Managing Your Legacy Systems: What Will Life Be Like After Windows Server 2003?

A TrendLabs℠ Primer

After Microsoft ended support for Windows® XP last April 8, 2014, users and organizations alike that continued to use the operating system (OS)[1] put their computers at risk of possible attacks that exploit vulnerabilities that are no longer addressed by security fixes. Exploits that target the outdated OS's vulnerabilities continued to spread, prompting Microsoft to release a patch once to address a zero-day vulnerability in Internet Explorer®. Despite the absence of support since 2014, the OS's market share[2] continued to increase.

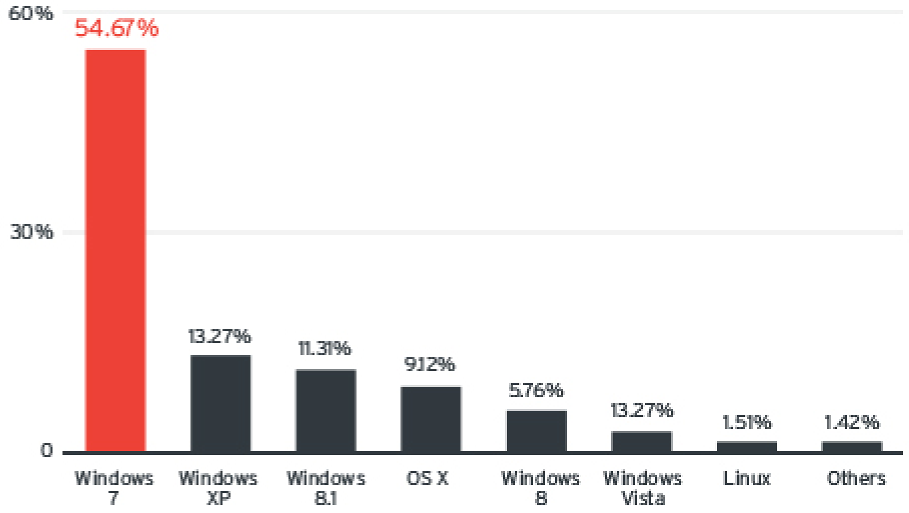

Figure 1. *Windows XP's market share (May 2014–May 2015)*
Source: *Statcounter.com*

Windows Server® 2003, another widely used OS, will soon join Microsoft's roster of unsupported software. With an estimated 2.6–11 million installations worldwide[3], the OS supports business-critical applications as well as email and directory servers, among others. Like Windows XP, Server 2003 will no longer receive security updates to address issues that surface after July 14, 2015. Microsoft will no longer issue regular

[1] Pawan Kinger. (8 April 2015). *TrendLabs Security Intelligence Blog.* "Windows XP—It's Not Dead Yet." Last accessed on 14 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/windows-xp-its-not-dead-yet/.

[2] Simon Sharwood. (2 March 2015). *The Register.* "Windows XP's Market Share Grows AGAIN! Not Even Nuking It from Orbit Will Do the Job, We Fear." Last accessed on 14 July 2015, http://www.theregister.co.uk/2015/03/02/windows_xp_markets_share_grows_again/.

[3] Nick East. (27 November 2014). *TechRadar Pro.* "Fighting Against the End of Life." Last accessed on 14 July 2015, http://www.techradar.com/news/software/operating-systems/fighting-against-the-end-of-life-1274656.

product fixes and vulnerability notifications for the OS as well. Enterprises are thus encouraged to migrate to newer OSs if they wish to stay safe from system and network exploitation that may result in malware infections, information loss, targeted attacks, and data breaches.

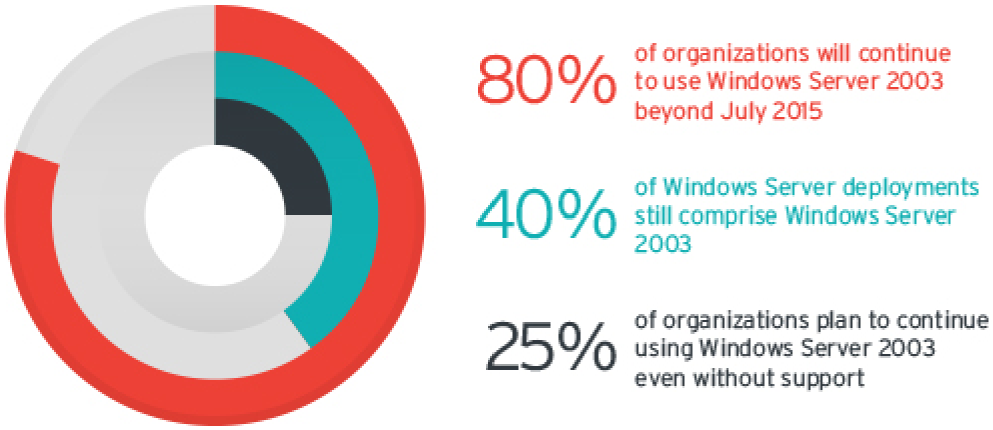

Figure 2. *Windows Server 2003 usage statistics*
Source: *Enterprise Strategy Group (ESG)*

What happens when software vendors cease to support products?

