E-BOOK

Protect, Detect & Recover: The Three Prongs of a Ransomware Defense Strategy for Your Enterprise Files

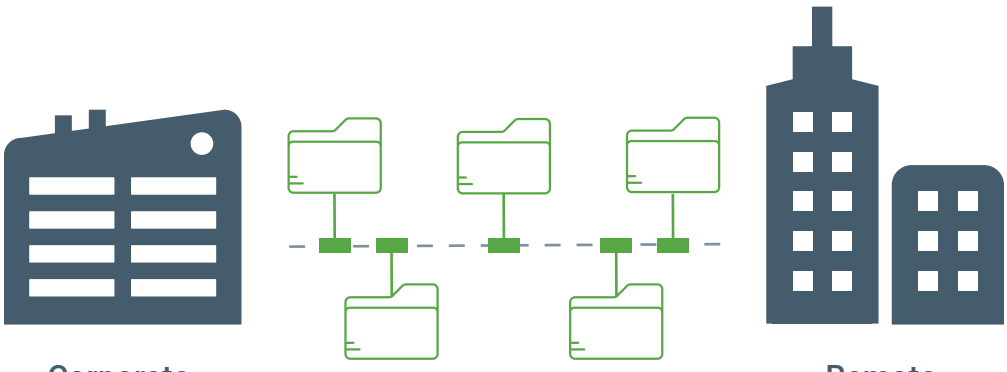
NASUNI®

Table of Contents

> In many cases, organizations have backups of their critical systems but do not regularly check whether these backups can actually be used to restore the system. However, due to configuration drifts, changes in the environment, or even a malicious attack that compromises the backups, they are faced with a reality in which they cannot use the backed-up data to recover."
>
> National Institute of Standards and Technology (NIST), Special Publication on Security Guidelines for Storage Infrastructure. (SP 800-209).

Increasingly, organizations realize that their ransomware strategy should impact their choice of storage solutions and platforms. According to Gartner, unstructured data stores will triple in size by 2026. This growth leads to a second Gartner prediction that by 2025, 40% of all enterprises will require storage products to have integrated ransomware defenses.

As the ransomware problem grows and morphs over time, it's becoming clear that traditional NAS systems and backup solutions are not equipped to provide the kind of rapid recovery that's needed to sustain business operations. A proactive stance towards ransomware should include looking at file data platforms that offer robust detection and recovery capabilities at scale today and quickly adding new advanced protection features without expensive retrofitting existing infrastructure. In this paper, we look at how to apply the three core requirements of your ransomware strategy to file data protection.

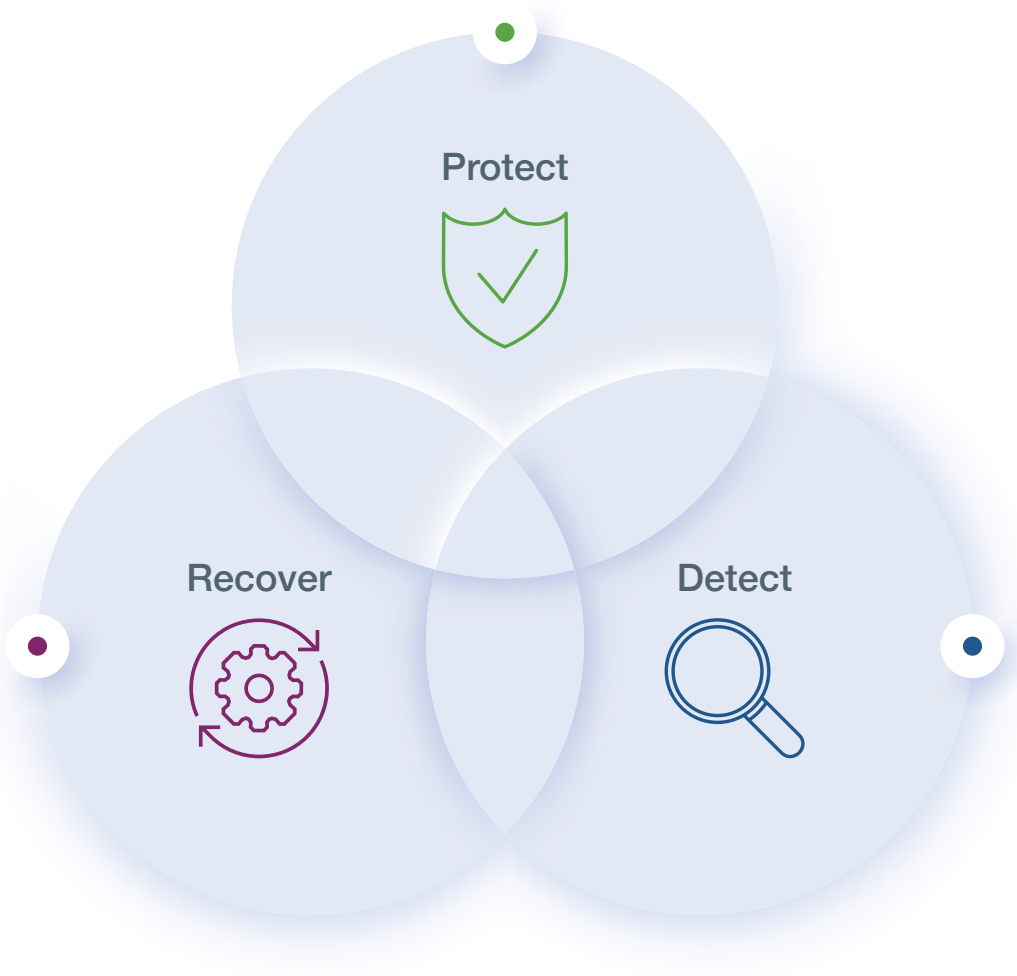


What's your Strategy?

