# Mitigating Threats and Defending Windows Server 2019: Essential Measures for Enhanced Security

Stuart N. Howard III

Old Dominion University

CYSE280: Windows System Management and Security:

Professor Malik Gladden

30 November 2023

# Mitigating Threats and Defending Windows Server 2019: Essential Measures for Enhanced Security

## Introduction

Protecting sensitive business data and infrastructure from cyber threats is not just important; it is vital. Server environments are particularly vulnerable to cyber-attacks that can cause data loss, unauthorized access, and system disruption, among other devastating outcomes. Enhancing the security measures of Microsoft's server operating system, specifically Windows Server 2019, is imperative to counter these threats. Compared to previous versions, this iteration offers faster performance, improved security, and hybrid cloud integration (Patrizio, 2020). This research provides an overview of the critical steps necessary to beef up the security of Windows Server 2019. Organizations can significantly reduce the risk of security breaches and data compromises by identifying potential threats, implementing best practices, and utilizing the right resources and tools. Do not let cyber threats compromise your server environment. Take proactive steps today to safeguard your valuable business data.

## Overview of the Research

Our analysis will focus on the threat landscape of Windows Server 2019, evaluating common attack vectors and emerging threats. We will identify this operating system's most prevalent vulnerabilities and potential risks. Our research objectives are to examine the most significant cybersecurity threats faced by Windows Server 2019 and explore their potential impact on server security. We will investigate how attackers can exploit Windows Server 2019 and identify ways to mitigate these risks. In addition, we will explore best practices for configuring network security on Windows Server 2019 and investigate how organizations can

implement robust intrusion detection and prevention measures. Furthermore, we will examine ways to harden server configurations and the role of group policy settings in securing Windows Server 2019 environments. Finally, we will discuss the scope and limitations of our research.

## Frameworks

### Windows Server 2019 Security Features

Windows Server 2019 is a modern server operating system that offers top-of-the-line security features to protect businesses from cyber threats. Its advanced security features, such as Windows Defender Advanced Threat Protection, Shielded Virtual Machines, Windows Admin Center, and Azure Active Directory integration, make it the best option for businesses prioritizing security. Upgrading to Windows Server 2019 is a seamless and stress-free process that allows you to keep your configuration settings, Active Directory, and server roles from older installations like Server 2012 (Patrizio, 2020).

As noted by Wayne Rash, Microsoft's multi-layered security approach is one of the highlights of Windows Server 2019. The improvements made to the Windows Defender ATP agent, Shielded VM, virtual network encryption, and System Guard Runtime Monitor provide better protection and patching capabilities, making it easier to secure your systems (Patrizio, 2020). Server 2019 has Storage Migration Service, allowing storage systems migration from Windows Server 2003 and Unix/Linux operating systems—a game-changer for businesses modernizing their systems (Patrizio, 2020). The Trusted Platform Module is an internationally recognized standard for a secure cryptoprocessor, providing a chip or microprocessor that carries out cryptographic operations with various physical security measures. This ensures high tamper resistance, making it impossible for hackers to access your systems (Rise & Engen, 2022). Lastly, Server Message Block is a Windows-based network that allows connected users to share,

create, modify, and delete shared files and folders and access devices such as printers and scanners. This feature provides a seamless network experience, allowing you to work efficiently and effectively (Rise & Engen, 2022). Windows Server 2019 is a modern server operating system that offers top-of-the-line security features to protect businesses from cyber threats. It has a multi-layered security approach that provides better protection capabilities, a storage migration service that allows easy and seamless modernization of systems, a trusted platform module that ensures a high degree of tamper resistance, and a server message block that enables a smooth and efficient network experience.

## Best Practices for Securing Windows Server 2019

Windows Server 2019 is a compelling and versatile operating system that supports numerous workloads and applications. However, its potential can only be fully realized when it is adequately secured and compliant with regulations. We will discuss some of the most effective methods for securing Windows Server 2019 and ensuring it remains protected from internal and external threats. Despite criticisms that the Windows operating system is one of the most complicated to secure, Microsoft has made significant strides in producing a secure operating system that is "secure by default" (Hartley, 2008). However, implementing all the best practices can sometimes lead to unmanageable systems in real-world environments (Hartley, 2008). To mitigate these risks, it is recommended that Windows system hardening be implemented using CIS Controls, a set of best practices that can provide assurance and confidence to IT and security management, engineers, and end-users while facilitating auditing and compliance processes (Sasidharan, 2022). Following the best practices can ensure that your Windows Server 2019 system is secure and compliant with regulations. Implementing these practices will give you peace of mind and help you realize your operating system's full potential.

