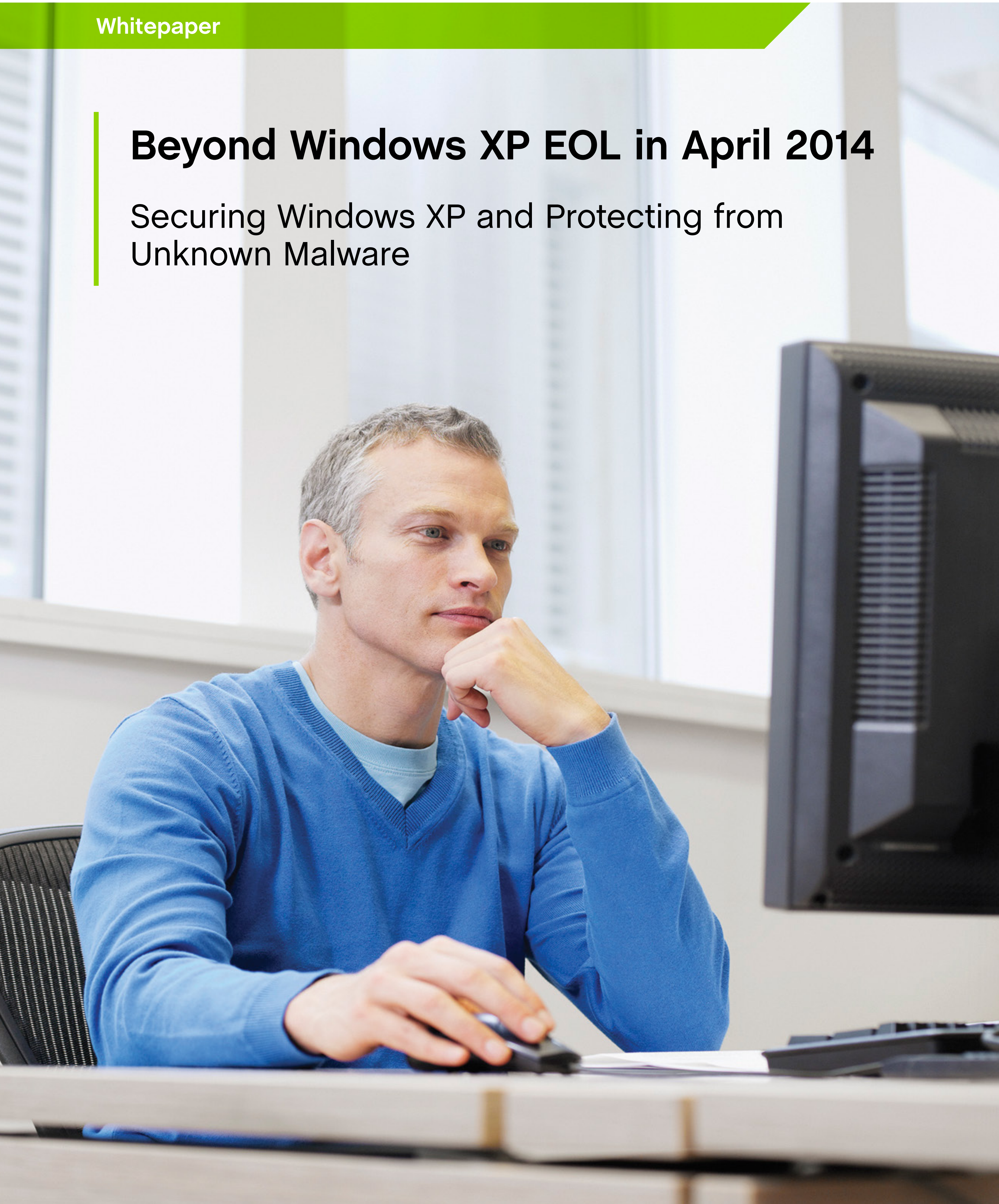
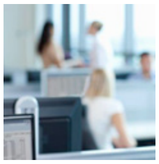
Whitepaper

Beyond Windows XP EOL in April 2014

Securing Windows XP and Protecting from Unknown Malware



Contents



Executive Summary

This guide provides helpful information to IT and business managers about the requirement for proactive desktop security and protection beyond the end of life (EOL) for Microsoft Windows XP in April 2014.

The threat from malware is real, growing, and expected to explode. Experts fear thousands of unknown vulnerabilities in Windows XP still await exploitation when Microsoft stops providing security fixes and service packs as part of Windows XP EOL. In this whitepaper, we will examine how and why this threat has changed and will continue to evolve, as well as how malware writers are fighting back against antivirus software.

