

Troy Bannister

CYSE280

Mike Gladden

31 JUL 2025

CYSE280 Research Paper:

Windows System Management Policies and Procedures

Introduction

Organizations rely on complex operating system (OS) management strategies to defend against an expanding landscape of cyber threats. With Windows Server 2019 and related client operating systems serving as the backbone for many organizations, having an effective system management strategy is important to making sure the confidentiality, integrity, and availability of data and services. This paper explores how structured policy enforcement, aligned with national cybersecurity frameworks like the NIST Cybersecurity Framework (CSF 2.0) can strengthen security outcomes in Windows-based environments. By looking at key tools like Group Policy, Windows Defender, and BitLocker, while also comparing them with alternative operating systems (OS) versions, this research will show the effective practices and the importance of process progress. Some case studies, like the WannaCry ransomware incident, will also show how mismanagement of known threats in Windows systems can create system-wide vulnerabilities within organizations.

Research and Required Information Overview

Operating system security crosses a lot of disciplines between access controls, update policies, software integrity and user authentication. According to Raza and Ahmed (2022), operating systems are responsible for functionality and upholding internal protection boundaries against malware. Windows platforms provide built-in mechanisms such as User Account Control (UAC), BitLocker and Windows Defender, which are not really utilized or configured in the most optimal way. Part of this research was to focus on those built-in defenses along with the structured policies and administrative oversight.

Policy enforcement is best understood through a standard framework that can be consistently applied. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF 2.0) provides such a structure, with its five functions: Identify, Protect, Detect, Respond, and Recover. It is a necessary tool for evaluating the Windows policy tools.

Also, cross-platform comparisons reveal that while Linux and macOS benefit from being quite modular in their configurations and have a leaning towards default ‘deny’ controls, Windows remains dominant in organizational settings holding 71% of the desktop OS market (*Desktop Operating System Market Share Worldwide | Statcounter Global Stats*, n.d.) and bears a larger burden of defensive enforcement which can be seen by how many systems were affected by the WannaCry ransomware campaign. (CERT-EU, 2022). It will be important to present the research in a practical way, connecting technical capabilities to policy standards.

Frameworks, Process, and Methodology

To look at how policy enforcement within Windows environments works, the NIST CSF 2.0 connections need to be integrated with administrative tools like Group Policy Objects, Active Directory (AD), and Microsoft Defender. Baker (2023) specifically mentions that the mismanagement of policy tools can create an opening for attackers, particularly when Group Policy is misused or misconfigured. When correlating policy-based tools to policy-based recommendations, using the frameworks developed by industry and community experts allows OSs to align with compliance standards and best practices. These recommendations are structured and outlined in the updated CSF 2.0 (National Institute of Standards and Technology, 2024).

NIST CSF 2.0:

- **Identify:** Asset Inventory, privilege delegation, user roles. (Done with AD and Group Policies)
- **Protect:** Password enforcement policies, BitLocker, firewall configuration
- **Detect:** Real-time protection alerts from Microsoft Defender and Event Viewer
- **Respond:** Incident response scripts, centralized Group Policy audits.
- **Recover:** Backup policies and volume shadow copies.

The WannaCry ransomware incident of 2017 is a key case study for policy failure.

“WannaCry targets SMB vulnerabilities in unpatched versions of Windows OS, even though patches were made available months earlier due to the EternalBlue incident earlier in the year.” (CERT-EU, 2017). This incident shows the need for automated patch deployment or centralized update enforcement as a policy default. Chen & Bridges (2017) even demonstrate how ransomware like WannaCry leverages OS-level functions like registry access to execute and deliver. The implication is that controls at the OS level could be an important way to contain threats if the controls were multi-layered and automated.

The policies themselves were assessed across domains like:

- Patch management frequency
- User privilege enforcement (local vs domain)
- User account lockout policies
- Logs and Audits configurations

Windows security hardening and applying the best current recommendations were found in Dunkerley & Tumbarello’s (2022) Mastering Windows Security and Hardening.

