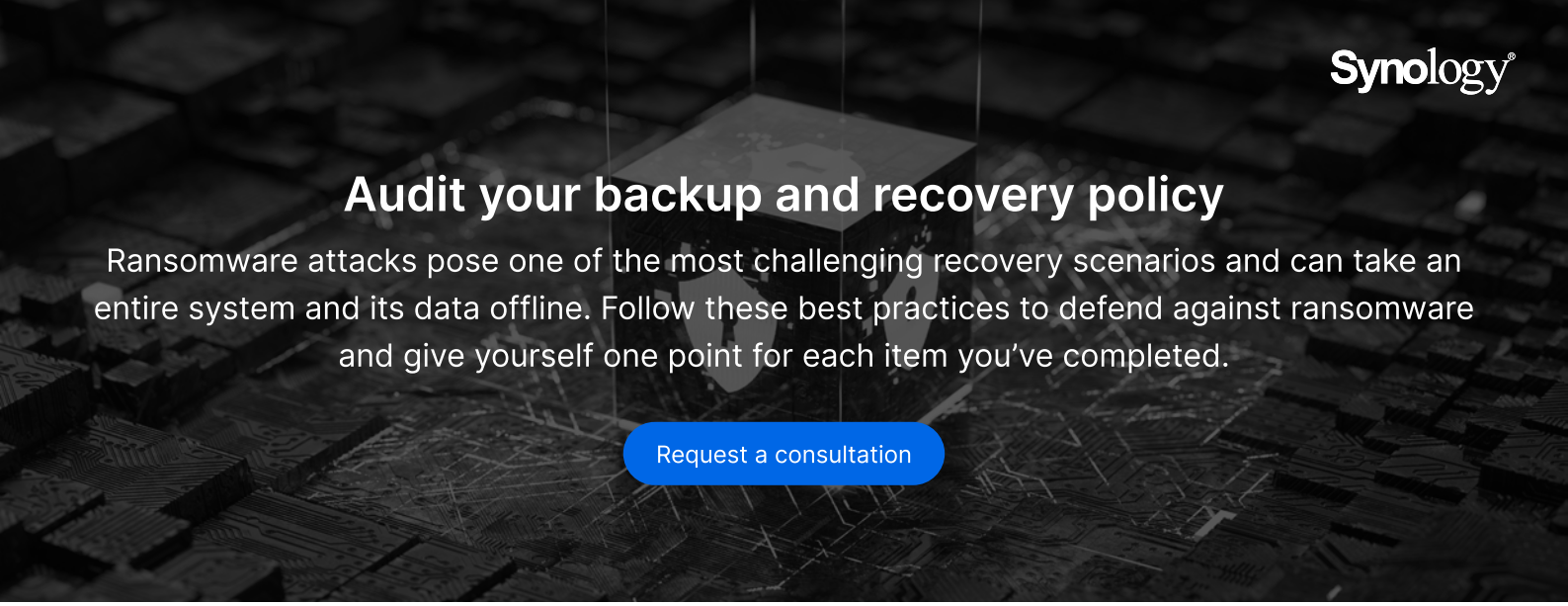


Audit your backup and recovery policy

Ransomware attacks pose one of the most challenging recovery scenarios and can take an entire system and its data offline. Follow these best practices to defend against ransomware and give yourself one point for each item you've completed.

Request a consultation

1 Protecting data wherever it is

Score / 5

Eliminate data silos and automate backups

Data silos are isolated collections of data that operate independently within an organization. As data silos don't communicate with other systems, they are harder to monitor and maintain, and can increase the risk of ransomware by creating exploitable security vulnerabilities. Define a schedule to audit every system, determine the backup requirements for each one, and make sure backups can happen automatically.

Ensure all data in cloud services is protected

Many organizations use cloud applications for communication, productivity, collaboration, and more. Data in these service might be targets of malicious deletion or tampering, but creating a true backup of cloud data isn't always straight forward. Review the cloud services used by your organization and develop a backup strategy for each one accordingly.

Develop a versioning and retention policy with ransomware in mind

Modern ransomware has a latency period that can last up to 90 days so it's important to set the retention period of your backups to a **minimum of 90 days**. With Active Backup for Business, you can set advanced retention rules for your VMs, servers, and computers. View guide

Audit the time required to recover systems (and check if there are faster options)

Since downtime of any system can result in costly disruptions, you might want a backup solution that offers cross-platform and cross-hypervisor restoration capabilities to mitigate downtime due to system outages. In the event of a disaster, Synology offers an array of options to recover your data and fail over your systems. Learn more

Schedule monthly or quarterly "fire drills" to test recovery processes

Backups are only useful if they can be successfully restored. Run mock ransomware "fire drills" for different systems according to a schedule, so that you can verify backups work correctly and you can familiarize yourself with the process. With certain Synology systems, you can take a backup with Active Backup and then simulate the restoration in Virtual Machine Manager. View guide

2 Protecting on-site systems with off-site backups

Score / 2

Make sure your off-site disaster recovery strategy fits your needs

For critical servers and virtual machines, consider replicating backups to a second site and preparing compatible hardware to failover services there, if something happens to the systems at the main site. For example, you can use Snapshot Replication to copy data from a primary backup server to a second server for fast recovery when necessary. View guide

