CORVASEC

Windows 11 Hardening Checklist

A practical Windows hardening checklist covering identity, device protection, Defender, firewall, updates, services, logging, networking, backups, and verification.

DOCUMENT CENTER

Compiled September 2026

Hardening is environment-specific. Start from a tested Microsoft security baseline, stage changes, validate application/device compatibility, document exceptions, and maintain a recovery path. Do not blindly apply every control to every system.

Use this guide as a practical reference. Verify commands, targets, permissions, paths, versions, and organizational policy before making changes. Examples with placeholders must be adapted to the environment.

Contents

#	Section	Entries
1	Identity and account security	8
2	Device, firmware, disk, and boot protection	8
3	Microsoft Defender, firewall, and attack-surface controls	10
4	Updates, applications, and services	10
5	Logging, auditing, and monitoring	8
6	Network, sharing, and remote access	8
7	Browser, data, backups, and user protections	8
8	Verification commands	18

Total reference entries: 78

1. Identity and account security

Check	Recommendation	Verification
1	Use standard user accounts for daily work and separate administrative accounts where operationally appropriate.	Review Local Users/Groups, Entra ID/AD roles, and privileged workflows.
2	Require strong authentication and MFA for remote/cloud/admin access where supported.	Review identity provider and privileged-access policy.
3	Disable or remove unused local accounts; rename/secure built-in accounts according to policy.	Get-LocalUser / net user.
4	Minimize local Administrators membership.	Get-LocalGroupMember Administrators.
5	Use Windows Hello for Business or other phishing-resistant authentication where supported.	Review sign-in options and organizational policy.
6	Set lockout/password policy using organizational standards and identity architecture.	net accounts / domain/MDM/GPO policy.
7	Protect recovery and break-glass accounts with documented control and monitoring.	Periodic access review.
8	Review saved credentials and privileged service accounts.	Credential Manager, services, scheduled tasks, managed accounts.

2. Device, firmware, disk, and boot protection

Check	Recommendation	Verification
1	Keep UEFI/firmware current through trusted OEM channels.	OEM update tooling and inventory.
2	Enable Secure Boot on compatible systems unless a documented requirement prevents it.	Confirm-SecureBootUEFI / System Information.
3	Ensure TPM is present and healthy on supported hardware.	Get-Tpm / tpm.msc.
4	Enable BitLocker/device encryption for supported system and data volumes.	Get-BitLockerVolume / manage-bde -status.
5	Back up BitLocker recovery information using approved enterprise process.	Recovery key escrow validation.
6	Protect BIOS/UEFI configuration and external boot policy according to device use case.	Firmware settings review.
7	Disable unused boot devices/interfaces only when operational requirements allow.	Firmware/device inventory.
8	Use modern hardware protections such as VBS/HVCI when compatible with workload and baseline.	Windows Security / Device Guard status.

3. Microsoft Defender, firewall, and attack-surface controls

Check	Recommendation	Verification
1	Keep Microsoft Defender Antivirus or approved EDR/AV active and healthy.	Get-MpComputerStatus.
2	Keep security intelligence current.	Update-MpSignature / management console.
3	Enable potentially unwanted application protection where compatible.	Get-MpPreference.
4	Minimize antivirus exclusions and document every required exclusion.	Get-MpPreference exclusions.
5	Keep Microsoft Defender Firewall enabled on Domain, Private, and Public profiles unless centrally replaced.	Get-NetFirewallProfile.
6	Remove obsolete firewall rules and avoid broad Any/Any inbound rules.	Get-NetFirewallRule / port/address filters.
7	Apply Attack Surface Reduction rules based on Microsoft baseline and staged compatibility testing.	Policy/Defender configuration.
8	Enable SmartScreen/reputation protections appropriate to managed browser/application environment.	Windows Security / policy.
9	Use controlled folder access where supported and compatible for ransomware risk reduction.	Defender settings.
10	Block or restrict legacy/insecure protocols that are not required.	SMB/TLS/authentication configuration and service inventory.

4. Updates, applications, and services

Check	Recommendation	Verification
1	Apply Windows quality/security updates on a managed cadence with testing appropriate to the environment.	Windows Update history / management platform.
2	Update third-party applications and drivers through trusted sources.	Software inventory and vendor update status.
3	Remove unsupported or unnecessary software.	Installed apps / package inventory.
4	Disable or uninstall optional Windows features that are not required after compatibility review.	Get-WindowsOptionalFeature -Online.
5	Review automatically starting services and scheduled tasks for business need.	Get-Service, Get-ScheduledTask.
6	Avoid exposing management services such as RDP/WinRM directly to untrusted networks.	Firewall, VPN, zero-trust access architecture.
7	Require Network Level Authentication for RDP where RDP is used and supported.	Remote Desktop policy.
8	Restrict PowerShell remoting to authorized administrators and management networks.	WinRM listeners, firewall, endpoint configuration.
9	Use application control/allowlisting for higher-assurance systems where operationally feasible.	App Control for Business/WDAC policy status.
10	Use Microsoft security baselines rather than an untested one-off baseline as the starting point for managed fleets.	GPO/Intune/security baseline comparison.

