NORDIC™

Global Health and Technology Consulting

JUNE 2023

AZURE WINDOWS SERVER

Best practices to secure Azure-hosted Windows Servers

AT A GLANCE AND WHAT THIS MEANS FOR YOU

Many healthcare systems' IT teams are familiar with the requirements of the wide array of applications needed to support patient care. With that comes a mix of versions of Windows Server, both on-premises and in the cloud. Managing all these versions, especially legacy ones, can be challenging and holds the possibility of introducing security vulnerabilities for older systems or unpatched ones. Microsoft Azure and Windows management tools offer turnkey solutions for managing this IT sprawl.

Microsoft recommends four best practices for securing the entirety of the Windows Server environment:

1. Check for patches and create a process for applying them
2. Use Windows Admin Center to manage infrastructure
3. Be aware of support ending for old versions and prepare to migrate
4. Use cloud-native services in Azure for better security and compliance

TECHNICAL DETAILS

1. PATCHING

It is critical to have a sound patching strategy and process, as well as the necessary infrastructure. No matter the industry, each organization needs the highest level of defense against malicious actors. Unpatched or vulnerable systems are easily exploited by bad actors. Some methods for managing patching include SCCM/Configuration Manager, WSUS, Azure automation accounts, or Group Policy.

Some best practices around patching include:

- Update non-production before production
- Allow security to dictate patching policy vs. business use
- Clearly written documentation and change control for patching
- Automate patching with a native or third-party tool

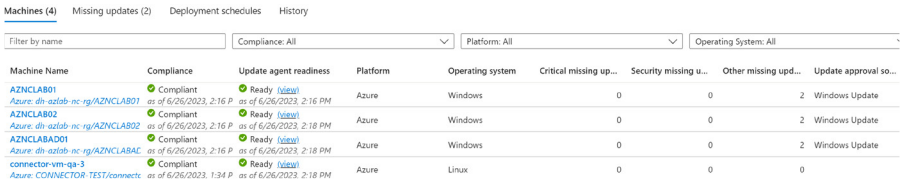

FIG. 1 *Microsoft Azure Automation Account Update Management.*

2. WINDOWS ADMIN CENTER

Windows administrators are likely very familiar with Microsoft Management Console (MMC) and Windows Server Manager. Microsoft has released a new tool called Windows Admin Center that can be used on-premises or natively in the cloud. This product replaces the legacy, per-server consoles with a browser-based tool for managing Windows Servers in your infrastructure. Microsoft has indicated this will be the future of Windows Server management and offers evaluation installations locally or through Azure. Healthcare systems should investigate moving from legacy management software to Windows Admin Center (See Figure 2).

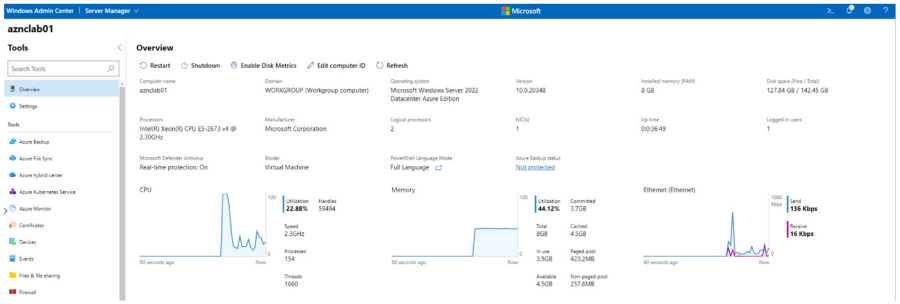

FIG. 2 *Windows Admin Center.*

3. END OF SUPPORT AND MIGRATION

Many healthcare systems still have legacy applications running on old versions of Windows Server, such as 2012 R2 or even 2008. Anything older than 2012 is already out of extended support from Microsoft and cannot receive any further security updates. Windows Server 2012 will be reaching the end of support on Oct. 10, 2023. Microsoft recommends planning to migrate to a newer version of Windows Server if any of these versions are still running.

Microsoft does offer extended security updates for up to three years, but this has an associated cost that could be mitigated by migrating versions of Windows Server, re-architecting for cloud-native infrastructure, or upgrading the application itself to be compatible with newer versions of Windows. Third-party systems and various Microsoft products, such as Azure Migrate, Azure Arc, Windows Admin Center, or PowerShell, can scan the environemtn for older versions of Windows Server.

Windows Server supports in-place upgrades in certain situations. This could potentially reduce cost by not requiring a new VM or server to migrate to an entirely new server as well as reduce downtime by allowing the application to come up faster on the existing machine instead of having to reinstall and restore from backup on a new one.

