Enterprise Strategy Group™ by TechTarget

RANSOMWARE

Trends, Impacts, and the Role of Data Storage

Scott Sinclair, Practice Director

MARCH 2023

CONTENTS

CLICK TO FOLLOW

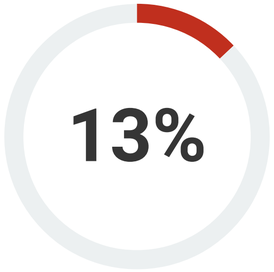
The Pervasive Threat of Ransomware

Ransomware Will Happen Whether You Like It or Not...

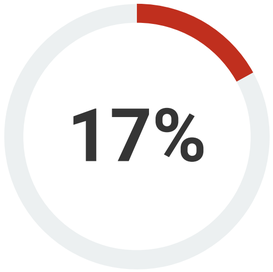
Unlike other disaster scenarios, ransomware is pervasive and a common occurrence for most organizations. According to research conducted by TechTarget's Enterprise Strategy Group, 79% of organizations have experienced a ransomware attack within the last 12 months, with 47% experiencing attacks on a monthly or more frequent basis. Given the frequency of these attacks, ransomware preparedness has become a top priority for businesses.

Ransomware attempts experienced in the last 12 months

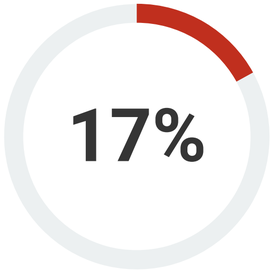
Yes, we've experienced ransomware attacks on **a daily basis**



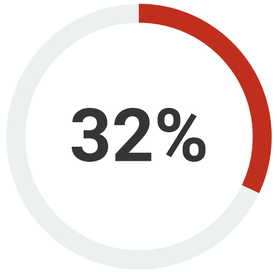
Yes, we've experienced ransomware attacks on **a weekly basis**



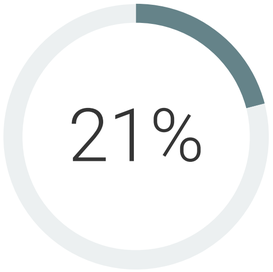
Yes, we've experienced ransomware attacks on **a monthly basis**



Yes, we've experienced ransomware attacks on a sporadic **(i.e., less than monthly) basis**



No, we have not experienced any attempted ransomware attacks in the last 12 months



79%
of organizations have experienced a ransomware attack **within the last 12 months.**

BACK TO CONTENTS

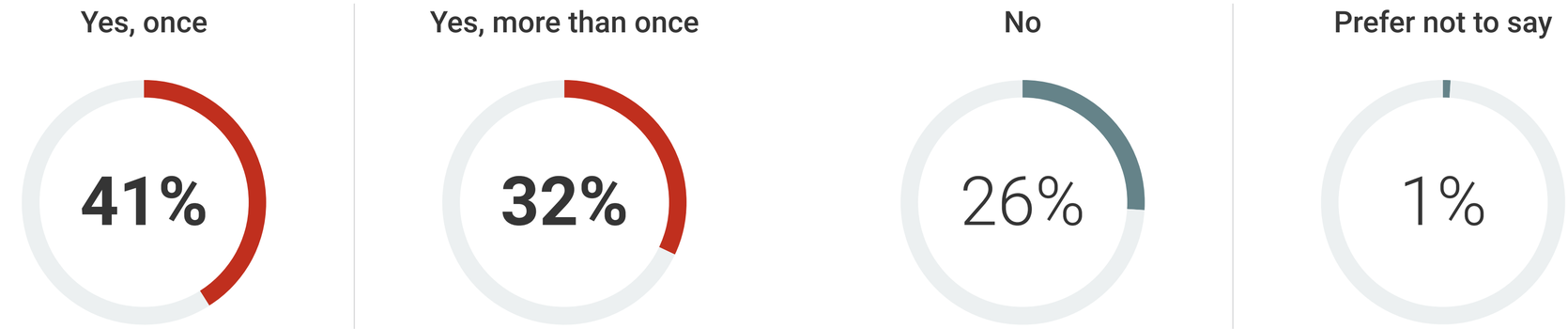
“Even more surprising, however, was that nearly a third of respondents **identified that they were the victim of more than one successful attack.”**

Majority of Targets Victim of a Successful Attack

Of those organizations that identified that they experienced a ransomware attack in the past 12 months, 73% of those organizations reported that the attack was successful, meaning that the attack had a negative financial impact or disrupted business operations.

