FILECLOUD

Zero Trust File Sharing

Industry-first set of capabilities that enable a Zero Trust security posture for collaboration and file sharing.

Hyper-Secure File Sharing & Sync

FileCloud is an enterprise-grade file sharing and sync solution:

- ✓ Zero Trust built-in to secure assets within and beyond the perimeter
- ✓ Compliance support and automation capabilities for CISOs and CTOs
- ✓ Deployment options (SaaS/self-hosted) and data governance for admins
- ✓ Collaboration and ease-of-access for end users

WWW.FILECLOUD.COM

Secure Digital Assets with Zero Trust in FileCloud

"The network location is no longer seen as the prime component to the security posture of the resource."
– NIST SP 800-207, Zero Trust Architecture. *https://doi.org/10.6028/NIST.SP.800-207*

Zero Trust moves cybersecurity beyond the static network perimeters – this paradigm focuses on securing users, assets, and resources over the network edge or segments.

Tenets of Zero Trust

Scrutinize Explicitly:

Use dynamic and static attributes to inform contextual, consistent, and conditional access to resources.

Assume a Hostile Environment:

Treat all users, devices, applications, environments, and NPEs as untrusted.

Presume Breach:

Consciously operate and defend resources with the assumption that an adversary has presence within the environment.

Never Trust, Always Verify:

Deny access by default; authenticate every device, user, application/workload, and data flow (with least privilege).

Apply Unified Analytics:

Apply unified analytics for Data, Applications, Assets, Services (DAAS) to include behavioristics; log each transaction.

***Source:** Department of Defense (DoD) Zero Trust Reference Architecture, Version 2.0, July 2022.
Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

FILECLOUD SUPPORTING THE

7 PILLARS* of ZERO TRUST

User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions. *

FileCloud enabled

- SAML/SSO Integration
- 2FA & MFA Support
- Role Based Access Control (RBAC)
- Authentication, Access Management & Re-validation (workflow/policy)
- Granular File & Folder Permissions
- Comprehensive Audit Logs
- ReCAPTCHA

Devices

Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request. *

FileCloud enabled

- Device Inventory
- Device Blocking & Remote Wipe
- Device Approval (workflow/policy)
- External MDM Integration
- Device Security Status
- Centralized Device Management

Data

Data transparency and visibility is enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging. *

FileCloud enabled

- AES 256-bit Encryption (data at rest)
- SSE-CPK & SSE-KMS Support
- Granular Folder & File Permissions
- Zero Trust File Sharing
- SSL/TLS Protocols (data in transit)

  NTFS Permissions Integration
- Custom DLP Rules (limit & manage file access)
- Public & Private File Sharing
- Workflow Automation (share approvals control)
- Metadata Tagging (user-defined)
- Automated Content Classification (with OCR support)

  Retention Policies
- Digital Rights Management (secure viewer, revoke permission, download limits)

Visibility & Analytics

Analyze events, activities and behaviours to derive context and apply AI/ML to achieve a highly personalised model that improves detection and reaction time in making real-time access decisions. *

FileCloud enabled

- Audit Trail
- Message Log (incoming and outgoing), Archival, & Search
- Alerts & Notifications
- SIEM Integration
- Default & Custom Reports

Automation & Orchestration

Automate security response based on defined processes and security polices enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions. *

FileCloud enabled

- Custom DLP Rules (block access based on attributes/metadata)
- Allow & Disallow Access Lists
- Workflow Automation (block device access)

Network & Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls. *

FileCloud enabled

- Air-gapped Network Configuration (NIPR, SIPR, & JWICS)
- Custom DLP Rules (limit access/login)
- Multi-tenancy

Applications & Workloads

Secure everything from applications to hypervisors, to include protection of containers and virtual machines. *

FileCloud enabled

- Private Cloud Configuration
- Air-gapped Configuration
- ICAP Integration

*National Security Agency (NSA) Cybersecurity Information Sheet: "Advancing Zero Trust Maturity Throughout the User Pillar"
https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF