TECHNICAL WHITE PAPER

Nasuni File Data Platform Security Model

Storing data in public or private cloud object storage presents new and exciting capabilities for enterprises. This modern approach also changes the risk profile for data storage. Implemented correctly, the use of cloud object storage can improve data security. The Nasuni® File Data Platform is designed to leverage cloud object storage as an economical, durable, and infinitely scalable repository for unstructured data.

March 2024

Table of Contents

Introduction 3

Section 1. Strong Encryption 3

Section 2. Separation of the Control Path and Data Path 5

Section 3. Preventing Version Conflict and Data Overwrites 8

Section 4. Rapid Disaster Recovery 8

Section 5. Immutable Snapshots with Air-Gap Protection 9

Section 6. Secure Telemetry for Customer Support 10

Section 7. Nasuni Trust Center Security Portal 10

Section 8. Ransomware Protection 10

Section 9. Additional Security Measures 10

Summary 13

Introduction

Storing data in public or private cloud object storage presents new and exciting capabilities for enterprises. This modern approach also changes the risk profile for data storage. Implemented correctly, the use of cloud object storage can improve data security. The Nasuni® File Data Platform is designed to leverage cloud object storage as an economical, durable, and infinitely scalable repository for unstructured data.

To help ensure the security of data stored by Nasuni in cloud object storage, Nasuni has developed a robust security model that combines strong encryption and local authentication with the native capabilities of top-tier cloud storage solutions such as Amazon Simple Storage Service (Amazon S3), Microsoft Azure Blob object storage, and Google Cloud Storage.

For enterprises that seek the benefits of cloud scale and agility without exposing data to a public cloud provider, Nasuni also integrates with leading private cloud storage solutions such as Dell EMC ECS, Hitachi Content Platform, IBM Cloud Object Storage, Scality RING, Pure Storage FlashBlade, Nutanix Objects, NetApp StorageGRID, and Cloudian Hyperstore. Nasuni cleanly separates its data path from its control path such that file system data and metadata can be stored solely in these private cloud storage solutions, and public cloud services are used only for orchestration and management. By taking this architectural approach, Nasuni helps enterprises ensure that no file data is ever transmitted outside their security perimeters.

Whether you deploy the Nasuni platform in a public cloud-only, hybrid cloud, or private cloud configuration, you can store, protect, synchronize, and collaborate on file data at an unprecedented scale, with lower cost and complexity, and without compromising security.

This white paper provides an overview of Nasuni File Data Platform security model, and explains how strong encryption, the separation of control path and data path functions, and other security measures help ensure that file data is always secure regardless of which deployment model is chosen.

Nasuni Access Anywhere is an add-on service to the Nasuni platform that offers high-performance, VPN-less file share access for remote and hybrid users, integrates an organization’s file shares with Microsoft Teams, and provides productivity tools such as desktop synchronization and external file and folder sharing to enhance user productivity and provide access to files seamlessly from anywhere on any device. For an overview of how Nasuni Access Anywhere extends the security model of the Nasuni platform with its own enterprise-class security elements, see the Nasuni Access Anywhere Security Model technical white paper.

Section 1. Strong Encryption

The Nasuni platform security model begins with a foundation of strong encryption. Nasuni Edge Appliances periodically send new and changed file data to cloud object storage, while keeping copies of the active data in-cache for high-performance access. As with traditional NAS and file servers, Nasuni Edges offers access to file data through standard SMB (CIFS) and NFS file-sharing protocols.

Unlike traditional NAS, however, each Nasuni Edge uses random AES-256 encryption keys to secure all file data and metadata before sending it to private or public cloud object storage, ensuring that the data is encrypted both in transit and at rest. In addition, the customer controls the asymmetric main key that is used to encrypt the AES-256 key.

This approach helps ensure that no one outside the customer’s organization can ever access data unless the customer chooses. This approach also prevents Nasuni and cloud storage providers from being able to “see” the data.

