TitanHQ™

Complete Network Security Checklist

This checklist provides IT administrators with some key tips and tricks to help strengthen your business cyber security posture.

TitanHQ.com

Want to make sure your network and organization are secure against threats internally and externally?

Need help getting started? If yes, then use our TitanHQ ‘Network Security Checklist. This checklist gives you the tips and tricks needed to get you started and guides you to the areas of IT security you need to focus on.

Don't have time to read guide now? Enter your details here and we'll email you a copy.

1. Cybersecurity Policies and Rules

Here’s a short list of the policies every company with more than two employees should have to help secure their network:

- Acceptable Use Policy
- Internet Access Policy
- Email and Communications Policy
- Network Security Policy
- Remote Access Policy
- BYOD (Bring Your Own Device) Policy
- Encryption Policy
- Privacy Policy

2. Provisioning Servers

In today’s business landscape, data is a valuable commodity easily sold or traded, and your servers are where most of your company’s most valuable data resides. Here are some tips for securing those servers against all threats. Your organization needs a provisioning strategy, so we created a server deployment checklist. Ensure that all the following are on the list, and that each server you deploy complies 100% with compliance policies before it goes into production.

Keep a Current and Updated List of Servers

Maintain a server list that details all the servers on your network - including name, purpose, IP address, date of service, service tag (if physical), rack location or default host, operating system, and administrator responsible for maintaining it.

Assign a Responsible Administrator Per Server

The person or team who knows what the server is for, and is responsible for ensuring it is kept up-to-date and can investigate any anomalies associated with that server.

Establish a Naming Convention

Naming conventions may seem like a strange thing to tie to security but being able to quickly identify a server is critical when you spot traffic anomalies, and if an incident is in progress. With incident response, every second saved counts.

Review Network Configurations

Ensure that all network configurations are done properly, including static IP address assignments, DNS servers, WINS servers, interface registration, binding order, disabled services on DMZ, 00B management, or backup networks.

Use an IPAM

All servers should be assigned static IP addresses, and that data needs to be maintained in your IP Address Management (IPAM) tool {even if that's just an Excel spreadsheet). When traffic anomalies are detected, it’s vital to have an up-to-date and authoritative reference for each IP address on your network.

Patching

Every server deployed needs to be fully patched as soon as the operating system is installed, and added to your patch management application immediately. When developers release security patches, all servers must be updated immediately to remediate known vulnerabilities and stay compliant with regulatory requirements.

Install Antivirus

All servers need to run antivirus software and report to a central management console for administrator review. Scanned exceptions must be documented in the server list so that they can be manually reviewed during incident response.

Install Host Intrusion Prevention and Firewalls

If you use host intrusion prevention, ensure that it is configured according to your standards, and it reports activity to your central management console. Software firewalls must be configured to whitelist legitimate traffic for your network, including remote access, logging and monitoring, and other services.

Remote Access

Pick one remote access solution, and stick with it. We recommend built-in RDP (Remote Desktop Protocol) for Windows clients, and SSH for everything else. You may prefer to remote into your Windows boxes with PCAnywhere, RAdmin, or any one of the other remote access applications for management. Whichever one you choose, choose one that follows compliance standards, and make sure developers continue to maintain it and patch vulnerabilities.

UPS and Power Saving

Make sure all servers are connected to a UPS (Uninterruptable Power Supply). If you don't use a generator, ensure that every UPS has the agent needed to gracefully shut down before the batteries are depleted. While you don't want servers to hibernate, consider spinning down disks during periods of low activity (like after hours) to save electricity.

All Servers Join a Domain

Unless there's a good reason not to, such as application issues or because it's in the DMZ, all Windows servers should be joined to a domain, and all non-Windows servers should use LDAP to authenticate users against Active Directory. The advantage is centralized management and a single user account store for all your users and authorization requests.

Rename the Administrator Account Reset Its Password

Rename the local administrator account, and make sure you set (and document) a strong password. It's not a foolproof approach, but nothing in security is 100% risk free. Good cybersecurity is a layered approach, so this strategy adds another layer of complexity for an attacker.

Assign Domain Group Memberships and Permissions

Make any appropriate assignments using domain groups when possible, and set permissions using domain groups too. Only resort to local groups when there is no other choice and avoid local accounts.

Correct OU with Appropriate Policies

Different servers have different requirements, and Active Directory Group Policies are a good strategy for enforcing policies. Create as many OUs (Organizational Units) as you need to accommodate the different servers, and set as much as possible using a GPO instead of the local security policy.

Report Events to a Management Console

No matter what you use to administer and monitor your servers, make sure they all report to a centralized management console before deploying servers to production. Administrators will then have a central location to review all servers in production, making them more efficient in identifying anomalies.

