ESG Solution Showcase

Compensating Security Controls for Windows Server 2003 Security

Date: May 2015 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: It is common knowledge by now that Microsoft will end-of-life Windows Server 2003 as of July 14, 2015 and no longer provide software maintenance or support. In other words, Microsoft will stop issuing software updates for patching software vulnerabilities discovered. Unfortunately, this is a cause of great concern for many organizations that are still running Win2K3 servers and may take some time before they can migrate these workloads to alternative operating systems. Organizations planning on continued use of Windows Server 2003 must implement compensating controls to add defense-in-depth protection and enhanced security monitoring capabilities. Trend Micro's Deep Security product can be helpful here by providing network, system and anti-malware security controls across physical, virtual, and cloud systems running W2K3.

Overview

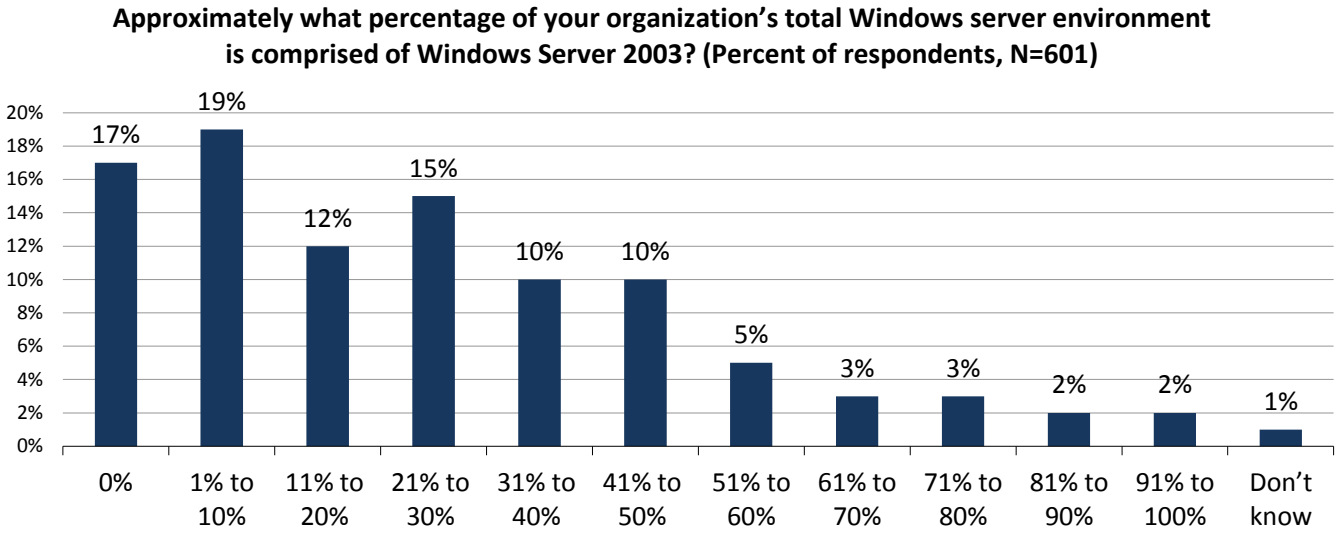
July 14, 2015 marks an important day in the annals of Information Technology. On that day, Microsoft Corporation will officially end-of-life its venerable Windows 2003 Server product, offering no further maintenance, software patches, or support.

From a software perspective, the retirement of Windows Server 2003 makes a lot of sense. After all, Win2K3 was first introduced in April 2003 and its successor, Windows 2008, has been around since February 2008. Based upon normal software product lifecycles then, Windows Server 2003's departure was long overdue. In spite of Microsoft's operating system progress however, many organizations continue to cling to Windows Server 2003 on the eve of its retirement. In fact, ESG research indicates that 35% of organizations report that more than 30% of their Windows server portfolio is still made up of Windows Server 2003 today (see Figure 1).[1]

[1] Source: ESG Brief, *Microsoft Windows Server 2003: The End is Nigh*, February 2015. All ESG research references and charts in this solution showcase have been taken from this research report, unless otherwise noted.

This ESG Solution Showcase was commissioned by Trend Micro and is distributed under license from ESG.
© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

FIGURE 1. Windows Server 2003 Remains Widely Deployed



Source: Enterprise Strategy Group, 2015

What Are Organizations Planning to Do?

CIOs have seen this movie before. For example, Microsoft ceased supporting its PC operating system, Windows XP, in April 2014, and other software vendors have similarly put older software versions out-to-pasture after years of useful service. In anticipation of Windows Server 2003's retirement, many organizations are already planning their next moves. For example, ESG research indicates that 73% of organizations plan to upgrade to Windows Server 2012 and reinstall applications, 35% want to move Win2K3 servers to public cloud infrastructure, and 32% are intent on retiring servers, operating systems, and resident applications (see Figure 2).

