FAQ for Nasuni® Master Subscription and Services Agreement

The Nasuni Master Subscription and Services Agreement (the “Agreement”) describes unique aspects and functionality of Nasuni products and services and governs the access and use of Nasuni Solutions. Nasuni also provides you with this FAQ to help explain Nasuni products and services, so you have context as you review the Agreement. This FAQ is provided for informational purposes only and does not form part of the contract between the parties.

The Nasuni File Data Platform is comprised of software installed and operating on your premises or in your preferred public cloud and interacting with your third-party cloud object storage, as well as a SaaS component that endows Nasuni software with a highly scalable control path. The Nasuni software tracks the changing relationship among portions of your encrypted data so that entire files do not need to be stored over and over as new changes to (or versions of) files are created. With Nasuni, you control, and you can recover, your files at each stage of their changing lives. All the while, your actual data – your file data objects - stay encrypted in your chosen cloud object storage. As a result, the Agreement is designed to accommodate and describe the unique features of Nasuni products and services, including the fact that we do not have access to the file data that you store in your third-party cloud object storage, except for specific instances where you request and authorize us to do so. We regularly review the Agreement and have tried to create a fair and balanced agreement based on customer feedback and industry accepted positions.

NASUNI FAQ

What am I buying?

Nasuni offers a file data platform and add-on file data services built for the cloud. Powered by the world’s only global file system – UniFS® – the Nasuni File Data Platform consolidates Network Attached Storage (NAS) and file server silos in compatible third-party cloud object storage, delivering massive scale, built-in backup, rapid ransomware recovery, global file sharing, and local file server performance, all for less than the cost of traditional on-premises file infrastructures and other cloud-based solutions. Through the Nasuni platform, customers may access our additional file data services, including Nasuni Ransomware Protection, which provides early detection, alerts, and policies to quickly mitigate ransomware attacks, and Nasuni Access Anywhere, which offers VPN-less file share access, desktop synchronization, external file and folder sharing, and Microsoft Teams integration to make remote office, home office, and mobile workers more productive.

You are responsible for purchasing third-party public cloud storage (e.g., Amazon Simple Storage Service, Microsoft Azure Blob Storage, Google Cloud Storage) from a public cloud storage provider and/or purchasing and deploying third-party private cloud storage (e.g., Dell EMC ECS, IBM Cloud Object Storage) on your own premises to use with Nasuni.

The Nasuni platform includes several software components:

- Nasuni Edge Appliances. Software that is either downloaded and installed on virtual machines deployed on your own virtual infrastructure or in the public cloud of your choice, or pre-installed on dedicated hardware branded by Nasuni and deployed on your own premises. Nasuni Edge Appliances serve two main functions:
  - cache copies of frequently used files from your third-party cloud object storage for high performance file access via standard SMB (CIFS) and NFS file sharing protocols.
  - transmit new files and file changes to your third-party cloud object storage where they are stored as the “system of record.”
- Nasuni Management Console. Software downloaded and installed on virtual machines deployed on your own virtual infrastructure on-premises or in the public cloud of your choice that enables you to provision, monitor, control, and report on your global file estate.
- Nasuni Orchestration Center. Software deployed in the public cloud as Software-as-a-Service (SaaS) that orchestrates and controls features such as Nasuni Global File Lock®, Nasuni Global Volume Manager®, Nasuni Continuous File Versioning® and product licensing. The Nasuni Orchestration Center (NOC) serves as the control path for Nasuni software, and does not process or store customer file data. Nasuni maintains and upgrades this software automatically for its customers.
- UniFS®. UniFS is the first global file system designed to reside and scale natively within public or private cloud object storage. Freed from the “box” constraints of legacy device or cluster-based file systems, UniFS has no limits on file, directory, snapshot, or volume size, and can scale with your chosen third-party cloud object storage. When an IT administrator creates a cloud storage volume in your third-party cloud object storage, UniFS is instantiated within it as the data structure representation of your file data, folders, and metadata.
- Nasuni Access Anywhere Server. Software that is either downloaded and installed on virtual machines deployed on your own virtual infrastructure or in the public cloud of your choice. Nasuni Access Anywhere Servers securely connect remote users to file data cached on Nasuni Edge Appliances, and deliver the capabilities of the Nasuni Access Anywhere addon, including VPN-less file access, desktop synchronization, accelerated data transfer, external file and folder sharing, and Microsoft Teams integration.