When Oracle ceased support for Java™ 6 in February 2013, attackers immediately trailed their sights on unpatched versions of the software. A few months after the Java 6 end of life (EOL), attackers attempted to exploit CVE-2013-2463, which affected certain versions of the software, including Java 6.5. Because Java 6 was no longer supported, Oracle did not release security updates, leaving users to fend for themselves. Even worse, the exploit was integrated into the Neutrino Exploit Kit, which can result in more future attacks.

A zero-day exploit targeting a vulnerability (CVE-2014-1776) in Windows XP also surfaced just weeks after Microsoft ended support for the OS. Successful exploitation of CVE-2014-1776 can result in remote code execution. Microsoft released a patch for the said vulnerability[4] but reiterated that it will no longer do so for succeeding vulnerabilities. Users and organizations will not even be notified of future vulnerabilities. In fact, throughout the second quarter of 2014, only four out of the 28 vulnerabilities affecting Windows XP[5] were patched.

Users of Windows Server 2003 may suffer the same predicament. Newly discovered vulnerabilities in the software will remain unpatched, allowing cybercriminals and threat actors to successfully launch damaging attacks.

[4] Jonathan Leopando. (27 April 2014). *TrendLabs Security Intelligence Blog.* "Internet Explorer Zero Day Hits All Versions in Use." Last accessed on 14 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/internet-explorer-zero-day-hits-all-versions-in-use/.

[5] TrendLabs. (2014). *Trend Micro Security News.* "TrendLabs 2Q 2014 Security Roundup: Turning the Tables on Cyber Attacks—Responding to Evolving Tactics." Last accessed on 14 July 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-turning-the-tables-on-cyber-attacks.pdf.

Why is it so hard to migrate to newer software versions?

Despite the pressing urgency, migrating to newer OSs is not as easy as some believe. IT professionals can, however, anticipate the challenges that come with major OS upgrades.

A Trend Micro research revealed that only 35% of businesses have finished migrating from Windows Server 2003. Two-thirds of the 63% who plan to migrate will do so in the next six months.

A joint study by ESG and Trend Micro[6], meanwhile, revealed that 25% of the OS's current users will continue to run Windows Server 2003 even without support and maintenance patches. The top reasons enterprises cited that prevented them from upgrading their software include:

- Too much time and effort needed to migrate
- Existing apps will not work on newer or other OSs
- Lack of resources or expertise to migrate
- Too costly to rewrite applications written for Windows Server 2003

Apart from the amount of time and resources it would take to complete migration, IT administrators are also concerned that business applications may not properly run on newer OSs, which could disrupt their business. The key challenges that enterprises and midsize businesses expect to face during migration include compatibility issues and lack of expertise.

[6] Jon Oltsik, Sr. (3 June 2015). *BrightTALK.* "Staying Secure After Microsoft Windows Server 2003 Reaches End of Life." Last accessed on 14 July 2015, https://www.brighttalk.com/webcast/12177/157259?utm_campaign=channel-feed&utm_content=&utm_source=brighttalk-portal&utm_medium=web&utm_term=.

The next big threat

Today's threats have substantially changed, creating a reality where vulnerabilities can put an entire company and its data at risk. As seen before, exploiting vulnerabilities that have been in systems, servers, and applications for years can have dire consequences.

Top concerns when running unsupported Windows software:

- Security compliance and vulnerability management
- Increased support costs
- More security risks like data theft
- Sudden increase in downtime
- Inability to meet regulatory compliance requirements

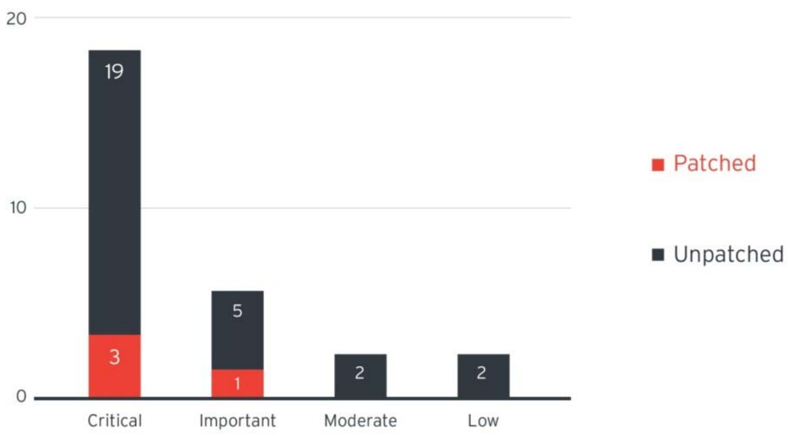

Figure 3. *Volume of Windows XP vulnerabilities found in the second quarter of 2014*

Cybercriminals and threat actors can easily exploit vulnerabilities even on systems and applications not previously thought vulnerable. An example of this is the Bash bug (Shellshock)[7], which affected servers and devices that have been there since 1989. Similarly, the FREAK vulnerability[8], which has been there since the 1990s, put users at risk of losing sensitive information such as credentials to attackers. Who knows? The next Heartbleed or Shellshock, which had a huge impact on users, could arise for unsupported software. Enterprises are thus advised to use virtual patching applications

[7] Trend Micro Incorporated. (29 September 2014). *TrendLabs Security Intelligence Blog.* "Summary of Shellshock-Related Stories and Materials." Last accessed on 14 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/summary-of-shellshock-related-stories-and-materials/.

