

The diagram illustrates the Nasuni Edge Security solution architecture, showing a five-step process for detecting, mitigating, and recovering from security incidents.

- 1. Snapshot Protection (RPO):** A blue circle labeled "1" with "Snapshot Protection (RPO)" inside. An arrow points from this circle to a cloud icon.
- 2. Edge Detection:** A blue circle labeled "2" with "Edge Detection" inside. An arrow points from this circle to a magnifying glass icon over a red virus icon.
- 3. Mitigation Policy:** A blue circle labeled "3" with "Mitigation Policy" inside. An arrow points from this circle to a pair of scissors icon.
- 4. Rapid Recovery (RTO):** A blue circle labeled "4" with "Rapid Recovery (RTO)" inside. An arrow points from this circle to a clock icon.
- 5. Incident Reporting:** A blue circle labeled "5" with "Incident Reporting" inside. An arrow points from this circle to a document icon.

The central cloud icon is labeled "NASUNI." and contains a "SNAPSHOTS" section with a clock and document icon. Below the cloud is a "Nasuni Edge" device icon. An arrow points from the cloud to the edge device. The edge device is connected to a laptop icon. The laptop is surrounded by red virus icons, indicating a security incident. The laptop screen shows a red virus icon and a green checkmark, indicating successful mitigation.

The "Incident Report" document icon shows a table with the following data:

| Incident Name | Severity | Status | Resolution |
|---------------|----------|-------------|------------------|
| Incident 1 | High | Resolved | 2023-10-27 10:00 |
| Incident 2 | Medium | In Progress | 2023-10-27 10:00 |
| Incident 3 | Low | Resolved | 2023-10-27 10:00 |
| Incident 4 | High | Resolved | 2023-10-27 10:00 |
| Incident 5 | Medium | In Progress | 2023-10-27 10:00 |

- 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 Recovery Times (RTO) measured in minutes
- 5 Incident reporting for auditing

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.

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.

Business Benefits

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 to quickly start recovering.



RECOVER millions of files in minutes.

Rapid Ransomware Recovery is the last line of defense, allowing in the worst 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. Whether a well-known threat or a new attack, The Nasuni Ransomware Protection Add-on service automatically detects the danger and sends detailed alerts for immediate response.
- **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 receiving convenient alerts through emails and notifications.
- **Incident Reporting** provides a comprehensive report to fully understand the source, scope, and timeline of the attack.

Early Detection and Response

Before



> 12 Hour Recovery

Ransomware Protection Add-on



< 1 Hour Recovery

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. With the Nasuni Ransomware Protection add-on service, IT is kept on high alert for all malicious ransomware behavior so remediation and recovery can start immediately.



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 network-attached storage (NAS) and file server infrastructure. For more information, visit www.nasuni.com.