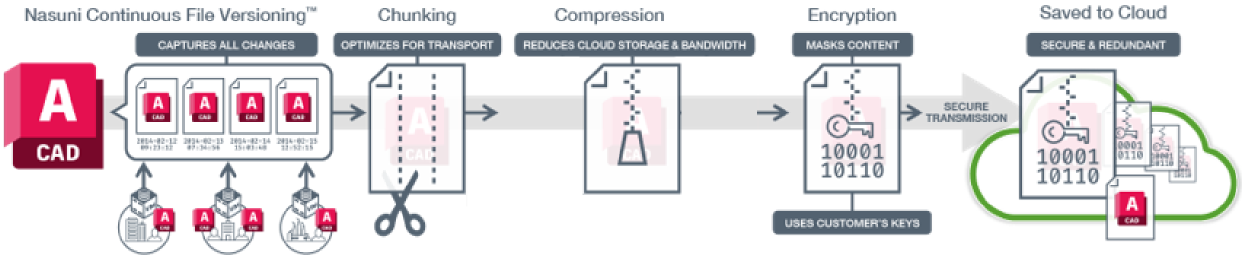

Figure 1: Nasuni uses randomly generated AES encryption keys and customer-controlled main keys to secure data in transit to and at rest in cloud storage.

Nasuni employs the non-proprietary OpenPGP protocol for public key-based encryption and decryption. OpenPGP establishes a framework for combining widely available security algorithms into a secure system. The OpenPGP community continuously enhances this open standard and source code using an extensive and thorough review process.

OpenPGP combines symmetric and asymmetric encryption technologies that not only protect the data but do so without compromising performance. Using fast symmetric encryption to encrypt the data and slower asymmetric encryption to encrypt the keys enables data to be encrypted efficiently and at a high level of granularity.

OpenPGP also specifies several important details, including proper salting (inputting random bits to a one-way cryptographic hash function) and cipher modes. OpenPGP's cipher feedback (CFB) mode also avoids the drawbacks of less secure techniques, such as Electronic Codebook (ECB).

Along with OpenPGP, Nasuni employs the AES-256 standard for symmetric encryption. Advanced Encryption Standard (AES) is the first publicly accessible and open encryption standard approved by the US National Security Agency (NSA) for top-secret information.

In addition to encrypting the data itself, Nasuni Edges also encrypt metadata in transit and at rest. This means that no identifiable information, such as file names or timestamps, is decipherable after it leaves the point of origin. Encrypted file metadata includes the file name, file size, timestamps, access control information, and location within the directory tree.

Nasuni's encryption technology also includes:

- **Random session keys** minimize the possibility of detecting patterns and reverse-engineering the encryption keys.
- **Transport Layer Security (TLS)** that provides end-to-end confirmation of data security and integrity.
- **Built-in tamper alarms** based on OpenPGP's Modification Detection Code (MDC), to detect any attempted tampering with data.

Section 2. Separation of the Control Path and Data Path

The Nasuni platform separates the control path and data path so that you can keep file data inside your organization's security perimeter if you cannot leverage the on-demand scalability, durability, and economics of the public cloud.

Section 2.1 Control Path Components

The Nasuni platform is a software-defined solution that includes an AWS-based cloud service as the "control path" for scalable management and orchestration of your global file infrastructure. The two main control path services are the Nasuni Orchestration Center (NOC) and the Nasuni Management Console (NMC).

Section 2.1.1 Nasuni Orchestration Center (NOC)

The Nasuni Orchestration Center (NOC), which has earned the "AWS Well-Architected" designation for its secure and efficient use of AWS services, provides scalable orchestration, and control functions for the Nasuni platform.

The NOC monitors the interactions between cloud object storage and Nasuni Edge appliances to help Nasuni support its customers. The NOC also coordinates the interactions among Nasuni Edges, allowing customers to perform management functions once and apply them to some or all Nasuni Edges through the Nasuni Management Console (NMC).

All information exchanged between the NOC, the NMC, and Nasuni Edges is encrypted with random AES-256 keys. Customers control the asymmetric key used to encrypt the random AES-256 key. All communications occur over the Secure Sockets Layer (SSL) utilizing port 443. This creates a Virtual Private Network (VPN)-like environment between the enterprise and the NOC and prevents any customer file data from being available to Nasuni or any public cloud provider. No enterprise file data is ever included in these transmissions.