What legacy IT infrastructure can Nasuni replace?

Nasuni and your third-party cloud object storage can replace many of the different products and technologies you currently use to store, share, and protect unstructured file data, including:

- Network Attached Storage (NAS) and file servers.
- Backup software, tape and disk-based backup hardware, media servers, and tape and disk media.
- Disaster Recovery (DR) sites, co-location facilities, and duplicate file infrastructure.
- Remote access, file replication, and file transfer infrastructure (e.g. MPLS, WAN acceleration hardware and software for file workloads, FTP, VPN).
- Enterprise file sync and share products such as Box and Dropbox.
- Ransomware and malware detection products.

What use cases does Nasuni address?

Customers use Nasuni for:

- **NAS and file server consolidation.** By migrating on-premises file infrastructure silos to your preferred cloud object storage, enterprise IT organizations can replace capacity planning with infinite, on-demand scale. The refresh cycle of having to purchase new NAS controllers or file servers and migrate data to new hardware every 3-5 years can be broken. By caching copies of actively used files in the nearest on-premises office location or cloud region on lightweight Nasuni Edge Appliances, Nasuni gives users and applications the high-performance file access of on-premises file servers, without a large hardware footprint, and without incurring public cloud storage latency or high public cloud data egress fees.
- **File backup modernization and rapid ransomware recovery.** With Nasuni, customers can eliminate legacy file backup infrastructure and gain instant file recovery to nearly any point in time. Nasuni Continuous File Versioning®

technology captures file changes in every location as often as every few minutes and stores them as immutable read only versions in your preferred cloud object storage. The costs of backup software, media servers, tape and disk media, and off-site storage, and the time needed to manage backup schedules and restore files from disks or tapes can all be eliminated. Should your file shares be attacked by ransomware, you can restore individual files, entire file shares, or entire volumes in minutes to the point in time just before the attack, minimizing the amount of data that needs to be recreated and avoiding costly ransom payouts.

- **Global file sharing and collaboration.** Nasuni streamlines workforce collaboration with file sharing that combines local performance with cloud scale. Nasuni Edge Appliances in multiple on-premises or cloud locations can be mapped to the same cloud object storage volumes, enabling users around the world to concurrently access the same files and shares. File changes from every location are synchronized first to your preferred cloud object storage, then to other Edge appliances that are caching copies of the same files. The secure use of internet links offloads the WAN from file transfer traffic, greatly reducing costs. Nasuni Global File Acceleration® technology uses machine learning to prioritize which locations get updated first for best-in-class file synchronization speeds. Nasuni Global File Lock® technology ensures only one user at a time in any location can edit shared files, helping minimize data losses caused by version conflict.

- **Disaster recovery for files**. Nasuni enables file access to be restored in the event of local or regional disasters in minutes without having to build and maintain separate DR infrastructure. Since Nasuni Edge Appliances only cache copies of actively used data and the “gold copies” of all files are stored in your preferred cloud object storage, no data is lost if disaster strikes. New Edge Appliances can be installed in any safe location – or in the cloud – and rehydrated with the metadata for the actively used files from your preferred cloud object storage, often in less than 15 minutes.

  Files will be brought into the Edge Appliance cache in the background to rapidly restore access to file data as users are browsing the file system.

- **Data analytics.** With all file data consolidated in and accessible through one global file system, enterprises can more easily apply analytics and AI services to gain valuable business insight.

- **Multi-cloud compliance.** Nasuni gives you the choice of using cloud object storage from one or more third party cloud providers to be the authoritative source(s) of all files and metadata. Nasuni also give you the choice of using analytics and AI services from one or more third party cloud providers to help you gain greater insights from your unstructured data.

