THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM

SECURE WINDOWS SERVERS

With five easy strategies

How to secure Windows Servers

An overview of recommended configurations for hardening your Windows Servers.

Business environments extend beyond on-premises networks, encompassing cloud apps, SaaS & PaaS solutions, remote workers, and off-site infrastructure. Security strategies must address both internal and external resources, and the Zero Trust model is the most effective approach. With infrastructure being a prime target, here's how to apply Zero Trust strategies to protect it from rising threats.

1. System security

System security begins at the hardware level and spans into tightening server configuration based on the role of the server. We recommend that you implement security and auditing tools to block, remediate, and alert you of any security incidents that do occur. A few strategies include:

Physical security

Standard security practices include badge access controls to your server rooms, surveillance systems, and locked cabinets or server racks.

BitLocker preboot authentication

Pair BitLocker Drive Encryption with a PIN and TPM, or use Network Unlock, to add an additional factor of authentication for accessing an encrypted volume.

Configuration and patch management

Microsoft recommends patching infrastructure separately from user machines. Exclude these servers from configuration management software's patch schedule, to allow for tighter management of software installations.

Restrict web browsing

Restrict or disable web browsing on Windows Servers. Browsing the internet leaves infrastructure susceptible to drive by downloads or malware infected utilities.

- Restricting general internet access to and from on-premises infrastructure is good practice and may be required by certain regulatory needs.

Use an allowlisting & EDR tool

Take a proactive approach to security with an allowlisting tool to significantly reduce the attack surface of your server infrastructure. Alongside a strong application allowlist, an EDR tool will help with a reactive approach if a compromise does occur.

Ensure registry integrity

Use a trusted registry check tool or a vulnerability scanner. This can alert you to any misconfigured security settings, such as having advanced LSA protection turned off.

PowerShell execution policy

Ensure PowerShell is disabled on machines that do not need it or is enabled and then promptly disabled on a per use basis. Malicious actors often use PowerShell to perform fileless attacks and initiate remote connections to move laterally through your network.

ThreatLocker® tip: ThreatLocker Application Allowlisting can prevent PowerShell from running as well as restrict it from interacting with specific applications and network locations.

- **Remove unnecessary roles or features**

Design your servers to run only what's needed. Roles, and features that are not required extend the attack surface of the server. For example, the telnet client feature is likely not required for infrastructure servers.

- Control V-254264 specifically mentions minimizing the number of installed roles, features, and services.
- An example of exploitation of services is the use of SMBv1 by the WannaCry ransomware attack.

Why this matters:

A multi-layered approach to system security, focused on least privileges and breach assumption, minimizes attack surfaces and helps manage server risks.

ThreatLocker® tip: ThreatLocker Ringfencing™ policies to restrict applications from accessing files, the internet, other applications and performing registry activities. For example, Putty cannot access PowerShell. This configuration mitigates malicious activity.

For information on securing domain controllers, check out this article from Microsoft.

2. Ports and services

Threat actors use open ports and unused services to gain access to a system and attempt to move laterally through your environment. Disable services or block ports that are not explicitly needed for the functionality of a server to harden your infrastructure. To enhance port and service security, consider the following:

- **Ports and services commonly exploited:**
  - Remote Desktop Protocol (3389)
    - **Config Tip:** Aside from blocking port 3389 or disabling RDP via system properties, services Remote Access Connection Manager, Remote Desktop Configuration, Remote Desktop Services can be disabled to remove remote access capabilities.
  - SMBv1 or CIFS (445) – If needed, use SMBv3
    - **Config Tip:** To disable SMBv1 from PowerShell: Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
    - **Config Tip:** To enable SMBv2/v3 from PowerShell: Set-SmbServerConfiguration -EnableSMB2Protocol $true
  - FTP (20-21) – Use SFTP (22) if needed
  - Telnet (23)
  - LDAP (389) - Consider using 636 to encrypt communication
  - NetBIOS (137-139)
  - VNC (5900-5901)
  - Database ports (1521,3306, 5432,27017)
  - Link-Local Multicast Name resolution (LLMNR 5355)
  - DCOM & RPC (port 135 and dynamic ports)

Why this matters:

By closing ports and disabling services commonly exploited, you further reduce the risks of a security breach.