Disable Unnecessary Services

If a server doesn't need to run a particular service, disable it. You'll save memory and CPU, but it also reduces risk should the service have vulnerabilities.

Configure SNMP

If you are going to use SNMP (Simple Network Management Protocol), make sure you configure your community strings and restrict management access to known systems.

Install All Agents

With backup agents, logging agents, management agents, and any other software you use to manage your network, make sure all appropriate agents are installed before the server is deployed to production.

Configure Backups

If it's worth building, it's worth backing up. No production data should ever be stored on a server until it is configured with a backup strategy.

Confirm Backups

No backup should be trusted until you confirm it can be restored. Some backup applications use various methods to ensure that backups are not corrupted, but administrators should validate backups by restoring them occasionally.

Scan for Vulnerability

If you really think the server is ready for production, review the checklist for any missing elements and scan the server for vulnerabilities. Run a full vulnerability scan against each server before it goes to production to make sure nothing has been missed. Then, ensure it is added to your regularly scheduled scans.

Sign Servers into Production

Someone other than the person who built the server should spot check it to be sure it's ready before it's signed into production. By "signing" it, the second user says that they confirmed the server meets your company's security requirements and is ready for service. This secondary person is an additional pair of eyes, so you are much less likely to find that something got missed.

3. Deploying Workstations

Don't overlook the importance of making sure your workstations are as secure as possible. Follow this general checklist for workstations and any other user devices connected to the network.

Keep a Workstation List

Keep a list of all workstations -- just like the server list -- that includes the issued user and when the workstation's lease is up, or it has reached the end of its depreciation schedule. Don't forget those service tags!

Track the Assigned User

Track the locations of your workstations by ensuring that each user's issued hardware is kept up to date.

Establish a Naming Convention

During a network audit, it helps to have workstations named for the user who has it. Naming conventions make it much easier to track down device locations when anomalies are detected.

Configurations

You'll probably assign device IP addresses using DHCP but ensure that your scopes are correct. Use a GPO (Global Policy Object) to assign any internal DNS zones that should be searched when resolving flat names.

Patch Workstations

Since your users are authenticated, browsing the web and running programs on your workstations, they are at a much higher risk than servers, so patching is even more important. Make sure all workstations are fully up to date before they are deployed, update your master image frequently, and ensure that all workstations are being updated by your patch management system.

Install Antivirus

Every workstation should have antivirus installed to reduce cybersecurity risks and stay compliant. Add workstations to a central server responsible for updating them at least every six hours. The central server should download updates from software vendors regularly, but workstations should be configured to download updates when they cannot reach the central server. All workstations report status to the central server, and you can push updates from the central server to workstations as necessary.

Configure Host Intrusion Prevention and Firewalls

Consider using a host intrusion prevention or personal firewall product to provide more defense for your workstations, especially laptops that frequently connect to the cloud externally from the corporate network.

Enable Remote Access

Like servers, pick one remote access method and stick to it. Disable all other remote access features and applications. The more ways an attacker can access a workstation, the more ways the attacker can attempt to exploit the machine. Ensure that only authorized users can access the workstation remotely, and that they must use their network credentials, instead of a universal admin and password combination.

Use Power Saving

Consider deploying power-saving settings using the network GPO to help extend the life of your hardware and save on electricity. Make sure that you have Wake-on-LAN compatible network cards, so you can deploy patches after a workstation goes into sleep mode from inactivity.

Join a Domain

All workstations should be joined to a domain, so administrators can centrally maintain them with domain credentials and access policies.

Rename the Administrator Account and Reset Its Password

Use a script to create random passwords and store them securely where they can be retrieved in an emergency.

Assign Local Group Memberships and Permissions

Set appropriate memberships for local administrators and power users for each workstation.

Configure OUs with Appropriate Policies

Organize your workstations in Organizational Units (OUs) and manage them with group policies as much as possible to ensure consistent management and configuration.

Report Activity to a Management Console

Validate that each workstation reports antivirus and patch management activity to a central console before you turn it over to an assigned user, and then audit it frequently.

Configure Backups

You probably won't perform regular full backups for workstations but consider folder redirection or cloud-based backups to protect critical user data. Should a user lose their workstation or damage it, data stored on the workstation could be lost or corrupted. Storing data in the cloud by redirecting directories and storage locations reduces risk of data loss.

Enable Local Encryption

All laptops and portable drives must have local storage encryption enabled to protect confidential data. Whether you use BitLocker, TrueCrypt, or hardware encryption, local drive encryption should be mandatory.

Scan for Vulnerabilities

Perform regular vulnerability scans of a random sample of your workstations to help ensure they are up to date with the latest security patches and software updates.

4. Network Equipment

Your network infrastructure is easy to overlook, but it's also critical to secure and maintain. We'll start with some recommendations for all network equipment and then look at some platform-specific recommendations.