## Challenges

Ensuring the safety of server environments against cyber threats is of utmost importance in today's digital world. Windows Server 2019 faces a significant challenge in protecting organizations from the severe consequences of cyberattacks, including data loss, service disruption, reputational damage, and legal liability. Cyber threats come in many forms, such as malware, ransomware, improperly configured servers, and outdated patches. To combat these threats, administrators must perform regular risk assessments to identify vulnerabilities and proactively safeguard their valuable data and systems. Ransomware has become a popular tool for hackers and a severe challenge to organizations for several years, causing millions of dollars in damage to companies. According to McDonald et al.'s findings from their analysis, the impact of ransomware on Windows Active Directory Domain Services. It found that the ransomware did not stop the services (2022). Another challenge that has been identified is improperly configured servers. PhD Gerald Auger stated that improperly configured servers also pose a significant cyber-security threat in the industry, leading to vulnerabilities and attacks (2023). For example, the default setting, open ports and services, insecure root accounts, open permissions, and weak encryptions are not adequately implemented, resulting in weak configurations (Ciampa, 2022, p. 12). Finally, managing updates and patches is a challenge, given the human factor involved. However, proactive security patch management is vital as the first line of defense to protect a corporation's computing infrastructure (Hartley, 2008). By taking these proactive measures and strengthening their defenses, organizations can mitigate the risks of cyber threats and safeguard their future.

## Tools

Amidst the constant changes of our digital world lie infinite possibilities, and it is crucial to have robust security measures in place to safeguard critical organizational assets. This is where Windows Server 2019 shines. By leveraging a suite of tools designed to enhance the overall security posture, Windows Server 2019 has proven to be a formidable stronghold against evolving cyber threats. Windows Server boasts one of the most powerful security features available with Windows Defender ATP. With a multi-layer protection system, it provides the ultimate defense against malware and other harmful threats. Not only does it monitor and respond to changes in Windows Server, but it also seamlessly integrates with Azure and Office 365 ATP (Rash, 2019). With advanced intrusion detection and prevention capabilities, it detects and prevents attacks on servers and devices, keeping your data safe and secure (Rash, 2019). Additionally, it offers top-of-the-line endpoint protection and anti-malware capabilities, scanning and removing any malicious software (Rash, 2019). Trust Windows Server with Windows Defender ATP to protect your business from all threats.

Another feature that enhances the security of Windows Server 2019 is Shielded Virtual Machines, which encrypt and isolate virtual machines from unauthorized access. Virtual machines offer the advantage of being encrypted when stored on disk, preventing unauthorized access by malicious parties. Improved security measures have been implemented by deprecating the Active Directory-based attestation for the host guardian service in favor of a more straightforward host key attestation mechanism. Moreover, virtual network encryption can be employed alongside Shielded VMs to safeguard network data during transmission, thwarting interception or tampering attempts (Patrizio, 2020).

Windows Server 2019 also simplifies managing and monitoring security settings and policies with Windows Admin Center, a web-based console that integrates various tools and

functions. Windows Admin Center allows administrators to configure, update, and troubleshoot Windows Server 2019 from any device and location. Windows Admin Center also supports the integration of CIS SecureSuite tools, which automate, manage, monitor, and report on the system hardening process and compliance status (Sasidharan, 2022). CIS SecureSuite tools include CIS-CAT Pro Assessor, CIS-CAT Pro Dashboard, CIS Benchmarks, and CIS Build Kits (Sasidharan, 2022). These tools help administrators apply the best practices and standards for securing Windows Server 2019.

Windows Server 2019 is a powerful operating system with many tools to protect and manage critical organizational assets. Its security features include Windows Defender ATP, Shielded Virtual Machines, Windows Admin Center, and CIS SecureSuite tools, making it a comprehensive and robust security solution that can withstand the evolving cyber threats of the digital world. By using these tools, administrators can ensure the confidentiality, integrity, and availability of their data and systems and comply with the best practices and standards for system hardening and security in today's business era.

## Discussion

The security landscape of Windows Server 2019 is analyzed to reveal a multifaceted approach to counter cyber threats. Microsoft has incorporated advanced features like Windows Defender Advanced Threat Protection, Shielded Virtual Machines, and Windows Admin Center, showcasing its commitment to fortifying server environments. Collectively, these features provide a robust defense mechanism against malware, ransomware, and unauthorized access. The research highlights the common challenges faced by Windows Server 2019, including the persistent threat of ransomware and the risks associated with improperly configured servers. The latter emphasizes the importance of following best practices for system hardening, mainly

through implementing CIS Controls. However, it acknowledges the difficulty of balancing robust security and system manageability in real-world scenarios.