Even more surprising, however, was that nearly a third (32%) of respondents identified that they were the victim of more than one successful attack, suggesting that for many victims, ransomware is not a “one and done” occurrence; the culprits will often return to the same victims after a successful attack.

Percentage of organizations that experienced a successful ransomware attack



73%
of those organizations reported that **the attack was successful.**

BACK TO CONTENTS

Ransomware Attacks Continue to Impact Operations

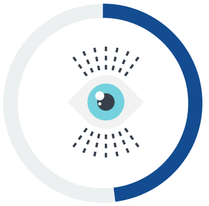
When it comes to the disruption presented by ransomware attacks, the impacts are often multifaceted. The majority of victims of successful attacks experienced a disruption to their operations (51%), while other impacts reported include data loss (50%) and data exposure (49%).

In addition, respondents reported that successful ransomware attacks negatively impacted business value in a multitude of ways, such as having a direct impact on customers and partners (39%), damaging the business's reputation (32%), exposing compliance issues (30%), and subjecting third parties to liability issues (29%).

Impacts of successful ransomware attacks

51%
Operational disruption

50%
Data loss



48%
Data exposure

40%
Financial loss

39%
Direct impact to employees/customers/ partners

32%
Reputational damage

30%
Compliance exposure

29%
Third-party liability

BACK TO CONTENTS

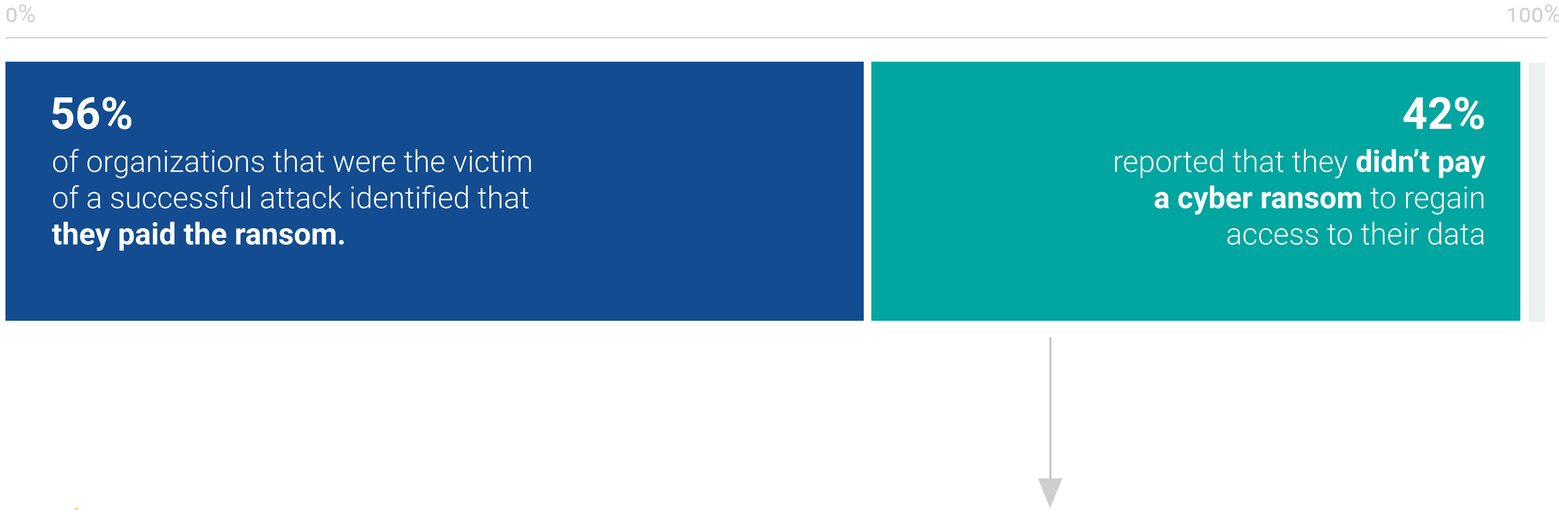
Organizations Are Learning that Paying a Ransom Is Futile

