NASUNI

White paper

Nasuni UniFS® Security White Paper: A Zero Trust Aligned Architecture for the Enterprise Cloud Era

WRITTEN BY Scott Gass, Senior Solutions Engineer

Table of contents

Executive Summary

Enterprises today face an unprecedented challenge: securing data in an environment defined by distributed workforces, hybrid infrastructures, and escalating cyber threats. Traditional approaches to storage security are no longer sufficient to protect against ransomware, insider risks, and state-sponsored actors.

Nasuni UniFS, the first global file system built for the cloud, addresses these challenges by combining scale-out storage with an advanced security architecture. The platform natively integrates Zero Trust principles — ensuring that access is continuously verified, least privilege is enforced, and data is always protected at rest, in transit, and in use.

This white paper highlights how Nasuni UniFS:

- Delivers end-to-end encryption and immutability to secure enterprise data against ransomware and tampering.
- Aligns with the NIST Zero Trust Architecture (SP 800-207), enabling organizations to modernize their security posture without costly rip-and-replace.
- Provides continuous data protection and rapid recovery, ensuring operational resilience against outages or attacks.
- Supports customer compliance efforts by providing technical safeguards aligned with frameworks such as SOC 2, HIPAA Security Rule, GDPR, and FedRAMP
- Supports global scalability while maintaining consistent security and governance across regions and cloud providers.

Contrast with Legacy Storage Vendors

Legacy storage systems — including traditional vendors such as NetApp, EMC, and on-premises NAS/SAN platforms — were not built for the security demands of today's cloud era. While many now bolt on "cloud gateways" or incremental security features, their architectural foundations remain tied to perimeter-based trust models and data center silos.

- **Fragmented Security:** Legacy storage often requires third-party tools or add-ons for encryption, immutability, or ransomware protection. Nasuni UniFS provides these capabilities natively, eliminating gaps and reducing complexity.
- **Perimeter-based Trust:** While legacy vendors now integrate with modern IAM systems, their enforcement models still assume trusted network segments and centralized infrastructure. Nasuni enforces identity- and policy-based access decisions at every edge appliance, independent of network location, aligning more directly with Zero Trust principles of continuous verification and distributed enforcement.
- **Limited Global Scale:** Traditional NAS/SAN systems rely on hardware replication and data center footprints, creating high costs and complexity at scale. Nasuni's cloud-native UniFS scales globally without hardware sprawl, while maintaining a unified security posture.
- **Reactive vs. Proactive:** Legacy vendors emphasize backup and disaster recovery after data loss or compromise. Nasuni UniFS ensures continuous data protection and immutability, preventing malicious alteration and enabling near-instant recovery.
- **Compliance Gaps:** Older storage frameworks struggle to map to modern compliance mandates across multi-cloud and global enterprises. Nasuni UniFS was designed with compliance-first principles, offering auditable access, encryption, and governance across all regions.

By integrating storage and security into a unified, cloud-native platform, Nasuni UniFS enables organizations to manage data efficiently while supporting strong security controls across the data lifecycle.

This combination of Zero Trust alignment, operational resilience, and enterprise compliance makes Nasuni UniFS a cornerstone for organizations looking to strengthen their cyber resilience strategies in the cloud era — in sharp contrast to legacy vendors, whose architectures can no longer keep pace with modern security requirements.

Executive Insight:

Nasuni UniFS unifies storage and security into a Zero Trust–aligned, cloud-native architecture — delivering resilience, compliance, and global scale where legacy vendors fall short

Capabilities Overview

Nasuni UniFS delivers a comprehensive set of capabilities that secure, govern, and optimize enterprise data. The following overview highlights the core security foundation, ransomware protection strengths, and FileIQ analytics that establish a Zero Trust-aligned, resilient architecture.

Core Security Capabilities

Nasuni UniFS provides enterprise-grade security controls designed to safeguard unstructured data across hybrid and multi-cloud environments.

