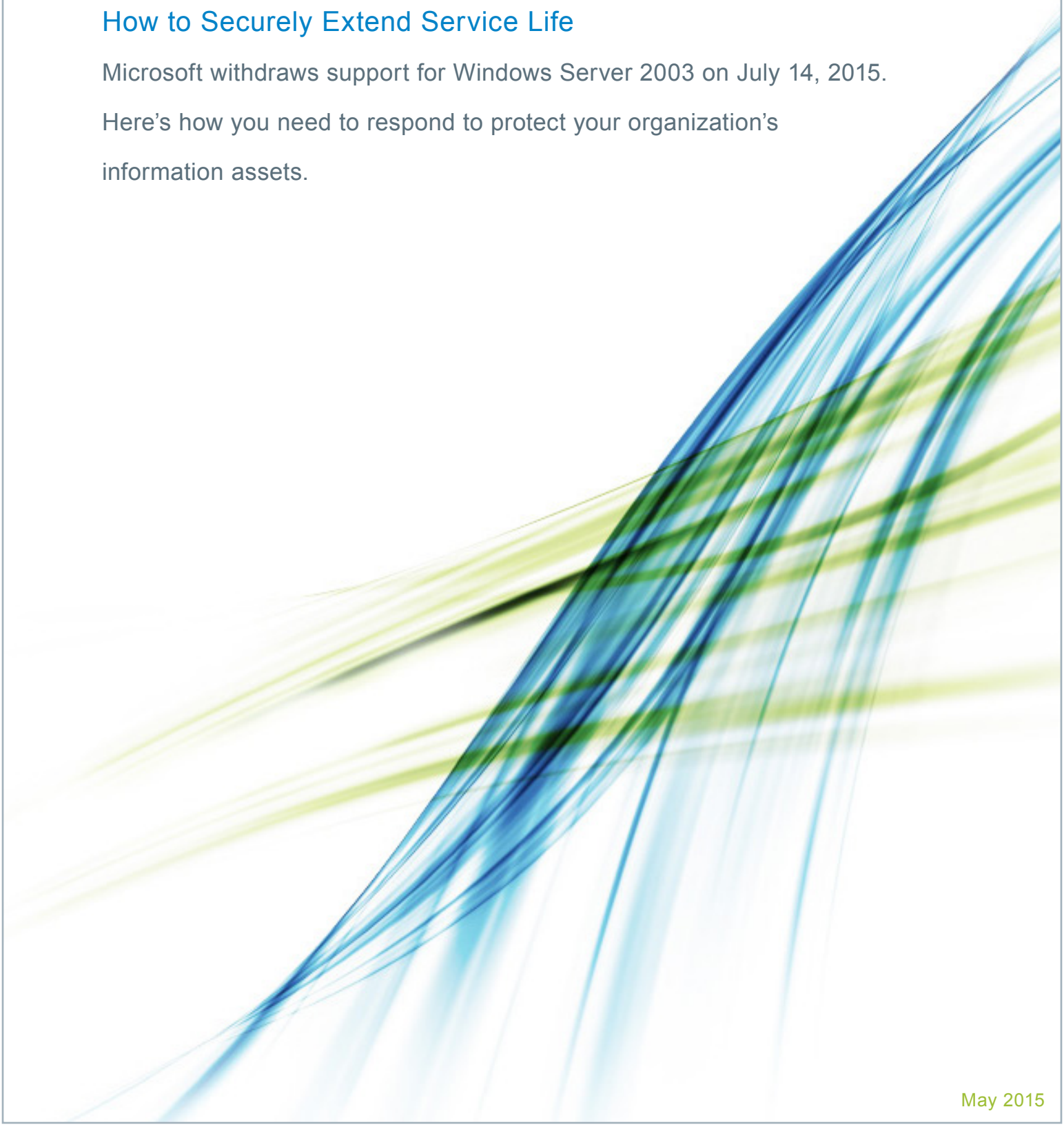
Windows Server 2003 End-of-Support

How to Securely Extend Service Life

Microsoft withdraws support for Windows Server 2003 on July 14, 2015. Here's how you need to respond to protect your organization's information assets.



