White paper

+1.857.444.8500
nasuni.com | sales@nasuni.com

Ransomware Defense for Multi-Site Enterprises: How to Recover Faster

NASUNI

Ransomware is evolving, forcing enterprises to change how they prepare for attacks. While the focus on preventing attacks continues, forward-thinking organizations have accepted that no defense is impenetrable, and that any solid ransomware strategy must include a robust, reliable, and testable recovery plan. This white paper reviews the standard methods of protecting data against ransomware and highlights the features a multi-site organization should look for in a ransomware recovery solution.

The Expanding Reach of Ransomware

The FBI's Cyber Crime division defines ransomware as "an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them." These attacks impact individuals, state and local governments, and businesses of all kinds, from small local operations to global multinational corporations with offices on multiple continents. Last year:

- Ransomware attacks on organizations increased by 41%
- The average ransom paid by organizations rose to $190,946
- Attacks on enterprises rose by 12%

The FBI's Cyber Crime division defines ransomware as "an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them."

Once ransomware finds its way into a system, the malware encrypts data on local hardware and backups, and even spreads to other networked computers and distant locations. Some attacks are powerful enough to impact dozens of globally distributed offices within a few hours.

One of the more significant cases in the last year is that of Norwegian multinational Norsk Hydro. A new variant of ransomware infiltrated the company's network and spread quickly. The company incurred an estimated $40M in losses from the attack, which struck 150 manufacturing locations and factories and offices in 40 countries.

Why Ransomware is Difficult to Prevent

The FBI details several recommendations for protecting your organization against these attacks and minimizing the likelihood of a ransomware infection. These include strengthening firewalls, updating systems frequently, and teaching employees to avoid suspicious websites and resist clicking on unusual links. Unfortunately, in the case of large global enterprises, these guidelines are difficult to adhere to for several reasons, including:

Number of Users

When you have thousands or tens of thousands of workers, there is a greater likelihood that one or two of them click on an unusual link in an email or visit an odd website that secretly has drive-by downloading, in which the malware infects a computer without a click.

Out-of-Date Hardware

Remote and branch offices within large global organizations often do not have the latest storage and data protection hardware, or the IT resources necessary to ensure that all machines have the upgrades and patches that might prevent ransomware attacks.

More Sophisticated Attacks

Ransomware itself is constantly evolving and attackers are finding new and creative ways into systems, so even if an organization strengthens its defenses against one known variant, there is always a chance that another one will appear with a means of evading those defenses.

The FBI advises those impacted by ransomware to avoid paying the ransom, in part because there is no guarantee that the attackers will provide working keys to decrypt your data. Some businesses pay their attackers, however, reasoning that the cost of recovering their maliciously encrypted data would be far greater than the ransom demand. How many organizations pay these ransoms anyway, and how much they pay, is unknown. Naturally, enterprises are reluctant to admit to massive security breaches – Norsk Hydro is a rarity, but that company's case might not be uncommon.

The FBI advises those impacted by ransomware to avoid paying the ransom, in part because there is no guarantee that the attackers will provide working keys to decrypt your data.

Traditional Backup & Ransomware Recovery

The evolution of ransomware has spurred many organizations to focus on plans for recovering from these attacks as quickly and efficiently as possible. A data protection solution with good Recovery Point Objectives and Recovery Time Objectives allows organizations to restore access to recent versions of data and return to business as usual without having to pay the ransom. In addition to its efforts to educate organizations on ransomware prevention, the FBI stresses the importance of having a robust, reliable, and testable backup process in place.

In theory, reliance on backup is a sound strategy. Yet even this approach can be flawed, for the following reasons:

Long Backup Windows: If you only have the capacity to push backups once a week, or you have a long backup window, there is a risk that the files you do recover will be out of date. Instead of recovering recent data, you will only restore older files, and employees will have lost all the intervening work.

Slow Recoveries: The more files involved, the larger the risk of a slow recovery. The latest ransomware variants spread quickly through networked systems, infecting every folder and file they can touch. Restoring high volumes of files can take days to weeks.

Inconsistent Backup Procedures Across Sites: If different remote offices rely on varying approaches to backup and data protection, the degree of difficulty associated with manually recovering data through these solutions increases exponentially. Companies that have parts of their value chain, or customer service process spread across multiple teams and sites can be even more impacted by an uneven recovery process.

Lack of Testing: Testing backup and restore procedures can take a back seat to more frontline data protection measures. Many victims of Ransomware are putting their file restore capabilities to the test for the first time during an attack, which can lead to delays and uncover gaps in knowledge.

Cloud Backup May Utilize A Slower Tiered Storage Option: A cloud backup option might offer lower cost, long term storage, but not necessarily provide fast retrieval in an emergency. Restores might be both slow and expensive.