Section 2.1.2 Nasuni Management Console (NMC)

The Nasuni Management Console (NMC) enables all Nasuni Edge appliances in all locations to be managed from a single, centralized web-based interface.

The NMC runs as a virtual machine hosted in your environment. To support the management of remote Nasuni Edges, cloud-based message queuing with Amazon Simple Queue Service (Amazon SQS) is used. The cloud-based message queue ensures that changes made to an unavailable Nasuni Edge will be delivered the next time it is available.

All management communications are encrypted using random AES-256 keys, creating a VPN-like connection between the NMC and Nasuni Edges. Only configuration and management information is shared. No enterprise file data is ever included in these transmissions.

Section 2.2 Data Path Components

The data path for the Nasuni platform is the direct path that file data and metadata takes from the instant it is created at the edge to the point it is stored in private or public cloud object storage. The two main data path components are the UniFS® global file system and the Nasuni Edge appliance.

Section 2.2.1 UniFS

Nasuni's UniFS® global file system is an XML representation of your file and folder structure, along with all associated metadata. UniFS gets fully instantiated in your public or private cloud storage when you create a Nasuni volume from the NMC. UniFS is the end of the data path; when your file data is stored in your preferred object storage, it resides in the UniFS secure, encrypted format.

Section 2.2.2 Nasuni Edges

Nasuni Edges are lightweight virtual machines or Nasuni hardware appliances that replace traditional Windows file servers and NAS devices. Nasuni Edges are the beginning of the data path, and they perform several key functions:

1. Present SMB (CIFS) shares and NFS exports, enabling existing drive mappings, applications, and scripts to continue to read and write data as they do today with traditional file servers and NAS.
2. Apply data reduction techniques and "chunk" the files into objects before transmitting them to cloud object storage, so that cloud object storage capacity is needed to store data.
3. Encrypt data using randomly generated AES-256 encryption keys that are further masked by a customer-controlled asymmetric encryption key so that no external party can gain access to the data while it is in transit to or at rest in cloud object storage.
4. Cache copies of the active files and file system metadata to provide high-performance file access to users and applications, minimize latency, reduce egress charges (when public cloud storage is used), and reduce WAN traffic (when private cloud storage is used).

Section 2.3 Data Path Scenarios

The separation of the data path and control path enables you to implement the Nasuni data path in three ways:

- On-premises-only, with the UniFS® global file system instantiated in private cloud object storage and Nasuni Edges deployed in any office that requires high-performance access to actively used files.
- Hybrid cloud, with the UniFS global file system instantiated in public cloud object storage and Nasuni Edges deployed in any office that requires high-performance access to actively used files.
- Public cloud-only, with the UniFS global file system instantiated in public cloud object storage and Nasuni Edges deployed in the cloud. This assumes latency and bandwidth to the cloud are sufficient to provide direct, in-cloud access to actively used files.

Section 2.3.1 On-Premises (Private Cloud) Data Path

In this scenario, Nasuni stores all file data and file system metadata as encrypted objects in private cloud object storage.

The control path takes advantage of AWS public cloud services to provide orchestration and management functions at a global scale.

However, in this configuration, the data path is entirely on-premises, and no file data is ever transmitted outside the enterprise security perimeter.