We will provide some best practice guidelines to enterprises and government organizations looking for ways to stop the continuing infiltration of systems after Windows XP EOL. Further, we will acknowledge the necessary balance between increasing security, reducing IT administration overhead, and increasing employee productivity.

In addition, we'll explore how AppSense can help you stop malware and protect your antivirus client, while ensuring the integrity of your workstations and notebooks. AppSense solutions add value to any version of Windows and can be used to aid migrations to Windows 7 and 8.

Risks:

- Windows XP will become a soft target to exploit when security patches cease to be issued by Microsoft
- Windows XP still has many known vulnerabilities and possibly even more unknown
- Speculation exists whether “black hat” attackers are holding back exploit code for unpublished vulnerabilities to release once EOL occurs
- Simply maintaining up-to-date antivirus on Windows XP will not suffice
- Network exploitable vulnerabilities still being found
- In the first quarter of calendar year 2013, NIST.gov published 28 network exploitable vulnerabilities affecting Windows XP
- Local administrator accounts leave Windows XP desktops open to exploitation

Malware poses significant financial, legal and resource risk to an enterprise. Brand equity is also at risk through the loss of internal and customer data.

Introduction

Since the late 1990's, malicious computer and network attacks have become increasingly stealthy. No longer are most attacks designed to create visible effects, such as denial-of-service or blue screen a desktop. Instead, today's threats are silent, and quite often employ many interconnected machines - or bots - to conduct their operations. Thousands of bot networks (botnets) have appeared, creating a dark dimension to the Internet. A dimension that operates silently, may already include your organization's devices, and could grow exponentially come April 2014. And you may not even know it's happening.

Existing Security Measures

Multi-layered IT security has increased the time and complexity of administration beyond where IT managers would like it to be; yet network and system vulnerabilities continue to be exploited at an ever increasing rate.

Despite continuing enhancements in perimeter security and antivirus solutions, malicious software (malware) presents an ever increasing threat to the stability and security of enterprise systems and their data. As far back as 2007, Symantec Antivirus had definitions for over one million viruses[1]. Since then, hundreds of thousands of new viruses and a large number of variants for existing viruses have been unleashed on the Internet, making a definition-based approach a highly reactive counter measure to identifying malware running on an endpoint device.

Unfortunately, many security measures can be bypassed by user actions, especially users who have been provided local administrator privileges on their Windows desktop, whereby they, or malware can easily access and manipulate security services.

Microsoft Windows XP End of Life

As a mobile workforce and widespread use of the Internet and e-mail make the network perimeter less relevant, the securing of endpoints (desktops, laptops and virtual desktops) across the enterprise becomes more vital. Stopping unknown sources of attack from within and outside the organization is the next battlefield for IT security.

Organizations still using Windows XP beyond its EOL need to protect against the next wave of unknown malware aimed at exploiting vulnerabilities that will not be fixed no matter how severe. (Nimda, Code Red). Most likely with XP EOL looming, the more organized and well-funded teams of malware writers have already started creating code targeted at individual corporations and even individual users. For businesses that choose to stay on Windows XP beyond April 2014 without a support agreement risk increases significantly.

According to NIST.gov[1] , between January 2013 and March 31st, 2013, Microsoft released 34 high severity updates for Windows XP. Of these, 28 were exploitable via the network. Some of these vulnerabilities could be exploited even when up-to-date antivirus is in place. Antivirus is intended as a last line of defense - to detect and clean up the mess once malware has been executed and delivered its payload. Even then, many areas are outside its scope of control or ability to respond in a timely manner. A recent New York Times article shares that "...By the time [antivirus] products are able to block new viruses, it is often too late. The bad guys have already had their fun, siphoning out a company's trade secrets..." (Perlroth, 2012)[2] .

Windows XP is fundamentally less secure that its successors. A Microsoft report (Microsoft, 2012)[3] notes that malware infection rates of Windows XP are double that of Windows 7.

Many industry watchers believe that cybercriminals may even step up their rates of attack (Sheldon, 2012)[4] as EOL approaches and that "black hat" attackers may hold back exploit code for release after April 2014. The moment support patches stop for Windows XP on April 8th, 2014 a major layer of defense for the operating system disappears.

Moreover, when Microsoft stops supporting Windows XP, many applications vendors will follow suit, discontinuing support and patch security for their Windows XP applications and choosing instead to allocate resources Windows 7 and 8 applications.

[1] NIST.gov, Advanced search for Windows XP vulnerabilities. Web, searched April 1st 2013

[2] Perlroth, Nicole, "Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt", New York Times. Web December 31st 2012.

