

Nasuni AI Activate

Security Overview

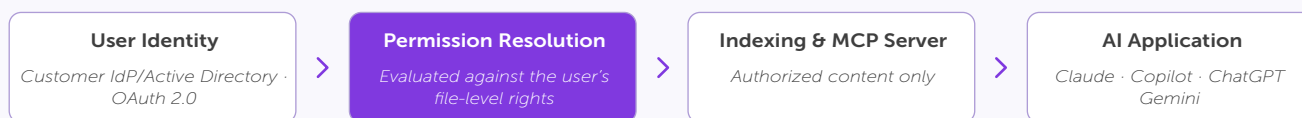
Governed AI access to enterprise file data, with each user's existing permissions enforced **before the AI ever reads the content.**

Nasuni AI Activate connects MCP-compatible AI applications to enterprise file data through a hosted indexing service and a Model Context Protocol (MCP) server, enforcing every user's file-level permissions before any content reaches the model. More detailed information on security and data handling, including data-flow boundaries, key management, and residency, is available on request.

/ PERMISSION ENFORCEMENT — BEFORE RETRIEVAL, NOT AFTER

- **The user's identity governs access, not the AI application's.** Users authenticate through the organization's existing identity provider using OAuth 2.0, and permissions resolve against Active Directory group membership at query time.
- **Enforced pre-query.** Nasuni AI Activate evaluates every query against the requesting user's file-level (NTFS) permissions before AI processes any content. It excludes unauthorized content at the data layer, so the model never reads it and never returns it to the AI application.
- **No privileged service accounts.** The AI application's view matches the authenticated user's view. A user can retrieve nothing through AI Activate that they could not already access as themselves.
- **Permissions stay live.** AI query results reflect new group memberships, revoked access, permission changes, and file deletions in near real time.
- **Scope control.** Per-volume dataset scoping lets security and IT teams restrict which content on an enabled volume AI applications can reach.

PRE-QUERY ENFORCEMENT FLOW



Excluded at the data layer: Content outside the user's permission scope is never accessed, processed, or returned.

Nasuni AI Activate resolves and enforces permissions before content reaches the MCP server or the AI application. Other implementations filter content only after the model has already retrieved the full dataset.

/ AI ADOPTION IS OUTPACING AI GOVERNANCE



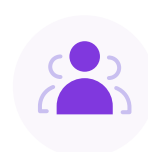
97%

of enterprises are piloting or deploying AI agents



43%

cite data security as the top barrier to scaling AI



31%

centrally manage and automatically enforce AI agents' data access

Source: Nasuni, The State of Enterprise File Data, Annual Report 2026 (Sapio Research, n=1,000)

/ WHY THE ENFORCEMENT MODEL MATTERS

Pre-query enforcement vs. post-query filtering

Approaches that filter results after retrieval force the model to ingest unauthorized content first. That exposure exists regardless of what the user sees, and one that auditors and regulators treat as a data-access event. Nasuni AI Activate excludes off-limits content before anything accesses or processes it.

Identity-mapped access vs. self-built pipelines

Custom AI data pipelines commonly run under shared service-account identities that no one can tie to an individual user. They also add indexing, refresh, and audit surfaces you have to govern separately. Nasuni AI Activate enforces the identity and permission model you already run, with nothing new to secure, patch, or maintain.

/ HOW NASUNI AI ACTIVATE HANDLES YOUR CONTENT

- **Reads only enabled volumes.** To build a searchable index, the service reads content only from the file volumes an organization explicitly enables. It retrieves content on demand through a read-only access layer, and never copies files out of the organization's cloud object storage, alters them, or deletes them.
- **Keys stay where they belong.** File content in UniFS stays encrypted under customer-owned keys. AI Activate extends authorization scope to Nasuni-hosted infrastructure to read volume data, consistent with how Nasuni already manages your volumes today. The AI Activate index is a separate store, encrypted at rest under Nasuni-managed keys, and TLS encrypts all traffic in transit.
- **No model training.** Nasuni does not use customer content to train, fine-tune, or improve any foundation or machine-learning model.
- **Full detail on request.** Data-flow boundaries, key management, and data residency details are available on request.

/ COMPLIANCE & GOVERNANCE

Nasuni's current compliance commitments extend to the AI Activate service.

- Nasuni products, including AI Activate, undergo independent third-party penetration testing at least annually.
- Nasuni designed AI Activate's architecture and controls with industry-standard security principles, including NIST CSF and ISO 27001.
- AI Activate works with existing enterprise identity, including Okta and Microsoft Entra ID.
- Nasuni AI Activate includes, as part of technical support case investigations, logging of MCP service activities, including authentication events and user queries, all recorded against the authenticated user identity behind each query.
- The Nasuni platform consolidates and eliminates distributed NAS security management across sites and vendors, reducing the need for ungoverned, shadow AI workarounds.

Trust & Assurance Collateral

To support formal security review, Nasuni makes detailed security and compliance documentation available on demand at trust.nasuni.com

/ SHARED RESPONSIBILITY AT A GLANCE

NASUNI	CUSTOMER
• Service operation, availability, and patching • Infrastructure security (inherited from the hosting provider) • Pre-query permission enforcement logic • Encryption of the AI Activate index and index key management • Data encryption in transit (TLS)	• Accurate file-level permissions (ACLs) in UniFS® • Identity provider configuration and accuracy (Okta, Entra, AD) • Selection of enabled volumes and dataset scoping • Selection and governance of connected AI applications • End-user communication and acceptable-use policy

/ CONTINUE YOUR REVIEW

Let's walk through the [full security architecture](#), share the security and compliance documentation, and arrange a [CISO peer reference](#). Request the [Security and Data Handling](#) document to complete your evaluation.



Nasuni is a leading unstructured data platform for enterprises where file data is mission-critical for both people and AI. We power the operational file layer where work happens — helping organizations manage, protect, and activate data so teams can work smarter, reduce costs, and operate securely without limits.

Built on a patented architecture that fuses cloud object storage with enterprise file services — including permissions, versioning, and a global namespace—Nasuni delivers high-performance file access, global data availability, and a scalable, governed, AI-ready single source of truth across every major cloud.

Trusted by more than 1,300 enterprises globally, Nasuni helps organizations modernize file infrastructure, strengthen data security, and support AI-driven operations. Learn more at www.nasuni.com.