Tools, Resources and Results

When looking at the Windows tools and their capabilities when matched to the CSF 2.0 subcategories, as Table 1 shows a qualitative connection. The ‘Effectiveness Rating’ is measured at how well each tool aligns with the recommendations gathered from Dunkerley and Tumbarello (2022); Microsoft security recommendations, and the National Institute of Standards and Technology (2024); Effectiveness ratings were chosen with:

- **High:** Direct and consistent with the related subcategory; built-in automation or enforcement.
- **Moderate:** Strong baseline coverage but may require additional configurations or needs to be paired with external tools.
- **Low (if used):** Little to no relevance to the subfunction or relies on manual input, third party tools with no visibility.

Table 1

Common Windows Tools and Specific NIST CSF 2.0 Subcategories				
Windows Tool/ Feature	NIST CSF Function(s)	Subcatergries	Effectiveness Rating	Reasoning
Group Policy	Govern (GV) Protect (PR)	• GV.AC-01 • GV.PO-01 • PR.AC-01 • PR.AC-05	High	Used to enforce passwords, access control and account lockouts
Windows Defender	Protect (PR) Detect (DE)	• PR.DS-01 • PR.DS-04 • DE.MN.02	Moderate– High	Signature based and behavioral malware detection; integrated with Microsoft Threat intelligence.
Event Viewer	Detect (DE)	• DE.MN-01 • DE.MN-06 • DE.MN-09	Moderate	Logs are passive unless monitored; detection relies on active oversight or 3rd-party SIEM (Security Information Event Management)
BitLocker	Protect (PR)	• PR.DS-01 • PR.PT-04	High	Encrypts drives; meets data protection criteria especially for laptops and removable drives
Windows Firewall	Protect (PR) Detect (DE)	• DE.MN-06 • DE.MN-09 • DR.PT-05	Moderate– High	Basic inbound/outbound traffic filtering. A little outdated to Next Gen Firewall tools.

Note: Ratings are qualitative based on feature automation and integration with CSF 2.0 (adapted from Dunkerley & Tumbarello, 2022; Microsoft, 2023).

Result: The effectiveness connection to the CSF 2.0 reinforces the strengths of native Windows tools and when used in alignment with a security framework. Group Policy’s integration with account-level controls, Defender’s baseline protections and BitLocker’s role in data-at-rest integrity all show compliance with the core subcategories of the CSF 2.0. But the table also shows where some improvements can be made, specifically where it relies on manual configuration or a third-party addition that weakens the overall security positioning. Looking at

the tools from this view shows the importance of aligning between policy design and tool functioning and deployment, instead of just assuming having the tool available alone is good enough for compliance or protection.

While Windows Server 2019's built-in security tooling gives users a somewhat central, policy driven place to work from, many organizations operate in mixed environments that include Linux or macOS systems. Which raises a question about how each OS enforces its security standards by default and where gaps may exist. Raza and Ahmed (2022) noted that while Windows gives you integrated policy enforcement that is streamlined, Linux relies heavily on manual configurations. MacOS's security model is tightly controlled but lacks policy administration that is centralized for organizational level management tools. Table 2 shows how each platform satisfies key CSF 2.0 Subcategories. The primary criteria include if the security tool is built-in or third party, centrally managed or user managed and automated or manual. The criteria were then rated in a High, Medium and Low along the operating systems native tools and how much of the criteria is met.

- **High:** Built-in, centrally managed and automated
- **Medium:** Partial coverage with some user configuration or third-party help
- **Low:** Mostly manual or fragmented tools that need user configuration.

