RushFiles

RushFiles Security & Recovery Architecture

RushFiles is designed with end-to-end security in mind, from encrypted storage and transmission to strict user access policies and real-time audit trails. Whether you deploy in the cloud, on-premise, or a private environment, your data remains protected and fully under your control.

External Threats Layer

Data encryption eliminates external breaches. Fail-safe triggers ensure near-complete protection.

Application Layer

File versioning, ransomware recovery mechanisms, user access controls, and encryption.

Storage Layer

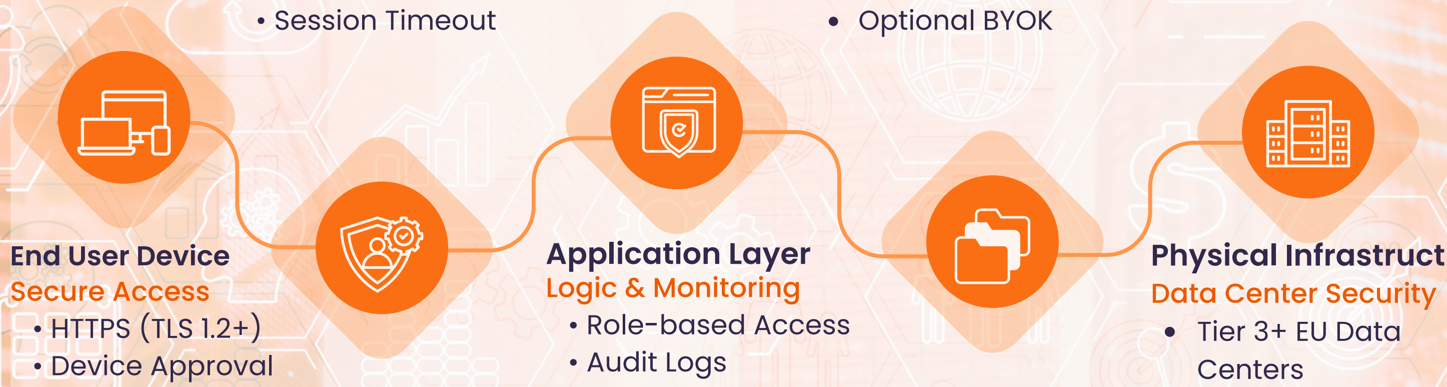
S3 buckets distributed across multiple storage nodes, RAID redundancy and failover mechanisms.

Data Center Layer

Tier 3 data center features: fire zones, power redundancy, cooling systems. Optional Geo-Replication for disaster recovery.

Contact us

End-to-End Protection Overview



End User Device
Secure Access
- HTTPS (TLS 1.2+)
- Device Approval
- IP Filtering

Authentication & Authorization
Identity Controls
- Active Directory / LDAP
- 2FA
- Password Policies
- Session Timeout

Application Layer
Logic & Monitoring
- Role-based Access
- Audit Logs
- File Versioning
- Public Link Expiry

Storage Layer
Data Protection
- AES-256 Encryption at Rest
- Redundant S3-compatible Storage
- Ransomware Recovery
- Optional BYOK

Physical Infrastructure
Data Center Security
- Tier 3+ EU Data Centers
- Firewalls, Surveillance, Fire Suppression

Built-In Tools to Match Any Security Policy

Control Type	Options & Details
Authentication	AD/LDAP sync, 2FA, lockout settings, custom password rules
Access Management	NTFS rights mapping, IP whitelisting, geo-blocking, device approval
Encryption	AES-256 at rest, TLS 1.2+ in transit, optional BYOK encryption
Visibility & Logging	File-level audit trails, exportable reports, real-time user activity dashboard
Backup & Rollback	File versioning, ransomware recovery, restore points

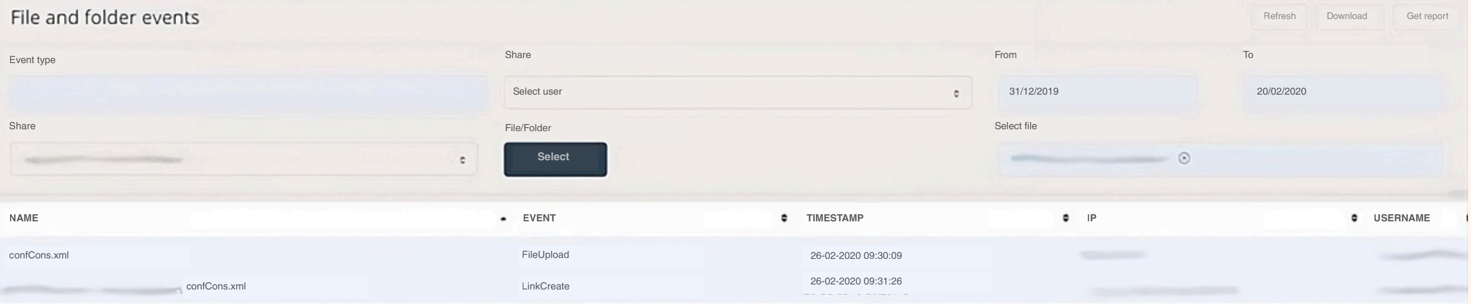
Audit Logs & Policy Enforcement

Monitor Everything.
RushFiles offers a complete audit trail covering logins, file access, public links, and more.