- **Strong Encryption & Data Protection** - Nasuni encrypts both metadata and file data at rest and in transit. Architecturally, metadata orchestration is separated from file payload storage, which remains entirely within the customer's cloud account.
- **Separation of Data & Control Path** - Many legacy vendors rely on centralized control planes and vendor-managed services that expand the trusted computing base, in contrast to Nasuni's model where file data always resides in the customer's cloud storage account. Nasuni operates the control plane required to orchestrate the global file system, but does not access customer file content or encryption keys.
- **Immutable Snapshots & Air-Gap Protection** - Continuous versioning captures unlimited immutable snapshots. This ensures data cannot be altered or deleted by ransomware or malicious insiders, creating an effective logical air gap. Geo-redundancy adds further resilience.
- **Governance & Compliance** - Independently audited under SOC 2 Type II and ISO 27001, with built-in encryption, access controls, audit logging, and monitoring capabilities aligned with HIPAA Security Rule and GDPR security requirements. Compliance depends on customer implementation and governance.
- **Operational Agility & Scalability** - A global file locking service, elastic scaling in the cloud, and central console management provide global reach without hardware refresh cycles.

Executive Insight:

Core controls make Nasuni a security-first platform that removes the need for bolt-on tools.

Ransomware Protection: A Security-First Platform

Nasuni UniFS is more than a global file system — it is a security model designed from the ground up. Where traditional vendors bolt on security, Nasuni embeds it directly into the architecture with a comprehensive three-prong strategy of Protect, Detect, and Recover.

- **Zero Trust Enforcement at the Edge** - Enforcement of least-privilege access, integration with enterprise IAM, and Zero Trust edge enforcement minimize risk of unauthorized access or lateral movement.
- **Real-Time Anomaly Detection & Zero-Day Protection** - Anomaly detection at the edge monitors unusual activity such as file encryption bursts or suspicious renames. Nasuni combines signature detection with behavioral analytics to catch both known and novel ransomware variants.
- **Immutable Recovery Points with Version History** - Continuous versioning creates unlimited, WORM-style recovery points that eliminate dependence on legacy backups. Nasuni's immutable snapshot technology enables restoration of millions of files in minutes, not days or weeks.
- **Industry-Leading MTTR** - Enterprises report mean time to recovery (MTTR) of under 15 minutes — detect in 5 minutes, respond in 5 minutes, recover in 5 minutes. Legacy vendor solutions require lengthy rebuilds spanning days, with detection taking 30 minutes to 12 hours, response taking 2-24 hours, and investigation adding another 1-6 hours before recovery even begins.
- **Executive Attack Reports & Incident Visibility** - Nasuni's Ransomware Protection Report (RWP) instantly shows the blast radius, impacted users, and the last clean snapshot. The report reduces investigations from hours to seconds — a critical differentiator for compliance and cyber-insurance reporting.
- **SIEM & SOAR Integrations** - Direct SIEM/SOAR feeds ensure alerts and logs are visible in enterprise dashboards, correlated with other tools for layered defense, and rich enough for forensic and compliance audits.

CISO Perspective

Fast recovery and forensic reporting reduce both downtime and regulatory risk. This unmatched MTTR ensures ransomware incidents are business disruptions, not business disasters.

File IQ Security Capabilities & Data Loss Prevention

File IQ extends Nasuni's native security model with advanced intelligence and visibility across file environments, transforming raw telemetry into actionable insights for both operations and security teams. File IQ transforms SecOps from reactive to proactive by catching behavioral anomalies before they cascade into breaches.

- **Environment Baselines & Anomaly Detection** – Provides 90-day (Basic) or 1-year (Premium) metrics for NEAs, volumes, and users, establishing a baseline to measure normal vs. anomalous behavior. Dashboards highlight spikes in usage, unusual activity by user or group, and deviations from baseline performance. File IQ detects abnormal deletions or access spikes, insider threats and compromised accounts, and AI-driven anomalies.
- **File Integrity & Access Behavior Monitoring** – Tracks renamed or deleted files, enabling teams to quickly identify potential malicious activity or operational errors. Monitors unauthorized access detection and identifies access attempts from unknown IPs or subnets.
- **User Behavior Analytics & Storage Growth Insights** – Tracks individual user activity, exposing opportunities for license optimization. Dashboards surface storage growth hotspots, allowing IT to optimize cost allocation and forecast capacity needs.
- **File IQ Appliance Health Monitoring** – Monitors appliance cache, DB, and volume activity. Alerts administrators to potential issues before they become outages.
- **Historical Reporting & Global File Lock® Visibility** – Retains up to 1 year of reports (Premium), simplifying audit preparation and enabling long-term trend analysis. Shows directories and files under lock, helping manage collaboration and prevent conflicts or misconfigurations.