[3] Microsoft, "Microsoft Security Intelligence Report Volume 13 English", Microsoft, Web (PDF), November 8th 2012.

[4] Sheldon, Robert, "Windows XP End of Support: What are the risks for users?", TechTarget, Web, November 2012

The Growing Market in Computer Crime

Roughly 10 million Americans have their personal information misused in some way every year, costing consumers $5 billion and businesses $48 billion annually.

The Federal Trade Commission estimates that roughly 10 million Americans have their personal information pilfered and misused every year, costing consumers $5 billion and businesses $48 billion annually. The introduction of vast profits in this area has spawned a growing black market. Hackers and malware writers offer their services to order. Stolen data auctions move gigabytes of proprietary information. Whole botnets can be hired for specific purposes, such as massive spam email campaigns and denial-of-service attacks against e-commerce websites.

As this form of crime drives the exploitation of users and machines, its extreme profitability has attracted the attention of organized crime. The power and resources it can apply to computer crime means that the tools employed are sophisticated - professionally produced and controlled.

Specialists tout their skills on unadvertised websites and forums, while loose teams of cyber criminals under the control of highly organized crime syndicates deliver malware in the form of viruses, Trojans, keyloggers, and botnets. Although these don't always rely on a system vulnerability to gain access, many do. What we are seeing is the development of a cybercrime business model. Without regular patches, Windows XP is a soft target in the digital war between IT departments and organized crime.

The Vulnerable Network

The ongoing evolution of cyber security threats has led many organizations to adopt a layered security architecture with different solutions protecting each level of the enterprise. This is 'defense in depth' strategy has significantly increased the overall complexity of IT security.

When an infiltration occurs, this complexity increases the time taken to discover it and respond adequately. Often, each solution requires a different management interface to control, monitor and update.

Some of the main examples of network entry points are:

- Appealing websites that exploit vulnerabilities in Internet Explorer
- SSL encrypted content cannot be screened on the network perimeter
- Specially written e-mails inviting users to open an attachment
- Local Administrator user accounts providing easy, elevated access for Malware
- Peer-to-Peer clients trading illegal, copyrighted material
- Public Instant Messaging
- Removable Media such as CDs/DVDs and USB drives
- Games, screen savers and utilities that often contain Trojans
- Video and audio file downloads

Cyber Threats: Malware tools of the Trade

Trojans, keyloggers, and rootkits are common forms of malware that intrusion prevention systems are designed to detect and block or disable. An ongoing challenge for IT is keeping these systems up to date since they generally rely on signatures or behavioral rules. Antivirus products, for example, use a signature database to identify threats. Even a firewall rules database may need to be altered to close a certain communications port and, of course, Windows needs to be patched regularly to remove vulnerabilities.

Trojans

A Trojan is a mechanism for distributing malicious code that tricks users into executing it by disguising the code as something useful such as a patch, a game, interesting video file, or important message.

The most notable example of this was the Sober e-mail worm. At the height of the Sober outbreak in December 2005, it accounted for 1 in 12 e-mails. The body of the e-mail contained an apparent warning from the FBI or National High Tech Crime Unit that the recipient had been detected visiting websites containing illegal material. The victim was then directed to complete a form attached to the e-mail that infected them with Sober.

Trojans continue to be one of the most common methods of propagating malware because the desktop user remains one of the least protected elements in the IT environment, especially users with local administrator privileges.

Keyloggers

Many forms of malware contain keyloggers that steal information from machines they infect. In February 2006, Brazilian police arrested 85 people for seeding the computers of unwitting Brazilians with keyloggers that recorded their keystrokes whenever they visited their banks online. Using stolen user names and passwords, the fraud ring diverted approximately $4.7 million from 200 accounts at six banks. It is likely that the use of this form of malware will increase in the future as cybercriminals expand their trade in stolen information to industrial espionage.

Rootkits

A rootkit hides the existence of certain processes or programs from normal methods of detection and enables continued privileged access to a computer. The term originally referred to a maliciously modified set of administrative tools for a Unix-like operating system that granted “root” access. It has come to be applied to any technique or code used to conceal activity or objects in a system.

The shift in the purpose of malware has meant that it is increasingly important for an infection to remain undetected as it allows the continued theft of data and the illicit usage of the victim’s bandwidth for purposes such as spam relaying. This has led to an increase in the use of rootkit functionality and a growth in its capability. There are two forms of rootkits used in Windows environments: user level and kernel level.