May 2015

WP-EN-05-10-15

Just after enterprises have finished migrating their desktops from Microsoft Windows XP, they now have to turn around and move away from Windows Server 2003. The venerable (and now vulnerable) operating system reaches end of support on July 14, 2015. But many companies will continue to use the software after that deadline, and that has serious security implications.

July 14, 2015
Last day Microsoft will support Windows Server 2003

Microsoft itself couldn't state it any clearer: "After July 14, Microsoft will no longer issue security updates for any version of Windows Server 2003. If you are still running Windows Server 2003 in your datacenter, you need to take steps now to plan and execute a migration strategy to protect your infrastructure."

Just what's at stake? Starting July 15, Microsoft will no longer provide security updates or support for any edition of WS 2003: Itanium, x64, Datacenter, Enterprise, Compute Cluster or Web. There will be no security patches or hotfixes. Zero-day vulnerabilities will remain liabilities forever. And depending on your industry, you could quickly run afoul of data security regulations.

And rest assured, there's no shortage of threats. In 2013, Microsoft released 37 critical security patches for WS 2003. In 2014 the number was 26. That pace will likely continue for 2015 — and it may even tick higher as attackers rush to exploit unpatched systems.

In fact, Redmond is already skipping WS 2003 patches. In January 2015 it released a patch to the Network Location Awareness service for all versions of Windows Server except 2003. Even though that version was affected, Microsoft said it was "infeasible to build the fix for Windows Server 2003."

There are a few options for addressing the issue, from ignoring the problem to ripping out every instance of the operating system. From a security standpoint, however, there's only one real solution, and that's application control in the form of intelligent whitelisting — for reasons that will become clear.

26
Number of critical Windows Server 2003 security patches in 2014

But while WS 2003 end of support presents a significant challenge, it also represents a tremendous opportunity. That opportunity lies in gaining experience with application whitelisting in the short term and improving your security posture across the enterprise going forward.

Continued »

State of the OS

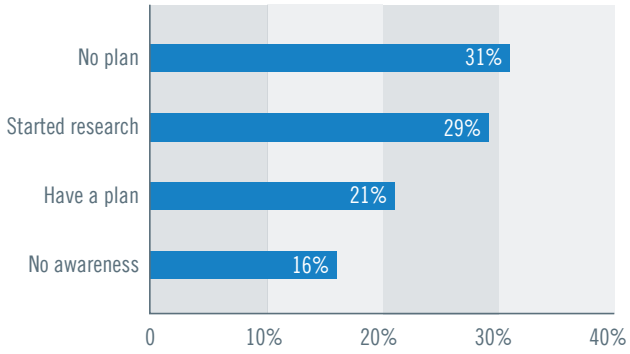
Estimates for the number of installed WS 2003 boxes vary. In 2014 Gartner pegged the number at 8 million. HP said 11 million. Microsoft reported 24 million instances, half physical, half virtual.

How many of those servers are migrating? As of late 2014, only one-fifth of companies using WS 2003 had a plan for migration, according to a survey of 1,000 IT pros at Fortune 500 companies by AppZero. (See Figure 1.) Less than one-third had started researching migration. And nearly half either had no migration plan or were unaware support was ending. (A recent survey of 1,300 IT pros, primarily in the U.S. and Europe, by the IT community Spiceworks returned quite similar results.)

What's more, only one-third of companies are certain they'll complete migration from WS 2003 before Microsoft withdrawals support. (See Figure 2.) Another third or so say they'll migrate later this year or in 2016. And nearly a third are unsure when they'll migrate. At the same time, one-quarter of organizations have more than 500 WS 2003 machines.