These legitimate options provide an upgrade path off of Windows Server 2003, but migration processes can be time consuming and resource intensive. This may be why industry research indicates that 15% to 20% of PCs are still running Windows XP, more than a year after its official end-of-life deadline. Server operating system migrations may be even more onerous, since these upgrades can be impacted by:

- **Regulators and auditors.** In some cases, regulatory bodies need to certify specific application/operating system configurations. This is not unusual in the health care industry where it can take months before government agencies complete their certification process and approve new application/OS combinations. While IT and compliance auditors may not need official operating system certification, they may ask for several months to familiarize themselves with new application/OS combinations before they are willing to consider them as "in compliance."

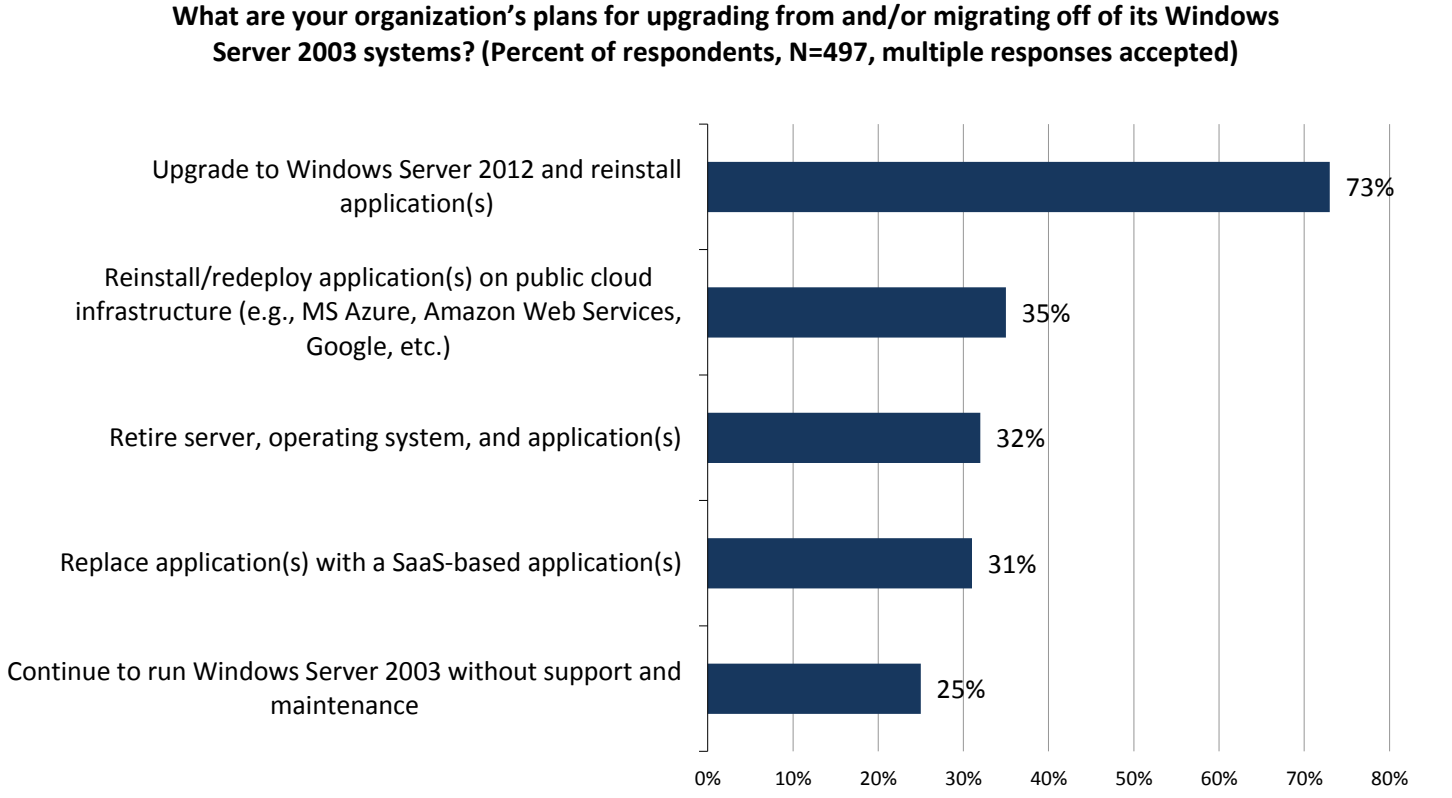
- **Packaged application vendors.** Certain packaged application vendors may also need some lag time before they are willing to support the migration of their applications to OS versions beyond Windows Server 2003. This is especially true for fixed-function applications such as industrial control systems, manufacturing equipment, and health care devices.

- **System qualification and testing.** Even organizations that plan on moving to Windows Server 2008, 2012, or public clouds will still be faced with projects to qualify their applications on new operating environments, test application functionality, modify IT and security operations, and deploy new servers on production IT networks. Yes, moving

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Windows Server 2003 workloads to the cloud may be slightly easier, but IT managers will still demand ample time for qualification, testing, and IT process re-engineering. Since this process can take months to accomplish, CIOs may also slow-roll operating system upgrades in favor of higher-priority projects that deliver more tangible business benefits.