A user-level rootkit works intercepts and subverts calls made to various application programming interfaces (APIs), which request services from the operating system. Simple ones might intercept requests being made by file system utilities, such as Explorer and command prompt, and modify the data returned. Any scanning tools that also use these APIs will be incapable of detecting this. More sophisticated versions work at lower levels, subverting requests made by user mode elements prior to being forwarded to the kernel mode elements of Windows. In this situation, no scanning tools that work in user mode would be able to detect the interference.

Kernel-level rootkits are even more powerful. They work by intercepting the API calls made between the Windows kernel and the low-level operating system components it controls.

This can result in the kernel being incapable of fully enumerating the contents of its local storage, for example whether its request for the contents of sectors of the local disk is altered prior to being returned. In this situation, virtually all tools used to check for malware infection would be incapable of discovering it.

There are various websites and other places on the Internet that offer malware developers with code that will provide their tools with the functionality of both forms of rootkit. The use of this technology is certain to increase as malware writers look to maximize profits from selling vulnerabilities and exploits after Windows XP EOL.

Today it's not just music, but entire movies and DVD's which are being shared, and of course, malware.

Peer-to-Peer and Bit Torrent clients

In 1999, a young man named Shawn Fanning stayed awake for 60 hours to write a small piece of software called Napster. It allowed people to easily locate and copy music files from other peoples' computers using the Internet. Peer-to-peer (P2P) file sharing was born.

Today, Napster is gone, but file sharing is not. In addition to music, entire movies and DVDs are shared, and, of course, malware. Malware is often embedded into the files downloaded by the naïve user who is expecting nothing more than an album, film, or game. Unfortunately for enterprise security, this could load malware directly onto an endpoint. Peer-to-peer file sharers also consume massive amounts of bandwidth, which reduces network performance everyone. Services and systems that rely on bandwidth can slow to a crawl or fail.

Clearly Internet usage needs to be effectively controlled and, while educating employees is important and necessary, it's never enough. Companies must ask themselves two questions:

- Are users able to install Peer-to-Peer and Bit Torrent clients?

  Unfortunately, many Windows XP users have local administrator privileges and as such have the capability to install and execute new software, in this case peer-to-peer and Bit Torrent clients. Therefore many Windows XP users may already have file sharing technologies installed on their endpoint device and possibly a large number of other non-work related applications, which provide additional routes for malware to access a Windows XP machine.

- Can they identify, quarantine, and remove any infected file downloaded before it can execute its payload?

  Educating employees is one approach, but it's not going to work for some individuals. Why not stop them from installing peer-to-peer applications in the first place? Unfortunately many Windows XP users have Local Administrator privileges and as such have the capability to install and execute new software, in this case Peer-to-Peer and Bit Torrent clients.

Therefore many Windows XP users will already have file sharing technologies installed on their endpoint device, perhaps with a large number of other non-work related user introduced applications. These applications will provide additional routes for Malware to continue to access a Windows XP machine and exploit vulnerabilities which are no longer being addressed.

CIOs and CSOs rank employees second only to hackers as the source of malicious attacks.[5] The Global State of Information Security® Survey 2014 PwC, CIO magazine, and CSO magazine.

“I see the insider threat looming larger in my windshield than in the past. And it’s important to note that insider threats are not necessarily a ‘bad guy’ with bad intentions; it could be a good employee doing righteous work in an insecure manner. Our problems are more human than technological.”

- Michael A. Mason, Chief Security Officer for Verizon Communications

Acceptable use, user behavior and disgruntled employees

As stated, users are one of the most vulnerable parts of any computer system. Their desire to boast, assist other people, curiosity about what they see and read, and their susceptibility to suggestions make them easy targets. Even if users are cautious and only open e-mails from trusted sources or browse reliable websites, they can still become the victims of cyber-attacks.

While indispensable for knowledge workers, Internet and e-mail use in the workplace pose significant risks to corporations, especially when acceptable use policies (AUPs) are ignored. For example, nearly all workers install instant messaging clients on their machines. Many download music or videos and access non work-related websites during working hours.

So if AUPs are not enforced, users can knowingly or unknowingly install software or launch executables that have the potential to cause enormous damage. The EOL of Windows XP simply makes these potential breaches much more likely. Likewise, the ability for unhappy employees to compromise systems and data from within an organization should never be underestimated.

The case of AOL employee Jason Smathers is a disturbing example of the damage a disgruntled employee can cause. After being disciplined, Smathers stole 92 million e-mail addresses and sold them to an email spammer, who used them and resold them. This one theft ultimately generated several billion spam e-mails. Smathers was jailed in 2005.

