Synology

Protect your organization against ransomware

Ransomware attacks are forecast to cost organizations a combined US trillion in 2023 alone.[1] Data protection plans with fast restoration options are crucial for mitigating the impact of ransomware and other forms of cybercrime.

Date 13 Oct 2023

Backups: the last line of defense when disaster strikes

When data is lost following malicious deletion or modification, backups allow you to restore mission-critical data and avoid costly downtime. Leverage Synology's data protection solutions to design a backup strategy for your entire IT infrastructure.

Complete protection

Safeguard endpoints as well as primary backups to create multiple safety nets for your data.

Fast recovery

Reduce downtime to a minimum when disaster strikes with instant recovery options.

Immutable storage

Prevent unauthorized changes to data and snapshots.

License-free backups

Back up as much data as your storage allows, without limitations or hidden fees.

Centralized protection against ransomware

Consolidate backups from fleets of workstations, servers, virtual machines, and cloud applications. Optimize storage consumption and avoid bandwidth bottlenecks with data deduplication and incremental backup technologies. https://www.synology.com/dsm/solution/infrastructure

Physical workloads

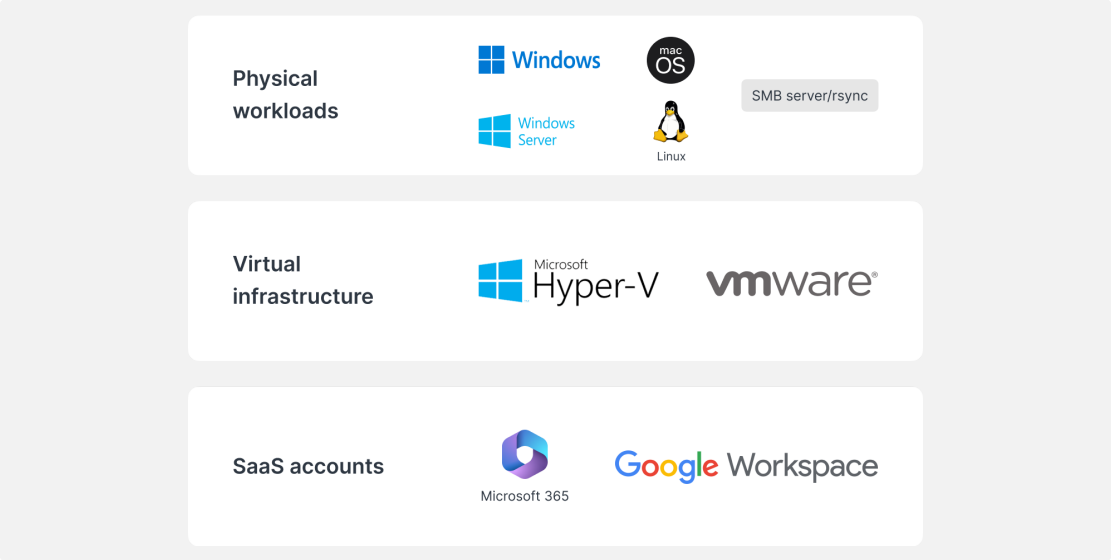
Protect endpoints in the event of malicious attacks with comprehensive bare-metal backup and flexible file-level recovery.

Virtual infrastructure

Back up VMware® vSphere™, Microsoft® Hyper-V® VMs, and LUNs with powerful data reduction technologies.

SaaS accounts

Enable continuous protection for data stored on the cloud, with automatic detection of newly added accounts.



Efficient recovery

Minimize downtime for critical production systems by rapidly restoring backups from a local or off-site Synology system.

Near-zero RTO

Mount backup images on VMware®, Hyper-V®, or Synology Virtual Machine Manager to resume work as quickly as possible. Restore VMs to an alternative hypervisor to avoid service disruption.

Minimal RPO

Configure backup frequency according to your needs, minimizing the amount of data potentially affected during an attack. Protect systems fast thanks to incremental backups and deduplication technology.

Intuitive operation

Let employees browse and preview emails, contacts, and files from a convenient portal before restoring them, delivering a more user-friendly experience and reducing the burden on IT teams.

Add an extra layer of protection

Adhere to the 3-2-1 backup strategy by storing a third set of data off-site or on the cloud, shielding your data against fire, natural disaster, or theft.

To off-site servers

Store backups to a Synology server at a secondary location to defend against physical disaster and replicate immutable snapshots for added ransomware protection.