Only 20% of data resides in highly protected, secure databases for most enterprises. The other 80% is unstructured data in file systems scattered across multiple NAS devices and file servers across numerous business locations. And that 80% of data is vulnerable to threats because of its distributed nature and the number of users accessing it every day.

Most organizations understandably have focused their efforts on the protection of ransomware attacks. But more advanced strategies for file storage should also include the ability to detect both latent and ongoing attacks and provide comprehensive and rapid recovery capabilities. Detection of both active and latent attacks, preferably as near to the entry point of the corrupted files/malware, aka "edge detection," is also highly desirable for rapidly containing a potential attack and protecting it from spreading to multiple workgroups and data sets. Rapid recovery is key to minimizing actual file data loss and human productivity.

Three Prong Ransomware Strategy



Protection

Ransomware attacks can be launched – intentionally or not – by internal users who have access to corporate networks. And the average user has access to over 20 million files. All it takes is a single "bad click" to cause catastrophic damage. If a compromised user account has full access, the "blast radius" of the attack can be devastating, exposing sensitive data, causing privacy violations and destruction of intellectual property or more. It is possible to reduce the potential blast radius of an attack by protecting internal or compromised users from having unlimited access to your organization's files.

Therefore, one of the first places to start is the protection of ransomware attacks with a **comprehensive authentication and data access control review**. The focus should be on the authentication of users and limiting their access to files and areas related to them vs. full access to all company data.

Other vital elements of your protection strategy should include:

Zero trust authentication: The adage "trust is earned, not given" can be applied to a zero-trust authentication approach to cloud file access. A solution offering zero-trust authentication ensures a least-privilege model that enforces continuous verification of authorized users before access to files is granted.

Intelligent file indexing: It's critical to index and classify files data to understand their nature and levels of sensitivity better and assess the risk and potential impact on the business if data is seized, encrypted, or exfiltrated. For example, does the data contain PII, does it fall under GDPR, CCPA, or HIPAA compliance regulations? Intelligent file indexing can discover and classify sensitive files within your data stores. The function should offer an initial index to organize files and subsequent scans to reclassify files as necessary.

Specific to your file data platform, look for the following capabilities that support protection:

Smart immutable snapshots: The ability to retain unlimited, incorruptible snapshots for as long as you need them is not a given in most file data platforms. Seek a solution that stores immutable snapshots providing a strong line of protection for your files.

Detailed audit logging: Detailed audit logging trails offer insight into every single open, move, modify, create, and delete – that is, every single operation or permissions change in the file platform environment. Such a capability enables detailed investigation and remediation into events (sensitive data events, service account admin events, failed events) and even specific operations, locations, and users. It helps you keep a pulse on what's happening in your file data environment. Detailed logging is the underpinning for more sophisticated threat analysis by a ransomware solution and can enable even earlier alerts around potential threats.

Detection

Because of its distributed nature, the ability to detect and stop live suspicious activity at the edge of your file storage deployment is a crucial component of a ransomware strategy. Ransomware and advanced persistent attacks are often successful because they slip under the figurative radar.

Look for the following capabilities that support detection:

Edge Detection: Once suspicious activity is detected, whether from an insider threat, bad actor, or bot, that account and the files it has compromised must be isolated and neutralized. Edge detection refers specifically to the ability to detect malicious file behavior early to help isolate and protect further spread to other file servers, users, and storage repositories.

Alerting: The solution should analyze the behavior of the people and machines accessing your organization's data must also alert them to misbehavior and integrate with your detailed audit logs so each compromised file can be recovered.

Identifying suspicious file behaviors: File servers can track large amounts of file activity at scale. Detecting suspicious behavior should be a natural add on to this capability, including the ability to spot:

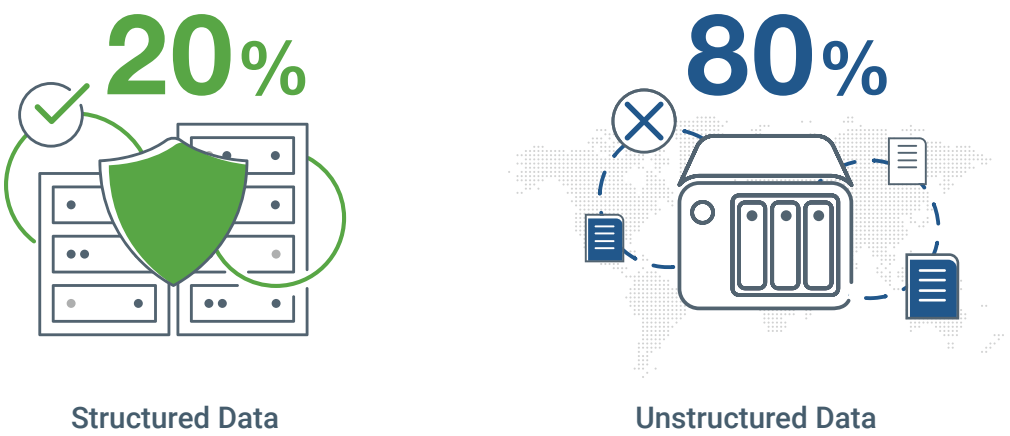
- When a user deviates from their normal behavior
- When an account that is supposed to belong to a human begins behaving in an automated way
- When an account that is supposed to belong to a human begins behaving differently, that might signal ransomware, such as rapid changes or rapid streams of files, encryption of multiple files, or a ransom note.

Ideally, with a more advanced file data platform, these types of events throw a 'red flag' to administrators and trigger automated procedures to respond.

Recover Rapidly, Completely, and Confidently

As organizations' unstructured file data servers grow in volume and become increasingly distributed, security becomes complex; many additional threat vectors, through which attackers can gain access to systems and data, are brought into play.

Unstructured Data is Vulnerable



For most enterprises, only 20% of data resides in highly protected, secure databases, and 80% is unstructured data residing in distributed NAS devices and file servers that are vulnerable to threats.

In this landscape, traditional backups have proven inadequate. Restoring 200,000 files from a single mission-critical snapshot takes about eight hours on average. An organization will have to execute a massive, distributed restore operation across multiple backup servers in a real-world ransomware attack. It could feasibly take many days to regain the entire operation at this rate. After decades of investment in state-of-the-art backup solutions, it may be difficult for your company's culture to admit that backup won't happen fast enough to counter a ransomware impact. Still, the sooner this is acknowledged, the better. Ransomware and malware recovery need their own strategy that focuses on the highly rapid recovery of good data, with both precision and depth to counteract latent infections.

Look for the following attributes in a file storage solution that support the business requirements for recovery:

Rapid Ransomware Recovery: The right file data platform solution can recover millions of files within minutes, at once from multiple physical offices or worker locations. Don't accept hours or days to recover files that have been identified for restoration. After detecting and scoping the attack, your recovery of files should be the shortest operation in your response timeline.

Granular Restores: Many snapshot solutions can only recover an entire volume of files, not specific files or directories. That means users will lose work even if they were not infected because the whole volume gets restored from the previous week's (or worse) snapshot. Look for a solution that has the granularity to restore individual files, directories, or entire volumes as needed.

Immutable snapshots with infinite recovery points: Newer ransomware attacks can employ a time-bomb effect that might take days, weeks, or months to detect. If file backups and snapshots are not retained for long enough, the risk is more significant for losing data and not recovering. Many platforms require expensive add-ons beyond their built-in snapshot limit, and the snapshots themselves are not immutable. Advanced solutions should provide unlimited snapshots, store them in an immutable format, and offer long-term retention at a low cost.

Testable/verifiable: Your file data platform should allow you to create a test location, either a test directory containing files or a test volume with directories and files, to verify the speed and viability of the restore process. Having confidence in your ransomware restore times helps build the business case for investing in a comprehensive ransomware solution and can even lower your cyber insurance premiums.

Simplicity: While not a technology imperative, having a standard file data platform for all your locations and workgroups can also speed time to ransomware recovery. Your IT staff needs to train only on one system, preferably, and conduct a restore process from one central console. With a single, standardized platform, there is less likely that confusion, time zone differences, and human error will exacerbate the attack's impact.

A Best-of-Breed Ransomware Strategy for Your File Data

Cloud-centered solutions can offer scalable, affordable ransomware protection, detection, and recovery for your file storage. Given the rapid growth and distributed nature of unstructured data, it makes sense to evaluate a file data platform that leverages the cloud as a potentially superior alternative to on-premises NAS storage and backup.

Your best-of-breed strategy should include protecting the corruption of data and backups and detecting – and stopping – suspicious behavior. Round out the capabilities of your ransomware protection with a recovery strategy that meets the needs of the business by design.

This three-pronged symphony of Protect, Detect, Recover will enable an organization to:

1. Protect backups and snapshots from being attacked by hackers.
2. Detect suspicious user or account activity, so suspicious activity can be shut down suspicious quickly.
3. Rapidly restore any compromised files, directories, and volumes without lag or downtime.

It's time to elevate your ransomware protection plan to a best-of-breed ransomware strategy.

Related Resources

On-demand webinar
Accelerating the Fight Against Ransomware with the Cloud

Video
Recover over 1 million files in under a minute with Nasuni Rapid Ransomware Recovery

NASUNI

NORTH AMERICA HEADQUARTERS | Boston, MA | +1 (857)444.8500 **UNITED KINGDOM** | London, England | +44 20 3695 7895