5. Logging, auditing, and monitoring

Check	Recommendation	Verification
1	Configure audit policy to capture authentication, privilege, process, policy, account, and object events needed by your environment.	auditpol /get /category:* / central policy.
2	Enable process creation command-line logging where justified and privacy policy permits.	Audit Process Creation / policy.
3	Centralize important Security, System, Defender, PowerShell, and application logs.	SIEM/collector coverage.
4	Protect log retention from routine user modification and size logs for operational needs.	wevtutil / Event Viewer policy.
5	Monitor high-value events such as 1102, 4625, 4688, 4697/7045, 4720, 4728/4732, 4740, 4768/4769/4771.	SIEM detections and event collection.
6	Enable enhanced PowerShell logging according to risk, privacy, and storage requirements.	Script Block/Module/Transcription policy where appropriate.
7	Monitor Defender detections and security configuration changes.	Defender portal/SIEM/local logs.
8	Maintain time synchronization.	w32tm /query /status / domain/NTP architecture.

6. Network, sharing, and remote access

Check	Recommendation	Verification
1	Use the correct Windows network profile and keep Public networks restrictive.	Get-NetConnectionProfile.
2	Disable unused network adapters and protocols only after validation.	Get-NetAdapter, adapter properties.
3	Prefer SMB 3.x and remove SMBv1 where not explicitly required.	Get-WindowsOptionalFeature / Get-SmbServerConfiguration.
4	Review administrative shares and SMB share permissions.	Get-SmbShare, Get-SmbShareAccess.
5	Restrict anonymous/guest access according to baseline.	Local security/GPO settings.
6	Use DNS and proxy settings managed by policy where appropriate.	Get-DnsClientServerAddress / WinHTTP proxy.
7	Use VPN or approved zero-trust access for remote administration.	Remote access architecture review.
8	Segment sensitive systems and restrict inbound management traffic.	Firewall/network policy verification.

7. Browser, data, backups, and user protections

Check	Recommendation	Verification
1	Keep supported browsers updated and apply enterprise browser security policy.	Browser version and policy page.
2	Use password manager/credential protections approved by the organization.	Identity/security policy.
3	Minimize local storage of secrets, tokens, and exported credentials.	Credential/file review.
4	Maintain tested backups that are protected from routine endpoint compromise.	Restore test and backup-console review.
5	Use OneDrive Known Folder Move or equivalent managed backup where appropriate.	Management platform status.
6	Protect sensitive data with access controls and encryption in transit/at rest.	NTFS/share permissions, BitLocker, application controls.
7	Enable screen lock and appropriate inactivity timeout.	Policy verification.
8	Train users to report suspicious prompts, MFA fatigue, phishing, and unexpected downloads.	Awareness program and reporting channel.

8. Verification commands

Command	Purpose / Notes
`Get-ComputerInfo`	Collect system/OS information.
`Get-MpComputerStatus`	Check Defender health.
`Get-MpPreference`	Review Defender preferences and exclusions.
`Get-NetFirewallProfile`	Review firewall profile state.
`Get-NetFirewallRule -Enabled True`	Review enabled firewall rules.
`Get-BitLockerVolume`	Review BitLocker protection.
`Get-Tpm`	Review TPM status.
`Confirm-SecureBootUEFI`	Review Secure Boot where supported.
`Get-LocalGroupMember Administrators`	Review local administrators.
`Get-WindowsOptionalFeature -Online`	Review optional features.
`Get-Service | Where-Object StartType -eq Automatic`	Review automatic services.
`Get-ScheduledTask`	Review scheduled tasks.
`auditpol /get /category:*`	Review audit policy.
`Get-WinEvent -LogName Security -MaxEvents 50`	Confirm Security event collection.
`Get-SmbServerConfiguration`	Review SMB server configuration.
`Get-NetConnectionProfile`	Review network profile categories.
`w32tm /query /status`	Review time synchronization.
`gpresult /h C:\Temp\gp.html`	Export applied Group Policy results.

Authoritative references

Use vendor and standards documentation for exact syntax, current behavior, version-specific details, licensing, and policy requirements.

Microsoft Security Baselines

https://learn.microsoft.com/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines

Microsoft BitLocker overview

https://learn.microsoft.com/windows/security/operating-system-security/data-protection/bitlocker/

Windows security documentation

https://learn.microsoft.com/windows/security/