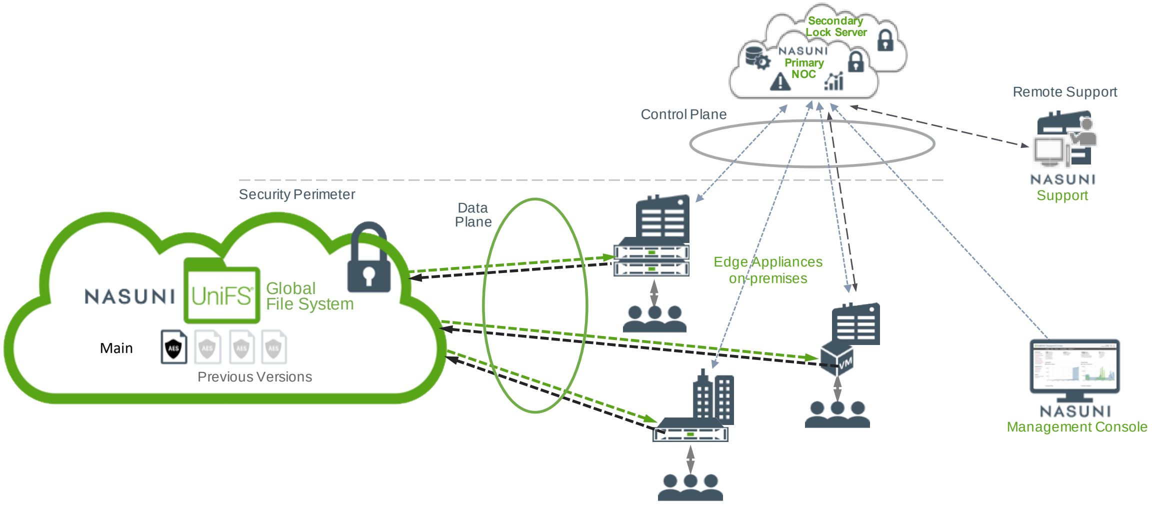

Figure 2A - On-Premises (Private Cloud) Data Path: Nasuni encrypts and stores all file data and metadata in on-premises object storage (the data path), while leveraging AWS public cloud services to provide orchestration and management functions at global scale (the control path). Nasuni Edges are deployed on-premises to provide cached access to data from within the customer's security perimeter.

2.3.2 Hybrid Cloud or Public Cloud-Only Data Path

In this scenario, Nasuni stores all file data and file system metadata as encrypted objects in public cloud object storage. Nasuni Edges may be deployed on-premises in a hybrid cloud configuration to cache copies of active files locally for high-performance access. Or, the Nasuni Edges may be deployed in the public cloud as part of a "cloud-only" data path configuration.

The control path takes advantage of AWS public cloud services to provide orchestration and management functions at a global scale.

In this configuration, the data path extends outside the enterprise security perimeter. However, all file data and metadata are encrypted using random AES-256 encryption keys that are themselves encrypted by a customer-controlled main key, ensuring that the data is secure in transit and at rest in cloud object storage. It is not visible to anyone without the main key, including Nasuni or the cloud storage provider.

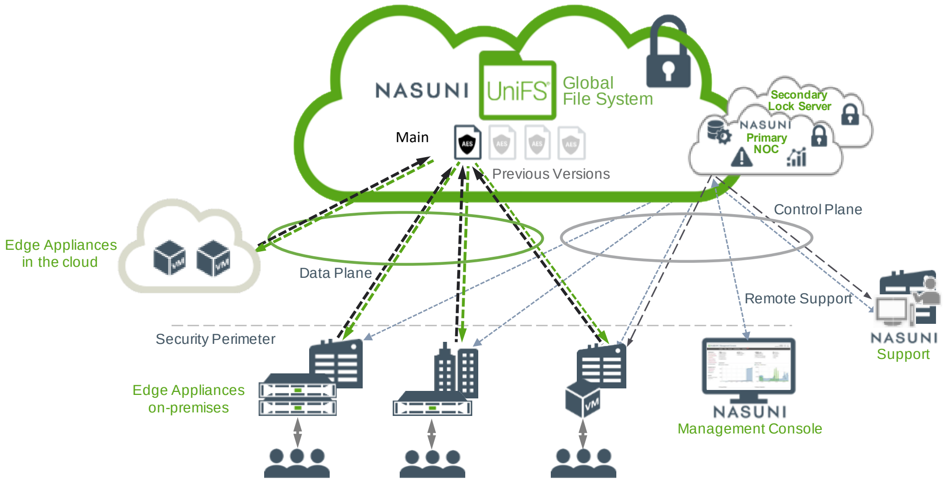

Figure 2B - Hybrid Cloud or Public Cloud-Only Data Path: Nasuni encrypts and stores all file data and metadata in public cloud object storage (the data path), while leveraging AWS public cloud services to provide orchestration and management functions at global scale (the control path).

