WHITE PAPER

Running Windows Server 2003 in a Post-Support World

By Nick Cavalancia

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.

TABLE OF CONTENTS

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.

You've heard it said — "All good things must come to an end." And with the end of support for Windows Server 2003 on July 14, 2015, the logical conclusion is it's time to upgrade to newer, supported, flavors of Windows Server. While most organizations have focused efforts around moving off of Windows Server 2003, not all of you are either ready to do it, or are more simply put — can't do it.

You'd think having been given enough warning, it would merely be an issue of planning and execution to move to, say, Windows Server 2012. But, given the average migration timeframe is 200 days, according to Microsoft, it becomes obvious that it's just not that simple.

With an estimated 9 million installations of Windows Server 2003 still existing months before the deadline demonstrate that organizations, like yours, have their reasons for remaining on this 11 year-old operating system. Budgetary constraints always come into play, as running Windows Server 2012 will not only require new licensing, but also new hardware. The inability to migrate off of critical applications that are no longer supported, have no current version, or have no equivalent replacement are reason enough. And then there are simply organizations with smoothly running instances of Windows Server 2003 where the age old "if it's not broke, don't fix it" adage applies.

Budgetary constraints always come into play, as running Windows Server 2012 will not only require new licensing, but also new hardware.

But, without support, is it really not broke?

Sure, the OS is functional, but it's important to also focus on whether the security and continued compliance of your Windows Server 2003 instance is also in tact. When you consider the OS and application vulnerabilities that are constantly being discovered that impact Windows Server 2003 (16 were discovered in the first quarter of 2015 alone), it becomes necessary to consider security as part of the overall health of both your Windows Server 2003 instances, as well as part of the security and health of your entire organization.

Microsoft has offered support contracts to help larger organizations who can afford the price of entry — starting prices are $600 per server. Even if you could afford this post-EOL support, these contracts only focus on critical updates. The reality is, like any innovator of software, Microsoft wants to move on and doesn't want to spend their time working on vulnerabilities found in a 12 year old OS.

So if you're going to continue running Windows Server 2003 beyond the end of support date, what should you be concerned about in a post-support world?

The Challenge of Staying on Windows Server 2003

Once your 2003 servers are running post-support, when you boil it down, you simply want them to continue running as they did on July 13th, 2015. To do that, it becomes critical that nothing changes on that server; as long as it remains static the server, and your organization, will remain operational.

Once your 2003 servers are running post-support, you simply want them to continue running as they did on July 13th, 2015.

But, with undiscovered vulnerabilities, an unsupported OS, and zero updates, is this even possible?

With no support and no updates, an organization has two very real concerns around running Windows Server 2003 that can materially impact the organization. The first is an inability to stay secure, and the resulting inability to remain compliant.

Staying Secure

Without the right tools, keeping an unsupported OS secure is a nearly impossible task. Shy of completely isolating it from every other device on the network (to protect against malware that spreads internally to a 2003 server), there is little you really can do.

The problem is vulnerabilities exist in the Windows Server 2003 OS. These vulnerabilities leave Windows Server 2003 exposed for malicious code to be run, or administrative privileges to be attained. And without support to both identify vulnerabilities and provide updates, your Windows 2003 servers and all devices connected to those systems will be insecure.

While known vulnerabilities should concern you (those you have updates for already), it's the ones you don't know about that should really worry you. These undiscovered exploits on unsupported OSes are referred to as negative zero day vulnerabilities. These vulnerabilities exist, are unknown to Microsoft, and are actively being exploited. (Remember, the day you hear about a new vulnerability in the news isn't necessarily the day it was released… it was the day it was discovered.)

Because of the common codebase that does exist across versions of Windows Server, it's easy to envision new vulnerabilities in Windows Server 2003 past the end of support. Whether the intended OS to exploit is Windows Server 2012 or 2003, Microsoft security bulletins show a single vulnerability impacting Windows Server 2003, 2008, and 2012, demonstrating someone can just as easily take advantage of a vulnerability in Windows Server 2012 and it still impact 2003.

And, without an ability to absolutely ensure security, it's equally difficult for an organization to maintain compliance.

It's easy to envision new vulnerabilities in Windows Server 2003 past the end of support.

Remaining Compliant

Compliance mandates do make an attempt to provide guidance on what should be implemented, but at the same time need to remain vendor agnostic since companies choose to run various platforms, operating systems, and applications. But some requirements are very specific around system hardening and patching. Take, for example, section 6.2 of the Payment Card Industry's Data Security Standard (PCS-DSS) that says:

> *Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.*

As of July 13, 2015, assuming every updated has been applied, your Windows Server 2003 instances are technically compliant – every patch and update available has been applied, meeting compliance requirements.

But on the 14th, it's a completely different story.

Not only will you no longer have access to updates, but every organization running Windows Server 2003 won't even know if a vulnerability has been exposed and is being taken advantage of. It's logical to conclude that without an ability to patch, your Windows Server 2003 instances, you simply will not be able to meet compliance objectives like those set forth in PCI. This is false.

Building a Vulnerability Mitigation Strategy

Every operating system, including Windows Server 2003, has vulnerabilities — many more than we know about today. It's only known vulnerabilities that your systems are currently protected against — assuming you have deployed the latest patches — and some of these vulnerabilities have actually been around for years. Take, for example, a recent March 2015 critical vulnerability affecting Windows Server 2003's Service Pack 2. SP2 was released in March of 2007!

So when running Windows Server 2003 post-EOL, it's actually virtually impossible to have a vulnerability strategy. Why? Because, it's called patching. A vulnerability is found, Microsoft puts out an update, you patch your server — that's vulnerability mitigation.

So when running Windows Server 2003 post-EOL, it's virtually impossible to have a vulnerability strategy.

