Synology®

ActiveProtect Cyber Recovery Guide

Secure your data with a powerful cyber recovery solution

Table of Contents

Overview

Cyberattacks are on the rise. Threats are taking place faster than ever before, with far-reaching effects. The average breakout time for attackers to move within an organization is 48 minutes, with the fastest case at 51 seconds.[1] By late 2024, voice phishing attacks rose by 442%.[1] Across industries, nation-state attacks grew 200-300%,[1] showcasing the need for better defenses against attacks. IT teams must understand that endpoint security itself is not enough to achieve cyber resiliency, highlighting the need to build a multi-layered strategy.

With a multi-layered security approach, Synology ActiveProtect appliance has been designed with resilience at its core. ActiveProtect aims to provide businesses with peace of mind and ensure continued business operations with no disruptions. ActiveProtect comes with powerful security controls, backs up a wide range of workloads, comes with immutable capabilities, as well as options to scale your storage.

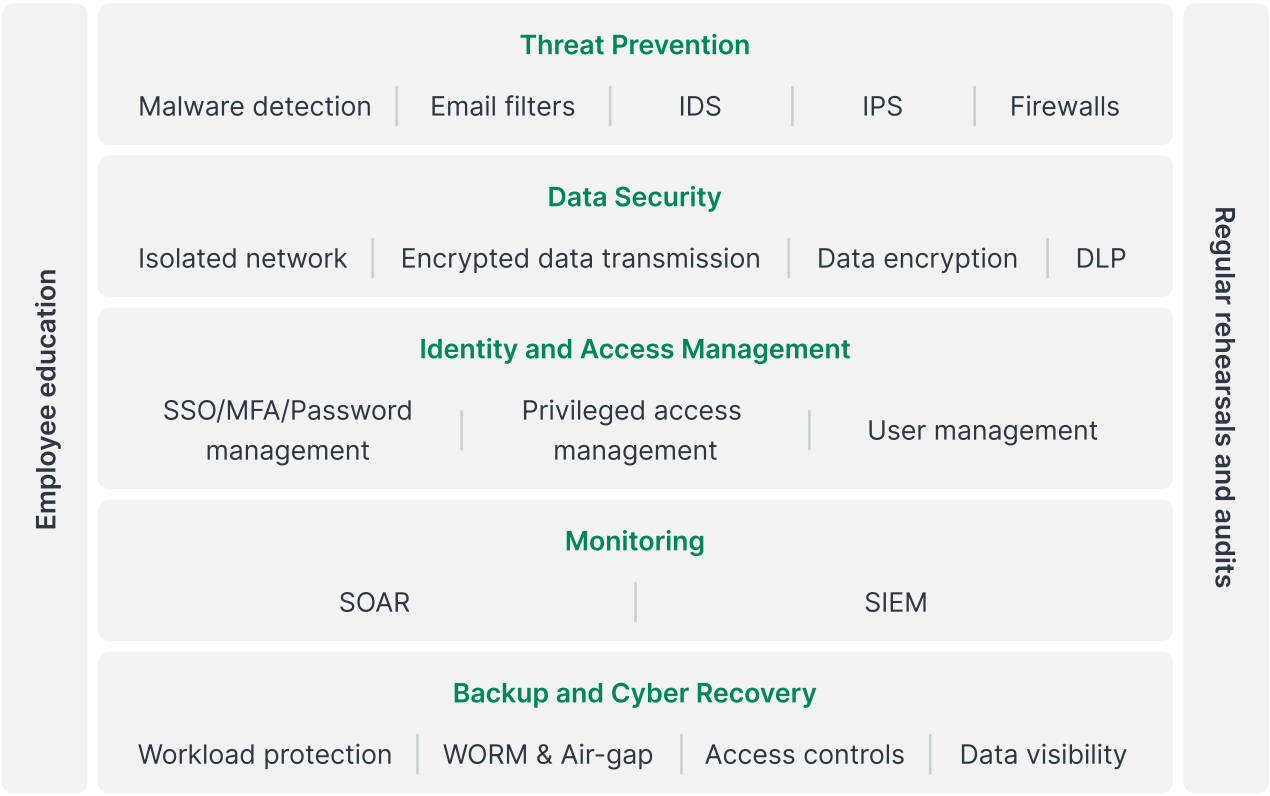
Synology is known for providing resilient, flexible, and orchestrated data recovery options; its new data protection lineup, ActiveProtect, is no less. ActiveProtect comes with flexible, automated data recovery options that allow companies to perform data restores within minutes. This effectively minimizes downtime and allows businesses to achieve business continuity in the face of sudden data loss.