- **Ransomware mitigation.** Nasuni Ransomware Protection is an add-on service that offers in-line detection of ransomware at each location where a Nasuni Edge Appliance is deployed, alerts that allow administrators to react more quickly to ransomware attacks by leveraging Nasuni’s rapid recovery features, and audits that summarize the date and time of attack, files affected, and users and applications that could be impacted.

- **Remote/hybrid work.** Nasuni Access Anywhere is an add-on service that offers the capabilities needed to support work-from-home. mobile user, and remote office initiatives, with features such as VPN-less file access, desktop synchronization, accelerated data transfer, external file and folder sharing, and Microsoft Teams integration.

Does Nasuni store my data?

No. Your third-party cloud object storage stores your data. Nasuni provides a global file system and ancillary file data services that add value on top of third-party cloud storage.

Can Nasuni see my data?

No. Nasuni does not have access to your data stored in your third party cloud storage, unless you ask us to provide certain professional services, such as data migration services, or support to you in the environment where you keep unencrypted data.

How does Nasuni secure my data?

Each Nasuni Edge Appliance uses random AES-256 encryption keys - keys that you control - to encrypt your data before sending it to your third-party cloud object storage. By encrypting your data both in transit and at rest, Nasuni helps protect your data from being accessed by anyone outside your organization unless you choose to allow it. This also prevents Nasuni and your third-party cloud storage providers from being able to “see” your data.

How does Nasuni enable compliance with data sovereignty policies?

Nasuni’s relationships with third party public and private cloud storage that you use to store your unstructured file data helps you comply with data sovereignty and residency policies. Public cloud storage solutions enable you to choose the region in which your storage volumes or “buckets” will be created. Nasuni Edge Appliances can be configured to connect and transmit data only to these public cloud storage volumes, helping to protect your data from leaving that region. Private cloud object storage solutions are deployed on-premises, enabling you to choose the office location and region in which your storage volumes will be created. Nasuni Edge Appliances can be configured to connect and transmit data only to these private cloud storage volumes, helping to protect your data from leaving that region.

How does the Nasuni software help backup and recover our file data?

Nasuni Continuous File Versioning® is a next-generation snapshot technology that continuously captures file changes made on Nasuni Edge Appliances in all locations and stores them in Write Once Read Many (WORM) format in your own third party cloud object storage. By creating a scalable version history of every file, the Nasuni software, together with your cloud object storage, eliminates the need for traditional file backup/archive software and hardware. The Nasuni software also helps you achieve up to a 1-minute Recovery Point Objective (RPO) and up to a sub-minute Recovery Time Objective (RTO). For fast self-service file recovery, files can be restored by end users using Nasuni’s integration with the Windows Explorer Previous Versions feature. For fast IT-assisted file recovery, files can be restored to any Nasuni Edge Appliance using the Nasuni Management Console.

How does the Nasuni software help mitigate ransomware?

Traditional file backup and snapshot technologies do not provide sufficient protection against ransomware for several reasons, all of which result in many enterprises being forced to pay ransoms to unlock their files:

1. **Recovery points are inadequate.** Because of the time it takes to copy data from primary file storage to backup file storage and the cost of separate primary, on-site, and off-site copies, your recovery point for enterprise file shares will likely be, at best, once a day. That means up to 24 hours’ worth of data may be lost.
2. **Recoveries times are long.** Copying data from backup tapes or disks back to primary file storage can take days or even weeks depending on the amount of data. This is often too long to ensure continuous business operations.
3. **Recoveries overwrite unaffected file data.** Restoring snapshots will return the entire file system back to a previous point in time. User and application files that were not affected by ransomware will also be overwritten, resulting in an unnecessary loss of data.
4. **Backup storage can be infected.** Ransomware may also infect the backups, so there may not be a “safe” version of a file to restore.
5. **Attacks are discovered too late**. Ransomware often sits undetected for days or weeks. Once finally discovered, restoring files back to a safe point in time may overwrite weeks’ worth of valuable data.
6. **Impact is not well-understood or documented.** Determining which users and applications are affected by an attack and providing proof of the root cause and all remediation steps taken is difficult or requires extensive manual effort.