To the cloud

Back up to any major cloud storage provider, keeping your data safe from unauthorized access through client-side AES-256 encryption. https://c2.synology.com/storage/nas

Trusted across different industries

"Synology [...] enabled us to reduce server hardware expenditure [...] while making infrastructure and workstation backups, system logging, and file management much easier."
https://www.synology.com/company/case_study/Investortools

"Thanks to Active Backup for Business, all our backups are now centralized and available 24/7, which helps us minimize downtime and stay compliant with FERPA's regulations."
https://www.synology.com/company/case_study/University_of_Washington

"[...] Active Backup for Business has astonishing backup speeds and works wonders on deleting duplicate data — it only took up 28 TB out of the total 58 TB on the server. [...]"
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

"[...] Active Backup for Business [...] allows us to centralize and manage all the backup tasks from a single console. Fast and reliable recovery also ensures business continuity."
https://www.synology.com/company/case_study/UNESCO

Frequently Asked Questions

What is ransomware?

Ransomware is a type of malware that encrypts victims' files. The attackers then demand a ransom to restore data access, often threatening to permanently destroy the data if no ransom is paid. Ransomware attacks can be highly disruptive and can cause significant financial losses for individuals and organizations. It is important to protect yourself and your devices against ransomware, such as by keeping your software up to date and backing up your files regularly.

What types of ransomware are there?

There are many different types of ransomware, and new strains are constantly being developed. Some of the most common types of ransomware include:

- **Encrypting ransomware** — The most common type of ransomware encrypts the victim's files so that they cannot be accessed without the decryption key. Attackers then demand a ransom payment in exchange for the key
- **Locker ransomware** — A type of ransomware locks victims out of their computer by changing the login credentials or displaying a message that prevents the victim from accessing their system. Attackers then demand a ransom payment to unlock the computer
- **Ransomware-as-a-Service (RaaS)** — A business model in which attackers offer ransomware to other individuals or groups who want to carry out attacks. The former will typically provide the ransomware and handle payments, while the latter receive a percentage of the ransom payments
- **Scareware** — Ransomware designed to scare victims into paying the ransom. It typically involves displaying fake security warnings or messages that claim the victim's computer is infected with a virus. The attacker will then demand a ransom payment to remove the supposed infection

How does ransomware spread?

Ransomware typically spreads through phishing emails or by exploiting vulnerabilities in a computer system. In a phishing attack, an attacker will send an email that appears to be from a legitimate source, such as a bank or a well-known company. The email will often contain a link or an attachment that, when clicked, will install the ransomware on the victim's computer. Exploiting vulnerabilities in a system is similar, except that the attacker will use a flaw in the system's security to install the ransomware without the victim's knowledge. In either case, once the ransomware is installed, it can quickly spread to other computers on the same network.

What is the typical process of a ransomware attack?

The process of a ransomware attack typically follows these steps:

1. The attacker gains access to a victim's computer, either by sending a phishing email or by exploiting a vulnerability in the system
2. Once the attacker has access to the victim's computer, they will install the ransomware on the system
3. The ransomware will then encrypt the victim's files, making them inaccessible to the user
4. The attacker will then demand a ransom from the victim, typically in the form of a digital currency like Bitcoin, in exchange for the decryption key that will unlock the encrypted files
5. If the victim pays the ransom, the attacker will provide the decryption key and the victim will be able to access their files again. However, there is no guarantee that the attacker will actually provide the key, and even if they do, the victim's files may be damaged or corrupted as a result of the encryption process

It's important to note that there are many variations on this process, and not all ransomware attacks will follow these steps exactly. Some attacks may not involve encrypting files at all, for example, while others may involve other forms of extortion or blackmail.

How can I get ransomware?

There are several ways that you can get ransomware. One of the most common ways is by clicking on a malicious link or attachment in a phishing email. This type of email is designed to look legitimate, often appearing to be from a well-known company or organization. When you click on the link or attachment, it will install the ransomware on your computer. Another way that you can get ransomware is by visiting a compromised website. These websites have been hacked by attackers, who have inserted code that will automatically install the ransomware on your computer if you visit the site. You can also get ransomware by downloading infected files from the internet. This can happen if you download a file from a suspicious website, or if you download a file that has been shared by someone you don't know. In short, it is important to be cautious when browsing the internet and to avoid clicking on links or downloading files from unfamiliar sources. This can help protect you from getting ransomware and other types of malware.

Who are the targets of ransomware?

Ransomware attacks can target anyone who uses a computer or other device connected to the internet. However, some groups are more likely to be targeted than others. For example, ransomware attacks often target businesses, as they often have more valuable data and may be more willing to pay a ransom to retrieve it. Hospitals, schools, and other organizations that provide critical services are also common targets, as a ransomware attack can disrupt their operations and put people's lives at risk. Individuals can also be targeted by ransomware attacks. In these cases, the attackers may try to extort money from the victim by threatening to delete their personal files or publish sensitive information unless a ransom is paid. The targets of ransomware attacks are often selected based on the value of their data and their willingness to pay a ransom to get it back.

What are the risks of paying ransomware?