Majority Pay the Ransom

Despite all the information on the cost and risk of ransomware attacks, the dominant response of organizations experiencing a successful attack continues to be paying the ransom. According to Enterprise Strategy Group research, 56% of organizations that were the victim of a successful attack identified that they paid the ransom.

42% reported that they didn't pay a cyber ransom to regain access to their data, which suggests that with the right ransomware protection and mitigation practices and technologies in place, it is possible for organizations to protect themselves. Ransomware attacks will happen, so every organization must have a plan in place for when they do.

Has your organization paid a cyber ransom?



With the right ransomware protection and mitigation practices and technologies in place, **it is possible for organizations to protect themselves.**

BACK TO CONTENTS

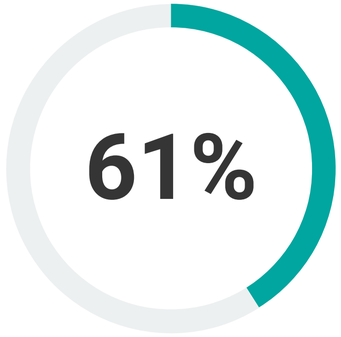
Payment Encourages Further Extortion Efforts

For victims, paying the ransom often does not end the extortion efforts. Of those that paid the ransom, 87% reported experiencing additional extortion attempts or other fees beyond the initial ransomware demand, with 61% of organizations that paid the ransom, identifying that they paid even more money to their attackers.

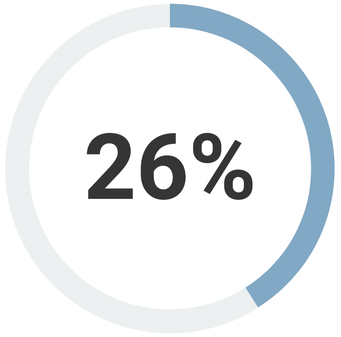
Every organization needs a robust and multifaceted ransomware preparedness strategy that spans readiness, prevention, incident response, recovery, and business continuity.

If you paid a ransom, did you experience an additional extortion attempt?

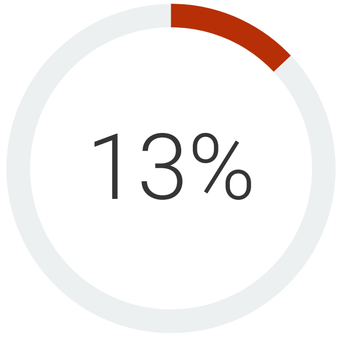
Yes, and we **paid more**

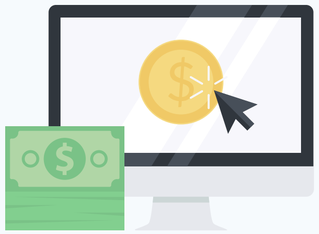


Yes, but we **didn't pay more**



No





For victims, **paying the ransom often does not end the extortion efforts**

BACK TO CONTENTS

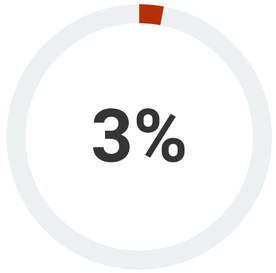
The Data and Storage Implications of Ransomware

Payment Does Not Equate to Recovery

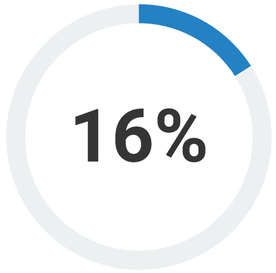
While payment often results in additional extortion demands, payment often does not result in an organization recovering all of its data. More than half of victims incurred 6 hours or more of downtime prior to recovery, and only 14% of ransomware victims that paid the ransom demanded recovered 100% of their data, with 61% reporting that they recovered 75% or less of their data.