4. CLOUD INITIATIVES

Microsoft offers a variety of cloud-native services that can enhance security and compliance for IT infrastructure, including on-premises systems. The update management in automation accounts is one example. Azure also offers Secure Score, Microsoft Defender for Cloud, Microsoft Sentinel, and Azure Network Security to guide administrators on compliance and security issues, and even includes recommendations for improving security or compliance (See Figure 3). For healthcare systems, there are HIPAA, HITRUST, and HITECH compliance tools that scan the entire environment for compliance.

On-premises IT infrastructure can access Azure tools by connecting them to Log Analytics, automation accounts, or Azure security tools by installing an agent locally or connecting them to Azure Arc. This allows a single pane of view of the entire organization's infrastructure.

If considering migrating on-premises infrastructure to Azure, Microsoft offers Azure Migrate as a potential solution. Nordic has expertise in Azure migrations for EHRs, reporting infrastructure, or any other enterprise application.

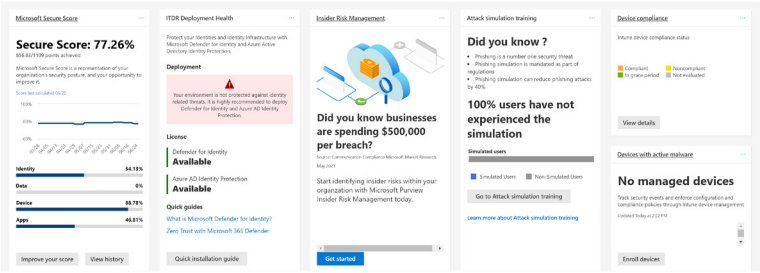

FIG. 3 *Microsoft Security Center.*

NORDIC IN ACTION

Using Azure's compliance tools, a healthcare system can track and improve its compliance with HIPAA/HITRUST. Azure infrastructure and on-premises infrastructure can be scanned and audited against the standards of HIPAA/HITRUST. This secures the environment and strengthens processes and documentation, as well as ensures potential higher success rates of an external audit. This audit can be found in Microsoft Defender for Cloud (See Figure 4). Many health systems successfully leverage this product to improve their Azure security and auditing.

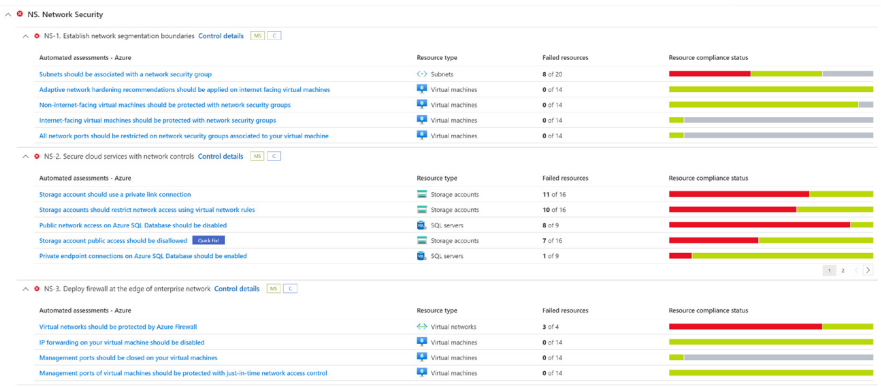

FIG. 4 *Microsoft Defender for Cloud HIPAA/HITRUST Audit.*

JOSHUA WOLEBAN
Solution Architect, Azure

SARAVANAN SONAISAMY
Cloud Solutions Lead, Digital Health

KEVIN ERDAL
Practice Leader, Digital Health

CloudPress@NordicGlobal.com

REFERENCES

1. Widjaja, P. (2023, March 8). *4 best-practices to keep your Windows Server estate secure and optimized.* Microsoft. https://azure.microsoft.com/en-us/blog/4-bestpractices-to-keep-your-windows-server-estate-secure-and-optimized/.
2. Microsoft. (2023, April 10). *Plan for software updates in Configuration Manager.* https://learn.microsoft.com/en-us/mem/configmgr/sum/plan-design/plan-for-software-updates
3. Microsoft. (2023, April 24). *Update management overview.* https://learn.microsoft.com/en-us/azure/automation/update-management/overview.
4. Microsoft. (2022, October 11). *Windows Admin Center*. https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/overview.
5. Microsoft. (2022, March 29). *Manage servers with Windows Admin Center.* https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/use/manage-servers.