Table 2

Security Function (CSF 2.0-aligned)	Windows	Linux	macOS	User Dependency
Identity and Access Management (PR.AC)	Group Policy (AD), Credential Guard	Pluggable Authenticate Module, System Security Service Daemon	Mobile Device Management, Keychain	• Windows: Low (centralized) • Linux: High (manual/conf-driven) • macOS: Low (tied to Apple ecosystem)
Application Control (PR.PS)	AppLocker, Windows Defender	AppArmor, SELinux (if enabled)	Gatekeeper	• Windows: Low • Linux: High • macOS: Medium
Data Protection (PR.DS)	BitLocker, Encrypted File System	Linux Unified Key Setup, , dm-crypt	FileVault	• Windows: Low • Linux: Medium • macOS: High
Threat Detection & Response (DE.CM, RS.AN)	Windows Defender, Event Forwarding	AuditD, Fail2Ban	XProtect, MRT	• Windows: Moderate (built-in, policy-managed) • Linux: High (manual or community-driven) • macOS: Low (opaque, Apple-managed)

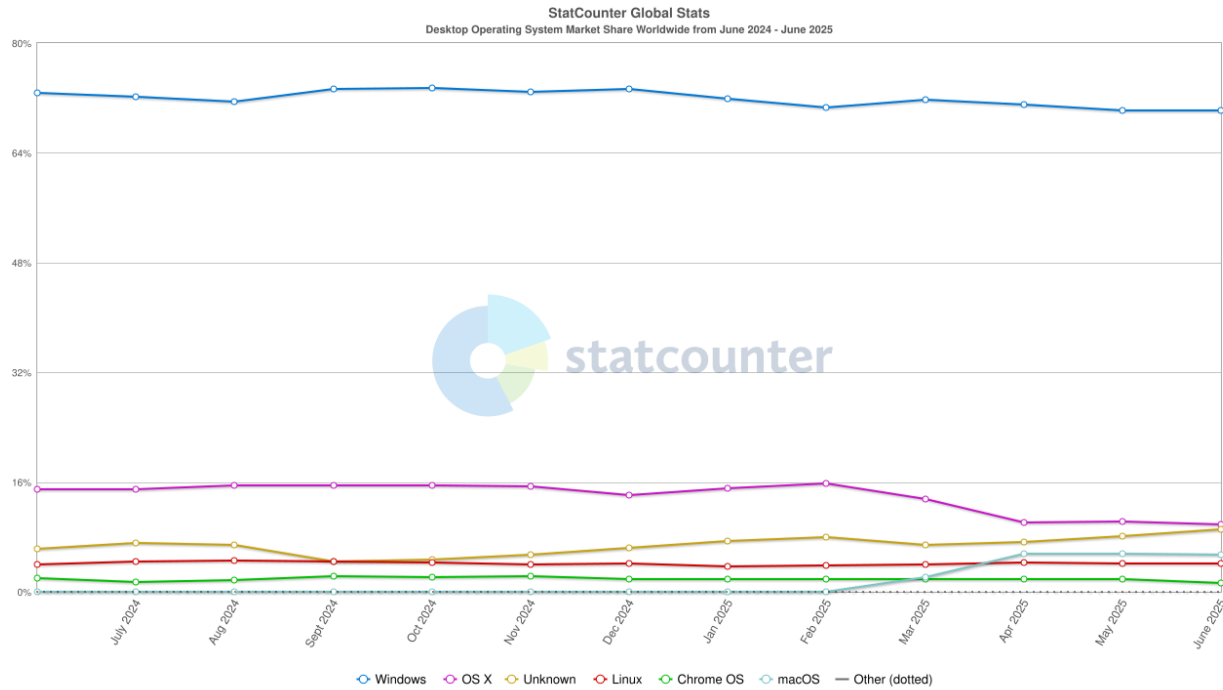
Note: Ratings are qualitative based on CSF 2.0 subcategories. Ratings were developed by the author using insights from Raza & Ahmed (2022), Paigude (2024), Microsoft (2023), and Mitra (2024).