Those machines will be increasingly vulnerable, and the consequences of those vulnerabilities will be increasingly dire. First, cyber-attacks are indisputably on the rise. More than 317 million new pieces of malware were created in 2014 — nearly 1 million a day, according the Symantec 2015 Internet Security Threat Report. Ransomware attacks grew 113 percent, and crypto-ransomware, in which files

Figure 1: WS 2003 Migration Readiness



As of late 2014, nearly one-half of organizations either had no plan for WS 2003 migration or were unaware support was ending.

Source: AppZero 2014 State of Readiness for Windows Server 2003 End of Support

Has Windows Server 2003 Support Already Ended?

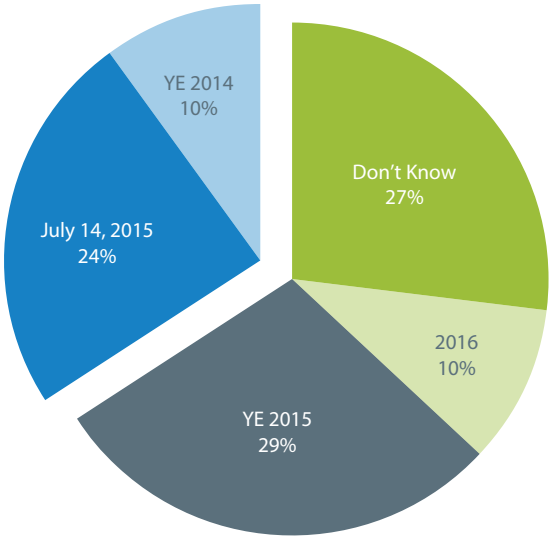
Windows Server 2003 support doesn't officially end till July 14, 2015, but Microsoft has already declined to patch important or critical vulnerabilities:

- MS15-005 (Important) — Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (January 2015)
- MS15-011 (Critical) — Vulnerability in Group Policy Could Allow Remote Code Execution (February 2015)

Continued »

are encrypted and held hostage without warning, rocketed 4,000 percent. Five out of six large enterprises were hit with spear-phishing attacks, a 40 percent jump, while 60 percent of targeted attacks struck small and midsize companies.

Figure 2: Migration Completion Targets



Only one-third of companies are certain they'll complete migration from Windows Server 2003 before Microsoft withdrawals support.

Source: AppZero, 2014 State of Readiness for Windows Server 2003 End of Support

317 Million
Number of new viruses in 2014

The financial implications of breaches are also ratcheting upward. The average cost of a security incident rose 15 percent to $3.5 million, according to the Ponemon 2014 Cost of Data Breach Report. The price tag for each lost or stolen record containing sensitive information grew 9 percent to $145.

As WS 2003 comes off support, expect attacks targeting the operating system to only escalate. WS 2003 shares code with the current version, WS 2012 R2. In fact, in January 2015 Microsoft released five security bulletins that affected both versions. Attackers can use such security bulletins to identify patched vulnerabilities in WS 2012 that they can exploit in the unprotected WS 2003.

$3.5 Million
Average cost of a data breach

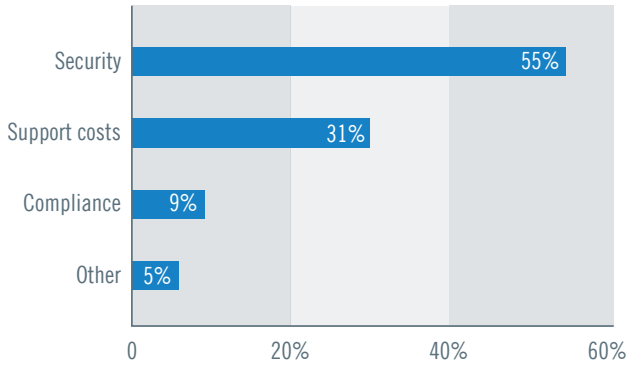
That's exactly what happened after Windows XP reached end of support in 2014. It has been the case for earlier Windows versions, as well. In the first two years after Windows XP SP2 went out of support, its infection rate spiked, reaching 66 percent higher than SP3. It's no wonder IT pros cite security as the leading risk of running WS 2003 after end of support. (See Figure 3.)