Paying a ransom to a ransomware attacker may seem like the easiest way to get your files back, but it can actually be a very risky decision. There are several risks associated with paying a ransom, including:

- There is no guarantee that the attacker will actually provide the decryption key. In many cases, victims who pay the ransom never receive the key and remain unable to access their files
- Paying the ransom may encourage attackers to continue their campaign of attacks. If attackers know that victims are willing to pay the ransom, they may be more likely to carry out more attacks in the future
- Paying the ransom may make you a target for future attacks. If the attacker knows that you are willing to pay a ransom, you may be more likely to be targeted in the future
- Paying the ransom may be illegal. In some cases, paying a ransom to a criminal organization may be considered a form of funding terrorism or other illegal activities

While paying the ransom may seem like the easiest way to retrieve your files, it can actually be a very risky decision. It is important to carefully consider the risks before making a decision.

What are the cost of ransomware?

The cost of a ransomware attack can vary greatly depending on a number of factors, such as the type of ransomware used, the number of files encrypted, and the effectiveness of the attack. In some cases, the cost of a ransomware attack can be relatively low, with attackers demanding a few hundred dollars in ransom. In other cases, the cost can be much higher, with attackers demanding thousands of dollars or even more to restore access to the victim's files. In addition to the direct costs associated with paying a ransom, ransomware attacks can also have significant indirect costs. For example, a ransomware attack can cause downtime and loss of productivity, which can result in lost revenue and income. It can also damage a company's reputation and customer trust, which can have long-term negative effects on the business. These indirect costs are often much higher than the ransom itself.

What are the symptoms of ransomware?

The symptoms of a ransomware attack can vary depending on the specific type of ransomware that is used. However, some common symptoms include:

- Your files are encrypted and you are unable to access them
- You receive a message from the attacker demanding a ransom payment in exchange for the decryption key
- You see unfamiliar programs or processes running on your computer
- Your computer becomes slow or unresponsive
- Your computer displays unusual error messages or pop-up windows

If you suspect that your computer has been infected with ransomware, it is important to act quickly. Disconnect your computer from the internet to prevent the ransomware from spreading.

How to prevent ransomware attacks?

There are several steps you can take to prevent ransomware attacks, including:

- Use reputable antivirus or security software and keep it up-to-date. This can help protect your computer from ransomware and other types of malware
- Be cautious when opening email attachments or links. Ransomware is often delivered through phishing emails, so it is important to be careful about what you click on
- Keep your operating system and other software up-to-date. Software updates often include security patches that can help protect your computer from ransomware and other threats
- Back up your files regularly. This can help protect your data if your computer is infected with ransomware. Make sure to adhere to one of the recommended backup strategies, such as the 3-2-1 backup strategy
- Be aware of the risks of ransomware and educate others in your organization about these threats. This can help prevent ransomware attacks and make it easier to detect and respond to them if they do occur

The best way to prevent ransomware attacks is to stay vigilant and to take steps to protect your computer and your data. This can help reduce the risk of a ransomware attack and make it easier to recover from one if it does occur.

How can Synology protect me against ransomware?

Preventative actions are essential to protect against falling victim to ransomware. Use these Synology solutions in addition to your antivirus software of choice:

- **Prevent access** — Reduce the spread of ransomware by setting file, application, and access permissions, and configure secure login credentials using Secure SignIn and C2 Password
- **Protect devices** — Outdated systems are at greater risk. Update all your NAS at once with Synology Central Management System (CMS), and safeguard other devices using group policies in Synology Directory Server and C2 Identity
- **Avoid suspicious files** — Spam and phishing emails containing suspicious files are common methods of spreading ransomware. Synology MailPlus provides strong anti-malware protection and spam prevention
- **Check for vulnerabilities** — Use Synology Security Advisor to routinely scan for malware, vulnerabilities, and abnormal login activities. Implement recommended changes to improve your NAS security. https://www.synology.com/dsm/overview/security

More ways to protect your data

Manage your fleet

Leverage extensive features to centrally manage data access permissions, software status, system health, and more.
https://www.synology.com/dsm/overview/administration

Monitor all your systems

Identify suspicious login activities, manage updates, and monitor device health, no matter where your devices are located.
https://www.synology.com/dsm/feature/active-insight

Safeguard your data

Follow the 3-2-1 backup rule to protect your data against accidental and malicious modification or deletion.
https://www.synology.com/dsm/solution/data_backup

Get started

Contact us

Contact regional sales for more information
https://www.synology.com/form/inquiry/sales

Where to buy

Find a Synology partner in your region
https://www.synology.com/wheretobuy

Notes:

1. eSentire, 2022 Official Cybercrime Report
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Protect your organization against ransomware

https://www.synology.com/en-au/dsm/solution/ransomware

Synology Website

https://www.synology.com/

Contact us

https://www.synology.com/company/contact_us