About this document

This guide is designed to help organizations better understand cyber resilience. It also aims to highlight how Synology ActiveProtect can help enterprises counter ransomware threats. With an in-depth analysis, we'll provide you with best practices associated with cyber resilience so that organizations can safeguard their IT infrastructure against the rising threats of cyber attacks.

This guide is intended for IT professionals, Information Security Officers, and Synology Partners, who are responsible for developing, implementing, and overseeing cybersecurity strategies.

Build a cyber resilient architecture



Note

There is no one-size-fits-all solution for cyber resiliency. Synology recommends adopting a multi-layered security strategy based on the National Institute of Standards and Technology (NIST) framework. This includes categories such as: Identify, Protect, Detect, Respond, and Recover.

As part of their ransomware defense strategy, organizations should still implement traditional security measures such as setting up firewalls, email and spam filters, anti-malware software, and more.

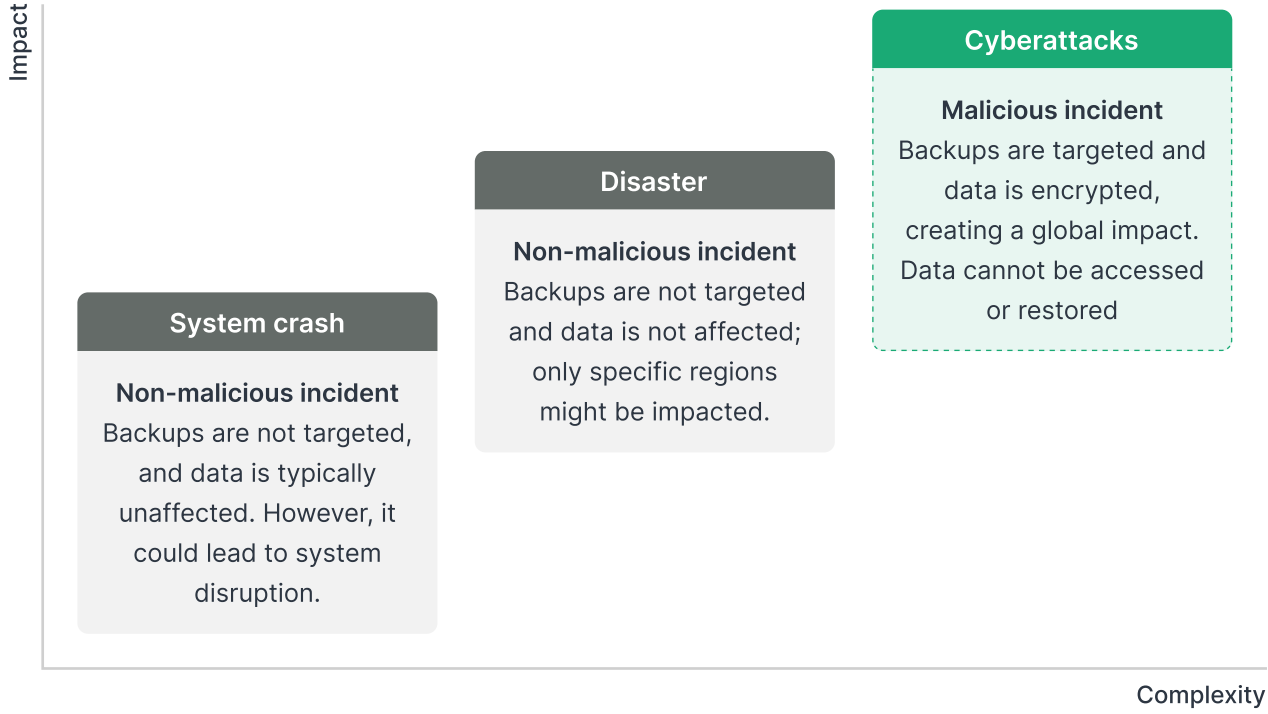
Cyber recovery explained

How data protection has evolved

The evolution of data protection can be divided into three stages: Backup recovery, Disaster recovery, and Cyber recovery.

In terms of data protection, backup recovery is considered basic as it protects workloads and focuses on providing fast, reliable, and effective recovery capabilities. However, this type of strategy is not enough for defending against website failures or cyberattacks. Disaster recovery builds upon Backup recovery by preventing data center failures and ensuring bandwidth efficiency, along with fast replication. It also provides some protection against cyberattacks.