[5] Global Statement of Information Security: CIO and PWC

Reactive Protection and Its Failings

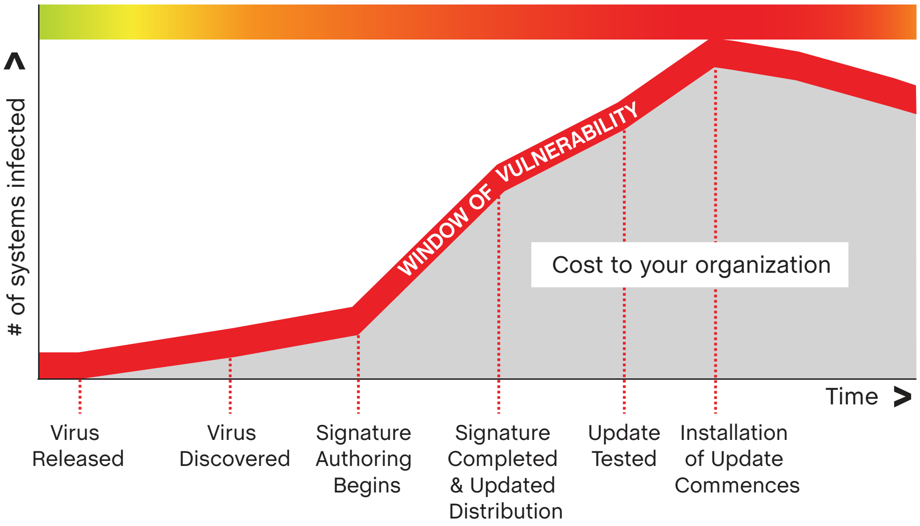
Most security experts agree that it's sensible to use multiple layers of protection against security threats. But this leads to the management complexity we've already discussed, which also includes the time and expense for training and accreditation in product use.

What's more, reactive solutions only protect against what is known. But most new malware is unknown code. For example, antivirus protection. A threat has to be observed and studied before a signature can be released for it. In addition, sophisticated malware can pass through antivirus cleaning. Beyond antivirus, commonly used reactive enterprise security measures include:

- Anti-spyware
- E-mail filtering
- Intrusion Prevention
- Content filtering

By definition, reactive protection cannot prevent zero-day attacks because they exploit previously unknown vulnerabilities. And no matter how fast technology vendors respond, it's never fast enough if your organization is under attack. This 'window of vulnerability' is what keeps CTOs up at night.

Window of Vulnerability:



When Microsoft officially enforces Windows XP EOL in April 2014, a window of vulnerability will stay open indefinitely.

Locking Down Systems

There are various measures intended to protect vulnerable users and endpoint machines. For a long time, perimeter security provided this protection. Over time, attackers have become adept at penetrating the perimeter and targeting attacks directly at users and their applications. Mobile computing has exacerbated this. A corporate firewall can't protect laptop users when they're mobile.

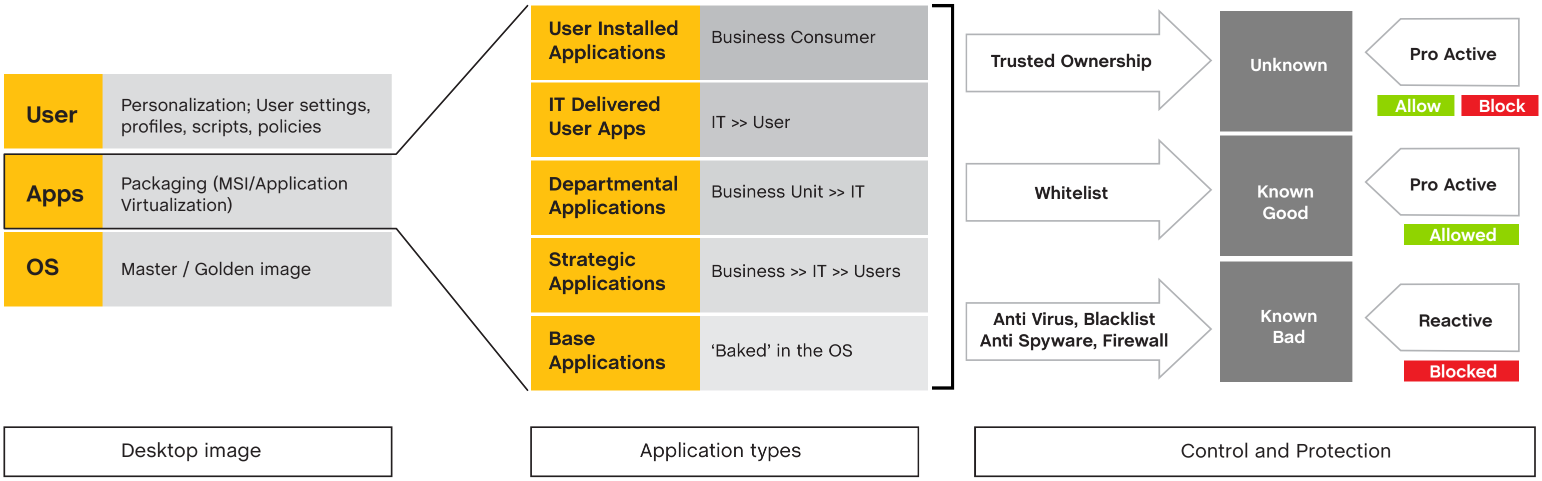
The response from the security industry has been to lock down user machines to limit and mitigate the risks posed by application and user-level attacks. This has proven to be problematic, even after the introduction of tools such as group policy. Gartner Group estimates that while more than 60 percent of organizations want to enforce desktop lockdown, 20 percent of enterprise desktops and fewer than five percent of laptops are locked down today[6] .

