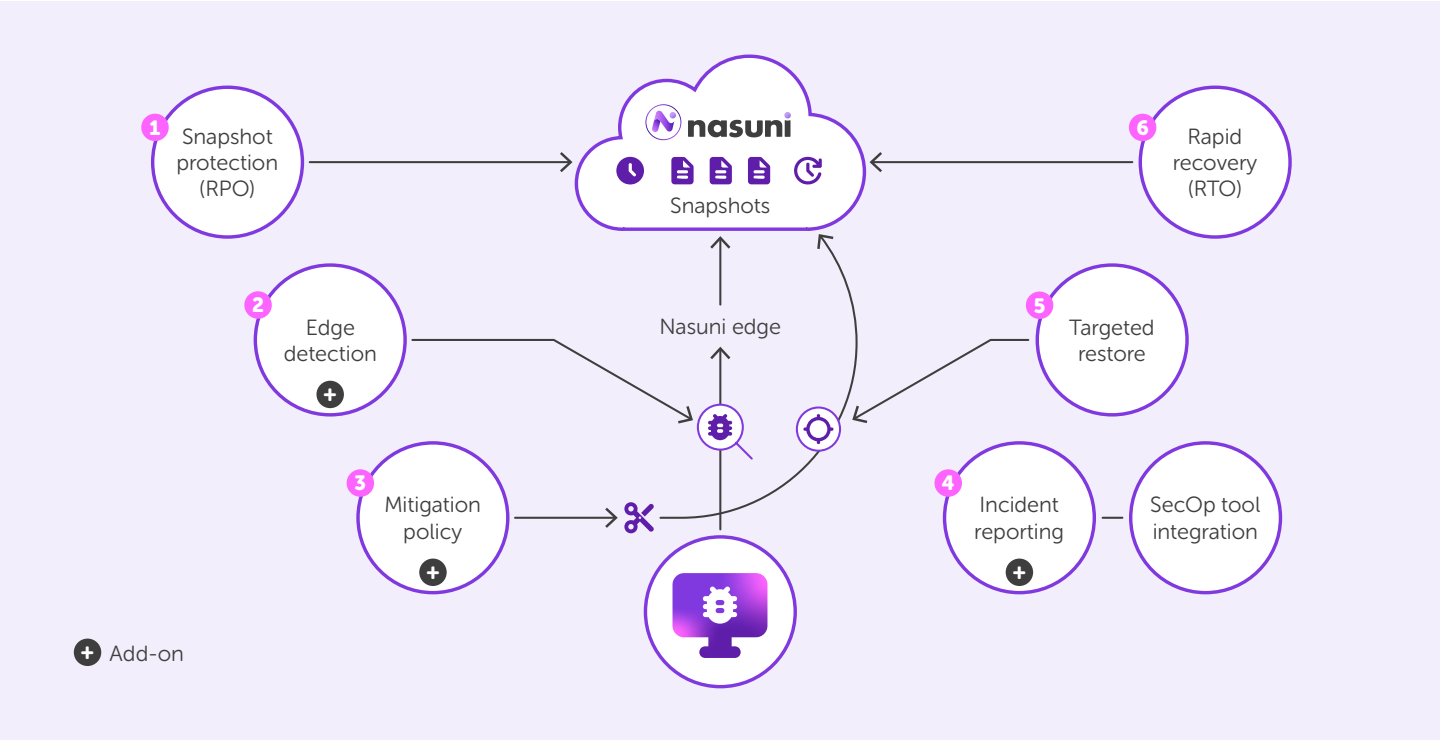

Nasuni Ransomware Protection

Detect, contain, and recover from ransomware in minutes, not days.

/ OVERVIEW

The Nasuni File Data Platform offers a full complement of ransomware services that helps protect and recover file data from ransomware attacks. Detection begins in real time, at the network edge, notifying IT teams of suspicious file patterns, malicious file extensions, and ransom notes across the entire organization. Mitigation policies reduce business impact before an attack can spread, and impacted files are rapidly recovered, bringing affected users back online fast. Comprehensive audit logs and incident reports keep detailed records of threat events to make reporting and the recovery process easier than ever.