## Recommendations and Future Directions

The challenges faced by Windows Server 2019, including cyber threats, ransomware, and system misconfigurations, necessitate proactive measures. As emphasized in the research, regular risk assessments are imperative to promptly identify vulnerabilities. Acknowledging the severity of ransomware attacks underscores the urgency for robust security protocols. Additionally, administrators must prioritize efficient updates and patch management to shore up the first line of defense. The suite of tools offered by Windows Server 2019, including Windows Defender ATP, Shielded Virtual Machines, and CIS SecureSuite tools, have proven instrumental in reducing vulnerabilities. Organizations should capitalize on these tools, ensuring they are integrated seamlessly into the security posture. Regular training on tool utilization and staying updated on their capabilities is essential for maximizing their effectiveness.

Looking ahead, future research efforts should concentrate on continually monitoring and adapting to emerging cyber threats. The integration of artificial intelligence and machine learning technologies into security frameworks holds the potential to enhance proactive threat detection and response capabilities. Collaboration between industry professionals, researchers, and Microsoft remains vital to maintaining the resilience of security measures. Future endeavors could also focus on developing streamlined and automated approaches for implementing security best practices and exploring the implications of emerging technologies like edge computing and the Internet of Things (IoT) on Windows Server 2019 security.

## Conclusion

Securing Windows Server 2019 is an ongoing and dynamic process that requires a multifaceted approach. This research has thoroughly examined the current threat landscape, security features, best practices, challenges, and tools available for enhancing the security of Windows Server 2019. Adopting advanced security features, best practices, and tools such as Windows Defender ATP, Shielded Virtual Machines, Windows Admin Center, and CIS SecureSuite has proven effective in mitigating cyber threats and reducing vulnerabilities.

Despite the challenges posed by evolving cyber threats, the research highlights the robustness of Windows Server 2019 as a secure and advanced server operating system. The tools discussed are crucial in fortifying the server environment and improving incident response outcomes. As organizations continue to face cyber threats, the recommendations for future research and ongoing security measures underscore the importance of adaptability and collaboration in maintaining the resilience of Windows Server 2019 against emerging challenges. By staying vigilant, proactive, and informed, organizations can ensure their server environments' long-term security and reliability in the face of an ever-changing digital landscape.

## References

Auger, Gerald, PhD. Simply Cyber. (2023/11/15) November 15's Top Cyber News NOW! https://www.youtube.com/watch?v=h_1ONH26JAE

Azeez, N. A., Odufuwa, O. E., Misra, S., Oluranti, J., & Damaševičius, R. (2021). Windows PE Malware Detection Using Ensemble Learning. *Informatics*, *8*(1), Article 1. https://doi.org/10.3390/informatics8010010

Ciampa, M. (2020). CompTIA Security+, Guide to Network Security Fundamentals, Information Security *Sengate*

Hartley, D. (2008). Defending Windows servers. *Network Security*, *2008*(10), 4–8. https://doi.org/10.1016/S1353-4858(08)70117-X

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: Analysing the Impact on Windows Active Directory Domain Services. *Sensors*, *22*(3), Article 3. https://doi.org/10.3390/s22030953

Patrizio, A. (2020). What to know before upgrading to Windows Server 2019: Even though it's only been one refresh cycle, the changes to the latest version of Windows Server are considerable. Microsoft makes the process of upgrading from Windows Server 2016 easy. *Network World (Online)*. https://www.proquest.com/docview/2333694736/abstract/5BBA7E2CAA7D49C4PQ/1

Rash, W. (2019, July 24). *Microsoft Seriously Beefs Up Security in Windows Server 2019*. PCMAG. https://www.pcmag.com/news/microsoft-seriously-beefs-up-security-in-windows-server-2019

Rise, H. R., & Engen, S. (2022). *Windows Server 2019/2022 and Azure Cloud security systems—A general recommendation* [Bachelor thesis, NTNU]. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3002835

Sasidharan, R. (2022). A Case Study to Implement Windows System Hardening using CIS Controls. *International Journal of Computer Trends and Technology*, *70*, 1–7. https://doi.org/10.14445/22312803/IJCTT-V70I7P101