Capabilities:

- File-level activity logging (create, delete, move, restore)
- Login tracking with IP, device type, and status
- Public link monitoring (creation, open, download, expiry)
- Export reports in .XML format for ISO/GDPR/HIPAA audits
- Custom date/user filters for targeted checks

Example: File and Folder Event Log — filtered by user, action, and folder



File and folder events

Event type:

Share: Select user

From: 31/12/2019

To: 20/02/2020

Share: [redacted]

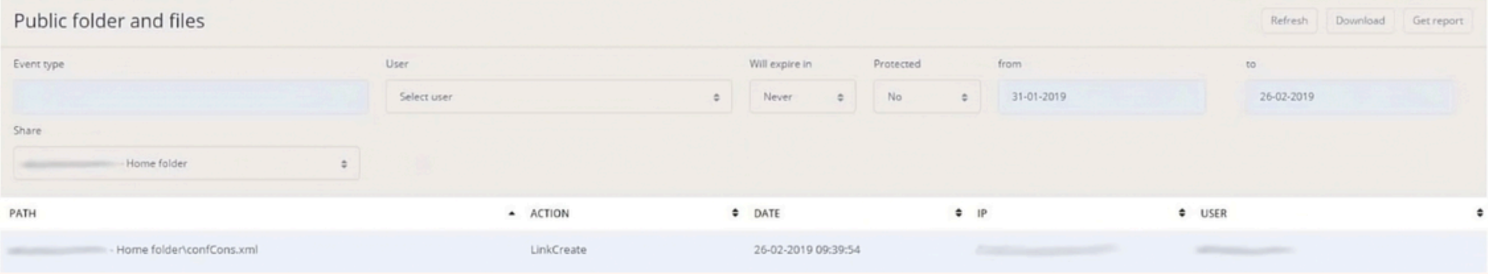
File/Folder: Select

Select file: [redacted]

NAME	EVENT	TIMESTAMP	IP	USERNAME
confCons.xml	FileUpload	26-02-2020 09:30:09	[redacted]	[redacted]
[redacted] confCons.xml	LinkCreate	26-02-2020 09:31:26	[redacted]	[redacted]

Admins can filter file and folder events by username, action type (e.g. upload, download), date range, and affected folders. Each log includes timestamps, IP addresses, and user identities, allowing full traceability

Example: Public Link Report — tracks downloads, opens, expiries



Public folder and files

Event type:

User: Select user

Will expire in: Never

Protected: No

from: 31-01-2019

to: 26-02-2019

Share: [redacted] Home folder

PATH	ACTION	DATE	IP	USER
[redacted] Home folder\confCons.xml	LinkCreate	26-02-2019 09:39:54	[redacted]	[redacted]

Track public link activity across users and files. Filter by action type, user, expiration, and password protection. Logs include IP, timestamp, and file path for full traceability.

Ransomware Recovery

Restore Encrypted Files in Minutes

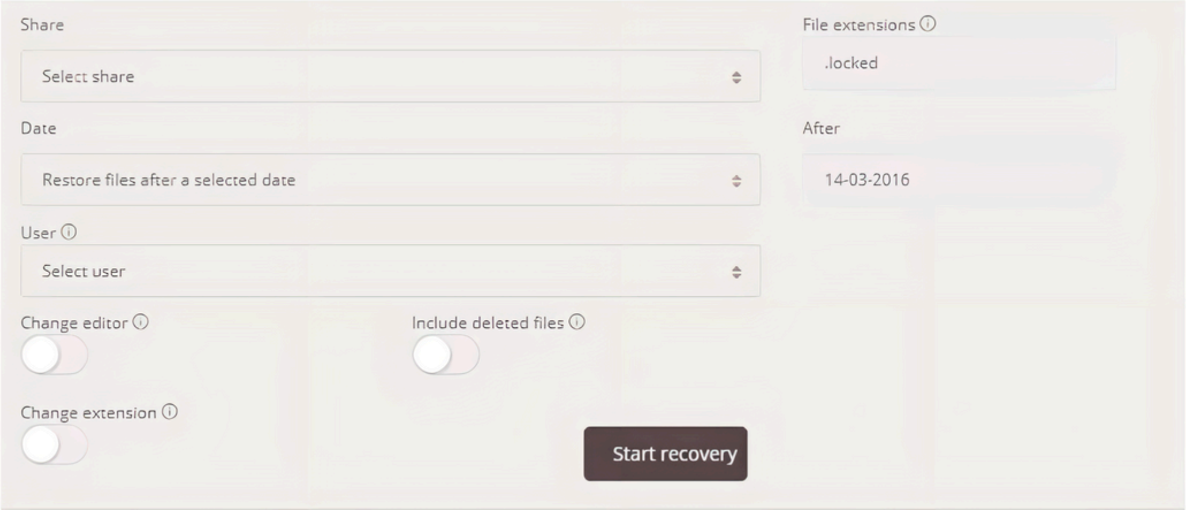
If files are encrypted due to ransomware, admins can use the Restore History tool to roll back affected files to a clean, earlier version without data loss. This recovery process is fast, traceable, and user-friendly.

Admins simply:

1. Select the affected share
2. Choose a recovery date before the incident
3. Specify the ransomware extension
4. Start recovery and confirm

You can immediately see the restored files in the web app. Within 5 minutes, the server will also return the correct version to your local machine and hard drive.

Example: File recovery menu



Share: Select share

File extensions ⓘ: .locked

Date: Restore files after a selected date

After: 14-03-2016

User ⓘ: Select user

Change editor ⓘ ○

Include deleted files ⓘ ○

Change extension ⓘ ○

Admins can recover encrypted files by selecting the affected date and ransomware extension, then instantly roll back to clean versions across all devices.

Contact us