ctera your files. your cloud.

CTERA White Paper

CTERA Enterprise Data Services Security Architecture

Table of Contents

Introduction

Enterprises today operate across distributed networks of data centers, branch offices, remote workers, and multi-cloud services. With this dispersion comes heightened exposure: ransomware, insider threats, regulatory scrutiny, and the rising complexity of compliance. CISOs and IT leaders are tasked not only with securing data everywhere but also with proving compliance, enforcing Zero Trust access, and ensuring business continuity in the face of advanced threats.

The CTERA Intelligent Data Platform was designed from the ground up to meet these challenges. It unifies edge-to-cloud file services with a security-first architecture that integrates encryption, immutability, ransomware detection, advanced logging, and compliance-driven governance into a single platform. This document examines the platform's security architecture in depth, presenting both the technical controls and the business relevance for security decision-makers.

Executive Summary for Security Decision-Makers

The CTERA Security Architecture delivers defense-in-depth for the modern enterprise file system. It provides advanced data immutability, real-time ransomware defense, compliance-grade logging, Zero Trust access models, and broad third-party integrations. For CISOs, the result is a platform that not only resists threats but demonstrates governance and audit-readiness.

Key Innovations

With all the changes described above, it should come as no surprise that a GFS must address a diverse set of requirements. Let's look at the key ones:

AI Security Intelligence for ransomware detection, anomaly analysis, and forensic insight.

CTERA Vault immutability enforced across NFS/CIFS and extended to S3 Object Lock.

CTERA Ransom Protect with behavioral detection and honeypot-based exfiltration traps.

Centralized audit forwarding via CTERA Messaging Service to SIEM and aggregation solutions such as Splunk and Microsoft Sentinel.

Zero Trust access through pre-signed URLs, mutual TLS, restricted shell, and session controls.

Cloud Storage Routing with storage classes and Thales CipherTrust integration via KMIP.

SMB v3 and NFS v4 encryption with fine-grained ACL enforcement.

Disaster Recovery with metadata-first restores, DFS failover, and Portal WebDAV fallback ensuring continuity.

Certifications and compliance alignment: FIPS 140-3, DISA APL, GDPR, HIPAA, NIST 800-171, PCI DSS, ISO 27001.

CTERA Portal Security

The CTERA Portal acts as the secure control plane for all enterprise data services. It mediates access, enforces authentication policies, and ensures data governance across distributed users and devices. With hardened OS layers, multi-tenancy isolation, and advanced RBAC, the CTERA Portal is engineered to operate as a Zero Trust foundation.

CTERA separates the control plane (identity, policy, orchestration) from the data plane (file I/O and content). File data never traverses the control plane; only signed metadata and commands do. This separation reduces the attack surface and confines high-value content to data-plane endpoints and storage targets.

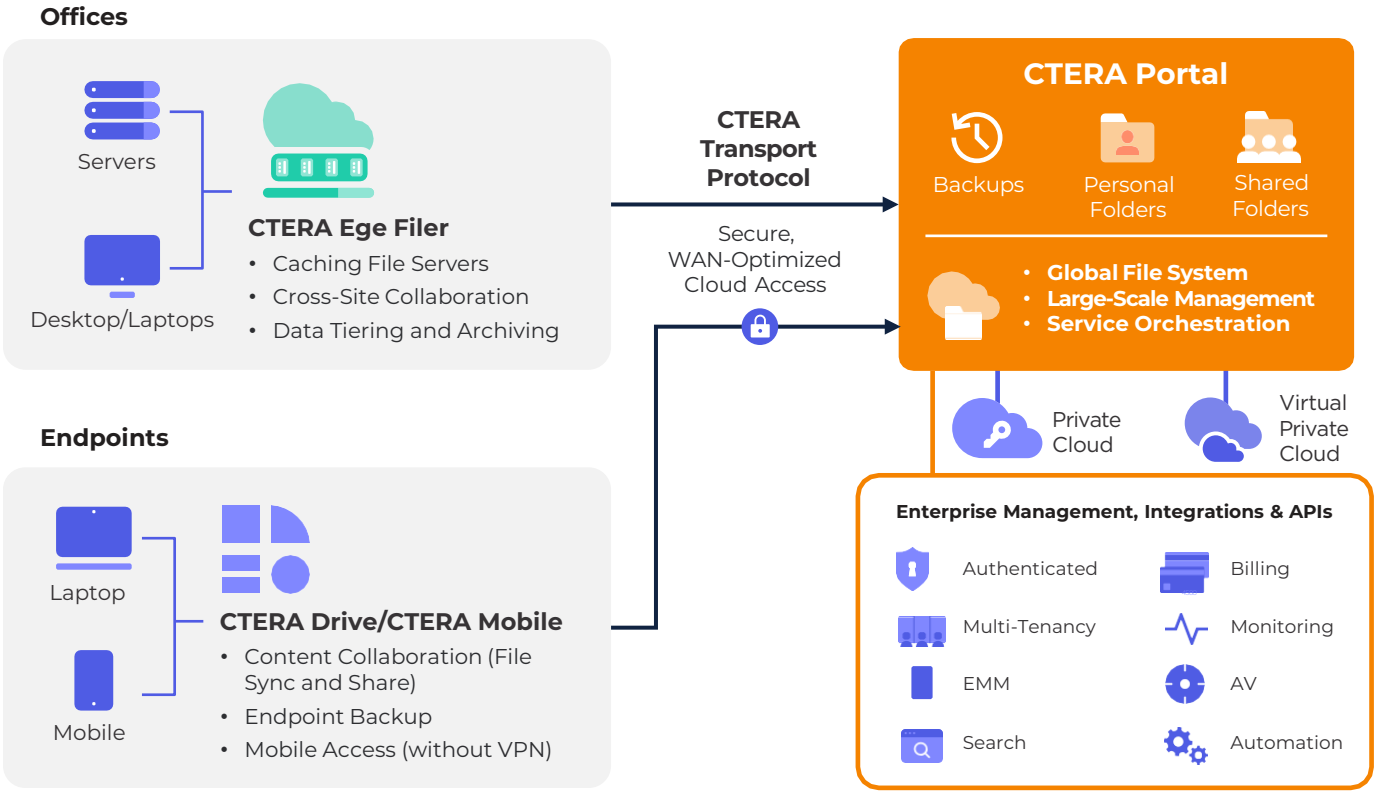
Authentication methods supported include:

- Local DB: Credentials stored securely in the Portal using PBKDF2-HMAC-SHA-512.
- LDAP/Active Directory: Full integration with enterprise directories for SSO.
- SAML/Kerberos: Federated authentication with modern identity providers.
- Client Certificates (CAC/PIV): Mutual TLS validation for government-grade security.

Client enrollment follows a secure workflow: a client requests a session, validates the CTERA Portal certificate, submits credentials or tokens, and receives a short-lived enrollment token. This token is used for subsequent sessions, avoiding storage of persistent user credentials.

Key Capabilities:

- Multi-factor authentication including SAML, Kerberos, and CAC/PIV cards.
- Role-based access control including Compliance Officer role for audit oversight.
- Multi-tenancy with segregation of data, keys, and configuration settings.
- CTERA Messaging Service for centralized audit aggregation and SIEM forwarding.
- Explicit separation of control and data planes.
- Hardened Linux OS with restricted shell and digitally signed operating system validation.



CTERA Edge Filer Security

CTERA Edge Filers bring cloud-scale storage resilience to branch and remote offices while maintaining enterprise security controls. They integrate tightly with existing directory services, enforce encryption locally, and protect against unauthorized access. CTERA Edge Filers also incorporate native anti-malware protection and namespace segmentation to reduce risk at the edge.

Key Capabilities:

- User authentication via Active Directory and Kerberos.
- Role-based ACL enforcement and SMB signing for secure access.
- AES-256 local volume encryption with PBKDF2-derived keys.
- Bitdefender antivirus with real-time scanning and quarantine.
- Namespace segmentation through Zones for access isolation.
- Local and remote management access secured through TLS and restricted shell.
- Hardened Linux OS with restricted shell and digitally signed firmware validation.

File Data Security

CTERA supports completely private deployments where all data and metadata remain on-premises. In hybrid and cloud deployments, source-based encryption ensures that sensitive data never leaves the customer's perimeter unprotected, and even storage administrators cannot access plaintext content without customer-controlled keys.