TIP

ThreatLocker® tip: Use ThreatLocker Network Control to restrict traffic to specific ports, allowing servers, such as an SQL server, to communicate only over its required ports.

Microsoft offers a list of default service settings for Windows server OS in this article.

3. Account and directory security

Identity serves as the primary security perimeter, acting as the digital front door. This makes privileged accounts a primary target for threat actors. User account credentials theft also leaves data exposed. As such, we recommend administrators adopt best practices related to account and directory security, including:

- **Enforce a strong directory password policy**

This includes password expiration, complexity requirements, and lockout after failed attempts. Additionally, train users to use passphrases. A passphrase like “swab-failing-purveyor27!” is inherently stronger than a password like “Spr1ng2024#!”.

- **Enforce multi-factor authentication (MFA)**

Password spray attacks are relatively common. Tie an MFA system like Duo or Microsoft’s authenticator to domain accounts and remote access to prevent access even if account credentials are compromised.

- **Remove or limit local administrators**

Implement a Privileged Access Management (PAM) tool, which allows for easier management and deactivation of local administrators and an elevation approval process for installs and other actions.

TIP

ThreatLocker® tip: Deploy ThreatLocker Elevation Control for granular control over (1) which applications you can elevate, (2) under what circumstances as well as (3) allow management of local administrators on servers and endpoints.

- **Follow the principle of least privilege (POLP)**

All accounts should use the least privilege access required for their job function. Microsoft recommends using Domain Administrators when it’s needed, then promptly removing them once a task is complete.

- **Remove deactivated accounts**

The Center for Internet Security (CIS) recommends deleting or disabling dormant accounts after 45 days of inactivity. Attackers will try to access an account after a user leaves the organization, or any lingering test accounts that are still active.

- **Disable Guest, Anonymous, and Everyone access on each server**

Each access type (Guest, Anonymous, and Everyone) is only necessary for specific cases. During access audits, keep an eye on the permissions since they are generally too broad.

Use a secure admin workstation

A workstation dedicated to performing administrative tasks provides greater protection from keylogging, pass the hash, and phishing attacks. You can configure servers to only allow connections from this workstation and enable them to only communicate over your LAN.

Remove Domain Administrators from file permissions

Assign file permissions to specific service or admin accounts, while denying access at the administrative group level. This ensures Deny permissions on groups override Allow permissions, preventing users in those groups from accessing the files and restricting access to only designated accounts.

Why you should implement this strategy:

Directory accounts are often the target of attack. A compromised directory account can exfiltrate data or take advantage of privileged access to infrastructure and network resources. As such, you need to explicitly verify and implement least privilege.

This Microsoft article provides an overview of best practices for securing Active Directory.

4. Network security

Infrastructure often fulfills network-based roles like DHCP and DNS servers. Security configurations surrounding these roles and other related categories include:

DNS server configurations

- Implement Domain Name System Security Extensions (DNSSEC) to enable DNS response validation. This will help mitigate cache poisoning and man-in-the-middle attacks.
- Using a split DNS configuration can separate internal and external DNS requests. This reduces spoofing and cache poisoning attacks.

DHCP server configurations

Limit your DHCP scope to what's necessary for the environment. DHCP exhaustion attacks can lead to the introduction of rogue DHCP servers by a threat actor, which then can lead to data interception.

Microsegmentation

Microsegmentation limits lateral movement, supports compliance, and applies tailored security policies to each server. For example, you can block direct workstation access to database servers while allowing communication to an application server.