[8] Trend Micro Incorporated. (4 March 2015). *TrendLabs Security Intelligence Blog.* "FREAK Vulnerability Forces Weaker Encryption." Last accessed on 14 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/freak-vulnerability-forces-weaker-encryption/.

to protect against vulnerabilities, especially in software for which patches are no longer available.

> *"EOL for an OS, specifically for Windows Server 2003, means the beginning of a lot of effort on your IT department's part. Organizations must prepare to deal with missing security updates, compliance issues, fighting malware, and other nonsecurity-related bugs. Users will no longer receive patches for security issues or vulnerability notifications. And they will no longer know when there are vulnerabilities that affect their servers."*
>
> *—Pawan Kinger,*
> *Trend Micro Director*,
> *Deep Security*

Securing your legacy systems

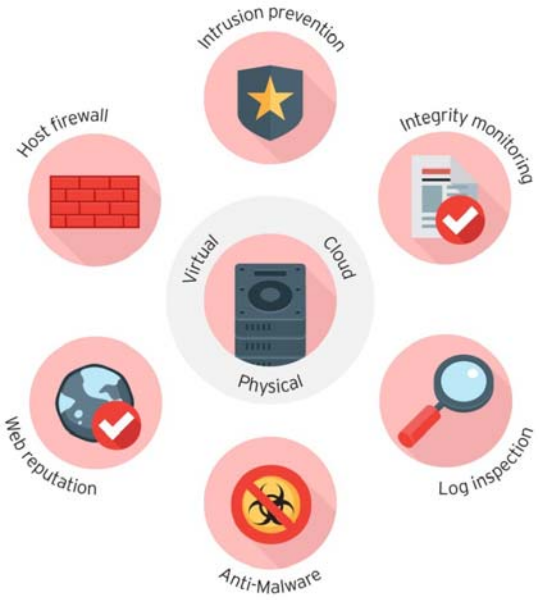

Figure 4. *Deep Security's features*

Migrating from one OS to another is not easy. It may take up several months, even years, for an enterprise to completely upgrade, given that it's not simple. Shifting to a newer OS can brings out compatibility and compliance issues with existing applications. These can open organizations to windows of exposure. The next big threat can surface anytime due to the absence of necessary security fixes. Attackers will use the exploits in their arsenals to infiltrate target networks. All is not lost though, as a security platform such as Trend Micro™ Deep Security[9] can help protect your organization from exploits for old and newly discovered vulnerabilities alike without disrupting your business and requiring emergency patching. Deep Security's intrusion detection and protection features shield unpatched vulnerabilities found in Web applications, servers, and software from exploits. As such, attacks targeting flaws like Shellshock, Heartbleed, and FREAK, among others, and the risks these pose, can be thwarted.

[9] Trend Micro Incorporated. (2015). *Trend Micro.* "Trend Micro Deep Security Platform." Last accessed on 14 July 2015, http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/.

Mitigating security risks: Virtual patching

While Microsoft offers customized emergency patches even for outdated software[10], giving companies extended support, availing this can be costly. Completely migrating to newer software may also take time. In the meantime, enterprises can opt to use security solutions with virtual patching features[11] such as Trend Micro Deep Security and Endpoint Security in Trend Micro Smart Protection Suites. These protect legacy systems, shielding them against old and newly discovered vulnerabilities alike even before these can be exploited without affecting users' operations due to system downtime.

As always, knowing is half the battle. For the latest vulnerability information, visit the Trend Micro Threat Encyclopedia[12].

[10] Trend Micro Incorporated. (April 2015). *Trend Micro Security Intelligence.* "The Clock Is Ticking on Windows Server 2003 Support." Last accessed on 14 July 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_windows-server-2003-end-of-support.pdf.

[11] Trend Micro Incorporated. (2015). *Trend Micro.* "Virtual Patching." Last accessed on 14 July 2015, http://www.trendmicro.com/us/enterprise/challenges/cloud-virtualization/virtual-patching/index.html?cm_mmc=VURL:USA-_-ENT-_-Deep+Security-_-Virtual+Patchin.

[12] Trend Micro Incorporated. (2015). *Trend Micro Threat Encyclopedia.* "Vulnerabilities—Alerts and Solutions." Last accessed on 14 July 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability.

Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICROTM

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

TREND MICRO™ Securing Your Journey to the Cloud