Nasuni’s modern, cloud-native approach to file data services overcomes each of these inadequacies, enabling you to recover your file data quickly and avoid paying any ransom.

1. **Recovery points can be as often as every few minutes.** Nasuni’s patented Continuous File Versioning technology captures file changes made on Nasuni Edge Appliances in all locations as often as every few minutes and stores them as unique versions in your cloud object storage. Using object storage and storing only deltas makes the storage of every file version cost-effective, and enables you to recover to the minute before the ransomware attack occurred, minimizing data loss.
2. **Recovery times are short.** Since Nasuni stores the “gold version” of all files in your cloud object storage, restoring previous versions does not require copying files back from backup storage. All you have to do is select an earlier version

of a file or file share, and the UniFS file system pointer in your cloud object storage is simply dialed back. This video shows how Nasuni can restore 1 million files in less than 60 seconds: https://www.nasuni.com/video/nasunirapid-ransomware-recovery/

3. **Recoveries can target only affected files.** Nasuni's combination of audit logs and selective file restore enables you to recover individual files, entire file shares, or entire volumes without overwriting files that were not affected by ransomware.
4. **There is always a safe backup version.** Nasuni stores every snapshot in your cloud object storage as an immutable, WORM (Write Once Read Many) version. Once written, it can never be changed. This model helps ensure that ransomware cannot infect previous versions, and that you always have a safe version of a file that can be restored.
5. **Attacks are detected immediately.** Nasuni Ransomware Protection detects ransomware as soon as it appears at any edge location and immediately alerts administrators, so safe versions can be restored right away, before days or weeks of other file changes are lost.
6. **Impact reports are automatically generated**. Nasuni Ransomware Protection creates reports that document the date and time of attack, files affected, and users and applications that could be impacted, making it easier to comply with internal audits and cybersecurity policies.

How does the Nasuni software help provide disaster recovery (DR) for our file data?

Because the Nasuni software enables use of your third-party cloud object storage as the back-end repository for all files and metadata, it can take advantage of the geo-redundancy options and multiple data copies provided by your cloud object storage solution. If a site or regional disaster should occur, Nasuni Edge Appliances can be instantiated in any safe location – or in the cloud itself – and rehydrated with the metadata for the actively used files from your cloud storage. Users can be redirected to the new Nasuni Edge Appliances and can instantly view and traverse the file system as copies of the files themselves are brought into the appliance cache in the background. As a result, you can restore rapid access to your file data – often in less than 15 minutes – without the high costs of dedicated DR sites and frequent DR scenario testing.

How does Nasuni help comply with legal or regulatory standards?

Because the Nasuni software enables use of your third-party cloud object storage such as Microsoft Azure Blob, Amazon S3, and Google Cloud Storage as the back-end repository for all of your unstructured file data, the compliance certifications and documentation of your cloud storage provider apply to your unstructured data. The Nasuni Orchestration Center SaaS component of the Nasuni software is hosted in AWS, so AWS compliance certifications apply to this control path service.

- **Microsoft Azure**: https://docs.microsoft.com/en-us/azure/compliance/, https://azure.microsoft.com/enus/overview/trusted-cloud/compliance/
- **AWS:** https://aws.amazon.com/compliance/
- **Google Cloud:** https://cloud.google.com/security/compliance/

In addition, an independent auditor has conducted an ISO/IEC 27001 assessment of Nasuni, which included Nasuni's compliance with the ISO/IEC 27001:2013 clauses and relevant annex controls, and covered all in scope personnel and facilities. Nasuni achieved ISO 27001 certification in January 2022 and a copy of its ISO Certificate of Registration and additional information regarding Nasuni's security is available at trustcenter.nasuni.com.