The Fulcrum Group, Inc.
(817) 337-0300

Windows Server 2003 End of Life

And 5 Additional Tech Updates That Should Be On Your Radar

This White Paper is brought to you by your friends at The Fulcrum Group, Inc.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Keller, TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

Windows Server 2003's Wrap Up
And 5 Tech Updates To Keep On Your Radar

This month, our white paper is divided into two related parts – first, we'll tackle the demise of Windows Server 2003. Then we explore the tech updates we feel should be under your consideration right now.

Part 1 - Windows Server 2003 End of Life

With the sun setting on support for Windows 2003 servers and a looming deadline of **July 14th, 2015**, Windows Server 2003 has remained a reliable part of many organizations' infrastructure, However, according to a wealth of good information on Microsoft's Server 2003 End of Life Resource page, Windows Server 2003 has been succeeded by many newer generations over the past decade and they've deemed the time has come for customers to take this conclusion of a lengthy life cycle seriously and make near-term plans to begin a migration plan.

It is important to note that customers who go beyond the termination of extended support place themselves at potential security risks and potentially in a regulatory noncompliance situation**.**

That said, we realize some companies find themselves in a state of "forced dependency" on Windows Server 2003 due to such issues as:

- custom-created or heavily customized apps reliant on Server 2003
- packaged applications not running properly on newer versions of Windows server
- the need to run a product that is no longer supported (or its support is reaching the end of its life cycle).

In cases such as these, we wish to encourage decision makers to ***consider the entire software ecosystem that remains on Windows Server 2003 today, and to lean toward choices that benefit the whole application stack and offer the longest return on investment*****.**

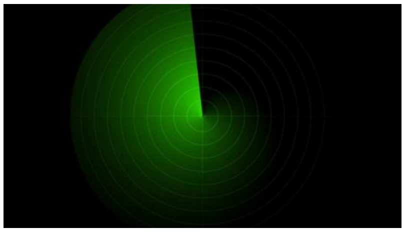
With that in mind, key concerns of remaining on Windows Server 2003 include:

- **Lack of patches/updates/non-security fixes** – No-cost, non-security related update support terminated on July 13, 2010. However, support for non-security-related updates was available on a for-fee basis to customers that felt it was important to continue to have access to fixes that could help their system run optimally and perform well.
- **Elimination of security fixes** – Customers see security fixes as being among the most critical fixes for their installed servers. These fixes will no longer be delivered to customers for their Windows Server 2003 servers, regardless of how severe a given issue may be. This may be less of a problem with many aging Windows Server 2003 applications, mainly because the applications still in use are increasingly likely to be inward facing rather than outward facing.

- **Lack of support** - Customers no longer have the ability to contact Microsoft for technical support in the event of a server problem. This becomes particularly important when a system experiences an outage and customers are unable to restore the system and recover data and applications from the stalled machine.
- **Application support challenges** – Application ISVs dislike having a complex support matrix and typically support current versions along with a finite number of earlier editions of the product. For most ISVs, an 11-year-old application is probably already past its rational support life cycle, and in most cases, these application ISVs are about to discontinue or have already discontinued support for aging operating system environments such as Windows Server 2003.
- **Compliance issues** – Customers in regulated industries or handling regulated data, including healthcare and payment card industry (PCI) data, may find that they are out of compliance, which could mean fines or being cut off from key trading partners that seek to protect their own regulatory compliance status.
- **Inability to leverage modern cloud options from Microsoft and other vendors** – Windows Server 2003 can run on virtually every hypervisor in the market, but that does not mean it is an equal player in these modern deployment scenarios. For example, Windows Server 2003 installations cannot be re-hosted in a Microsoft Azure environment, unless it is a 64-bit image, but the vast majority of Windows Server 2003 installations are 32-bit solutions. So even if customers bring the 32-bit image to the Azure cloud, they cannot continue using that operating system instance. When spinning up new infrastructure-as-a-service (IaaS) instances in Azure, Microsoft provides catalog images only for 64-bit instances of Windows Server 2012 R2. Customers looking to develop a hybrid cloud strategy will find that Windows Server 2003 will not offer the same level of convenience that Windows Server 2012, along with modern companion technologies such as System Center 2012 R2, brings to the table

With the predominance of mobile computing, BYOD, and cloud-based technologies hedging into our day-to-day work environments, we are choosing to see this as an ***exciting opportunity to prepare for the next generation in Information Technology!***

Part 2 - Top 5 Tech Updates That Should Be On Your Radar Right Now



While keeping systems secure and efficient is still on the brain, we thought we'd mention a few other IT updates that are smart to consider at this time:

