Avecto

Windows server 2003 expiration brings defense in depth

The termination of support for Windows Server 2003 (WS2003) is imminent, leaving many enterprises in a race against the clock before the system's security patches cease.

The challenge: understanding today's threat landscape

61% of businesses have at least one instance of WS2003 running in their environment, which translates into millions of installations across physical and virtual infrastructures. While many of these businesses are well aware of the rapidly approaching July 14th deadline, and the security implications of missing it, only 15% have fully migrated their environment. So why is it that many enterprises are so slow to make the move?

Migration déjà vu

The looming support deadline, the burst of security anxiety, the mad rush to move off a retiring operating system... sound familiar? This scenario is something we've seen before, coming just 12 months on from expiration of Windows XP support.

While there may be fewer physical 2003 servers in an organization than there were XP desktops, a server migration is more challenging and presents a higher degree of risk. From an endpoint perspective, replacing one desktop with the latest version of Windows affects only one user - meanwhile, a server might connect to thousands of users and services. Having a critical server unavailable for any length of time could cause major disruption and pose a threat to business continuity.

Compared to the desktop, server upgrades are significantly more complex, especially when you then add hardware compatibility issues and the need to re-develop applications that were created for the now outdated WS2003. Clearly, embarking on a server migration can be a very daunting process - much more so than the XP migration - which seems to be holding many organizations back.

The cost of upgrading vs. staying

Moving off WS2003 can be a drain on time resources. While most IT administrators understand how to upgrade an XP operating system, the intricacy of server networks means many migrations will require external consultancy, especially if they are left to the last minute. It's no wonder that companies this year are allocating an average of $60,000 for their server migration projects.

Still, it's a fair price to pay when you consider the cost of skipping an upgrade entirely. Legacy systems are expensive to maintain without regular fixes to bugs and performance issues. And without security support, organizations will be left exposed to new and sophisticated threats. Meanwhile, hackers will be looking to these migration stragglers as their prime targets. For those who fall victim to exploits as a result, it's not just financial losses they'll have to deal with, but a blow to their reputation as well. It also means that companies continuing to run on WS2003 after support ends will be removed from the scope of compliance, adding other penalties that could damage the business even further.

Avecto

If they haven't already, businesses still running on the retiring system should be thinking now about making an upgrade to Windows Server 2012. It's easier said than done, of course. A server migration can take as long as six months, so even if businesses start their migration now, there could still be a two month period during which servers run unsupported. This means that organizations should be putting defenses in place to secure their data centers for the duration of the migration and beyond.

Control admin rights

While sysadmins are notorious for demanding privileged access to applications, the reality is, allocating admin rights to sys-admins is extremely risky, since malware often seeks out privileged accounts to gain entry to a system and spread across the network. Plus, humans aren't perfect, and the possibilities for accidental misconfigurations when logging onto a server are endless. In fact, research has shown that 80% of unplanned server outages are due to ill-planned configurations by administrators.

Admin rights in a server environment should be limited to the point where sysadmins are given only the privileges they need, for example to respond to urgent break-fix scenarios. Doing so can reduce exploit potential significantly. In an analysis of Patch Tuesday security bulletins issued by Microsoft throughout 2014, the risk of 97% of Critical vulnerabilities affecting Windows operating systems could be mitigated by removing admin rights.

Application control

Application Control (whitelisting) adds more control to a server environment, including those that are remotely administered, by applying simple rules to manage trusted applications. While trusted applications run through configured policies, unauthorized applications and interactions may be blocked. This defense is particularly important for maintaining business continuity as dev teams are rewriting and refactoring applications.

Windows Server 2003 migration, a window of opportunity

It shouldn't take an OS end of life to spur change - especially security change. Organizations and their IT teams should always be thinking about how they can adapt their defenses, ensuring that they're primed to handle the new and sophisticated threats we see emerging every day. A migration is often the perfect time to revitalize an organization's security strategy. With a migration process a catalyst for reinvention, IT can lean on solutions like Defendpoint to not only lock down the migration, but carry beyond it too, providing defense in depth across the next version of Windows.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world's biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto's Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.