Keep your data safe with the 3-2-1 backup rule

The 3-2-1 backup rule can help mitigate the risk of data loss, including from ransomware attacks, by ensuring that you have at least three copies of your data on two different media types, with one copy stored off-site. For example, you can keep a primary backup on one Synology server, replicate to a second server as mentioned above, and keep a third copy of backups stored in a cloud service. View guide

3 Protecting data on your Synology NAS

Score / 5

Update firewall and autoblock rules for your systems

Create firewall rules on DSM to allow or deny access to certain network ports through specific IP addresses, thereby preventing unauthorized logins and controlling service access. View guide

Audit your login flows and implement multi-factor authentication

Two-factor authentication (2FA) can help reduce the chances of accounts being compromised. In addition, Adaptive Multi-Factor Authentication (AMFA) adds an additional layer of protection by requiring confirmation when admin accounts are accessed from untrusted external connections. View guide

Encrypt your backups

To defend against ransomware, backups must be secure, tamper-proof, and isolated from networks or physical threats, ensuring always available, clean copies for restoration. Use Hyper Backup to encrypt your NAS backups off-site or to the cloud. View guide

Monitor file activity for ransomware

Centralized management reduces complexity and makes it easier to ensure that all systems are working as expected. Once installed, Active Insight will monitor your Synology system and take a snapshot of your data if ransomware is detected. View guide

Make your off-site backups immutable

Immutable Snapshots safely store immutable copies of your LUNs and Shared Folders to defend against compromised administrator credentials. View guide

4 Developing a culture of security

Score / 8

Schedule recurring cyber security training sessions for employees

Educate employees about the dangers of ransomware and the importance of exercising caution when handling email communications. Teach them how to recognize common phishing indicators, such as misspelled URLs, generic greetings, and urgent requests for sensitive information.

Encourage better password hygiene

Use C2 Password to give each employee their own in-browser password manager, and use the Shared Vault feature to share credentials with your team securely. View guide

Follow the principal of least privilege

Take an inventory of all systems which require authentication. Then, streamline permissions for each user strictly to what their roles demand, minimizing unauthorized access risks. Utilize a centralized solution such as C2 Identity to manage user access to devices, cloud services, and on-premise infrastructure. View guide

Set a schedule to review and lock down access permissions

Enhance your access control with Synology Directory Server, which offers centralized authentication and access control for your Synology system. Explore our guide to learn how it can be used as an alternative to or in conjunction with Windows AD, providing actionable insights to strengthen your security posture. View guide

Have an incident response plan in place

Set up a security incident response plan to minimize recovery time in the event of an attack. Establish consistent and unhindered communication channels with service providers. If your organization lacks the resources to do so, make sure the solution providers have their own in-house PSIRT team.

Hire a PEN tester

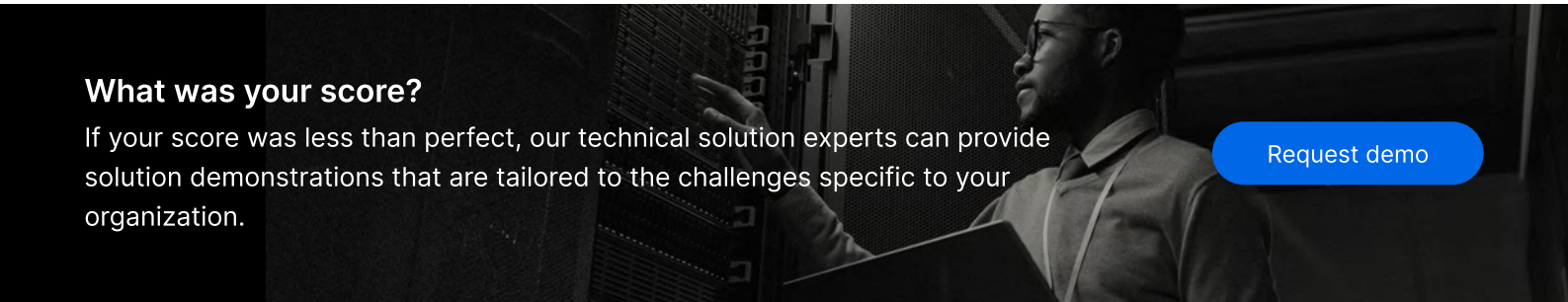
Take proactive steps to secure your IT systems by engaging a third-party security audit, which includes penetration testing. This comprehensive assessment simulates real-world attacks to pinpoint vulnerabilities, providing actionable insights and recommendations to strengthen your defenses against ransomware threats.

Insure your data

Cyber insurance provides financial protection if ransomware occurs, covering costs related to data recovery, legal fees, and regulatory fines. Discuss with an insurance agent what type of policy will best meet the needs of your organization, including whether you need first-party coverage, third-party coverage, or both.

Budget for security

Set aside enough funds to keep both software and hardware up to date. First, ensure that all operating systems, software applications, and security solutions are regularly updated with the latest patches and versions. Secondly, make a plan to phase out any software that does not have continuous improvement and updates.



What was your score?

If your score was less than perfect, our technical solution experts can provide solution demonstrations that are tailored to the challenges specific to your organization.

Request demo