More Reasons to Replace

But security concerns aren't the only reason to upgrade from WS 2003. Other factors should drive organizations to seriously consider moving to the latest version of Windows Server before end of support:

Continued »

Figure 3: Risks of Running WS 2003



Security tops the concerns of IT pros as Windows Server 2003 approaches end of support

Source: AppZero 2014 State of Readiness for Windows Server 2003 End of Support

Regulatory compliance — Companies that "go beyond the termination of extended support place themselves ... potentially in a regulatory noncompliance situation," according to an IDC report, "Windows Server 2003: Why You Should Get Current."

Nearly all U.S. states now have data privacy laws that require organizations to exercise due diligence in protecting personal information. Running an unsupported operating system could result in an officially recognized control failure by internal or external audit bodies. That could drive a public notification of your organization's inability to maintain its systems or customer data.

As the U.S. Computer Emergence Readiness Team (CERT) puts it, "Organizations that are governed by regulatory obligations may find they are no longer able to satisfy compliance requirements while running Windows Server 2003."

Exorbitant support costs — For companies that want to extend support for WS 2003 after July 14, Microsoft offers Custom Support Agreements (CSA) for a limited period. Under a CSA, Microsoft will issue security patches for vulnerabilities the company deems critical. Other vulnerabilities may be covered for additional fees. However, "this option is not for the faint of wallet and is intended only for organizations that are making a proactive effort to migrate off" WS 2003, IDC says.

The average cost to an organization will be $200,000 for the first year, according to reports from HP and others. In the past Microsoft has increased the cost of CSAs over time, sometimes doubling the price tag year over year.

$200,000
Projected first-year cost of a WS 2003 Custom Support Agreement

WS 2012 RS security — The latest version of Windows Server delivers new capabilities such as virtualization and cloud support. It also offers significant defense-in-depth advantages over WS 2003. (See Figure 4.) From a security standpoint, it simply makes good sense to upgrade.

Continued »

Figure 4: Windows Server Defense-in-Depth

Feature	WS 2003 with IE 8	WS 2012 R2 with IE 11
Allocation Randomization	✖	✔
ASLR	Limited	Extensive
Bottom-Up Randomization	✖	✔
Enhanced Protection Mode	✖	✔
Enhanced / GS	✖	✔
Force Image Randomization	✖	✔
Guard Pages	✖	✔
Header Encoding	✖	✔
Heap Hardening	Limited	Extensive
Heap Randomization	✖	✔
High Entropy Randomization	✖	✔
IE Protected Mode	✖	✔
PEB/TEB	✖	✔
SEMOP	✖	✔
Stack Randomization	✖	✔
Terminate on Corruption	✖	✔
Top-Down Randomization	✖	✔
Virtual Table Guard	✖	✔

The latest version of Windows Server offers significant defense-in-depth advantages over WS 2003.

Source: HP

Continued »

Four Steps to Windows Server 2003 Upgrade Success

Data security typically involves a four-step process, from understanding your environment to ensuring strong security over the long term. Organizations can apply the same approach to upgrading WS 2003:

- **Discover** — First, conduct a thorough review of your environment to determine exactly where WS 2003 is running throughout your enterprise. That's especially important for geographically dispersed enterprises—or those with an extensive virtual infrastructure—that might not have visibility into all their locations.
- **Assess** — Next, determine what the result of your discovery means for your organization. Do you have a business need for systems running WS 2003 or compatible applications? If you plan to upgrade to WS 2012 R2, is your hardware robust enough? Will you also need to upgrade or replace Microsoft or third-party applications?
- **Remediate** — Based on your assessment, you should now understand your best course of action. If you're a pure WS 2003 shop, your IT organization may face a learning curve. You also need a plan for hardware, operating system and application upgrades, with budgets, timelines and training. Keep in mind how changes to your environment might affect data security.
- **Monitor** — Once you've deployed your new technology, keep it in compliance with robust configuration management, patch management and application control.

