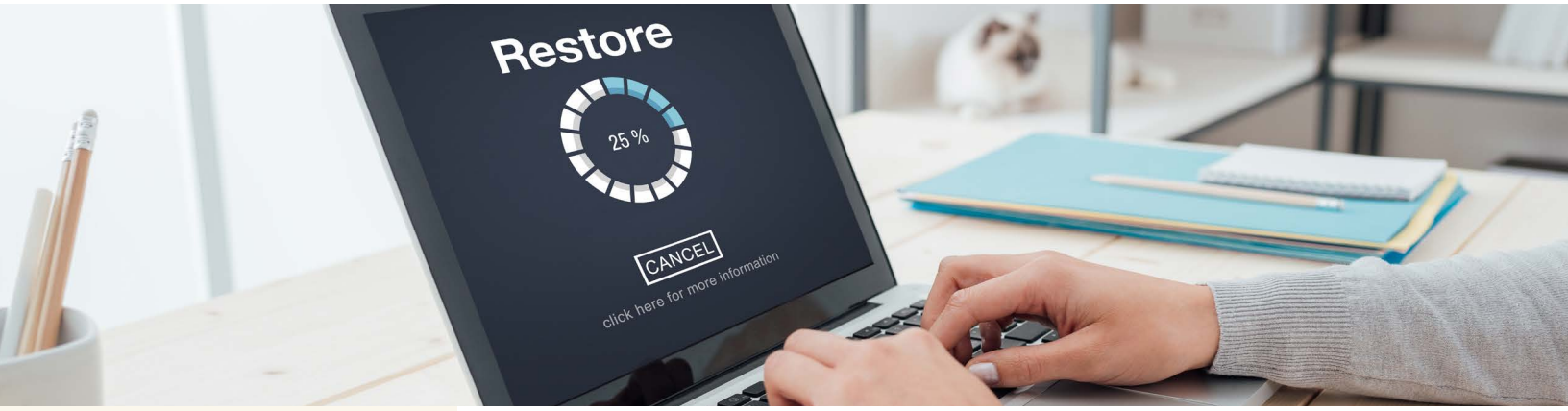
SOLUTION BRIEF

Nasuni for Rapid Ransomware Recovery



Ransomware Impact[1]

600%
Increase in malicious emails since COVID-19

$170,404
Average payout by a mid-sized corporation

$1.85M
Average cost for organization to recover

21 DAYS
Average company downtime from a ransomware attack
THE LARGEST COST

"Nasuni was **a true lifesaver** when we got hit by a ransomware attack," Stephen Held at LEO A DALY added. "Once we contained the attack, we were able to restore files quickly. **Our operations hardly missed a beat."**

Preparing for IT's Number One Disaster

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. Additionally, companies are finding themselves dealing with bad press, stopped orders, idle employees, and lost customer confidence. 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. According to the 2021 Cybereason Global Ransomware Study, 80% of companies that pay a ransom will get attacked again.

A Best-of-Breed Strategy for Ransomware

To be ready for a ransomware attack, IT needs an ecosystem of technology to *prevent, detect, and recover* from an attack. Defense technology from companies like Cisco, Check Point and Palo Alto Networks provide a perimeter defense to protect the network infrastructure using advanced firewall technologies and Layer 7 application profiling. If ransomware sneaks through the defense layer, software solutions from companies like McAfee, Norton, and Varonis can also help with detecting malicious activity. Nasuni works with leading prevention and detection leaders such as Varonis and Stealthbits, helping to keep ransomware at bay. Unfortunately, ever-learning ransomware sometimes slips past prevention and detection layers and by the time an attack is realized, a percentage of that organization's files will already have been encrypted. Nasuni provides the last line of defense with the ability to quickly recover files — which neutralizes the attack — so companies minimize data loss and avoid paying a ransom.

NASUNI®

Traditional Backup and Snapshots Are Not Good Enough

Having good Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) allow organizations to restore to 'clean' versions of file data and return to business as usual without having to pay a ransom. The FBI also stresses the importance of having a robust, reliable, and testable backup process in place. The key to quickly recovering from an attack relies on how quickly files can be RESTORED. Unfortunately, traditional and cloud-based backup have:

- Slow Recovery Times (RTOs): The more files and locations affected, the slower the recovery, which can take days or even weeks.
- Long Backup Windows (RPOs): Employees will lose all their intervening work done between backups.
- Limited Recovery Points: Newer ransomware attacks can employ a time-bomb effect that might take days, weeks, or months to detect. If file backups are not retained long enough, the risk is greater for losing data and not being able to recover.