/ NASUNI FILE DATA PLATFORM ENHANCEMENT

When combined with Nasuni core platform capabilities, which includes frequent immutable snapshots with infinite versions and Rapid Ransomware Recovery, the Nasuni Ransomware Protection add-on service provides a highly effective and integrated solution for protecting, detecting, and recovering from ransomware.

BENEFITS OF NASUNI

Scale

Nasuni offers a scalable file data platform for growing unstructured data that is easy to implement across petabytes of file data and hundreds of locations.

Savings

Spend less time and resources investigating where an attack happened, how it happened, and the extent of the damage with edge detection and immediate alerts to IT. Detailed logging of ransomware activity and IP addresses across all locations.

Security

With Nasuni, fewer employees will be affected, and they will return to business faster. Always-on file protection with real-time detection of ransomware attacks at the edge and the ability to recover and surgically restore files in minutes, delivers enterprise-grade business continuity that only Nasuni can provide.

PROTECT YOUR FILES FOREVER

Nasuni Continuous File Versioning®

Technology protects an unlimited number of files as immutable objects in low-cost and ultra-scalable cloud object storage provided by Microsoft Azure, AWS, or Google Cloud. This, in turn, provides Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that are measured in minutes to ensure file data is protected without requiring additional backup software.

DETECT THE LATEST THREATS

The Nasuni Ransomware Protection Add-On

Service delivers in-line edge detection of live ransomware attacks using up-to-date intelligence on emerging threats, and analysis of file system behavior to detect known, unknown, and zero-day ransomware variants. E-mails and notifications keep IT on high alert while customizable thresholds filter out false positives and only target real threats.

RESPOND QUICKLY AND AUTOMATICALLY

The Nasuni Ransomware Protection Add-On

Service's mitigation policies automatically stop the attack by quarantining active threats and preventing them from spreading. A comprehensive incident report allows full understanding of the attack details, which are automatically queued into the recovery process with Nasuni Targeted Restore.

RECOVER MILLIONS OF FILES IN MINUTES

Rapid Ransomware Recovery

The last line of defense, enabling the recovery of millions of files with laser precision in minutes accross any number of sites to just moments before the attack. With exact Recovery Point Objectives, down to 1-minute granularity, employees can quickly recover their work and minimize downtime.

Prerequisites

Ransomware Protection is an add-on service requiring Nasuni File Data Platform version 9.9.

/ FEATURES

- **Real-time edge detection** of suspicious incoming file patterns across all office locations, including known, malicious extensions and zero-day attacks
- **Up-to-date intelligence** on the latest ransomware variants
- **Mitigation policies** automatically contain ransomware attacks and prevent them from spreading to other areas of an organization
- **IT notifications** identify all impacted files and users involved with an attack and their source IP addresses while providing convenient alerts through emails and notifications
- **Incident reporting** provides a comprehensive report to fully understand the source, scope, and timeline of the attack
- **Integration** into SecOp tools, like Microsoft Sentinel, CrowdStrike, and Splunk for visibility and coordination of data security across the entire organization

/ EARLY DETECTION AND TARGETED RESTORE

Without knowing exactly when and where an attack has occurred, assessing the damage to determine all the files and users involved can take hours, days, or weeks. Instead, IT is kept on high alert for all malicious ransomware behavior so remediation and recovery can start immediately. With the Nasuni Targeted Restore Process, the system automatically takes care of the investigative work, minimizing the recovery process to just a few clicks.

Before Ransomware Protection Add-On

After Ransomware Protection Add-On

nasuni

Nasuni is the file data foundation for large enterprises where files are mission-critical for both people and AI. The work that drives modern organizations lives in files, the most operationally critical segment of unstructured data, including designs, project documentation, financial and compliance records, media assets, and the countless versions that evolve across distributed teams.

We help our customers manage, protect, and activate that content so IT can continuously reduce cost and risk, while teams and the AI that supports them become more productive through fast, governed access to the right information when and where they need it.

Unlike tools that focus only on data storage, backup, collaboration, or analytics, Nasuni operates at the source of truth for enterprise files, providing the core infrastructure that ensures permissions preserves version history, maintains file relationships, and keeps mission-critical files live, synchronized, and ready for action, serving as the foundation enterprise work depends on.

nasuni.com | sales@nasuni.com | +1.857.444.8500