity can slow down the network, placing an unnecessary burden on the IT department.

Employee productivity issues

VoIP and IM in particular can have business and productivity advantages. However, they can be a distraction if used inappropriately and in most cases these types of application are not required by end users for business purposes. A more extreme example of reduced productivity would be the use of games or sharing music and other files using peer-to-peer software.

> *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.*[4]

Strategies to control applications

In the light of these wide-ranging threats that legitimate but unauthorized applications can (perhaps surprisingly) cause, there are a number of actions that IT administrators have tried. While each strategy has some merit, there are also disadvantages.

Locking down computers

One of the most straightforward ways to stop the installation of unauthorized applications is simply to enforce a blanket lockdown on all computers and to assign only limited administrator rights. However, this is precisely where application control has broken down in the past.

Some departments – notably IT and technical support – have a clear and obvious need for administrator rights. It might seem an obvious answer to allow these technical groups to install applications and to prevent everyone else from doing so. Unfortunately in practice this is not as simple as it sounds.

Many organizations find it expensive to lockdown computers for some or all of their non-technical end users. 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 do require constant changing of the assigned rights. The increased staffing requirements and response times related to centrally administering every change to a computer create a significant cost for the business.

Installing specialist application control products

There are products on the market that are designed specifically for controlling which applications can and cannot be run on a computer. These products typically involve validating usage against large databases of allowed and blocked applications.

For IT administrators they are yet another product that needs to be evaluated, purchased, installed and managed. Management of these solutions is not an insignificant task and is often difficult due to

the size and complexity of allow and block lists. In addition, while application control products can be effective in blocking *execution* of applications, it is more difficult to stop the initial *installation*.

Finally, specialist application control products do not provide comprehensive protection against malware and businesses still have to invest in other security products to protect against viruses, spyware, and other threats.

> "*…while application control products do a great job at blocking execution of applications, it is more difficult to stop the initial installation of applications.*"[5]

Implementing corporate firewall rules and HIPS

Firewalls and HIPS (Host-based Intrusion Prevention Systems) are generally focused on blocking potentially malicious network traffic and attempts to execute a code, rather than controlling which applications users can and cannot install and/or run. They 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, but are far from an adequate solution to this problem.

Getting more from your anti-malware solution

Most anti-virus and anti-spyware solutions do not offer application control capability. However, a business will get more from its investment in protection against malware, if the same scanning and management infrastructure is used by the product to intercept and manage the use of legitimate software applications.

One client to deploy

Anti-virus is a necessary investment that IT administrators have no choice but to purchase, install and manage. By incorporating extra functionality into this mandatory client, IT departments can both increase the return on their investment and save system and management resources. Deploying a single client that incorporates anti-virus, anti-spyware, anti-adware and control of unauthorized applications will save time, money, system resources and improve security.

Simplified control and policy setting

If the anti-malware and application control features are combined in a single product, administrators can enforce company policies on removing unauthorized applications by using the central management function provided by the anti-malware component. Setting application control policies alongside anti-virus policies improves the efficiency of management and provides the opportunity to differentiate between the needs of different groups of computers. For example, VoIP could be blocked for office-based computers, yet authorized for remote computers, and/or the download and use of unauthorized IM or games software would be controllable.

Eliminates administrative overhead

Using the same management and updating mechanisms for application control as for anti-virus software has obvious infrastructure and overhead benefits. However, the overall success of this combination of features, in terms of efficiency, depends on the actual way in which applications are detected.

An approach that has been taken by some vendors, requires administrators to create their own application signatures using filenames that appear in the application. This approach is time-consuming and IT resource-intensive. It puts the burden of updating onto the administrator and is also unreliable as users can simply change the filename to avoid the application being detected.

An alternative approach (the one taken by Sophos) is for the vendor to create and update detection signatures in exactly the same way that malware detection is automatically updated.

In simplifying administration, updating and maintenance of detection, this second approach is a significant advance over solutions that require administrators to maintain allow and block lists or create signatures by files or filenames.

Reduces support burden

By using signature-based detection that not only stops applications from being run but also blocks their download and installation, organizations reduce the time that their technical support staff have to spend sorting out computers that have been destabilized by the installation of unauthorized applications.

Conclusion

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. A better solution is one which completely integrates the blocking of unauthorized applications into the existing anti-malware detection and management infrastructure. This gives IT administrators – for whom IT anti-malware protection is a must have – a simple solution that removes the cost and management overhead from the equation.

The Sophos solution

Application Control is an optional feature of Sophos Anti-Virus, version 6 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, not just security.

To find out more about Sophos products and how to evaluate them, please visit www.sophos.com

Sources

1 Sophos web poll

2 2006 Workplace E-Mail, Instant Messaging & Blog Survey from American Management Association (AMA) and The ePolicy Institute.

3 Skype End User License Agreement, Section 4 Utilization of Your computer

4 Wes Cherry, author of Microsoft Windows Solitaire, speaking to Sophos

5 Windows Application Control Solutions Provide an Alternative for Desktop Lockdown, Gartner Inc. March 2006

About Sophos

Sophos is a world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years' experience and consolidated anti-virus, anti-spyware and anti-spam expertise SophosLabs protects even the most complex networks from known and unknown threats. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries from viruses, spyware, intrusions, unwanted applications, phishing, spam and email policy abuse. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability. Our instant response to new threats is matched by business-focused, 24/7 technical support, and has led to the highest levels of customer satisfaction in the industry.

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

SOPHOS
WWW.SOPHOS.COM