Should I Stay or Should I Go?

For some organizations, however, there may be good reasons to stick with WS 2003, at least in the near term. One reason is application compatibility. Many 32-bit applications that run on WS 2003 should also run on the 64-bit WS 2012 R2 with an emulator. But security applications and system utilities that operate in kernel mode—such as backup—must be upgraded as part of the WS 2003 migration.

Likewise, custom applications or heavily modified standard applications may need to be upgraded to work with WS 2012 R2. That could involve substantial time and expense. And for some custom applications, the original developers—along with their knowledge and expertise—may no longer be available. A similar consideration is applications that themselves are approaching end of life or already out of support.

Continued »

In addition, migrating to WS 2012 could call for hardware upgrades. Upgrading a datacenter operating system can have cascading effects that extend far beyond the operating system itself. You need the staff and budgetary resources to make the upgrade a success.

26%

Whitelisting requires less CPU resources than AV, on average, under load

Another reason companies might remain on WS 2003 simply has to do with timing. The average end-of-life migration takes 200 days, according to multiple industry sources. With millions of WS 2003 instances still in operation, many organizations will simply run out of runway—and need to continue relying on WS 2003 after July 14, 2015.

With these factors in mind, and in lieu of upgrading to WS 2012 R2, organizations need to consider their next move. There are several options:

- **Upgrade to WS 2008** — Migrating to WS 2008 might be easier in the short term. But as that version of the operating system reaches end of support in five years, moving to WS 2008 only delays the inevitable.
- **Move to Linux or UNIX** — This option also requires rewriting applications, and it probably involves more short-term cost and risk than sticking with Windows Server.
- **Strengthen WS 2003** — You can improve WS 2003 security somewhat by deploying Microsoft's Enhanced Mitigation Experience Toolkit (EMET). This allows you to apply some mitigation technologies to certain applications.
- **Bandage WS 2003** — You could wrap your WS 2003 boxes in antivirus (AV) software and hope for the best. Of course, depending on what you use them for, some of your servers might not even require AV. But even for those that do require it, AV simply isn't adequate to protect against today's onslaught of continuously morphing malware.

White-Knight Whitelisting

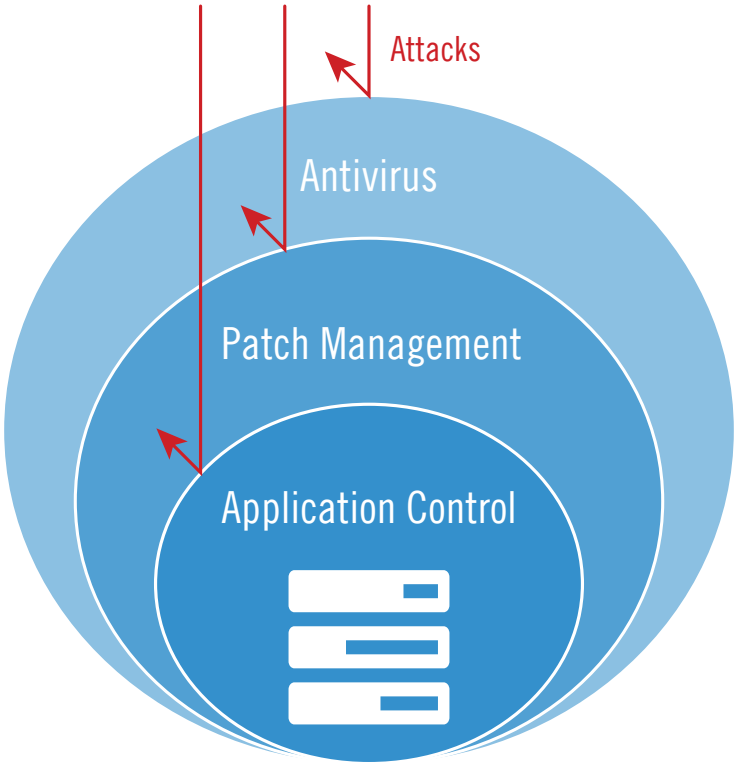
Organizations that haven't started replacing WS 2003 will have a very tough time completing an upgrade before support ends on July 14, 2015. Even those in the midst of a migration may struggle to meet the deadline. In the meantime, they need to ensure they're protecting their environments against software vulnerabilities.