Key Capabilities:

- AES-256 encryption at rest using FIPS 140-3 validated libraries.
- TLS 1.3 ensures confidentiality with AES-based AEAD encryption (AES-GCM-256) and protects integrity using SHA-256 during the handshake, with the AEAD cipher providing built-in authentication to prevent data tampering.
- CTERA Vault immutability for NFS/SMB shares with propagation to S3 Object Lock for supported object stores.
- Secure Erase for permanent, compliance-grade data removal.
- Integration with Thales CipherTrust via KMIP 1.0/2.0 for external key management.
- DEK/KEK hierarchy with customer custody of master keys.

CTERA Transfer Protocol (CTTP)

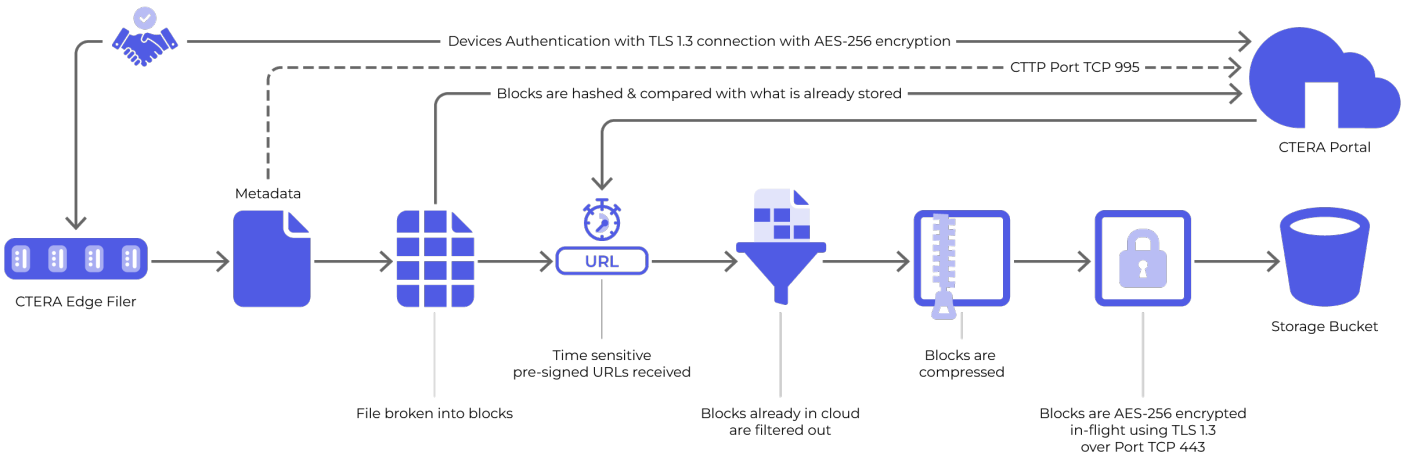
The CTERA Transfer Protocol (CTTP) is the secure transport layer that underpins all edge-to-cloud and client-to-portal communication in CTERA Enterprise Data Services. While CTERA supports industry-standard HTTPS and SMB/NFS protocols, CTTP was developed to optimize large-scale, distributed file operations without compromising on security.

Built on TLS 1.3 encryption, CTTP ensures that every byte transferred between an Edge Filer, endpoint, and the CTERA Intelligent Data Platform is both confidential and integrity-verified. Unlike generic HTTPS or SFTP, CTTP is designed to handle parallel metadata synchronization, deduplicated object transfers, and multi-stream uploads/downloads efficiently over WAN links.

From a security perspective, CTTP eliminates traditional risks by embedding end-to-end authentication, replay-attack prevention, and per-session encryption keys. Its firewall-friendly design operates over a single, predictable port (TCP 995) secured with TLS 1.3, allowing enterprises to deploy globally without complex network exceptions. For CISOs, CTTP means that performance and scale do not come at the expense of security — the protocol enforces the same cryptographic rigor as HTTPS while delivering the throughput and resilience required for global file system operations.

