EnduraData EDpCloud File Replication Security Brief

Version: 2.0 | Date: November 2025

Company: EnduraData Inc.

Website: www.enduradata.com

Contact: support@enduradata.com | 952-746-4160

1. Overview

EDpCloud is EnduraData's cross-platform file replication and synchronization software for secure, real-time data movement across servers, operating systems, and storage types. Security, data integrity, and compliance readiness are built into every layer of its design — from encryption and authentication to audit logging and configuration hardening.

EDpCloud enables organizations to protect, move, and recover data across on-premises, cloud, and hybrid environments while meeting strict data-protection requirements for government, healthcare, financial, and enterprise workloads.

2. Security Principles

Principle	Description
Confidentiality	All transfers are encrypted in transit (TLS) and can be encrypted at rest. Sensitive configuration data and credentials are stored securely.
Integrity	Every transferred file is verified with checksums; optional versioning and retention policies protect against corruption or tampering.
Availability	Replication services are fault-tolerant, resumable after interruptions, and support multi-node redundancy.
Auditability	System and transfer events are logged with timestamps and node identifiers for traceability and compliance audits.

3. Data Protection

3.1 Encryption

• In Transit: All network communication is secured using TLS 1.2+ with modern cipher suites.
• At Rest: Optional AES-256 encryption for staging areas and replicated data.
• Integrity: Checksums (SHA-256) validate file consistency pre- and post-transfer.

3.2 Authentication and Access

• By default, only system administrators have access to replication software and configurations.
• API keys and certificates can be scoped per endpoint.
• Only pre-authorized nodes can replicate data to remote nodes

3.3 Key and Certificate Management

• Certificates can be self-signed, CA-issued, or centrally managed.

4. Secure Deployment and Hardening

EnduraData provides a Security Hardening Checklist for Linux and Windows environments covering system patching, file permissions, privilege isolation, firewall configuration, and secure daemon setup. All default paths favor least privilege and segregated roles between endpoints and controllers.

5. Logging and Auditing

EDpCloud records detailed logs for authentication attempts, configuration changes, file transfer events, and node health. Logs can be exported to other apps. Different log levels exist for the sending and receiving nodes.

6. Compliance Alignment

Regulation / Standard	EDpCloud Contributions	Customer Responsibilities
HIPAA	Encryption in transit/at rest, audit logs, integrity verification	Implement HIPAA policies and BAAs
CJIS / FedRAMP Low	TLS communication, controlled access, event logs	System authorization, enclave boundary enforcement
GDPR	Secure replication and deletion workflows, data-subject portability	Implement consent and retention policies

ISO 27001 / NIST 800-53	Access control, incident response, audit controls alignment	Define risk management processes

7. Vulnerability Management

EnduraData maintains a secure software development lifecycle (SSDLC) with code analysis, SBOM generation, and advisories for each release. Security updates are prioritized and communicated to registered customers.

8. Disaster Recovery and Business Continuity

EDpCloud supports replication topologies that ensure recovery and continuity through checkpointed transfers, replication scheduling, and integrity verification to meet defined RTO/RPO objectives.

9. Documentation Package

- EDpCloud Security Brief (this document)
- Security Hardening Guide (Linux/Windows)
- SBOM and release notes
- Logging & Observability Guide
- Disaster Recovery Playbook

10. Contact and Support

Security Team: support@enduradata.com

General Support: support@enduradata.com

Phone: 952-746-4160

Website: www.enduradata.com

11. Disclaimer

This brief summarizes EDpCloud security features as of November 2025. Configurations and capabilities may vary. Always follow EnduraData’s current Security Hardening Guide and organizational security policies.