Keep a Network Hardware List

Maintain a network hardware list like your server list. Include device name and type, location, serial number, service tag, and responsible party.

Network Configuration

Have a standard configuration for every device and network resource to help maintain consistency and ease of management.

Use an IPAM

Assign static IP addresses to all management interfaces, add A records to DNS, and track everything in an IP Address Management (IPAM) solution.

Patch all Equipment

Network hardware runs an operating system too, called firmware. Keep hardware firmware up to date for all security patches and updates.

Keep Remote Access Consistent

Use the most secure remote access method your platform offers. For most, the security method is SSH version 2 (SSH-2). Disable Telnet and SSH-1 and set strong passwords on both the remote and local (serial or console) connections. Passwords for sensitive resources should be at least 12 characters with numbers, uppercase and lowercase letters, and special characters.

Assign Network Credentials

Use TACACS+ (Terminal Access Controller Access Control System) or other remote management solution so that authorized users authenticate with network credentials.

Configure SNMP

If you use SNMP, change the default community strings and set authorized management stations. If you aren't, disable SNMP.

Set Up Backups

Take regular backups of your configurations before making changes and validate that they aren't corrupted by restoring them as a test.

Scan for Vulnerabilities

Regularly scan all network resources to detect vulnerabilities early. Any vulnerable resources should be patched or updated as soon as possible to stay compliant and avoid a data breach.

Install VLANs

Use VLANs (Virtual LANs) to segregate traffic types, such as workstations, servers, out-of-band management, backups, and any other critical infrastructure.

Protect from Promiscuous Devices and Hubs

Set port restrictions so that users cannot run promiscuous mode devices, connect hubs or connect unmanaged switches without prior authorization.

Disable Unnecessary Ports

Unassigned ports should be disabled or set to a default guest network that cannot access the internal network. This prevents outside devices from accessing the internal network from empty offices or unused cubicles.

Configure Firewalls

Firewalls must be configured with explicit permits and implicit denies. "Deny All" should be the default configuration on all access lists both inbound and outbound. All violations and alerts should be logged for further review. Use only secure routing protocols with authentication, and only accept updates from known peers on your perimeter.

5. Vulnerability Scanning

Vulnerability scanning catches any misconfigurations, unpatched resources, and exploitable applications. Your environment should have vulnerability scanners that run frequently to catch and remediate issues quickly. Here are a few tips for scanners:

Schedule Weekly External Scans

Configure your vulnerability scanning application to weekly scan all your external addresses.

Compare Differences Weekly

Validate any differences from one week to the next against your change control procedures to make sure no one has enabled an unapproved service or connected a rogue host.

Schedule Internal Scans Monthly

Perform monthly internal scans to help ensure that no rogue or unmanaged devices are on the network and that all resources are patched.

6. Backups

Without backups, your organization is at risk of losing critical data. Data loss prevention includes backup schedules, which ensure that productivity can be restored reasonably quickly after an incident and that business continuity is preserved. Backups are a critical component in disaster recovery plans.

Establish a Tape Rotation

Make sure you have a tape rotation established that tracks the location, purpose, and age of all tapes. Never repurpose tapes that were used to back up highly sensitive data for less secure purposes.

Destroy Old Tapes

When a tape has reached its end-of-life, destroy it to ensure no data can be recovered from it.

Secure Offsite Storage

If you are going to store tapes offsite, use a reputable courier service that offers secure storage.

Encryption

Even reputable courier services have lost tapes. Ensure that any tape transported offsite -- whether through a service or by an employee -- is encrypted to protect data against accidental loss.

Restricted Access to Tapes to a Backup Operators Group

Backup tapes contain sensitive data, and backup operators can bypass file-level security in Windows to back up all data. Secure the physical access to tapes and restrict membership in the backup operators group just like you do to the domain admin group.

Restore Regularly

Backups are worthless if they cannot be restored. Verify your backups at least once a month by performing test restores to ensure your data is safe.

Consider Using Cloud Storage

Tapes and local backups are popular, but you still risk data corruption or device damage. The cloud has virtually limitless storage capacity, and it's much more reliable and available than a tape backup.

7. Remote Access

Most administrators need remote access to at least one network resource. Here are a few tips for configuring remote access on your network:

- Set up and maintain an approved method for remote access and grant permissions to any user who should be able to connect remotely. Ensure that your company policy prohibits other methods.
- Consider using two-factor authentication (2FA) such as tokens, smart cards, certificates, or SMS solutions to further secure remote access.
- Perform regular reviews of your remote access audit logs and spot-check with users if you see any unusual patterns, such as authentication in the middle of the night or during the day when the user is already in the office.
- Set strong account lockout policies and investigate any accounts that are locked out to ensure attackers cannot use your remote access method to break into your network.
- If you split tunneling, enforce internal name resolution only to further protect users on public networks.
- Protect your traveling users who may be on public wireless networks by tunneling all their traffic through a VPN instead of enabling split tunneling.