Among the reasons for this low rate are concerns about usability. There are many scenarios where users require local administrative rights to work effectively. Many applications allow changes to hardware settings or network adapters and all of which require administrative privileges to execute. This also includes web application updates, the installation of Active-X components, Adobe, Flash, and Java updates, printer drivers. Yet administrative access leaves the desktop vulnerable to malware.

[6] Gartner Report: Windows Application Control (G00137032)

Best Practices: Beyond Reactive Protection

It's clear that enterprises and government organizations need to reimagine their security environments in a broader context and balance those priorities with more efficient IT management. For the purpose of establishing best practice guidelines, it is useful to look at three categories of application-level change: known bad, known good, and unknown.



User	Personalization; User settings, profiles, scripts, policies
Apps	Packaging (MSI/Application Virtualization)
OS	Master / Golden image

User Installed Applications	Business Consumer
IT Delivered User Apps	IT >> User
Departmental Applications	Business Unit >> IT
Strategic Applications	Business >> IT >> Users
Base Applications	'Baked' in the OS

Securing applications from malicious activity has predominantly concentrated on the known bad. With that in mind, the following section summarizes proactive security best practices.

Trusted Ownership Checking

Trusted ownership checking automatically protects systems without complex configuration and constant management. It can block unknown spyware, malicious mobile code and other web-based threats, including executable viruses, Trojans, worms, keyloggers, script attacks, and rogue Internet code.

Trusted ownership checking provides enterprise-wide protection inside and outside the corporate network, adding a valuable layer of security for a mobile workforce. It prevents 100 percent of user-introduced, unauthorized applications, preserves the integrity of gold-build images, and increases user productivity by refocusing resources on business applications.

It examines the NTFS owner of an application prior to execution. If the application is from a 'trusted owner,' anyone is allowed to execute the application. If not, no one may execute the application.

A predetermined list of trusted owners quickly determines which applications are unwanted. By default, only domain administrators are trusted, which ensures only applications installed by IT are allowed to run. A trusted owner list can be extended as required.

Whitelists, Blacklists, and Digital Signature Checking

Whitelists guarantee only known and trusted applications can execute on a system, which means they block the unknown; blacklists protect only against known threats and problem applications.

Digital signature (electronic fingerprint) checking ensures that applications and files installed on a system remain unaltered, preserving system integrity and lowering maintenance costs. Digital signatures are the ultimate identify check for an individual file. If one bit of a file is changed, the digital signature also changes.

For advanced security, this method assigns SHA-1 digital signatures to applications and files and checks them against black or whitelists. Modified or spoofed applications are prevented from executing. However, digital signatures can bring high management overhead as new signatures need to be taken each time a file is updated by means of a service pack or patch.

Self-Healing

Even though trusted ownership checking will prevent the execution of unknown applications, scripts or malware, self-healing technology can correct unauthorized changes to retain a systems desired state. Automated monitoring and self-healing systems can increase security, lower costs, reduce complexity and take much of the manual labor out of managing IT systems - minimizing the business impact of security or system failures.

Self-healing technology automatically protects and repairs essential elements of the system and users' environment. For instance, if a user deletes important configuration settings in the system registry or removes vital files, this can be automatically corrected. The ability to ensure that computer and user settings are restored to their original state in the event of a system failure or unauthorized changes is a major advantage in today's hostile environment. A wide range of items, from processes and services, to files and registry, can be self-healed.