The challenge with a vulnerability mitigation strategy is 1. You have to actually know the vulnerability exists and 2. You have to have a patch. Since Microsoft will no longer be providing updates, (and even those of you that can get a support contract, you won't be getting updates for every vulnerability), this strategy will, at a minimum, have rather large gaps in it, leaving your 2003 servers exposed.

So how can you mitigate the risk of malicious attacks via OS vulnerabilities?

The Answer: Threat Mitigation

You might start by asking what's the difference between vulnerability mitigation and threat mitigation. Let's look at the simple example of you protecting your house during the zombie apocalypse to differentiate each type of mitigation.

Those zombies are a hungry bunch and you want to stay alive. Your house is made of concrete, so, in general, it's relatively protected. However, like every house, yours has a number of entry points — a few windows and doors — that are great when life is normal, but become points of zombie entry when the apocalypse hits — making you vulnerable.

If you were to work to mitigate the vulnerabilities in your house, you'd board up those doors and windows to keep the zombies out. Why? Because you don't want the zombies to come into your house and become a threat. You see, the real threat is not the windows or doors. The threat is the zombie and what they will do once they come into your house. So like any good zombie prepper, you have your trusty shotgun ready, as your threat mitigation strategy is to blow those zombies away should they enter.

Bringing the analogy back to reality, vulnerabilities in Windows Server 2003 are the "windows and doors" through which malicious code can enter a system. And given new vulnerabilities are being found each month, it's likely your Windows Server 2003 systems have plenty of undefined vulnerabilities yet to be discovered.

But that's not your biggest problem.

The biggest issue is not whether you have an entry point exposed; it's what malicious code (the "zombie") can do once inside.

The biggest issue is not whether you have an entry point exposed; it's what malicious code (the "zombie") can do once inside. Most common forms of malware need to do something — run an executable, take control, etc. Threat mitigation focuses on the business-as-usual processes on a given server or endpoint, whitelisting those processes that are supposed to run, and "pulling the trigger" on those that are not. In essence, implementing a threat mitigation strategy on Windows Server 2003 is like watching for anyone other than your family inside your home — should a zombie make its way in, it gets blown away with your shotgun.

Technologies like User Access Control and Group Policy-based software restriction policies will get you part of the way, but to truly lock down a Windows system, you may need to look at a third-party solution that monitors for and restricts unauthorized processes.

Because out of support systems like Windows Server 2003 become very fixed function, the process of monitoring and controlling change on them is a natural fit, creating a protective layer that, when a vulnerability is taken advantage of, there is no ability to actually run or deposit anything malicious on the system.

Threat Mitigation and Compliance

While it's been demonstrated that compliance standards often have specific verbiage around the required use of patching, and threat mitigation takes an obviously different route to address actual threats.

Can threat mitigation meet compliance requirements?

The saving grace is something called a compensating control. Because compliance standards are written from a generic standpoint, they usually allow a different security control to be used in place of the defined security control that either meets or exceeds the security value of the one specified in the compliance standard. And because patching in Windows Server 2003 will become non-existent for most organizations, mitigating threats through application whitelisting, proving enforcement of only running approved applications becomes a compensating control, leaving your Windows Server 2003 instances compliant.

One day you're going to get rid of Windows Server 2003.

While a threat mitigation strategy helps better address malicious attacks and helps to maintain compliance, you will eventually need to move to Windows Server 2008 or 2012.

So is threat mitigation only a post-support tool?

Threat Mitigation as part of the Upgrade Plan

One day you're going to get rid of Windows Server 2003. Some of you may hold out for years, and some may be in the planning phases of a not to distant migration. Remember, the longer you take, the more vulnerabilities in Windows Server 2003 will be identified and exploited by those wanting to do harm. At this point, it's obvious that until you're completely off of Windows Server 2003, you will need to mitigate threats.

But is that the only place threat mitigation has in your upgrade plans?

Considering the common codebase issues that create vulnerabilities that impact Windows Server 2012 all the way back to 2003, or even Windows 2000 Server, it becomes evident that the right approach is to utilize a threat mitigation strategy regardless of the operating system.

Threat mitigation is something you should implement on your Windows Server 2003 instances to keep them secure today, but given the existence of zero day vulnerabilities, it becomes critical to keep the same threat mitigation controls in place on your 2008 and 2012 servers.

Thinking of it another way, someday your Windows Server 2008 instances will be in this very same situation, perhaps more frequently than we've experienced with 2003, justifying the need for continual threat mitigation. The EOL scenario will happen again with 2008 at some year in the future and, given published release schedules, perhaps will occur more frequently.

The EOL scenario will happen again with 2008 at some year in the future and, given published release schedules, perhaps will occur more frequently.

Conclusion

The end of support for Windows Server 2003 hasn't created a vulnerability problem; it has only highlighted the need to protect against vulnerabilities and, at the same time, emphasized the inefficiencies vulnerability mitigation has in trying to protect the organization against threats.

Focusing solely on vulnerabilities and patch management only provides a false sense of security, relying on Microsoft to tell you about the latest one found. It's important to recognize that whether or not you are told a vulnerability exists, zero day vulnerabilities do exist and are being exploited.

By putting a threat mitigation strategy and controls in place, you're building a process that includes an additional layer of protection regardless of whether you are in sync with the Microsoft support calendar. ■

With nearly 20 years of enterprise IT experience, Nick Cavalancia is an accomplished consultant, speaker, trainer, writer, and columnist and has achieved certifications including MCSE, MCT, MCNE and MCNI. He has authored, co-authored and contributed to over a dozen books on Windows, Active Directory, Exchange and other Microsoft technologies. He has spoken at conferences such as the Microsoft Exchange Conference, TechEd, Exchange Connections, and on countless webinars and at tradeshows around the world.

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.