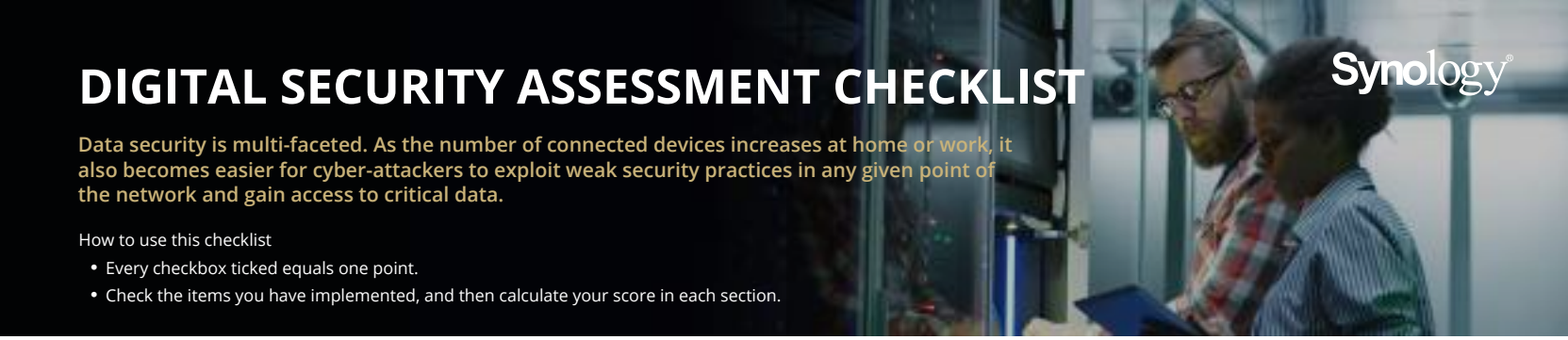
DIGITAL SECURITY ASSESSMENT CHECKLIST



Synology

Data security is multi-faceted. As the number of connected devices increases at home or work, it also becomes easier for cyber-attackers to exploit weak security practices in any given point of the network and gain access to critical data.

How to use this checklist

- Every checkbox ticked equals one point.
- Check the items you have implemented, and then calculate your score in each section.

A Perimeter defense / Router

TOTAL SCORES /14

System security

- ☐ 01. Use a custom administrator account and disable the default "admin" and "guest" accounts
- ☐ 02. Enable 2-step verification
- ☐ 03. Change the system default ports, e.g. port 8000/8001 for the management interface if you use Synology Router Manager (SRM), to new custom ports
- ☐ 04. Enable IP Auto Block against brute-force attacks
- ☐ 05. Enable HTTPS for services running on SRM with a valid SSL certificate
- ☐ 06. Enable email, SMS or push notifications to stay on top of critical events
- ☐ 07. Enable automatic update for the router's firmware and all built-in security databases

Network security

- ☐ 08. Access devices in office or at home via VPN
- ☐ 09. Enable Synology Safe Access to block malicious domains and IP addresses
- ☐ 10. Enable Threat Prevention and Deep Packet Inspection
- ☐ 11. Enable DNS over HTTPs encryption to prevent DNS hijacking
- ☐ 12. Enable GeoIP Firewall rules
- ☐ 13. Enable Mac filtering and whitelist known devices for Wi-Fi usage
- ☐ 14. Enable regularly scheduled traffic reports to monitor network usage

B Endpoint protection / NAS

TOTAL SCORES /12

- ☐ 01. Use a custom administrator account and disable the default "admin" and "guest" accounts
- ☐ 02. Enable 2-step verification
- ☐ 03. Apply password strength rules to all your users
- ☐ 04. Restrict users' access privileges to only the shared folders and services they need
- ☐ 05. Change the system default ports, e.g. port 5000/5001 for the DSM management interface to new custom ports
- ☐ 06. If port forwarding is enabled for your NAS, use custom public ports on the router instead of well-known ports (e.g. 5000/5001)
- ☐ 07. Enable IP Auto Block against brute-force attacks
- ☐ 08. Enable HTTPS for services running on DSM with a valid SSL certificate
- ☐ 09. Enable email, SMS or push notifications to stay on top of critical events
- ☐ 10. Enable automatic update for DSM
- ☐ 11. Run Security Advisor regularly to uncover system vulnerabilities and identify malware
- ☐ 12. Install an antivirus package and regularly conduct full scans

C Endpoint protection / Computers & mobile devices

TOTAL SCORES /4

- ☐ 01. Keep your operating system up-to-date
- ☐ 02. Run a reliable antivirus software and regularly conduct full scans
- ☐ 03. Only enable the Remote Desktop Protocol (RDP) when remote access is absolutely required, protecting you from attacks that exploit this protocol
- ☐ 04. When using public Wi-Fi, always encrypt the connection by using a VPN

D Endpoint protection / IoT devices

TOTAL SCORES /4

- ☐ 01. Use a strong password
- ☐ 02. Block devices (e.g. IP cameras, printers, phones, etc.) from accessing the internet unless the device requires communication with the server in order to function
- ☐ 03. Connect IoT devices to the guest network and segregate them from user-owned devices such as computers, smartphones, and NAS to prevent an IoT device from being hijacked and attacking other devices in the same network
- ☐ 04. Block a device immediately if it shows signs of suspicious activities, investigate into the incidents, and reset/reinstall the device if needed

E Data backup

TOTAL SCORES /10

Computers

- ☐ 01. Enable Synology Drive to back up important files and folders
- ☐ 02. Enable Active Backup for Business to back up the entire system

NAS backup

- ☐ 03. Enable Hyper Backup to back up shared folders, LUNs and system/package configurations
- ☐ 04. Configure an alert threshold in Hyper Backup for file changes between two backup versions, so that it automatically notifies you of abnormal behavior and prevents all intact versions from being silently overwritten
- ☐ 05. Enable Snapshot Replication to take snapshots of important shared folders
- ☐ 06. Enable Cloud Sync to continuously back up files and folders to a secure public cloud provider such as Synology C2 Backup

External devices (e.g. USB drives)

- ☐ 07. Use USB Copy to back up all external devices to your NAS and manage the files from one place

Backup execution

- ☐ 08. Keep at least one offsite copy for disaster recovery
- ☐ 09. Schedule all your backup tasks to run automatically
- ☐ 10. After setting up a backup task, immediately test and see if you can restore data from the backup copy, and repeat this regularly afterwards to ensure that you can always make full restoration in time when accidents happen