Protecting the Registry from Unknown Malware exploitation

Key areas of the registry, such as the list of programs set to run at user logon, can be set to always be in a known good state. If any malware does configure itself to launch at logon, this self-healing functionality will have removed the call to execute at logon - even though trusted ownership checking will have prevented the execution of the file itself. Similarly, there is also a list of per-user processes configured for launch within the user's profile that can be hijacked by malware and this can be protected with self-healing.

Self-healing can be used to guarantee that critical applications, such as security software, always run, providing additional protection against the threat of Trojans, worms, and spyware. If users had the ability to disable their anti-virus programs (a common practice for users who have heard that anti-virus degrades performance), their entire desktop session will be unprotected until they logoff and back on again. Self-healing can be used to ensure that if these processes terminate for any reason, they are immediately launch again.

The perfect balance between user productivity, security and lower desktop TCO is to control user privilege at an application or individual task level.

Flexible Application and Device Lockdown

Administrators are looking to strip out unwanted functionality from third-party software either for security reasons (i.e. protection of confidential data and removal of potential security loopholes) or to reduce the level of complexity for the end user. Lockdown actions can be used to hide or disable user interface controls and block keyboard shortcuts for all, or specific applications. Behavioral containment of this kind can also extend to all modes of removable media, including USB drives to limit the threat of infection and confidential data loss.

Local Administrator Accounts and Privilege Management

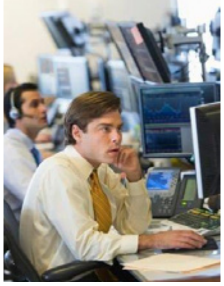
Improper privilege management control creates undue business risk and significantly adds to support costs. Giving users administrative privileges also creates legal and liability issues and makes compliance with guidelines such as Sarbanes-Oxley, HIPAA, COSO and FERPA difficult to accomplish.

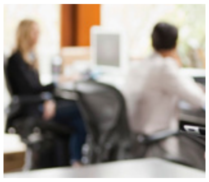
The perfect balance between user productivity, security and lower desktop TCO is to control user privilege at an application or individual task level. By making sure users have only elevated privileges for the applications, processes, or tasks that need them, enterprise TCO falls and managing end points becomes easier with fewer support calls. Users can still do everything they need without introducing security vulnerabilities.

Application Network Access Control

Application network access control (ANAC) intercepts and blocks requests made to prohibited network resources and controls outbound network connections by IP, host name, URL, UNC, or port based on the outcome of rules processing. It prevents user or malware from accessing network resources by controlling network access without complex controls such as routers, switches, and firewalls.

Process rules enable outbound network access to be determined by the specific process, i.e. different applications can have different restrictions. Process rules allow IT to determine what processes (children) can be run by the application (parent). This can prevent malware from accessing the corporate network from an infected machine.





Security checklist

When looking to source new security solutions, ensure they can deliver the following benefits:

Mitigate risk

Stop all unauthorized applications through proactive protection resulting in more robust security policy enforcement and less reliance on vulnerable and reactive security systems. Eliminate local administrator accounts and utilize a privilege management solution to increase security and reduce risk.

Leverage Existing Security Investments

Add to any existing security systems in a way that helps them maintain their integrity through automatic self-healing to ensure that they are always operational.

View and Audit All Potentially Malicious Activity

Get a true picture of what is really going on at the application level of all endpoints, with instant alerts to inform of any attempted breach. Audit and report at a granular level.

Reduce IT Management Costs

Reduce reliance on roaming profiles, patching, and system updates via self-healing, and application and system hardening - decreasing administrative tasks and lowering support costs.

Enable Compliance

Increase visibility into endpoint behavior with report and auditing capabilities that enable compliance.

Stop zero-day attacks. Stop patching chaos; well, there won't be any patches available... ...With one, easy, proven solution

Protect Once, Protect forever

AppSense is licensed on a per-user basis, which means when you're ready to migrate to Windows 7 or 8, the technology can be used again to continue protecting your users, their desktops, and your data, increasing return on investment.

AppSense has helped, and continues to help, many organizations migrate to Windows 7 - significantly reduce the cost, time and complexity of the migration.

To learn more about how we can help your organization migrate to Windows 7 or 8, please visit appsense.com.

Prepare for Windows XP EOL with AppSense

AppSense desktop security solutions provide centrally deployed, enterprise-class protection Windows endpoints that stops all unknown and unauthorized executables. Unknown threats cease to be a problem, and so does your lack of Windows XP updates, patches, and hotfixes.