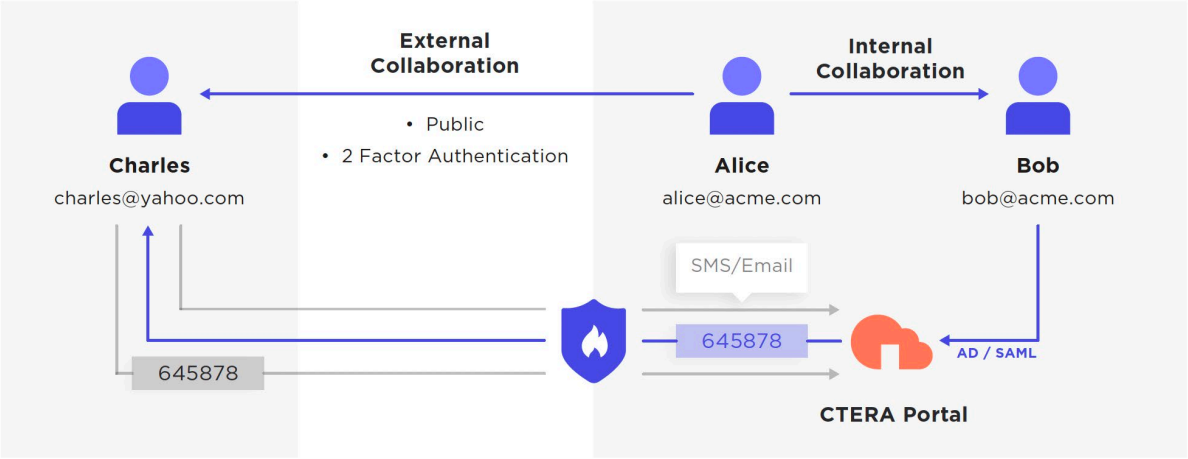
Key Capabilities:

- TLS 1.3 encrypted channel ensuring confidentiality and integrity in transit.
- Operates over TCP 995 with predictable firewall configuration.
- Parallel multi-stream transfers for large files and metadata synchronization.
- Replay-attack prevention with per-session nonces and key rotation.
- WAN optimization with built-in deduplication awareness.
- Firewall-friendly design, minimizing required network exceptions.
- Session-level authentication integrated with SAML, Kerberos, and CAC/PIV certificates.



File-Sharing Security

CTERA enables secure internal and external collaboration while preserving compliance. Sharing policies are enforced centrally, with options for read-only, upload-only, preview-only, or full access. Documents can be watermarked to prevent leakage, and all activity is logged for audit compliance.



Key Capabilities:

- Role-based sharing with granular permissions (read, write, preview-only).
- External sharing with two-factor authentication (SMS/email codes).
- Watermarking and preview-only modes to prevent data exfiltration.
- 'Shared by Me' dashboard for user-level visibility.
- Audit logging of all share and access events.

Endpoint Security

CTERA Drive and Connect agents extend secure file access to endpoints. Agents encrypt data before it leaves the device and integrate with enterprise identity solutions for seamless authentication. By using pre-signed URLs, agents maintain a Zero Trust posture while minimizing credential exposure.

Key Capabilities:

- End-to-end AES-256 encryption for synchronization and backup.
- Single sign-on via Kerberos and token-based authentication.
- Support for pre-signed URLs for secure, ephemeral file transfers.
- Automatic key management with OS-level keychains.
- Seamless integration with CTERA Portal for policy enforcement.

Mobile App Security

The CTERA Drive Mobile app extends enterprise file access to iOS and Android devices. All cached files are encrypted and isolated within a sandbox, with keys secured by device keychains or hardware security modules. Administrators can enforce MDM policies and remotely wipe data from lost or stolen devices.

Key Capabilities:

- AES-256 encryption of cached files on mobile devices.
- PIN-derived KEKs with key storage in device keychain/HSM.
- Integration with MobileIron, Intune, JAMF, and AirWatch MDM platforms.
- Remote wipe capabilities for compromised or lost devices.
- Sandboxing to prevent data sharing with non-managed apps.

System Management Security

Centralized management through the CTERA Portal ensures consistent policy enforcement across distributed environments. Role segregation and SIEM integrations ensure compliance while providing administrators full visibility into system operations.

Audit logs are granular and cover authentication attempts, configuration changes, file access events, and system anomalies. Logs are formatted in JSON, making them easy to parse in SIEM platforms.

Example log entry:

```
{
  "timestamp": "2025-09-01T12:45:23Z",
  "event": "ransomware_detected",
  "user": "jdoe",
  "host": "edgefiler-23",
  "action": "session_quarantined",
  "status": "success"
}
```

This log can be forwarded to log data platforms and SIEM where alerting rules trigger SOC workflows. Administrators can configure retention periods, set thresholds for storage utilization, and define responses to logging failures.