ThreatLocker® tip: ThreatLocker Network Control enables you to use dynamic access control lists to block unapproved east-west traffic by automatically opening and closing ports, allowing only permitted devices to access network resources.

Encryption

Consider encrypting what you can. This includes Transparent Data Encryption (TDE) for SQL servers, applying SSL/TLS certificates to hosted web applications, AD certificate services, and key management.

Why this matters:

Securing network elements on your Windows server will mitigate specific attacks and ultimately reduce attack surface in your environment.

ThreatLocker® tip: When using ThreatLocker Unified Audit you will see all actions that occur within your environment and can be sorted by action type like network events.

Consider reviewing this article for best practice recommendations for DNS client settings in Windows Servers.

5. Basic and advanced audit policies

Insights into security events provide valuable details on what is happening in your environment daily. Depending on the necessity, some organizations might only require a broad level of auditing while others might want to granularize what is being audited. Consider the two types when implementing an audit policy in your organization:

- **Basic audit policies offer categories of security-related events such as:**
  - Audit account management
  - Audit directory service access
  - Audit policy change
  - Audit system events
  - Audit privilege use

- **Advanced audit policies allow the selection of behaviors that you explicitly want to monitor. For example:**

Account management

- Audit computer account management: Audits if a computer account was created, changed, or deleted.
- Audit distribution group management: Some examples are if a distribution group was created, changed, or deleted as well as if a member was added or removed from a distribution group.

System security

- Audit security state change: Includes system startup & shutdown, system recoveries, and change of system time.
- Audit security system extension: Audits if a security extension code is loaded, such as authentication or a security package. Attempts to install or load security system extensions are labeled as critical as it can indicate a security breach.

Privilege use

- Audit sensitive privilege use: Audits events like creating a token, loading device drivers, modifying firmware environment values, and more.

- **You can leverage other useful audit policies to track suspicious activity, such as the deployment of ransomware through Group Policy. These policies include:**

Audit directory domain service changes: Record when objects are created, deleted, modified, moved, or restored. Key event IDs to track include:

- 4732: A GPO was created.
- 4733: A GPO was linked.
- 4739: A GPO was modified.

Audit process creation: Track newly created processes, including the application or user responsible. Specific event IDs include:

- 4688: A new process has been created.

Audit file system: Monitor user attempts to access file system objects, which helps track access to deployment scripts or install files. Specific event IDs include:

- 4663: An Attempt was made to access an object.

Why you should implement this strategy:

Monitoring security-related events provides valuable information for troubleshooting and threat investigation.

ThreatLocker® tip: Use ThreatLocker Detect to create rules that notify or action on specified events on endpoints. For more information surrounding advanced security auditing, see this Microsoft article.

CONCLUSION

Securing Windows Servers starts with configurations tailored to their use case and organizational needs. Incorporating a Zero Trust security model strengthens your strategy. Key steps include physically securing servers, limiting ports and services to essentials, enforcing the Principle of Least Privilege, and routinely auditing security events.

ThreatLocker offers a multi-layered approach to securing your infrastructure. Learn more about how ThreatLocker can secure Windows Servers even more by booking a free demo.

More information on baselines and best practices:

- Securing infrastructure with Zero Trust | Microsoft learn
- Securing domain controllers against attack | Microsoft learn
- Advanced security audit policy settings | Microsoft learn
- What is DNSSEC on DNS server in Windows server? | Microsoft learn
- Center for Internet Security (CIS) benchmarks - Microsoft compliance | Microsoft learn
- Security baselines guide | Microsoft learn

About ThreatLocker®

ThreatLocker® is a Zero Trust Endpoint Protection Platform that improves enterprise-level server and endpoint security with Zero Trust controls, including: Allowlisting, Ringfencing™, Storage Control, Network Control, ThreatLocker® Detect, Elevation Control, and Configuration Manager.

sales@threatlocker.com

+1-833-292-7732

threatlocker.com