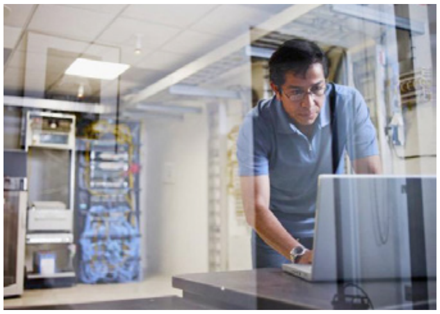
For example, many viruses are e-mailed to users using attachments. If they receive an e-mail with a virus attached and they click on the attachment, AppSense prevents it from executing. There is no need to worry about what the virus is; no need to identify it and wait for a signature to be produced. Whether it's well known or the latest, newly released malware, it‘s stopped.

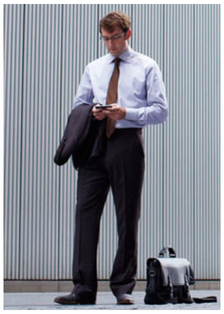
It's also common for users to introduce unwanted applications like games or peer-to-peer utilities, which often contain spyware to harvest e-mail addresses and other information. The AppSense trusted ownership mechanism stops these applications from running, preventing data loss.

AppSense is true protection from the unknown, including zero-day threats. More effective than an intrusion detection system, it stops intruders in their tracks. Hacking tools don't run. Trojans don't give unauthorized backdoor access. And spyware cannot send out your business critical information. It also stops executable viruses from inflicting any damage and infecting other systems, while anti-virus vendors catch up with its specialized detection signature.

AppSense provides security professionals with a whole new range of tools and options they can use to ensure system integrity and secure vulnerable endpoints. It augments firewalls, intrusion detection systems, and anti-virus clients as it helps IT administrators:

- Reduce security risk
- Ensure compliance
- Maintain systems in desired state
- Enforce Licensing
- Decrease IT management complexity
- Lower desktop TCO





The Technology

The AppSense approach, which has been designed to meet public sector and intelligence agency standards, is a revelation for anyone who has had to spend weeks configuring options on a new solution. It requires virtually no configuration; protection is nearly immediate.

AppSense comes with its own centralized deployment technology that can work independently or as part of an Active Directory implementation. This effectively eliminates the need to visit individual computers. Once in place, AppSense logging and reporting is centralized so administrators have a clear picture of user activity.

After the AppSense agent is installed, its kernel-level driver intercepts all requests to execute files and prevents unauthorized applications from starting via AppSense trusted ownership checking. If the NTFS owner of an application is not a trusted owner, the application is unauthorized and it's execution prevented.

If more granularity is required for specific applications or users, AppSense Application Manager can allow or block applications based on rules you define. This can be done by placing either the executable's location or its digital signature into a whitelist or blacklist. These additional rules can be applied to individual users, specific machines, or to groups extracted from Active Directory.

If you're unsure whether you have a problem or are concerned about the effect of blocking unauthorized executables, AppSense offers the unique ability to passively monitor the files users execute without alerting them. It creates an audit trail of all applications you haven't authorized and gives you true visibility into what is happening, without impacting business processes.

To learn more about AppSense, call us at 866. 277 7367, email iwanttoknowmore@appsense.com, or visit us on the web at appsense.com.

appsense.com

Twitter:
@appsense

email us:
iwanttoknowmore@appsense.com

USA
AppSense, Inc.
17 State Street
19th Floor
New York, NY 10004
USA
T +1 212 597 5500
us-info@appsense.com

100 Mathilda Place
Suite 200
Sunnyvale
California 94086
USA
T +1 408 343 8181
us-info@appsense.com

United Kingdom
AppSense Ltd
3300 Daresbury
Business Park
Daresbury
Warrington, WA4 4HS
United Kingdom
T 0845 223 2100
uk-info@appsense.com

100 Longwater Avenue
Green Park
Reading
RG2 6GP
United Kingdom
T 0845 223 2100
uk-info@appsense.com

Australia
AppSense Sydney
Level 33, Australia Square,
264 George St,
Sydney, NSW
2000
Australia
T +61 (0) 2 9258 1862
australia-info@appsense.com

France
AppSense France
17 Square Edouard VII,
75009 Paris
T + 33 01 53 43 5148
france-info@appsense.com

Germany
AppSense GmbH
Werner-von Siemens Ring 17
85630 Grasbrunn/München
Deutschland
T +49 89 559 9970
de-info@appsense.com

Netherlands
AppSense Benelux Ltd
Entrada 501
1096 EH Amsterdam
The Netherlands
T +31 20 3701282
benelux-info@appsense.com

Nordic region
AppSense AS
Tærudgata 1
2004 Lillestrøm
Norway
T +47 41 43 23 30
nordics-info@appsense.com

AppSense®