The most effective way to achieve that protection is through application control in the form of intelligent whitelisting. The good news is that whitelisting is a key component of layered, defense-in-depth security. (See Figure 5.) Not only is it more effective against all forms of malware, including zero-days, but it also reduces performance impacts on your servers.[1] So whitelisting is a weapon you should have in your security arsenal anyway.

[1]Tolly Enterprises, Improving Server Performance and Security: An Impact Comparison of Application Control and Traditional Anti-Virus Solutions (April 2013)

Continued »

Figure 5: Intelligent Whitelisting Layered Defense



Intelligent whitelsiting can protect against server attacks that would otherwise be missed.

What's more, often the most effective way to deploy whitelisting is in a phased approach. You start by tightening control on a defined subset of your environment, gaining experience and fine-tuning your configuration to be sure your implementation of whitelisting reflects your business needs. When you're ready, you roll out the whitelist enterprisewide.

A WS 2003 upgrade affords precisely this opportunity. You can deploy whitelisting to protect your no-longer-supported WS 2003 servers today. As your upgrade reaches completion, you can extend the protection of intelligent whitelisting throughout your environment tomorrow.

Intelligent whitelisting is an approach to application control that lets you prevent malware and unapproved software from running on your machines, while giving you the flexibility to adapt to changing business needs. It starts with a local whitelist and a trust engine that lets you define criteria for trusted applications. You can specify trusted publishers, updaters, paths or locations. You can also specify trusted authorizers, so certain users can use software that would otherwise be blocked.

Continued »

Intelligent whitelisting also lets you maintain a blacklist of denied applications. The blacklist can override the whitelist to block specific applications, regardless of publisher or path, for example.

WS 2003 end of support presents a significant challenge — and a tremendous opportunity to gain experience with application whitelisting in the short term and to improve your security posture across the entire enterprise going forward.

You can define upfront the sorts of changes you'll allow — on your endpoints, for instance—so you don't have to manually vet every update. For example, you can automatically extend trust based on criteria such as vendor (digital certificate), updater (patch management agent) and path (where the application is located). You can even allow local users to install on their own PCs and laptops, while automatically monitoring and logging what they're doing. That lets IT focus less on day-to-day maintenance and more on strategic activities.

Note that intelligent whitelisting doesn't replace AV or patch management. In fact, the most effective whitelisting combines AV, patch management and application control in a single solution. This gives you a true layered approach to security that protects your information assets while allowing your organization to be as productive and effective as possible.

WS 2003 is a venerable operating system that was supported for 12 years — a lifetime in the IT industry. Because it's so widespread, its end of support presents organizations with inevitable challenges. Fortunately, application whitelisting offers the enterprise an effective means of ensuring robust security until a WS 2003 upgrade is complete. Even better, it provides an opportunity to achieve a stronger security profile over the long term.

Next Steps

Here are some tools to help you protect the WS 2003 systems you can't migrate in time:

- **Discover** – use the Application Scanner tool to see which machines in your environment as still running this unsupported OS.
- **Learn** – read this study by Tolly which shows how application whitelisting not only protects against malware and zero-days, but improves performance.
- **Test** – request a demo of the Lumension® Endpoint Management and Security Suite to see how you can better protect your environment.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 3,000 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, Antivirus and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Texas, Florida, Washington D.C., Ireland, Luxembourg, Singapore, the United Kingdom, and Australia. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Global Headquarters
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255 USA
phone: +1.480.970.1025
fax: +1.480.970.6323

Lumension®
IT Secured. Success Optimized.™