Executive Insight

File IQ makes the invisible visible — anomalies, rogue access, and growth trends become instantly actionable.

TANGIBLE BUSINESS OUTCOMES

Reduced Downtime and Enhanced Resilience

Reduced Downtime and Enhanced Resilience – With continuous immutable snapshots and the Nasuni Ransomware Protection module, enterprises recover in minutes rather than weeks, minimizing revenue loss and protecting brand reputation while eliminating the need for costly, complex legacy backup infrastructure.

Case Study: APi Group (Construction & Building Services) – APi Group, a Minnesota-based holding company with 40 businesses operating across 200 locations, faced the dual challenge of standardizing infrastructure across acquisitions while protecting critical project data from ransomware.

Results:

- Successfully recovered from actual Cryptolocker attacks with "less effort for IT and less productivity loss for users"
- Saved hundreds of thousands of dollars by eliminating on-site storage hardware across 200 locations
- Recovery in minutes vs. days with previous NetApp infrastructure
- Standardized 227TB across global operations with zero user disruption
- Integrated Microsoft Sentinel for enterprise-wide security visibility

> Nasuni continues to improve and add value to their product. With the latest Nasuni release we have enhanced our business resiliency strategy by enabling the ability to detect, alert and respond to ransomware attacks, as well as rapidly recover from any possible data encryption.
>
> **Brian Erickson**, IT Implementation & Acquisition Manager, APi Group

TANGIBLE BUSINESS OUTCOMES

Compliance-Driven Risk Reduction

Nasuni's alignment with NIST Zero Trust (SP 800-207) and support for SOC 2, HIPAA Security Rule, GDPR, and ISO 27001 helps enable customers to meet their compliance requirements while demonstrating security posture that improves audit readiness and instills customer confidence.

Case Study: Austin Radiological Association (Healthcare/Medical Imaging)

ARA, an outpatient imaging services provider operating 17 centers across central Texas, needed to manage explosive growth in medical image sizes (3D mammography images are 20x larger than 2D predecessors) while maintaining strict HIPAA compliance for over 900,000 annual radiological exams.

Results:

- Avoided $1.3 million capital investment in traditional storage arrays
- Achieved 40-50% cost reduction over 3 years vs. legacy infrastructure
- Expanded capacity by 150TB in one day vs. months with traditional procurement
- Recovery in minutes vs. 10-month migration windows previously required
- Full HIPAA compliance with customer-controlled AES encryption keys—neither Microsoft nor Nasuni can access patient data
- Azure geo-redundancy provides disaster recovery across multiple data centers

Executive Insight

Customer-controlled encryption and cloud-native immutability enable healthcare organizations to meet strict compliance mandates while maintaining full ownership of sensitive patient data.

TANGIBLE BUSINESS OUTCOMES

Operational Efficiency & Strategic Agility

RAMBØLL

Security functions like encryption, ransomware detection, and access controls are integrated natively, reducing tool sprawl. Centralized visibility reduces IT and security workload while eliminating third-party point solutions.

Case Study: Ramboll (Global Engineering & Architecture)

Ramboll, a top 10 global AEC firm with 16,000+ employees across 300 offices, struggled with slow recovery times, unpredictable storage growth, and collaboration friction across distant project sites. Weekly infrastructure updates were not scalable for a company of their size.

Results:

- 90% reduction in local file storage hardware infrastructure
- Scaled from 200TB to 3PB during pandemic without hardware constraints
- Near-instantaneous recovery vs. “frustratingly slow” NetApp SnapMirror environment
- Deployed new Edge Appliance and made data available in new location within 2 hours
- Single global file system consolidated 300+ office silos
- Seamless performance—users “unable to tell the difference” during migration

> We were pleasantly surprised by how each Edge Appliance can deliver the same file server experience as our NetApps using a much smaller local disk footprint. We don’t want to be bound by data centers. Nasuni makes a lot of sense because it gives us unlimited object-based file storage in the cloud and the flexibility of deploying a new appliance within two hours in order to make data available somewhere else.
>
> **Morten Madsen**, IT Project Manager, Ramboll

Summary: The Power of Nasuni UniFS in Securing Enterprise Data within NIST Zero Trust Architecture

Enterprises today face unprecedented threats to their most valuable asset: data. Nasuni UniFS, the cloud-native global file system, delivers a security-first architecture that maps seamlessly to the NIST Zero Trust Architecture (SP 800-207) framework, transforming how organizations secure and govern their entire data estate.