Section 3. Preventing Version Conflict and Data Overwrites

Nasuni is unique in its ability to provide shared access to files with locking that is supported across the enterprise, independent of file system size or the number of locations. Nasuni Global File Lock⍰ enables users in multiple locations to actively work on the same file at the same time without version conflict by ensuring that only one user at a time can save changes.

Nasuni Global File Lock, implemented as part of the Nasuni Orchestration Service (NOC), is a highly available, elastic AWS cloud service with redundant lock servers and built-in failover. This architectural approach of making Global File Lock independent of any single device or server enables it to scale across the enterprise without using additional resources or internal WAN resources.

Snapshot locking is handled in a similar way for the short time when a volume snapshot is being written to cloud storage, or when data is being pruned to meet data retention policies. This provides a scalable way to make sure that two Nasuni Edges with changes to the same volume do not write snapshots at the same time.

Section 4. Rapid Disaster Recovery

Nasuni Edges can be rapidly restored for fast disaster recovery (DR), a major advantage over traditional file servers and NAS. If a Nasuni Edge is ever rendered inoperable or is destroyed, enterprise file data can be quickly and easily recovered by instantiating a new Nasuni Edge hardware appliance or VM in a safe location or in the cloud and reconnecting it to your cloud object storage. All that's required is the customer-controlled main key and a connection to the object storage.

To facilitate this fast file system restoration, Nasuni Edge configuration information is stored encrypted in the NOC. No configuration information is accessible to Nasuni or any cloud provider because the data is encrypted with the key under the customer's control. No file data is ever included in these transmissions.

Section 5. Immutable Snapshots with Air-Gap Protection

Nasuni Continuous File Versioning� is advanced snapshot technology that captures new files and file changes from each Nasuni Edge based on the schedules that you set up. Snapshots can be as frequent as every minute, providing recovery points that are unequaled by traditional file backup and snapshot technologies.

Snapshots are compressed, encrypted (as described in 1. Strong Encryption), and chunked, then transmitted to your preferred cloud object storage where they are written as immutable, Write Once Read Many (WORM) versions. Once written to object storage, they can never be changed.
The combination of snapshot immutability and frequency ensures that there is always a healthy, recent version of a file, directory, file share, or volume that can be restored after an accidental deletion, ransomware attack, or file corruption.

Nasuni's use of cloud object storage as its repository also provides built-in "air gap" data protection, since each of the major public cloud providers automatically copies objects across zones and regions based on the durability level that you select. For example, if you use Azure Blob GRS Cool with Nasuni, Azure will copy your file data and snapshots synchronously three times within a single physical location in the primary region, then copy your file data and snapshots asynchronously to a physical location in a secondary region that is hundreds of miles away from the primary region.

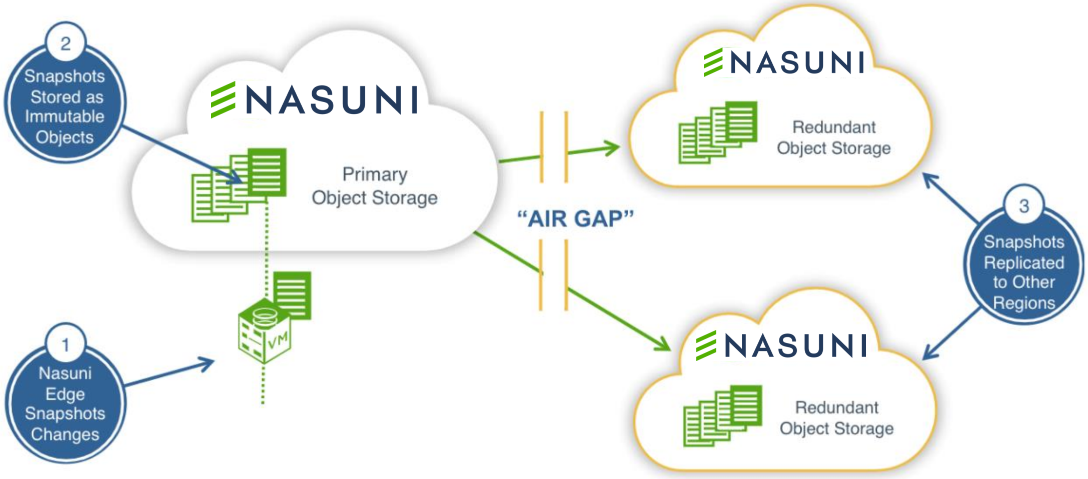
2
Snapshots Stored as Immutable Objects
NASUNI
Primary Object Storage
NASUNI
Redundant Object Storage
"AIR GAP"
3
Snapshots Replicated to Other Regions
VM
1
Nasuni Edge Snapshots Changes
NASUNI
Redundant Object Storage