In summary, paying the ransom is not a viable strategy to recover data.

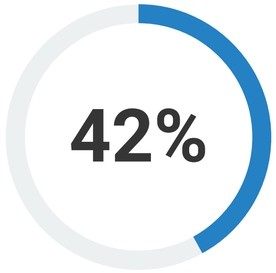
Percentage of data recovered after paying the ransom



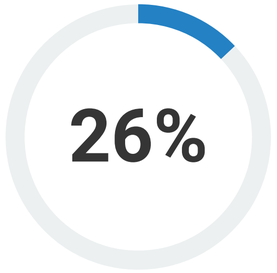
recovered **25% or less** of their data



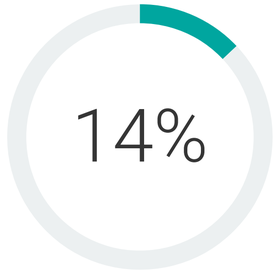
recovered **26% to 50%** of their data



recovered **51% to 75%** of their data



recovered **76% to 99%** of their data



recovered **100%** of their data

61%
report that they recovered **75% or less of their data.**

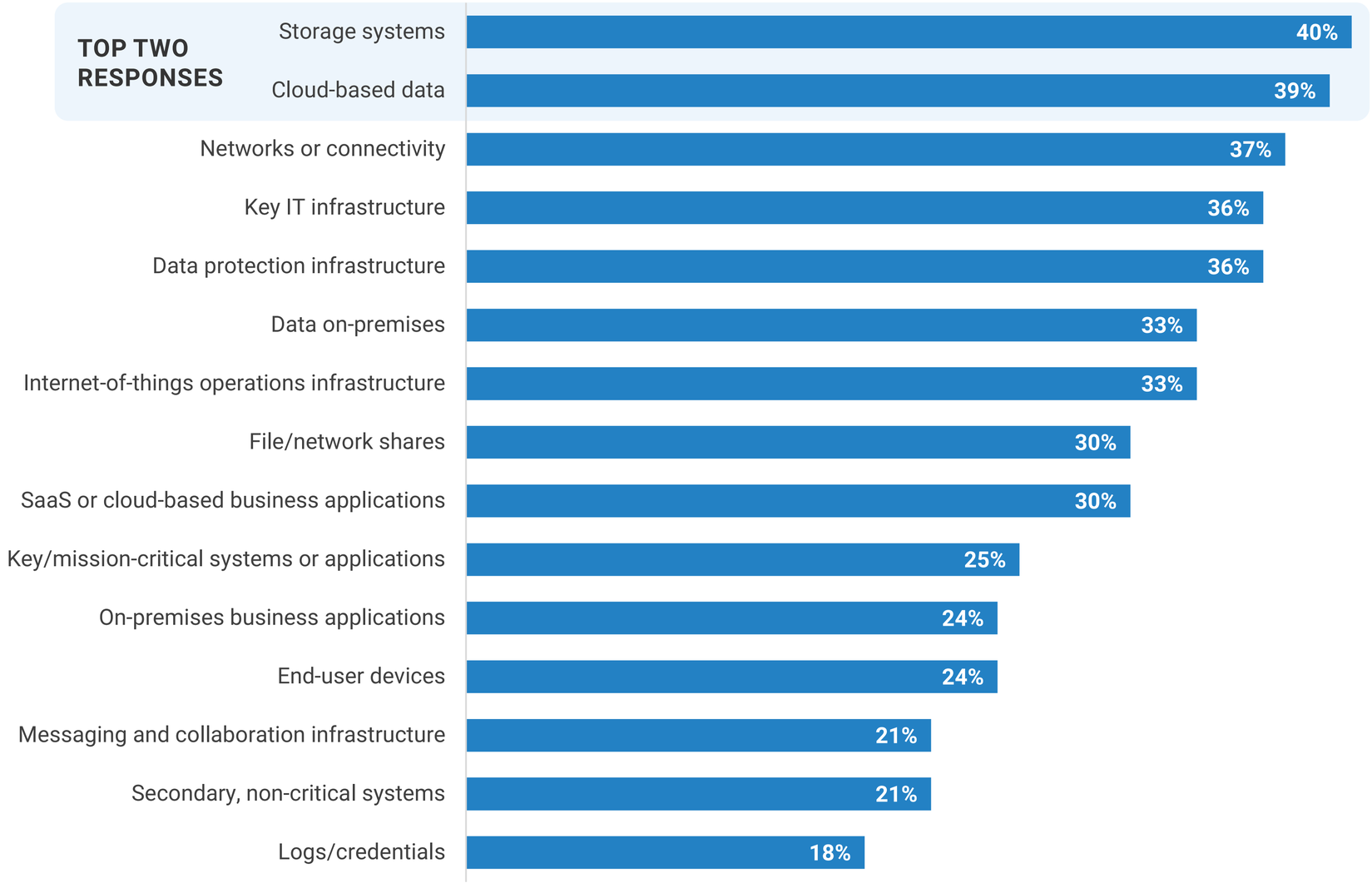
54%
of IT organizations surveyed said it took **6 hours or more** to resume normal business operations after a ransomware attack.