Key Capabilities:

- Fine-grained roles: Global Admin, Portal Admin, Compliance Officer, Support.
- Centralized log aggregation via CTERA Messaging Service.
- Integration with SIEM products including but not limited to Splunk and Microsoft Sentinel.
- DAG, DLP, and DAC Integration with platforms like Varonis and Microsoft Purview.
- JSON-formatted audit logs for easy external parsing.
- Configurable retention and alert thresholds for log storage.

Ransomware Defense

Ransomware resilience depends not only on detecting threats but also on the speed and precision of response. CTERA Ransom Protect combines AI based behavioral analytics with honeypot triggers to provide real-time containment. Each detection is automatically mapped to enforcement actions and logged for SIEM correlation, providing both immediate defense and forensic audit trails.

Key Capabilities:

- AI-based behavioral anomaly detection with tunable thresholds.
- Honeypot decoys to detect exfiltration attempts.
- Automated isolation of compromised sessions or shares.
- Real-time SIEM integration for alerting and correlation.
- Forensic evidence preservation for incident response.

Key Management

Encryption key management is central to CTERA's Zero Trust model. Keys are generated and managed client-side wherever possible, and enterprises can choose to manage master keys in their own KMS/HSM. This ensures that only the customer ever controls access to plaintext data.

Key Capabilities:

- DEK per object, wrapped by KEKs.
- Customer-managed master keys with BYOK/HYOK options.
- Integration with Thales CipherTrust and KMIP-compliant KMS.
- Audit logging of key lifecycle events.

Disaster Recovery & Business Continuity

CTERA ensures business continuity through a resilient and fast disaster recovery (DR) framework designed for modern distributed enterprises. Unlike traditional DR approaches that require lengthy manual restores or complex reconfiguration, CTERA leverages metadata-first recovery, CTERA Vault immutability, and intelligent caching to provide near-instant access to data even after site-level disruptions.

In the event of a hardware failure, site outage, or WAN connectivity loss, administrators can rapidly restore access through replacement CTERA Edge Filers. With Instant Disaster Recovery enabled, stub files (metadata) are available almost immediately, while hot datasets are prioritized for hydration. For mission-critical environments, CTERA supports pre-deployed DR Edge Filers configured with Microsoft DFS failover, allowing zero-interruption continuity when a primary site goes down. If both primary and standby filers are unavailable, users can connect directly to the CTERA Portal via WebDAV, ensuring that operations continue until services are restored.

Key Capabilities:

- Metadata-first recovery: stub files appear instantly with background hydration of content.
- Instant Disaster Recovery: frequently accessed files prioritized for immediate availability.
- Pre-deployed DR Edge Filers: DFS failover delivers zero-interruption continuity.
- Immutable recovery points via Vault (WORM) and S3 Object Lock.
- Direct Portal access via WebDAV or CTERA Drive Connect, or Mobile software as a fallback method.
- Cleanroom recovery options for forensic investigation.
- DB Backup to S3 for additional protections.

Data Residency & Control

CTERA enables enterprises to enforce strict data residency and compliance policies through a combination of Zones and Storage Classes. Zones allow administrators to segment the global namespace, defining which Edge Filers may present specific cloud folders or volumes. This segmentation enforces least-privilege access, workload isolation, and regulatory boundaries.

Storage Classes complement Zones by controlling where data is physically stored. Administrators can route files to specific storage targets — for example, keeping classified or regulated data on-premises while allowing non-sensitive data to replicate to external cloud object storage. This ensures compliance with frameworks such as GDPR, HIPAA, and ITAR while optimizing for cost and performance.

Together, Zones and Storage Classes provide a unified mechanism to align who can access data with where that data is allowed to reside, reducing risk, meeting regulatory requirements, and ensuring full visibility and control for CISOs.

Key Capabilities:

- Segment the global namespace into Zones for least-privilege access.
- Define which Edge Filers present specific volumes or cloud folders.
- Route data to approved storage targets using Storage Classes.
- Enforce data residency and sovereignty requirements across geographies.
- Support compliance mandates such as GDPR, HIPAA, ITAR.
- Reduce blast radius by isolating workloads and enforcing placement boundaries.

Compliance & Certifications

CTERA's security architecture aligns with leading compliance frameworks and certifications demanded by regulated industries. Cryptographic modules are validated under FIPS 140-3. The platform is listed on the DoDIN Approved Products List (APL), ensuring suitability for U.S. defense deployments. Additional alignment includes GDPR, HIPAA, NIST 800-171, PCI DSS, and ISO 27001. These frameworks are supported through encryption, logging, access control, and immutability controls.