Figure 5 – Air Gapped Data Protection: Nasuni's use of cloud object storage provides built-in "air gapped" separation of file data and snapshots based on the object storage durability level that you select.

Section 6. Secure Telemetry for Customer Support

Alerts and metrics are sent to the NOC to help Nasuni Support identify problems and help Nasuni Engineering improve performance. For simplicity, licensing is also controlled via the NOC. As with all other cases, no file data is ever included in these transmissions.

Section 7. Nasuni Trust Center Security Portal

Powered by SafeBase, the Nasuni Trust Center Security Portal gives customers access to compliance documents, answers common security questions, and fully discloses our security posture, all in one place. Visit the security portal at https://trustcenter.nasuni.com/ to review the latest security status or use the Subscribe button to receive email notifications on important updates, such as when compliance reports have been revised, or security vulnerabilities have been discovered.

Section 8. Ransomware Protection

Nasuni Ransomware Protection is an add-on service to the Nasuni File Data Platform that offers the industry's first in-line ransomware edge detection capabilities for file data, mitigation policies to limit damage from attacks, and incident reports that detail users and files affected and the timeline for recovery. The Nasuni Ransomware Protection service, together with the immutable snapshots and rapid recovery features of the core platform, align with The National Institute of Standards' (NIST) model for mitigating ransomware through identification, protection, detection, response, and recovery capabilities. For more information, read the Nasuni Ransomware Protection data sheet.

In addition to Nasuni's built-in ransomware capabilities, Nasuni's ransomware protection add-on is integrated with Microsoft Sentinel, allowing customers to capture and send Nasuni events to Microsoft Sentinel for analysis and further actions throughout their organization. The integration is available via the Azure Marketplace in the Sentinel Content Hub.

Section 9. Additional Security Measures

Section 9.1 Active Directory and LDAP Integration

Nasuni leverages each customer's existing authentication and access control procedures by having each Nasuni Edge Appliance join Active Directory and LDAP domains.

Data is accessed just as it would be through a Windows File Server or a traditional NAS device using existing credentials and identities. All identity and user controls already in place still apply. Existing ACLs can be migrated with the data, or the migration to Nasuni can be used as an opportunity to clean up problematic or outdated ACL structures.

Section 9.2 Hardened Nasuni Edge Appliances

Each Nasuni Edge Appliance is hardened using a "default-deny" approach. No ports are opened except the management port required to configure it. Once configured, no ports are opened beyond the ones needed to serve the configuration and port 222 for remote support via ssh. For example, if no NFS mounts are defined, no

NFS traffic will be accepted. In addition, the appliances include configurable onboard traffic partitioning, firewall, and anti-virus features.

Section 9.3 Zero Trust Framework

Zero Trust is a security framework that requires all users and applications, whether inside or outside an organization's network, to be authenticated, authorized, and continuously validated for security configuration before being granted access to data. Nasuni supports Zero Trust from Nasuni Edges to your preferred object storage by enforcing a trust relationship that requires all metadata writes to be orchestrated through the Nasuni Orchestration Center (NOC). Additionally, all Nasuni Edges are registered to each customer's Nasuni account with serial numbers, authentication codes, customer-controlled encryption keys and automatic API-based rotation of cloud credentials. This ensures that all writes to object storage are trusted and cannot be corrupted by a rouge Nasuni Edge.