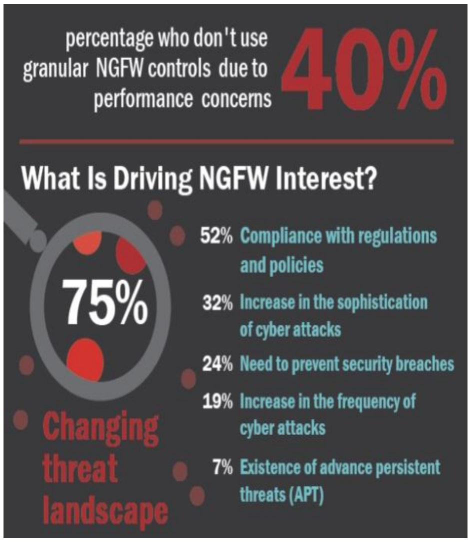
1. **Firewalls** – If you have a firewall that is 3 years old or older, there's a high probability that it does not protect your organization against the latest security threats. Next Generation Unified Threat Management firewalls from vendors such as SonicWALL and Cisco can protect you against the latest threats.

Traditional stateful inspection firewalls have effectively become obsolete because of two significant limitations. ***First, they don't inspect the data payload of network packets.***

Second, while more and more network traffic uses Web protocols--including legitimate business applications, non-business applications and attacks--traditional firewalls don't have the fine-grained intelligence to distinguish one kind of Web traffic from another and enforce business policies, so it's either all or nothing.

The most significant difference between NGFWs and traditional firewalls is that *NGFWs are application-aware; they use a variety of techniques to identify applications, including Web applications*. Thus, instead of allowing all traffic coming in via typical Web ports, a NGFW can distinguish between specific applications (for instance, Hulu vs. Salesforce.com) and then apply policies based on business rules.

NGFWs also use *deep packet inspection techniques* to examine traffic for anomalies and known malware. However, these devices are optimized so that packets need to be examined only once, rather than processed through multiple engines.



2. **On-Premise Email Servers** –The costs to building, maintaining, upgrading, and backing up on-premise email servers such as Microsoft Exchange nearly always outweigh the costs of hosting in the cloud, through hosted email options such as SPOT Hosted Exchange or Office 365. When you factor in the opportunity to spend your IT resources in other impactful ways,

   it's a no-brainer to switch to hosted email in the cloud. And most hosted email providers now provide HIPAA, PCI, and other levels of compliance, plus features like email encryption and archiving.

3. **Tape Backup** – If you're still writing your backups to tape, you likely are putting your business at significant risk, as industry experts estimate that more than 50% of restores from tape backup fail.

   With solutions like SPOT Protect Backup & Disaster Recovery, your backups can be completely automated, and stored not only locally to disk, but also in the Cloud for true disaster recovery.

   In addition to the high failure rate of traditional tape backup solutions, there are other issues with this kind of solution – mostly centered around **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)**.

   RTO is the amount of time that your business can afford to be down in the event of a disaster requiring recovery from backup. With traditional backup solutions, the RTO can be as much as 2 to 3 days, depending on a variety of factors including replacement hardware availability and the amount of data to be restored. ***With SPOT Protect BDR, you can be completely operational from a disaster in as little as 30 minutes.***

RPO is the amount of data that you can afford to lose in the event of a disaster requiring recovery from backup. With traditional backup solutions, the RPO can be up to 24 hours. ***With SPOT Protect BDR, you can set the RPO to as little as 15 minutes.***

4. **Fax Machines** – Sending and receiving documents via fax - especially manual fax machines - is a real drain on productivity.

Receiving faxes electronically – particularly when done through our **Digium Switchvox IP PBX phone system** - means that your users receive orders and other documents via fax quicker, and your staff can be more responsive.

Scanning documents to email can reduce your reliance on fax, and also improve productivity. Implementing electronic document delivery/signing solutions such as **Docusign** can significantly improve workflow and lower your labor costs related to document handling.

5. **Desk Phones** – This trend is just beginning, but the possibility to use your smart phone as part of your organization's phone system is now a legitimate option.

Switchvox Softphone for iPhone brings enterprise mobility to Switchvox by delivering all the power of the award-winning Digium IP Phones to your iPhone. Now you have the ability to:

- *Receive and make calls including extension dialing directly from your iPhone*
- *Advanced call control includes transfer, 3-way conference and record*
- *Control your status and see real-time status of your contacts*
- *Incredibly simple configuration*
- *Connectivity on any WiFi, 4G, or LTE network*

If you'd like to explore some of these technologies more, don't hesitate to reach out to us by phone or email - visit our website at www.fulcrum.pro to find out more about this issue and the solutions we recommend. Check out our blog for security alerts and other important information for business owners and managers – email *ljames@fulcrumgroup.net* if you'd like to be alerted when we post.

We always welcome the opportunity to speak with you – someone's always here and glad to offer a word of advice!

We have several **FREE assessment services** that may align well with your needs, now - call us today at **817.337.0300**.

THE FULCRUM GROUP
One Technology Solution: Yours