Cyber recovery is an advanced protection solution made for mission-critical applications and is specifically designed to safeguard against cyberattacks and ransomware attacks. This strategy includes security measures such as lockdown policies to prevent internal threats, network isolation to block external threats, as well as scanning and risk identification features to ensure that there is no issue with the recovery process and that your data is recoverable, no matter what happens.



Why businesses need to shift to cyber recovery

As cyberattacks become more complex, businesses must actively implement the cyber recovery strategy to ensure comprehensive data protection. Not only does ransomware encrypt critical operational files, but it also deletes backup data, which hackers demand a hefty ransom for decrypting your data. When this occurs, an entire business operation can be crippled, with the impact being further extended to the entire supply chain.

Network recovery focuses on whether or not critical systems and data can be restored correctly after cyberattacks, ransomware attacks, or data theft. It also places a greater emphasis on data integrity and security policies. This enables businesses to quickly recover after an attack and defend against future threats.

If businesses rely solely on backup and disaster recovery strategies, it may not be enough to prevent ransomware attacks. This is especially true if backup data has already been targeted and compromised. Even though disaster recovery strategies are capable of protecting against data center failures, it might not be enough to handle threats posed by modern-day cyberattacks, especially if systems have been infiltrated and the integrity of your backups are at risk.

Implementing a cyber recovery strategy is crucial as it offers the most advanced level of protection against growing threats. With a cyber recovery strategy, organizations are able to recover their data in a secure manner, maintain business continuity, and defend against evolving threats. This enables businesses to become resilient when dealing with the threats of ransomware.

	Disaster Recovery	Cyber Recovery
Event	Natural disasters, hardware failures	Ransomware, cyberattacks
Scope	Partial: Localized	Comprehensive: Entire enterprise or even the industry supply chain is disrupted
Data access	Able to back up and restore	Unable to back up and restore
Focus	System service availability	Data integrity and confidentiality

How to defend against ransomware

To mitigate these risks, organizations must proactively adopt security measures to safeguard their data and systems. Let's examine common attack methods and cybersecurity vendors' security solutions to combat these threats. ActiveProtect comes with backup and recovery capabilities and a wide variety of security measures so businesses can quickly respond to a ransomware attack. This also minimizes business disruption and data loss.

Step 1 & 2	Step 3	Step 4 & 5
Observe & Infiltrate	Lurk	Destroy & Negotiate

Blocking

- Encrypt your data
- Security mechanisms
- Firewall
- Access controls
- Employee awareness

Defenses

- Antivirus scanning
- Behavioral analysis
- Service monitoring
- Regular audits

Backup

- Secure backups
- Offsite backups
- Immutable storage
- Isolation zone
- Deduplication

Recovery

- Backup verification
- Recovery drills
- Granular restoration
- Instant restoration
- Disaster recovery

1 Phishing and social engineering attacks

Attackers often send fake emails or social media messages to impersonate legitimate organizations. These are designed to manipulate victims into providing sensitive data. If a victim clicks on these links or type in their credentials, hackers can gain unauthorized access to sensitive data or even infiltrate company systems.

Essential tools for enterprises

Educate your employees
Train your employees to recognize phishing emails by checking the sender address and avoid clicking on suspicious links.

Email security measures
Use an Email Security Gateway or URL filter to block malicious websites.

Multi-factor authentication (MFA)
Add an extra layer of security by requiring the use of MFA.

Boost your security with a data protection solution

Perform authentication with Active Directory and SAML 2.0.

Comes with role-based permissions to enable granular user delegation.

2 Password attacks

Attacks aim to gain unauthorized access to systems by attempting to crack or steal user account passwords. This includes techniques such as brute-force attacks, dictionary attacks, and credential stuffing. After gaining access, attackers can elevate their privilege, install malware, or steal sensitive data.

Essential tools for enterprises

Require strong passwords
Avoid weak passwords and passwords that are easy to guess.

Limit login attempts
Block IPs that generate multiple failed login attempts in a short period.

Multi-factor authentication (MFA)
Prevents unauthorized logins, even if passwords have been compromised.

Monitor compromised credentials
Regularly check employee credentials against leaked data lists and mandate password changes if necessary.

Boost your security with a data protection solution

Integrate with your organization's existing directory service such as Active Directory, LDAP, and SAML 2.0 for SSO.

Have a password policy that meets company requirements or follow password strength recommendations such as a combination of uppercase letters, lowercase letters, numbers, and symbols. Passwords should be changed periodically.

3 Ransomware and malware attacks

Attackers infect a victim's device with malicious software, which encrypts files and folders. Malicious software is usually spread via phishing emails, vulnerability exploits, or malvertising. Attackers then demand a hefty ransom to decrypt these files. If the ransom isn't paid on time, attackers may also threaten to leak sensitive data, resulting in potential financial losses and severe business disruptions.