CTERA's feature set ensures enterprises can demonstrate compliance without bolt-on solutions, reducing complexity and risk during audits.

Key Capabilities:

- FIPS 140-3 validated encryption libraries.
- DISA DoDIN Approved Products List certification.
- Alignment with GDPR, HIPAA, NIST 800-171, PCI DSS, ISO 27001.
- Immutable retention modes supporting compliance investigations.
- Granular role-based access controls to support segregation of duties.

CTERA Data Intelligence Security

CTERA Data Intelligence extends the Zero Trust principles of the CTERA Intelligent Data Platform into the domain of enterprise AI. Its private semantic Retrieval-Augmented Generation (RAG) engine continuously indexes distributed file data, enabling AI models to deliver context-rich insights without exposing sensitive information or bypassing governance policies.

Security is enforced at the core: all AI queries inherit existing identity-based permissions. Users and their AI assistants can only access the files they are authorized to view, eliminating the risk of data leakage. For organizations with strict sovereignty or compliance requirements, CTERA Data Intelligence can be deployed entirely on-premises, ensuring both the data and AI models remain within enterprise infrastructure.

Unlike generic AI connectors, CTERA ensures answer integrity by grounding outputs in verified enterprise data and providing citations for every response. This combination of access enforcement, deployment flexibility, and verifiable outputs allows CISOs to enable AI securely while maintaining compliance posture.

Key Capabilities:

- Sensitive data discovery
- Ingestion with data-filtering, guardrails and anonymization.
- Identity-based access enforcement aligned with existing ACLs.
- Private semantic RAG engine for secure indexing of live enterprise data.
- Full deployment flexibility: cloud, hybrid, or private on-premises.
- Encrypted ingestion and processing across edge and cloud via CTERA Direct.
- Secure enablement of third-party AI (e.g., Microsoft Copilot, OpenAI) without data exposure.
- Grounded, citation-based outputs that prevent data leakage and ensure auditability.

CTERA Insight

CTERA Insight is a multi-tenant SaaS analytics platform for the CTERA Global File System designed around security, scalability, and tenant isolation.

CTERA Insight also provides an immutable, air-gapped audit repository for the CTERA Global File System, ensuring that logs are persistently retained and cannot be altered or deleted. This repository records every file access event over extended durations, delivering the visibility required for regulatory compliance. In the context of ransomware defense, maintaining a tamper-proof audit trail is critical: forensic teams and auditors must be able to trace all user and system activities to detect suspicious patterns, investigate data exfiltration attacks, and demonstrate adherence to industry and government regulations.

Data flows securely and unidirectionally from customer environments into CTERA Insight, eliminating inbound connections and reducing the attack surface. Metadata and audit logs are uploaded via HTTPS/TLS 1.3 into per-portal Amazon S3 “dropzone” buckets. These buckets are encrypted with AES-256 and accessed only with short-lived AWS STS credentials, ensuring strict data segregation.

Each tenant has a dedicated big-data processing pipeline and private database, enabling both real-time and batch analytics while maintaining isolation. The analytics layer is powered by Apache Superset dashboards, secured with Single Sign-On (SSO) via OAuth2/OIDC and Keycloak as Identity Provider. Role-based access control (RBAC) and row-level security ensure users only see data relevant to their tenant.

Compliance and monitoring are built in: Insight is certified to meet SOC 2 requirements, undergoes penetration testing, and leverages AWS Security Hub, GuardDuty, and CloudWatch for continuous auditing and threat detection. Redundancy and disaster recovery features ensure high availability.

Onboarding is secure and streamlined: tenants receive unique API tokens, private resources, and SSO-protected dashboards. With layered defenses, tenant isolation, and AWS-native resilience, CTERA Insight delivers secure and compliant analytics for sensitive enterprise metadata.

Access by CTERA Personnel

CTERA personnel have no access to customer data, encryption keys, or file metadata. Customer content remains encrypted end-to-end, ensuring that CTERA staff cannot view, modify, or decrypt any information. Support activities are strictly limited to diagnostic data that administrators choose to share, preserving tenant isolation and aligning with Zero Trust principles.