Section 9.4 Integration with "Big 3" Cloud Storage Providers

Nasuni integrates with the premier public cloud storage providers, including Microsoft Azure Blob object storage, Amazon Web Services (AWS) Amazon S3, and Google Cloud Storage. These cloud leaders have invested billions in their datacenters to ensure data reliability, performance, availability, security, and accessibility.

Because of these investments, Nasuni's cloud storage partners offer geo-redundant storage with high levels of data durability, as well as extensive industry security and compliance certifications, including.

- ISO 27001 certification for standardized management of information security.
- American Institute of Certified Public Accountants (AIPCA) SOC 1 and SOC 2.
- Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) Certification, including an available Consensus Assessments Initiative Questionnaire (CAIQ).
- Payment Card Industry Data Security Standard (PCI DSS) Level 1 compliance, required for handling credit cardholder personal information
- Health Insurance Portability and Accountability Act (HIPAA)-compliant applications involving health-related and other personally identifiable information (PII) as well as Health Information Trust Alliance (HITRUST).
- FDA Code of Federal Regulations (CFR) Title 21 Part 11.
- Nasuni cloud storage partners provide detailed documentation of compliance the same way Nasuni does through the Nasuni Security Portal.

Section 9.5 Data Sovereignty

Many enterprises have data sovereignty requirements that stipulate that their data cannot leave a specific country or region. Nasuni enables customers to maintain complete control of where their data resides by integrating with public and private cloud storage providers. The following best practices help ensure compliance with data sovereignty requirements:

- Place Nasuni Edge Appliances and private cloud object storage systems in datacenters or locations that meet data sovereignty requirements.
- In conjunction with placing Nasuni Edge Appliances in appropriate locations, choose a public cloud provider's regions and/or datacenters that also meet data sovereignty requirements.
- Nasuni uses cloud-based services for control path functions, such as Global Volume Manager and Global File Lock, but these services do not process or store customer file data.
- Periodically, Nasuni Customer Support might request access to diagnostic information or access to an Edge Appliance to troubleshoot a problem. This diagnostic information consists of system logs and traces, none containing customer files, and customers can choose not to provide this information to Nasuni

Customer Support. Customers can also choose not to allow Nasuni Customer Support to access their Edge Appliances (the default setting).

Section 9.6 Rapid Software Releases

A critical component of any strong security model is a commitment to rapid software updates and improvements. Nasuni operates under an Agile software development model, with yearly major releases and multiple intermediate updates.

All Nasuni customers with an active subscription receive all Nasuni releases. Nasuni proactively scans every release of its software and proactively monitors all licensed and open-source components for security vulnerabilities.

Vulnerabilities are rated using a four-tier scale of Critical, Important, Moderate, and Low impact. Critical vulnerabilities are prioritized for immediate attention, with fixes targeted for release within 3 business days or less through normal signed software update channels. The other classes of vulnerabilities are triaged and evaluated for remediation based on other roadmap priorities and customer impact.

Summary

The rampant growth of unstructured file data and the need to store, protect, synchronize, and collaborate on files globally have outpaced the capabilities of traditional NAS and file server infrastructures. Enterprises are running out of space, failing to meet backup and ransomware recovery SLAs, putting off disaster recovery contingencies, spending too much of their IT budgets, and, in some cases, compromising on security as they attempt to keep up.

The Nasuni File Data Platform provides an advanced security model that enables cloud object storage to be safely used for scalable NAS and file server use cases. As a cloud service, Nasuni also separates its control path from its data path to meet the security needs of enterprises that don’t want file data to ever leave their security perimeters.

After reading this white paper, you should now understand how Nasuni works in private, hybrid, and public cloud configurations and provides the security measures needed to meet the most security-conscious enterprises.