Results: The table shows that Windows has significant centralized and automated enforcement across the CSF 2.0 Subcategories due to the built in tools like Group Policy, Windows Defender and BitLocker that support being used among large organizations with minimum user involvement. MacOS does well in areas like data protection and integrity but relies on integrations with MDM platforms. Linux, while flexible and powerful within experts, frequently depends on command-line and third-party packages making its security more fragmented.

This reinforces the broader point: Windows being the main OS among organizational environments is not just a reference to its market share, but also to how the tools and policy management integration have progressed. This advantage can also be misunderstood when user misconfiguration or misjudgment of coverage creates security gaps that appear to reflect poorly on the platform itself.

Conclusion

Figure 3



Note: Adapted from StatCounter Global Stats (2025). Retrieved from <https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202406-202506>

How effective and configurations will remain important to platform security; context is just as important. Figure 3 (*Desktop Operating System Market Share Worldwide | Statcounter Global Stats*, n.d.) illustrates that Windows has maintained a dominant hold (around 70%) in the global desktop OS market. The major gap between Windows and other Oss supports the core argument of this paper: because Windows is much of the organizational and personal desktop environments, it carries a disproportionate share of the cybersecurity burden. Throughout this research, the relationship between Windows tools and policy-based frameworks like the NIST

CSF 2.0 was not looked at by just having tools available, but by their alignment with policy enforcement, automation and integration depth. While Microsoft's tools like Group Policy, Defender and BitLocker show they are great tools for compliance and protection, how effective they are is based on whether administrators align them with the defined framework that is recommended. Comparing with macOS and Linux showed that, yes, they often benefit from a smaller vulnerability surface and isolated design, their tools are either very fragmented, user-dependent or designed for different threats altogether. Windows prioritizes the central policy management and wide-scale enforcement which are strengths that are overlooked when assessing security in isolation.

In the end, no single platform can claim to be perfect, but by evaluating tools in the contexts that can be outlined by frameworks created by industry leaders and recommendations, like NIST's Cybersecurity Framework 2.0; organizations can make informed decisions about configuration and defense. Windows native tools do not mean a security weakness, but an efficient baseline capable of reducing misconfiguration risks, enforcing policy and allowing users to scale protection when needed.

References:

- Baker, D. G. (2023, November 30). *Group Policy as an Attack Pathway*. Practical 365.
<https://practical365.com/group-policy-as-an-attack-pathway/>
- CERT-EU. (2017). *WannaCry Ransomware campaign exploiting SMB vulnerability*.
- Chen, Q., & Bridges, R. A. (2017). Automated Behavioral Analysis of Malware: A case study of WannaCry ransomware. *2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 454–460. <https://doi.org/10.1109/icmla.2017.0-119>
- Desktop Operating System Market Share Worldwide | Statcounter Global Stats*. (n.d.). StatCounter Global Stats. <https://gs.statcounter.com/os-market-share/desktop/worldwide>
- Dunkerley, M., & Tumbarello, M. (2022). *Mastering Windows security and hardening: Secure and protect your Windows environment from cyber threats using zero-trust security principles*. Packt Publishing Ltd.
- Mitra, R. (2025, June 18). *Stay compliant and protect sensitive data with Zero Trust security*. Microsoft Security Blog. <https://www.microsoft.com/en-us/security/blog/2023/04/24/stay-compliant-and-protect-sensitive-data-with-zero-trust-security/>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF 2.0)* [Report]. <https://doi.org/10.6028/NIST.CSWP.29>
- Paigude, S. D., Pangarkar, S. C., Dari, S. S., Patil, M., NIT Graduate School of Management, Shailaja Nilesh Uke, & Gujar, S. N. (2024). A Review of Cybersecurity policies in the public sector: Challenges and solutions. *Computer Fraud and Security*, 2024(7).
- Raza, A., & Ahmed, W. (2022). Threat and Vulnerability management life cycle in operating systems. A systematic review [Systematic Review]. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, 15010–15011. <https://www.jmest.org>