CTERA provides two optional mechanisms to assist with troubleshooting, both designed with customer control and transparency:

- **Automatic Crash Reporting** – Customers may enable crash reporting to automatically notify CTERA Support when an Edge Filer experiences a failure. Reports are encrypted in transit (TLS over TCP 443), contain no sensitive or personal data, and include only minimal identifiers such as the system DNS name.
- **Remote Support Sessions** – If direct troubleshooting is required, administrators can generate a time-bound access token (maximum seven-day lifetime) that allows CTERA Support to temporarily access the Edge Filer interface. This process requires explicit administrator action and uses secure outbound TLS over TCP 443. Once the token expires or is revoked, access is completely disabled.

Both features are opt-in and fully controlled by customer administrators. Combined with CTERA's strict encryption model, this ensures that no plaintext customer data is ever visible to CTERA personnel, satisfying enterprise requirements for security, privacy, and compliance.

Secure Development Lifecycle

CTERA's Secure Development Lifecycle (SDLC) underscores our commitment to embedding security into every stage of product development. Security is treated as a design principle, not an afterthought, ensuring resilience against vulnerabilities and reinforcing trust across our customer base.

Our SDLC aligns with industry frameworks such as OWASP, NIST SP 800-218 & 800-52r2, STIG, Secure Software Development Framework (SSDF), and SOC 2 Type II, combining disciplined engineering processes with continuous oversight.

1. **Requirements Analysis and Design**

   A dedicated Security Officer and designated Security Champions actively participate in requirements and design phases. Threat models, data-flow diagrams, and architecture reviews ensure that security controls are specified up front and aligned with regulatory and customer compliance mandates.

   All new features undergo security requirement validation before development begins, ensuring that protection mechanisms are integrated into the architecture from the start.

2. **Implementation and Training**

   CTERA is committed to a culture of security awareness and continual improvement. All product, engineering, QA, and DevOps personnel complete mandatory annual security training under our SOC 2 program, supplemented by quarterly awareness sessions led by the Security Officer.

   Secure coding practices, aligned with OWASP Top 10 and SANS CWE 25, are enforced through automated static analysis, dependency scanning, and source-repository checks that detect vulnerabilities or license risks early in the pipeline.

3. **Testing and Verification**

   Each release undergoes comprehensive security testing to identify and eliminate vulnerabilities prior to delivery. Automated Qualys and Tenable Nessus vulnerability scans cover release artifacts and deployment environments for every version, with reports distributed alongside release materials and made available to customers.

   Independent penetration tests are performed at least annually by accredited third-party experts. Discovered vulnerabilities are triaged according to strict SLAs and tracked to closure. No release is approved without a formal security sign-off, ensuring full traceability and accountability.

4. **Deployment and Release**

   Only signed and verified code is promoted to production through tightly controlled CI/CD pipelines protected by multi-factor authentication. Deployment procedures include cryptographic signing of binaries, controlled release promotion, and rollback mechanisms for immediate remediation if anomalies are detected.

   Incident response playbooks ensure rapid containment and communication in the event of any post-deployment issue.

5. **Post-Deployment and Continuous Monitoring**

   Following release, CTERA maintains continuous security monitoring across production systems. Telemetry and audit data feed into centralized SIEM tools for anomaly detection, correlation, and investigation.

   Regular audits, vulnerability assessments, and continuous improvement loops ensure that new threats, advisories, and lessons learned are integrated back into the development process, maintaining a living and evolving security posture.

CTERA's holistic SDLC ensures that security is systemic, not situational, protecting the integrity of our code, supply chain, and operations, and upholding the highest standards of trust demanded by modern enterprises.

Summary

The CTERA Intelligent Data Platform provides more than just secure file storage — it establishes a foundation of **Zero Trust security, resilience, immutability, and AI Security Intelligence** for the global enterprise. From metadata-first recovery and DFS failover, to CTERA Vault immutability, advanced ransomware defense, and the secure CTTP protocol, CTERA ensures that business continuity is never compromised.

For CISOs and IT leaders, CTERA delivers measurable outcomes: provable compliance with leading standards, rapid recovery from site or connectivity disruptions, full control over cryptographic keys, and strict enforcement of data residency through Zones and Storage Classes. CTERA Data Intelligence extends these protections into the AI domain, ensuring enterprise models and assistants inherit existing identity and governance controls.

Unlike traditional NAS or first-generation cloud gateways, CTERA unifies edge-to-cloud security under one architecture that scales globally and adapts to evolving threats. By combining technical depth with operational simplicity, CTERA positions enterprises to modernize their file services with confidence, knowing that their data is secure, immutable, intelligently governed, and always available.