

Windows Hardening

CONFIGURING YOUR WINDOWS PC TO BE MORE SECURE

WINDOWS HARDENING IS AN A-LA-CARTE SELECTION OF SECURITY CONFIGURATIONS

Turn off unnecessary services that create exposure to cybersecurity exploits

PURPOSE / INSTRUCTIONS

Safe Computing is seeking to facilitate a series of free courses covering a wide array of technologies used in the Information Technology field.

Hardening a Windows PC means reducing its attack surface, strengthening built-in defenses, and enforcing strict controls that prevent malware, credential theft, and unauthorized access. The goal is to transform a default Windows installation—often permissive and feature-rich—into a tightly secured workstation aligned with modern threat models like ransomware, script-based attacks, and credential compromise.

Core Security Priorities

Windows endpoints are frequent targets for malicious websites, phishing emails, and removable media. Hardening directly reduces the likelihood that these vectors succeed. According to guidance from national cybersecurity agencies, workstation hardening is essential because attackers routinely exploit unchanged defaults and weak configurations.

Operating System & Patch Hygiene

Keeping Windows fully updated is one of the most impactful defenses. A reliable patch cadence—zero-day deferral for quality updates and a structured reboot window—prevents exploitation of known vulnerabilities, which cause more incidents than any single misconfiguration.

Key actions:

- Enable Windows Update for Business or equivalent centralized management.
- Maintain a weekly reboot schedule to ensure patches apply.
- Use the latest Windows 10/11 builds to benefit from improved security defaults (e.g., VBS, HVCI, TPM 2.0).

Credential Protection

Credential theft remains a top threat. Hardening Windows authentication reduces the risk of lateral movement and privilege escalation.

Critical measures:

- Enforce long, high-entropy passwords (e.g., 16-character minimum).
- Disable legacy authentication such as NTLMv1.
- Enable **Credential Guard** when hardware supports it.

SAFE COMPUTING | Cybersecurity for Small Business

safe-computing.net • info@safe-computing.net • 512.228.0411 • 213 Bluff St, Buda, TX 78610

- Use **Windows Hello** for secure, phishing-resistant sign-in.
- Protect LSASS from dumping attempts using built-in exploit protection.

Application & Script Control

Most commodity malware relies on executing from user-writable directories or abusing scripting engines.

High-impact controls:

- Use **Windows Defender Application Control (WDAC)** or **AppLocker** to block execution from %TEMP%, %APPDATA%, and Downloads. This single change stops a large portion of malware.
- Restrict PowerShell to **Constrained Language Mode** for non-admin users.
- Disable Windows Script Host unless required.
- Block Office macros originating from the internet.
- Apply application hardening policies such as Attack Surface Reduction rules.

Network Hardening

Network misconfigurations are common entry points for attackers.

Key steps:

- Configure **Windows Defender Firewall** across Domain, Private, and Public profiles—each must be independently hardened.
- Block inbound traffic by default; restrict outbound traffic to approved applications.
- Disable SMBv1 and enforce SMB signing.
- Turn off LLMNR and NetBIOS over TCP/IP to prevent spoofing attacks.
- Use DNS-layer filtering to block malicious domains before connections occur.

Privilege & Account Controls

Limiting privileges reduces the blast radius of any compromise.

Essential controls:

- Remove or tightly restrict local administrator accounts.
- Enforce role-based access and least-privilege principles.
- Require MFA for privileged operations.
- Lock down Remote Desktop Services or disable them entirely unless needed.

SAFE COMPUTING | Cybersecurity for Small Business

safe-computing.net • info@safe-computing.net • 512.228.0411 • 213 Bluff St, Buda, TX 78610

- Disable unnecessary services such as Remote Registry, WinRM (unless managed), and Xbox services on enterprise endpoints.

Ransomware-Specific Defenses

Ransomware remains one of the most destructive threats.

Recommended layers:

- Enable **Controlled Folder Access** to block unauthorized encryption attempts.
- Maintain shadow copies with at least 14-day retention.
- Deploy honeypot files to detect early ransomware behavior.
- Allow-list only trusted processes for access to critical directories.

Logging, Monitoring & Response

Hardening is incomplete without visibility.

Key logging practices:

- Forward Windows Security logs, Sysmon events, and PowerShell logs to a central collector.
- Monitor for high-value indicators such as LSASS access attempts, suspicious Office child processes, and unauthorized scheduled task creation.
- Use centralized audit event logging to detect anomalies.

Automation & Configuration Management

Hardening one PC is easy; maintaining a fleet requires automation.

Best approaches:

- Use Group Policy, Intune, or similar tools to enforce baselines.
- Apply CIS-aligned profiles and track configuration drift over time.
- Test changes in pilot groups to avoid breaking line-of-business applications.

Conclusion

Hardening a Windows PC is a structured process: reduce unnecessary functionality, enforce strict authentication, control application execution, secure the network stack, and maintain strong monitoring. Modern Windows versions include powerful security features, but they must be configured intentionally. With a disciplined baseline and continuous patching, a Windows workstation becomes significantly more resilient against ransomware, credential theft, and targeted attacks.