8. Wireless

Whether you have a wireless network internally or must support remote users on Wi-Fi, your administrators must set up security to monitor and restrict remote users. Here are a few tips for wireless network security:

Configure an SSID

Use an SSID (Service Set Identifier) that cannot be easily associated with your company and suppress the broadcast of that SSID. Both aren't particularly effective against someone who is seriously interested in your wireless network, but it does keep you off the radar of a casual war driver.

Enable Encryption

Use the strongest encryption type you can, preferably WPA3 Enterprise. Never use WEP or WPA. If you have barcode readers or other legacy devices that can only use deprecated protocols, set up a dedicated SSID for only those devices and use a firewall so that they can only connect to central software over the required port.

Use Secure Authentication

Use 802.1x for authentication to your wireless network, so only approved devices can connect.

Secure the Guest Network

Use your wireless network to establish a guest network for visiting customers, vendors, and any other external users that need internet connectivity. Do not permit connectivity from the guest network to the internal network, but allow for authorized users to use the guest network to connect to the Internet. Authorized users on the guest network can then use a VPN to access the internal network, if necessary.

Establish a BYOD Policy

Create a “Bring Your Own Device" policy now, even if that policy is just to prohibit users from bringing their personal laptops, tablets, and smartphones and connecting over VPN.

9. Email

Use a multi-layered protection approach to email and don’t rely only on your email provider’s server filtering capabilities. Also add a third-party dedicated solution to filter your email and protect your data from phishing and malware. Here are a few more tips:

- Deploy an email filtering solution that can filter both inbound and outbound messages to protect your users and your customers.
- Ensure that your edge devices will reject directory harvest attempts.
- Deploy email filtering software that protects users from the full range of email threats, including malware, phishing, and spam.

10. Internet Access

Having full user access on the internet from your network leaves your environment vulnerable to malware, ransomware, and other malicious cyber-attacks. Take these steps to help avoid a critical cybersecurity incident from user web browsing activity:

- OTG (On the Go) protection: Protect your users when they are not in the office with 'On the Go' solutions that can help filter traffic on their laptops and identify when they are in the office and need to use the office filtering solution.
- Internet Security: Use internet filters, when possible, to protect your users and business from malicious websites. Ransomware is one of the most devastating types of cyber-attacks right now, and it can destroy your business. Provide your users with secure Internet access by implementing an Internet monitoring solution.
- Encryption: Use filter lists that support your company's acceptable use policy.
- Malware Scanning: Scan all content for malware, including file downloads, streaming media, or simply scripts contained in web pages.
- Bandwidth Restrictions: Protect your business-critical applications by deploying bandwidth restrictions, so user access to the Internet doesn’t negatively impact company functions such as email, business application usage, or the corporate website.
- Port Blocking: Block outbound traffic that could be used to bypass Internet monitoring solutions, so users cannot violate policy.

11. File shares

Files are necessary for business productivity, but they must be protected from threats. Attackers and ransomware will scan the network for file shares where they get access to intellectual property, sensitive data, and trade secrets. Here are some tips for protecting file shares:

- Everyone group: The default permissions for server operating systems and network resources are usually a little too permissive. Remove the Everyone group from legacy shares, and the Authenticated Users group from newer shares, and set more restrictive permissions, even to “domain users”.
- Least Privilege: Always assign permissions using the concept of “least privilege”. “Need access" should translate to "read-only” and “full control" should only ever be granted to admins.
- Groups: Never assign permissions to individual users, only use domain groups. This strategy is more scalable, easier to audit, and can carry over to new users or expanding departments much more easily than individual user permissions.
- Deny Access: If you have a file system that tempts you to use “Deny Access” to fix a problem, you are probably doing something wrong. Reconsider your directory structure and higher level permissions such as moving critical files or directories to avoid using “Deny Access” permission restrictions.

12. Log Correlation

If you have more servers than you can count, you have too many servers for manual log reviews. Use a logging solution that aggregates logs from all your servers, so you can parse and correlate event logs from one location for review.

13. Time

Use a central application for time management within your organization for all systems including workstations, servers, and network gear. NTP (Network Time Protocol) can keep all systems in sync, making correlating logs much easier since the timestamps will all agree.

Cybersecurity is not an easy strategy. It’s a sensitive and complex area, so don’t try managing it without help. Many experienced managed service providers and security experts are available with the knowledge you need to help protect your business.

Need help getting started? If yes, then use the TitanHQ ‘Network Security Checklist. This checklist gives you the tips and tricks to kickstart your cybersecurity strategy

GET IN TOUCH