BACK TO CONTENTS

Ransomware Detection and Mitigation Should Be Built into Storage

When it comes to protection, organizations need to take a multifaceted approach. Prevention and detection are essential, but investments in immutability and rapid recovery are just as important.

IT systems and components impacted by successful ransomware attack(s)



BACK TO CONTENTS

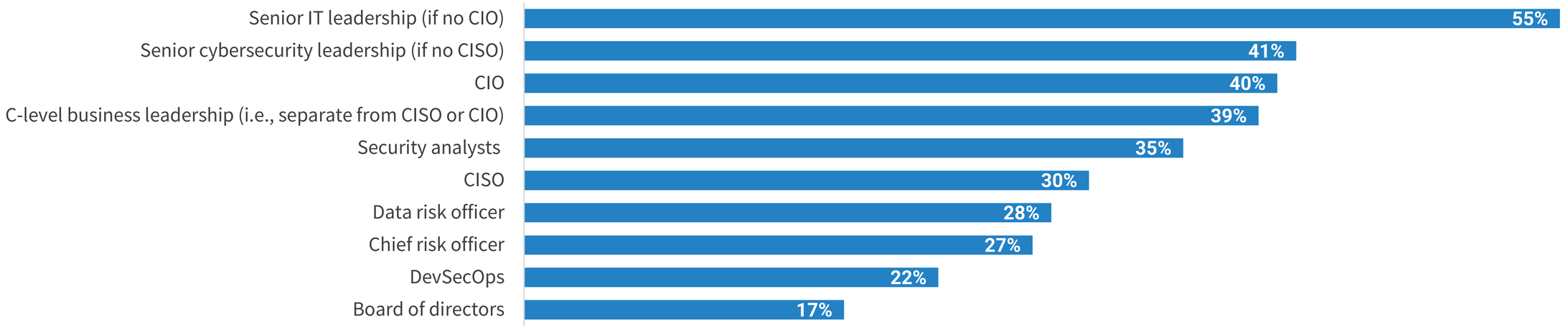
Insights from Nasuni's Customers

Nasuni is a leading file data platform with built-in ransomware protection. The following insights were gleaned from interviews that Nasuni conducted with top customers about ransomware and how it is being handled at the executive level.

- Organizations recognize that mitigation and resiliency are just as important as protection
- IT managers and business executives are starting to see cyber threats in the same way they see natural disasters, war, and other business continuity events, as problems that WILL happen and therefore need preparation not just to prevent but to recover from them.
- Executives are playing an important role in ransomware preparedness.
- Fast backup usually uses a streaming method, which does not allow for prioritizing what files get restored when. This can prevent the business from getting access to critical data right away when it is needed after an attack.
- Solutions like Sharepoint Backup only restore files, not actual sites, resulting in an organization being left with many files but not the original sites those files came from.

