



Resilio Workspace: VPN-less File Access

Resilio Workspace gives remote users LAN-like access to files on Nasuni storage, with the file server's own permissions enforced, and no VPN tunnel in the path. Data never leaves the customer's environment.

/ How it works

Three components deliver VPN-less access, with a management plane behind them:



Primary Storage Agent - Sits next to the Nasuni Edge Appliance (NEA). Reads and writes files on the user's behalf, using the golden copy of data on the Nasuni File Data Platform.



User Agent - Lightweight client on each end user's workstation (Windows or Mac). Presents the file namespace locally and streams bytes on demand.



Management Console - The control and policy plane. Authenticates participants, distributes job configuration and policy, and collects telemetry. Critically, the Management Console is not in the data path, data moves agent-to-agent. If the console becomes unavailable, transfers in flight continue; only scheduled job starts and new user joins are affected. The console supports active/passive clustering for high availability.

/ Identity and zero-trust access

The identity model is the heart of the VPN-less story. The end user authenticates through the customer's own identity provider, Entra ID or Okta, over OIDC. The customer's existing MFA and conditional-access policies apply automatically, because it is their IdP performing the authentication.

The Management Console resolves the authenticated identity to the user's domain account in Active Directory or Entra Domain Services. Resilio uses that directory natively and in real time, it never copies AD into a separate store or syncs on an interval. A disabled account or group-membership change takes effect immediately, with no window in which a deprovisioned user retains access.

When the user opens a file, the Primary Storage Agent impersonates the user via Kerberos delegation and accesses the file server as that actual user. The file server enforces its own NTFS ACLs exactly as it would for someone sitting in the office. There is no service account, no permission remodeling, and no drift. The perimeter is the authenticated user and the individual file, not a network tunnel. This is what makes Resilio a zero-trust application.

/ Streaming, caching and syncing

A user opening a file does not wait for the entire file to download. The User Agent presents the namespace and streams only the bytes the application actually requests. A 12 GB design file opens in the time it takes to read its header and the regions currently in view. Three behaviors, controlled by IT policy, govern how data reaches the endpoint:



Streaming - Bytes are delivered on demand as the application reads them. This is the default user-visible experience.



Caching - Instead of replicating a full copy of the share to every endpoint, the End-user Agent presents the namespace as placeholders and hydrates a file on first read, which is why a large CAD, BIM, or media file opens at near-local speed over the WAN. Once hydrated, the file is held in the local cache and subsequent opens are served locally. A configurable cache size cap bounds the footprint on the user's disk: when the cap is reached, the coldest unpinned content by access time is dehydrated back to placeholders and the space reclaimed, so the cache manages itself. The cap is set by administrator policy and can be configured differently per caching location.



Syncing - Administrators can pin files and folders so they are fully synced to the endpoint and held there, exempt from cache eviction. Pinning is how IT guarantees that an active project or working set is resident before anyone opens it, so the first open is instant and the content stays available if the user goes offline. File locking is centralized and stays in sync with the primary storage filer, so office and remote users see the same lock state and nobody silently overwrites anybody.

/ Transport and security

Resilio uses μ TP3 / Zero Gravity Transport (ZGT), a UDP-based WAN protocol with RTT-aware congestion control and interval acknowledgments. ZGT fills whatever link the remote user has, high-latency home broadband, hotel Wi-Fi, far more completely than TCP-based file access, which is why streaming a large file from home feels local rather than like a VPN copy.

Received blocks are hash-verified, and files are assembled and verified in a scratch area, then moved into their final location only after they pass integrity checks. A partially written or corrupted file is never exposed to the application.

/ Deployment and security posture

Resilio is not a cloud service, it runs entirely behind the customer's firewall. Data never leaves the customer's environment, and there is no Resilio-side store of files or identities. The solution is air-gap friendly: the Management Console's outbound license and support contact is optional and can be fully disabled.



Encryption - End-to-end using TLS and AES-256 with one-time session keys providing forward secrecy. Agents and console mutually authenticate.



Nasuni placement - Deploy one dedicated NEA as the Resilio interface into the Nasuni File Data Platform, with one Primary Storage Agent next to it. Give that NEA access to every share and volume to be served through Resilio. If data residency requires it, deploy one NEA and Primary Storage Agent per region. Never add the same folder or share to more than one Primary Storage Agent.



Distance insensitivity - The Primary Storage Agent does not need to be near end users. Place it next to the storage. ZGT is WAN-optimized and insensitive to latency, so a user a continent away reaches the Primary Storage Agent with no proximity penalty, the inverse of a VPN or branch-cache design.



Certifications - SOC 2 Type II and TPN Blue (M&E). Because data stays in the customer's environment, GDPR, HIPAA, and FedRAMP postures are unaffected by the deployment.

Why Resilio?

Competing solutions such as Egnyte and LucidLink require migrating data into their cloud and, in some cases, remapping permissions. Resilio leaves data and the permission model where they already are and makes them reachable. Access runs as the real user, never a service account. The file server's existing NTFS permissions are the enforcement point, with nothing to remodel and nothing to drift out of sync. The customer's identity provider, not Resilio, is the authentication authority, so existing identity controls extend to remote file access without additional configuration.



Nasuni is the file data foundation for large enterprises where files are mission-critical for both people and AI. The work that drives modern organizations lives in files, the most operationally critical segment of unstructured data, including designs, project documentation, financial and compliance records, media assets, and the countless versions that evolve across distributed teams.

We help our customers manage, protect, and activate that content so IT can continuously reduce cost and risk, while teams and the AI that supports them become more productive through fast, governed access to the right information when and where they need it.