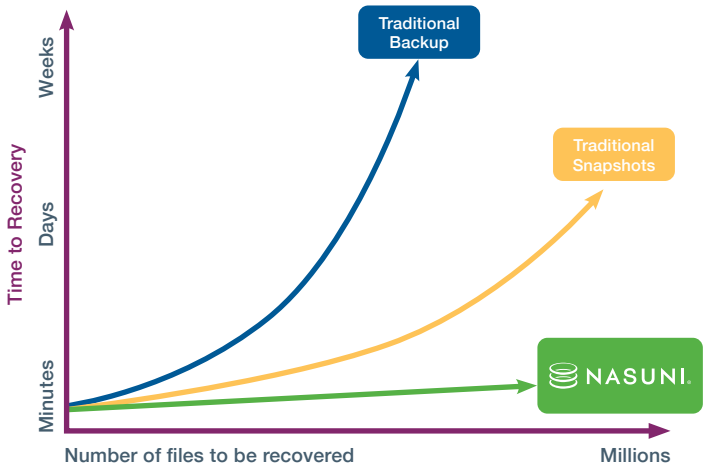
Nasuni Cloud File Storage At-a-Glance

Nasuni provides companies and organizations of all sizes with modern file storage and backup in the cloud that is a simpler and lower-cost approach. This Software-as-a-Service platform was built for the cloud, and is the only solution that couples a global file system with object storage. The combination of Nasuni with Microsoft Azure, Amazon Web Services, or Google Cloud provides unlimited file server capacity on-demand, built-in backup and DR, unlimited snapshots, and file sharing across any number of locations. This unique cloud architecture allows customers to restore very quickly and recover from ransomware attacks.

Immutable, Continuous File Versioning® – The Secret Sauce

You shouldn't have to choose between protecting your company's file data and your budget. Nasuni Continuous File Versioning provides built-in unlimited, read-only snapshots that allows customers to recover files, directories, or entire volumes from ransomware (or other disasters, such as fire or equipment failure) within minutes. From one to millions of files, your organization will be back in business within minutes.

Nasuni Rapid Ransomware Recovery is Fast



Unlike other backup technology that takes more time to recover more files, Nasuni can restore tens of files to millions of files within minutes.

"If it wasn't for Nasuni, **we would have lost 1-2 weeks of work,** but we were up and running in less than a day!"

– IT Director

Recover Millions-of-Files-a-Minute

When a ransomware attack takes place, the clock starts ticking on your ability to detect it, stop it, and restore your data. File shares are everywhere and hold up to 80% of company data, so it's common for them to be the target of an attack. With traditional network-based backup solutions, restoring files can take hours, days, or even weeks. But not with Nasuni. After you've stopped and scoped the impact of the attack with Nasuni's comprehensive file auditing, recovering your files takes just minutes.

Recover Millions-of-Files-a-Minute

Percentage of Nasuni customers surveyed who used Nasuni to recover from a ransomware attack

0

ZERO, the number of Nasuni customers who paid a ransom

"Once we identified which files had been hit, we were able to quickly restore them from the most previous snapshot. **No data was lost, nor was any ransom paid**."

– IT Director

Current RPOs and "Surgical" Recovery

With Nasuni, you simply "dial back" to the very point in time before the attack occurred, without having to move any data. Customers have the flexibility to restore specific files, directories, or even entire volumes to surgically recover just the files that were corrupted, to within as little as 1 minute prior to an attack. Likewise, Nasuni lets you focus on restoring only the files that have been affected vs. an entire volume – realizing even greater time efficiencies. Most users will never know that an attack happened.

Immutable and Infinite Snapshots

Unlike other cloud storage vendors approaches to snapshots, Nasuni's snapshots are unlimited, incorruptible, and can be retained for as long as you need them. Nasuni snapshots are stored automatically in your choice of unlimited, low-cost cloud object storage. This Nasuni advantage is what lets customers rely on a rapid ransomware recovery as part of their ransomware protection strategy.

Cyber Insurance Policies

Many cyber insurance or business insurance policies that cover business interruption or extortion may also cover losses related to a ransomware event. Business without a strong ransomware strategy in place may be considered softer targets than companies that have implemented a multi-wall approach to staying protected, detecting attacks, and recovering. Having a three-tier strategy with rapid recovery included can help with negotiating insurance rates for the right type of policies for your business.

Sources
1. DCIG Whitepaper, 2021 *The Role of Immutable Storage in Ransomware Protection and Recovery.*

NASUNI®

ABOUT NASUNI CORPORATION

Nasuni provides modern cloud file storage, powered by the world's only cloud-native global file system. Nasuni is a cloud replacement for traditional network attached storage (NAS) and file server silos, consolidating file data in instantly expandable cloud object storage at a fraction of the cost. Nasuni also eliminates the need for complex legacy backup and disaster recovery infrastructure, dramatically simplifying IT administration. Nasuni is headquartered in Boston, Massachusetts, USA.