Further highlighting the critical importance of ransomware strategy, senior executives and leadership are commonly playing a meaningful role in ransomware strategy.

Stakeholders commonly involved in the organization's ransomware preparedness program



BACK TO CONTENTS

Recovery Insights

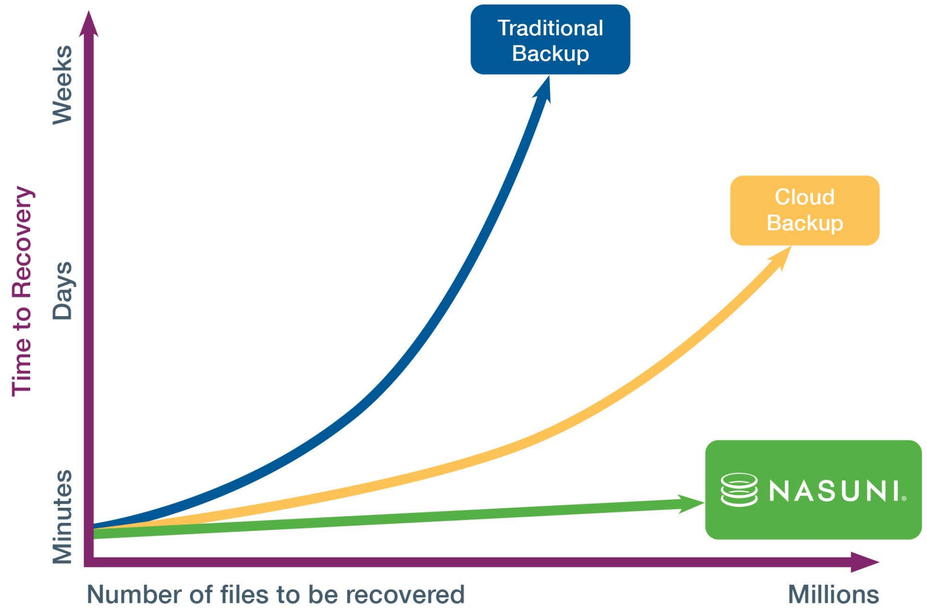
• Overall, the cost of preventing a ransomware attack from being successful is much lower than the combined costs of paying the ransom and all the associated costs of recovery.

• Having a platform that people already know how to use for restores can distribute and speed up your recovery, providing organizational resilience.

• Restoring databases and servers is much faster and easier to do than restoring files. Even if you use SSDs in your backup server, restoring a million small files from your server is going to take a long time.

• Backup requires a few specially trained people – who easily become overloaded during an attack. Choose a solution that allows distributed restores of file data throughout the organization because it's easy and part of the platform.

Nasuni Rapid Ransomware Recovery is Fast



Unlike other backup technology that takes more time to recover more files, Nasuni can restore 10s of files to millions of files within minutes.

The Nasuni platform can restore **1 Million files** in less than a minute

SC AWARDS

2022 SC Media – Best Business Continuity/Disaster Recovery Solution

The CLOUD Awards WINNER 2022-23

2023 The Cloud Awards – Best Cloud DR/Business Continuity Solution

 Source: Nasuni

BACK TO CONTENTS

“Nasuni continues to improve and add value to their product. With the latest Nasuni release we have enhanced our business resiliency strategy by enabling the ability to detect, alert and respond to ransomware attacks, as well as rapidly recover from any possible data encryption.”

- API Group, Inc.

The Nasuni Ransomware Protection Add-on service is designed to proactively defend your file shares, stop attacks, and give you a detailed report of files affected by an attack so that you can rapidly return to productivity when an attack occurs. Combined with the Nasuni File Data platform’s core protection and rapid recovery capabilities, it delivers enhanced ransomware resilience for your file shares, regardless of how much data you have or where it is located.

LEARN MORE

BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.