Distributed Attacks: Ransomware now has the capacity to infect dozens or even hundreds of locations in just a few hours. Managing the recovery process across multiple sites is a slow and arduous task even with a centralized cloud backup solution.

This last flaw is especially alarming for multi-site enterprises, as it reveals a fundamental weakness in the core design of many leading centralized cloud backup solutions. Multiple sites can be protected with one solution, but if all of these sites are simultaneously infected by a distributed attack, centralized backup software my require restoration one site at a time. This is manageable with a few sites, but once this scales up to dozens of offices, manufacturing plants, job sites, or design studios, organizations may have to wait weeks before every office is up and running again.

The unfortunate truth is that traditional backup and even state-of-the-art cloud backup do not guarantee the kind of recoveries that global enterprises deserve.

Ransomware Recovery with SaaS Cloud File Storage

As ransomware has evolved, so has the cloud. An increasing number of large organizations are modernizing their file storage and data protection infrastructure by reducing their reliance on local hardware and utilizing SaaS cloud file storage. If you are evaluating a SaaS cloud file storage offering, consider a platform that deliver data protection with the following features:

- **One Consistent Solution Across Sites:** Immediately after an attack your team can begin restoring files to multiple locations at the same time, using the same procedures. If the infection spreads throughout your network, you are able to restore hundreds of sites, Windows File Servers, and machines simultaneously, working through one management console.
- **Predictable RPOs and RTOs:** Your organization should be able to control or set your RPOs and RTOs according to the needs of your business. Furthermore, recoveries should be scalable, working across many sites simultaneously. Organizations should not have to restore one site or local government office at a time.
- **Testable:** A strong ransomware recovery solution must be testable. Your chosen cloud file services platform should allow you to verify the speed and ease of the restore process, and the viability of cloud versions.
- **WORM-based:** The newest ransomware strains can infect online backups, so you should look for a data protection plan that relies on strong encryption and Write Once Read Many (WORM) storage. Files should be chunked, encrypted, sent to the cloud securely, ¬and stored as immutable objects in a secure cloud volume.
- **Continuous:** A strong cloud file services platform should be continuous, with no "window" or time lapse. This ensures that recent copies of files will always be available and minimizes data loss and/or loss of productivity.
- **Automatic:** Data protection against ransomware should not require constant oversight or management. Files should be continuously versioned to the cloud, and stored securely as WORM objects, without the need for human maintenance.
- **Cost-effective:** Finally, a cloud file services platform should offer significant cost savings relative to the cost of storing and protecting file data using traditional storage and backup.

Ransomware Recovery Functionality	Traditional Tape Backup	Cloud Backup & Cloud Tiering	SaaS Cloud File Storage
Fast file restores	No	No	Yes
Simultaneous multi-site restores	No	Some software requires sequential site restors	Yes
Centralized management of File Recovery	No	Depends on configuration	Yes
User Designated RPO and RTOs	Frequently misaligned with business continuity requirements	Varies by site	Yes—to within minutes of most recent file changes
Easily testable restore process	No	Yes for single site	Yes
Uncorruptible file backup copies & offsite location	Yes	Varies by solution; Yes for offsite location	WORM file format & geo-redundant object storage

The threat of ransomware is not diminishing. In fact, the rise of ransomware-as-a-service offerings, which allow anyone to utilize the malicious code, suggest that these infections will become more prevalent. Educating your end users and taking steps to protect your systems against infiltration are an essential piece of a good ransomware defense strategy. But as hackers increasingly target the enterprise, traditional and even centralized cloud backups will be challenged to meet business continuity requirements. IT leaders should investigate a SaaS file storage platform that offers consistent fast file recovery, multi-site restores, and an easily testable configuration.

The rise of ransomware-as-a-service offerings, which allow anyone to utilize the malicious code, suggest that these infections will become more prevalent.

About Nasuni

Nasuni® is a file services platform built for the cloud, powered by the world's only global file system. Nasuni consolidates network attached storage (NAS) and file server silos in cloud storage, delivering infinite scale, built-in backup, global file sharing, and local file server performance, all at half the cost of traditional file infrastructures. Enterprise customers use the Nasuni software-as-a-service platform for NAS consolidation; backup and recovery modernization; multi-site file sharing; and rapid, infrastructure-free disaster recovery, while also serving as a foundation for data analytics and multi-cloud IT initiatives.

Leading companies from a wide-array of industries rely on Nasuni to enhance workforce productivity, reduce IT cost and complexity, and maximize the business value of their unstructured data. Sectors served by Nasuni include consumer goods, manufacturing, creative services, engineering and construction, technology, pharmaceutical, oil and gas, financial services, and public sector agencies. Nasuni is based in Boston, Mass. USA. For more information, visit www.nasuni.com.

NASUNI.
One Marina Park Drive
Boston, Massachusetts 02210
United States
www.nasuni.com
SAL-0131 09/20