By adopting Nasuni UniFS, enterprises transform security from a cost center into a business enabler. Reduced risk exposure, stronger compliance, and faster recovery times translate directly into financial savings, competitive advantage, and shareholder value. In a climate where cyber resilience is a board-level concern, Nasuni's security solutions provide both the technical foundation and the business justification for transformation.

Executive Insight

Nasuni UniFS extends Zero Trust principles deep into the data layer — enforcing identity-driven controls, isolating risks, and enabling resilient recovery at scale. In doing so, it transforms file storage from a passive repository into an active defender of the enterprise data estate

Appendix A – Nasuni vs. NIST Zero Trust Architecture

This appendix illustrates how selected Nasuni UniFS capabilities support core Zero Trust Architecture concepts outlined in NIST SP 800-207. It is provided for reference and does not represent full implementation of all Zero Trust components.

NIST Zero Trust Principle	Nasuni UniFS Alignment
Policy Decision/Enforcement	Global file system namespace + edge appliances act as distributed enforcement points.
Micro-segmentation	Separation of metadata from file payloads, independent encryption, and access policies.
Continuous Diagnostics & Monitoring	Telemetry feeds, File IQ anomaly detection, and ransomware protection modules.
Assume Breach	Immutable snapshots and rapid ransomware recovery ensure fast restoration with minimal impact.
Automation & Orchestration	NDS API for automated ACL scanning and remediation across millions of files.

Appendix B – References & Frameworks

- NIST SP 800-207: Zero Trust Architecture
- NIST Cybersecurity Framework (CSF)
- CISA Zero Trust Maturity Model v2.0
- DoD Zero Trust Reference Architecture
- AICPA's SOC2 - Type II requirements
- HIPAA Security Rule requirements
- GDPR Data Protection Requirements
- ISO/IEC 27001:2022 Information Security Management Systems

Appendix C – Technical Controls Matrix

The controls below illustrate how Nasuni's capabilities align with selected industry security frameworks and regulatory requirements. This mapping is provided for reference purposes only. Customers remain responsible for their own compliance obligations and configuration of controls.

Domain	Nasuni Capability	Security Function
Data Confidentiality	AES-256 encryption in transit & at rest, with customer-managed keys	Protect
Ransomware Resilience	Immutable snapshots; ransomware detection & recovery in minutes	Detect, Respond, Recover
Access Governance	Integration with enterprise IdPs and MFA; fine-grained ACLs	Policy Enforcement
Anomaly Detection	File IQ ML-based anomaly & insider threat detection	Continuous Diagnostics
Incident Reporting	Executive Attack Report; SIEM/SOAR integration	Visibility & Analytics
Micro-segmentation	Metadata/content separation; independent encryption	Protect
SIEM/SOAR Integration	Streaming telemetry and API-driven security events	Detect, Respond
Data Remediation	API-enabled scanning and remediation workflows	Respond
Resiliency & DR	Geo-distracted storage; rapid restore capbilities	Recover

Let’s talk

Want to find out more about how Nasuni can provide your business with a fluid data infrastructure designed for the hybrid cloud world?

Nasuni’s hybrid cloud platform unifies file and object data storage to deliver effortless scale and control at the network edge.

Learn more

Nasuni is a scalable data platform for enterprises facing an explosion of unstructured data in an AI world, eliminating the choice between expensive tinkering or an overwhelming transformation of your entire data infrastructure.

The Nasuni File Data Platform delivers effortless scale in hybrid cloud environments, enables control at the network edge, and meets the modern enterprise expectation for protected, insight- and AI-ready data. It simplifies file data management while increasing access and performance.

Consolidate data, cut costs, and empower users – all while transforming your data from obstacle into opportunity.

NASUNI