Essential tools for enterprises

Perform regular backups
Back up critical data on a regular basis and store your backups in a secure and isolated environment to prevent ransomware encryption.

Leverage behavioral analysis tools
Detect abnormal file access or encryption activities with behavioral analysis tools.

Restrict user access
Reduce your attack service by restricting user access to critical systems.

Strengthen your endpoint security
Deploy Endpoint Detection and Response (EDR) solutions as well as antivirus software to block threats proactively.

Boost your security with a data protection solution

Ensure data resiliency by implementing the 3-2-1-1-0 backup strategy.

Detect and restore corrupt data, verify backups, and test your disaster recovery strategy in a sandboxed environment with built-in hypervisors.

Secure your backed-up data with WORM technology and isolate your data with air-gapped backups.

Leverage bare-metal or file-level restoration to restore data or perform P2V or V2V restoration to instantly recover data.

Maintain control over data by granting access permissions such as workload restoration and data viewing rights.

4 Distributed Denial-of-Service (DDoS) attack

During a DDoS attack, attackers overwhelm a website or servers with unnecessary traffic, making it inaccessible. They exploit botnets to flood their target with malicious requests, which then exhausts system resources and disrupts legitimate website access.

Essential tools for enterprises

Detect traffic spikes
Keep an eye out for potential attacks by identifying unusual spikes in traffic.

Implement firewalls & Intrusion Prevention Systems (IPS)
Protect critical services with the use of firewalls and IPS to filter out malicious traffic.

Manage and filter traffic
Minimize the impact of attacks with the use of methods such as traffic distribution, packet filtering, and IP blacklisting.

Boost your security with a data protection solution

Protects against DoS (Denial-of-Service) intrusions and prevents malicious attacks over the Internet.

Comes with built-in auto-block mechanisms which block IP addresses that have too many failed login attempts.

Enable default ports for backup and recovery purposes via a whitelist. Users must manually configure third-party firewalls to open additional ports; this is set up via an allowed list.

5 Zero-Day attack

A zero-day attack exploits unknown software vulnerabilities before a patch is even available, making it extremely dangerous. It can lead to data theft, compromised systems, or malware injection.

Essential tools for enterprises

Update operating systems and software regularly
Update software and operating systems on a regular basis to help reduce the risk of unpatched vulnerabilities so that they cannot be exploited by attackers.

Implement behavior-based threat detection

Identify suspicious activities beyond the traditional signature-based detection methods. This helps to detect previously unknown threats, based on behavior anomaly.

Leverage zero-trust architecture

Strict access controls are enforced so that each and every user and device must verify their identity before gaining access to resources. This requires multi-factor authentication (MFA) to improve security measures.

Boost your security with a data protection solution

Synology's security team actively monitors vulnerabilities via SBOM, or Software Bill of Materials, and releases software updates on a regular basis. This includes security fixes and performance optimization.

Generate backup status reports so that companies can track backup execution and store reports for a business' record keeping requirements. Any backup anomalies will result in notifications being sent promptly.

The system stores logs of all operations and anomalies so that a centralized report can be exported for behavioral analysis.

Shared Responsibility Model for Cyber Resiliency

Ownership	Responsibility	How Synology ActiveProtect can help
Security firm	Threat prevention	Integration
	Data security	Cooperation
	Identity and access management	Integration
	Monitoring	Integration
Backup vendor	Data Protection and cyber recovery	Full support
Users	Employee education	Cooperation
	Regular rehearsals and audits	Cooperation

Best practices

The National Institute of Standards and Technology (NIST) framework outlines five key actions: Identify, Protect, Detect, Respond, and Recover. Organizations should aim to align their backup and recovery strategy with this framework and integrate relevant solutions to strengthen their security posture to protect against ransomware.

NIST	Best Practices
Identify	Version management, Zero trust policies, Network segmentation, Employee training
Protect	Zero trust model, Immutable storage, Backups, Network segmentation, Antivirus scanning
Detect	Behavioral analysis, Antivirus scanning, Intrusion detection
Respond	Rehearsals, Employee training, Behavioral analysis, Antivirus scanning
Recover	Rehearsals, Backups, and Rapid recovery optimization

1 Network segmentation and configuration

Isolate network segments with strict segmentation controls to prevent lateral movement of malware. Enforce least privilege access principles across all systems and users.

2 Behavioral analysis

Deploy Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to detect and respond to threats in real time. Detect anomalies, identify insider threats as well as any unusual access patterns by monitoring user and system behaviors.

