ctera your files. your cloud.

ENSURE DATA INTEGRITY, IMMUTABILITY, AND REGULATORY COMPLIANCE WITH CTERA VAULT

CTERA's Write Once, Read Many (WORM) tamper-proof protection technology fortifies data resilience while enabling strict compliance with industry regulations.

Immutable Storage: Industry Need Meets Security Necessity

CTERA Vault's WORM technology effectively safeguards data: preventing it from being modified, deleted, or tampered with in any way, either accidentally or maliciously. It gives enterprises full control over sensitive data, with the granularity and flexibility to be applied to any business or regulatory requirement.

CTERA Vault enables the creation of trustworthy and verifiable business records, which are essential not only for regulatory compliance, but also for cybersecurity best practices and in the creation of a permanent record that can be trusted and relied upon for critical decision-making processes.

With CTERA Vault, data is immune to ransomware, accidental deletions, and unwanted changes.

Maintain The Highest Levels of Compliance

WORM-compliant or immutable storage is a requirement spanning multiple industries and verticals. CTERA Vault enables compliance for the likes of HIPAA and 21 FDA CFR Part 11 for healthcare, NIST 800-53 for government, Sarbanes-Oxley for legal services, and Financial Industry Regulatory Authority (FINRA Rule 4511[c]) for financial services, to name just a few.

Access Game-Changing Benefits

CTERA Vault provides organizations with peace-of-mind and confidence in their data management practices:

Elevated Regulatory Compliance

CTERA Vault's WORM-compliant storage meets stringent regulatory compliance requirements, specifically those relating to data retention, preservation, management, immutability, archiving, and auditability. It also helps enterprises meet their legal and ethical obligations.

Maximal Data Integrity

By offering immutability and preventing modification, deletion, or corruption, CTERA Vault provides the ultimate in data integrity – helping combat data loss due to accidental or malicious deletions. Data is now tamper-proof, secure, and reliable, with scalability built in as a core feature.

Enhanced Data Security

CTERA Vault secures data from intentional or accidental tampering. It also ensures data authentication, affords effective safeguards against cyber-attacks, gives a comprehensive audit trail, and provides advanced access controls.

Unmatched Flexibility and Granularity

The CTERA Vault solution is completely customizable, from access controls and user permissions to retention policies, modes, grace periods, and more.

www.ctera.com info@ctera.com USA: (917) 768-7193 Intl.: +972-3-679-9000

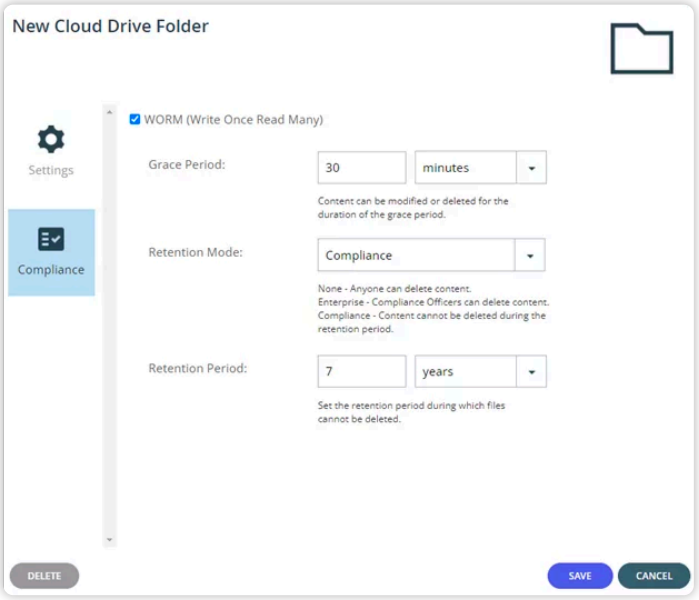
Solution Features

Compliance Officer

This role manages any compliance-related access to files and folders. There are two new settings available for this role: “Allow permanent deletion of files and folders,” and a second setting allowing for management of compliance settings. Even for the Compliance Officer, any permanent deletion requires a valid reason and two-factor authentication.

Customizable Parameters

A grace period offers a window of time before a compliance policy becomes effective and enforceable. After this period, data cannot be modified or deleted, with retention modes of “None” where anyone can delete content; “Compliance” where only the Compliance Officer can delete content; and “Enterprise” where no one can delete content. A retention period can be set ranging from days to years. In Enterprise mode, files cannot be altered or deleted, but a Compliance Officer has the authority to permanently delete them if required. In Compliance mode, even a Compliance Officer cannot delete such files.



Complete granularity and flexibility: including Grace Period, Retention Mode, and Retention Period

Gain Full Visibility

Compliance Officers and Administrators with appropriate permissions gain extra visibility into file properties. Along with typical file details, the Compliance Settings tab provides insight into the WORM setting, retention mode, and expiration date for the file.

Everything is Logged and Traceable

Any attempt to perform an illegal action on a WORM-protected file, such as renaming, moving, modifying, or deleting it (assuming there is an active retention policy, such as Enterprise or Compliance) – whether accidental or intentional – will trigger an error indicating that the action is rejected by the WORM policy. Simultaneously, the system will generate an audit log in the portal, and if available, on a syslog server.