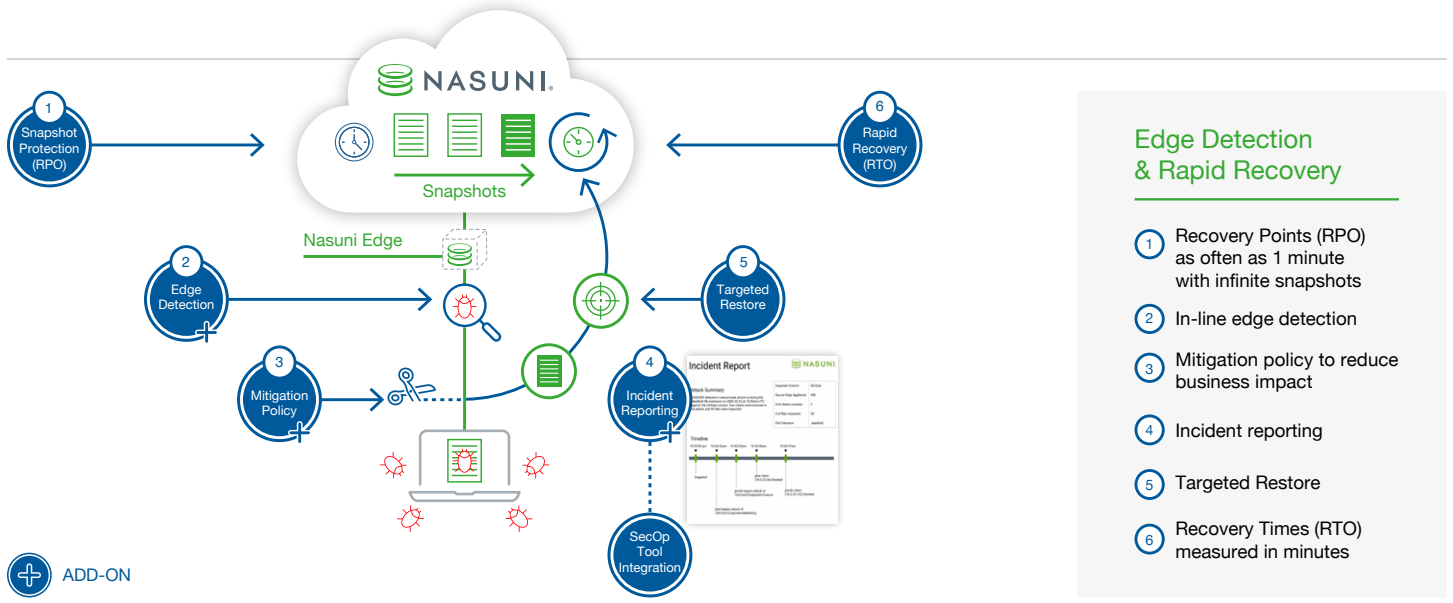


Nasuni Ransomware Protection

Nasuni File Data Platform Add-on Service



Edge Detection & Rapid Recovery

- 1 Recovery Points (RPO) as often as 1 minute with infinite snapshots
- 2 In-line edge detection
- 3 Mitigation policy to reduce business impact
- 4 Incident reporting
- 5 Targeted Restore
- 6 Recovery Times (RTO) measured in minutes



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 at the network edge where users are located, 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 across an office location. Files that were impacted can quickly be recovered, bringing affected users back online fast. Comprehensive audit logs and incident reports keep detailed records of threat events.

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.

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

Business Benefits

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 lets IT scope and identify the sources of attacks significantly faster.

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. 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 stops the attack by quarantining active threats and preventing them from spreading. A comprehensive incident report allows full understanding of the attack details, that are automatically queued into the recovery process with Nasuni Targeted Restore.



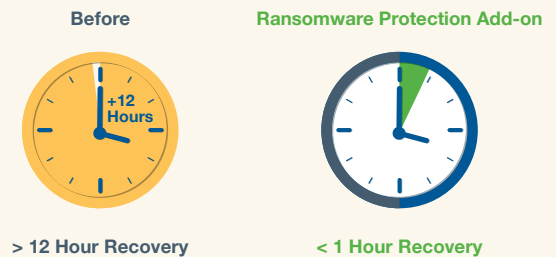
RECOVER millions of files in minutes.

Rapid Ransomware Recovery is the last line of defense, allowing in the worse case, the recovery of millions of files with laser precision in minutes across 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.

Features

- **Real-time Edge Detection** of suspicious incoming file patterns, including malicious extensions and ransom notes, across all office locations.
- **Up-to-date Intelligence** on the latest ransomware variants.
- **Mitigation Policies** automatically contains 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 receiving 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, 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. IT is kept on high alert for all malicious ransomware behavior so remediation and recovery can start immediately, and with the Nasuni Targeted Restore Process, the system automatically takes care of the investigative work, minimizing the recovery process to just a few clicks.



ABOUT NASUNI CORPORATION

Nasuni is a leading file data services company that helps organizations create a secure, file data cloud for digital transformation, global growth, and information insight. The Nasuni File Data Platform is a cloud-native suite of services offering user productivity, business continuity, data intelligence, cloud choice, and simplified global infrastructure. The platform and its add-on services replace traditional file infrastructure, including Network-Attached Storage (NAS), back-up, and DR, with a cloud-scale solution. By consolidating file data in easily expandable cloud object storage from Azure, AWS, Google Cloud, and others, Nasuni becomes the cloud-native replacement for traditional NAS and file server infrastructure. For more information, visit www.nasuni.com.