3 Antivirus scanning

Run scans on a regular basis to prevent malware infections. Leverage antivirus with behavioral capabilities to detect and analyze potential threats. Monitor endpoints and respond to suspicious activity with the use of Endpoint Detection and Response (EDR) systems.

4 Zero-trust model and security policies

Require authentication for users, devices, and applications always. Use role-based access controls (RBAC) and 2FA or MFA for access management. Review permissions on a regular basis to ensure minimal access.

5 Educate your employees

Improve cybersecurity awareness by training your employees to prevent social engineering attacks. Train employees to spot phishing emails, avoid clicking on suspicious links and attachments, and report suspicious activity immediately.

6 Implement the 3-2-1-1-0 backup strategy

Adopt the industry-standard 3-2-1-1-0 backup strategy to ensure data redundancy and offsite storage. This ensures data availability in the event of a ransomware attack. Test your backups on a regular basis to ensure quick data recovery when needed.

7 Historical data analytics and threat prediction

Through Security Information and Event Management's (SIEM) advanced analytics, companies can study past security events to spot emerging threats to predict potential attacks. Detect anomalies via machine learning techniques and link past incidents to identify trends. The system learns from historical data to improve detection and enable proactive security.

8 Immutable storage

Secure your data from ransomware or malicious alterations. Implement WORM technology to prevent unauthorized deletions or modifications. Leverage air-gapped backups to prohibit attackers from directly accessing your data.

9 Disaster recovery drills

Test your backup and disaster recovery systems on a regular basis. Run disaster recovery drills for cyberattacks such as insider threats or ransomware. Make sure to review and update your response plans according to the test results and update your plans to combat new threats.

10 Version management and system updates

Update all operating systems, applications, and security patches on a regular basis. Maintain version control by ensuring all environments support the same versions. Set up automatic updates or reminders for system maintenance.

11 Rapid recovery optimization

Create a disaster recovery plan to restore your systems with speed. Leverage instant recovery or snapshot capabilities to reduce downtime and prioritize your recovery by monitoring critical apps.

Mitigate challenges of cyber threats with ActiveProtect

Synology ActiveProtect ensures that your data can be recovered anytime, anywhere, including large-scale recovery solutions. Rest assured as companies can maintain business continuity, even when dealing with a ransomware attack. Synology provides a comprehensive cyber resilience solution that exceeds traditional backup solutions.

Synology takes a business value approach to cybersecurity challenges, such as cyber threats, by providing resilience strategies. From data protection to backup verification and management solutions, counter cybersecurity threats and ensure data integrity and recoverability with enterprise solutions such as Synology ActiveProtect.

The Challenge

Traditional solutions are slow, fragile, and difficult for recovery

Synology ActiveProtect eliminates dependencies between previous backup versions. With Changed Block Tracking (CBT), only changed data is backed up. This enables fast backups that can also be recovered fast from any previous points. This is essential for ransomware attacks or system failures.

The Challenge

Manual setup results in unprotected workloads and users

Synology ActiveProtect is capable of automatically detecting new workloads and applying predefined protection plans. Backup coverage remains intact even as users or systems change, preventing data silos and coverage gaps.

The Challenge

Backed up data could be vulnerable to tampering or deletion

Synology ActiveProtect complies with Sheltered Harbor standards by using retention lock policies to protect backups and setting up isolation zones. This protects backups from any unauthorized changes, including internal threats.

The Challenge

Limited data visibility as well as limited control across sites

With a centralized console, IT admins can monitor all workloads, verify SLA compliance, and restore data without relying on the central backup server, even if data is located across multiple sites. This ensures a limited impact on the business.

The Challenge

Restoring an offsite backup is complex and time consuming

Even if the primary server fails, Synology ActiveProtect allows users to quickly recover their data from offsite backups via a centralized platform. This reduces downtime and business disruption.

Conclusion

With a surge of increasingly sophisticated cyberattacks, businesses have to step up and safeguard their data to ensure business continuity. As this guide points out, organizations have to create a robust strategy to secure corporate data against the threat of ransomware. Synology ActiveProtect can help businesses bolster resiliency with a future-proof cyber recovery strategy.

By following best practices, implementing powerful security features, and achieving fast data recovery, Synology ActiveProtect empowers organizations to combat cyber threats with confidence. By protecting your data, securing your backups, and ensuring swift recovery, Synology ActiveProtect allows you to achieve your cyber recovery goals with ease.

Note

Study conducted by CrowdStrike.

Synology®

synology.com