FIGURE 2. Upgrade and Migration Plans for Windows Server 2003



Source: Enterprise Strategy Group, 2015

Windows Server 2003 and IT Risk

The ESG research indicates that 25% of organizations will continue to run Windows Server 2003 without support or maintenance while many others will need time to migrate to newer versions of Windows or cloud-based alternatives. In the meantime, continuing use of Windows Server 2003 can only increase IT risk.

IT risk will be on the rise because hackers and cyber-criminals also understand that Windows Server 2003 will be hanging around for a while. Unfortunately, this means that cyber-adversaries are likely to accentuate their efforts to find 0-day vulnerabilities for exploitation and resale. Once discovered, black hat security researchers will sell them to the highest bidders who will then develop exploit kits and look for other buyers on cyber-crime websites. Others will pile on, offering malicious payloads for sale. It won't take long before this black market activity leads to real Windows Server 2003 cyber-attacks and data breaches.

Normally, Microsoft would usurp this process with an emergency response or a regular software update on "patch Tuesday." After July 14 however, Microsoft will be out-of-the-loop, leaving organizations to defend against inevitable attacks on their own.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Compensating Controls for Windows Server 2003

With no help from Redmond after mid-July, CISOs must take up the slack by employing compensating security controls to protect their Windows Server 2003 systems. These compensating controls should include things like:

- **System hardening.** Security professionals will want to lock down Windows Server 2003 with hardened configurations that can disable unnecessary services, set up ACLs for file access, and limit administrator actions. Hardening guidelines are available from Microsoft as well as organizations such as NSA, NIST, and others.

- **Network security controls.** CISOs may want to use the network to isolate traffic to-and-from remaining Windows Server 2003 systems. Network security controls can include firewall rules, ACLs, and network segmentation using IP subnets or Layer 2 VLANs. Host-based IDS/IPS, particularly when deployed at an affected host like Windows Server 2003, can also offer vulnerability-facing protection through the use of "virtual patching." This is done by updating IDS/IPS signatures with specific rules for blocking exploits aimed at newly discovered software vulnerabilities. As such, virtual patching may be very effective in protecting exposed Windows Server 2003 systems after July 14.

- **System security controls.** Security teams can also take action on the server itself in several ways. Existing host-based security software should be configured for maximum protection by enabling features for real-time malware detection/prevention. In some cases, the security operations team may want to install file integrity monitoring software (FIM) on servers with configurations that rarely change (i.e., single or fixed-function servers). CISOs may also want to explore whether they can utilize trusted hardware such as the Trusted Platform Module (TPM) to improve system integrity and attestation. Finally, Windows Server 2003 instances can be run as VMs so they can take advantage of security functionality at the hypervisor level.

Organizations may also want to increase their monitoring activities related to all instances of Windows Server 2003. This can include frequent reviews of log activity and network flows for anomalous/suspicious activities like network communications with esoteric server processes and services. CISOs may also want to create specific rules and dashboards in security analytics tools to make Windows Server 2003 monitoring easier for the SOC team.

Trend Micro Can Help Protect Windows Server 2003

While CISOs recognize the impending security issues around Windows Server 2003, they may not have the time, resources, or skills to piece together a security strategy on their own. Organizations that fall into this category should look instead for security technologies delivering strong Windows Server 2003 security in a comprehensive and easy-to-use package.

Security leader Trend Micro can help here as its Deep Security product offers virtual patching, system integrity controls/monitoring, and anti-malware capabilities. Furthermore, Deep Security supports physical, virtual, and cloud-based servers, giving IT and security managers the ability to balance IT flexibility with strong security. Finally, Deep Security provides central management across all security controls, helping to streamline server security operations.

Given these capabilities, organizations running Windows Server 2003 after mid-July 2015 may want to contact Trend Micro and explore how Deep Security can help them maintain strong security in an operationally efficient way. Trend Micro is committed to helping organizations smoothly transition from Windows Server 2003, and has extended support for Deep Security until 2020 to provide enough runway for migration.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

The Windows Server 2003 situation represents a fragile balancing act for organizations. Real business, regulatory, and/or IT issues are forcing IT managers to hang onto Win2K3 beyond its end-of-life date in July, but this means living with obsolete and unprotected software residing on production networks.

This certainly presents a real challenge for CISOs as they must figure out how to support business realities while addressing the foreseeable increase in IT risk. Smart security professionals will implement layers of compensating controls for Windows Server 2003 across the network and the systems, thus creating a specific defense-in-depth architecture for these vulnerable servers. The SOC team will also pitch in by increasing server monitoring and developing triggers, alerts, and rule sets to focus on incident detection and response for Win2K3 servers.

Of course, security professionals are already quite busy with daily activities and may be overwhelmed by additional tasks for Windows Server 2003 security. In these instances, CISOs should look for turnkey security tools, like Trend Micro's Deep Security, that can help them reinforce Win2K3 server security in an effective and efficient manner, and also provide security to the new platforms, whether in the data center or in the cloud.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an integrated IT research, analysis, and strategy firm that is world renowned for providing actionable insight and intelligence to the global IT community.

© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.