

Sun StorEdge™

NAS Compliance Archiving Software



The rapid growth of electronic fixed content, where data has been written once and never altered, along with business practices and regulatory compliance rulings regarding the retention and protection of information, is forcing organizations to rethink the way they address information management.

Highlights

- Fast, online access to your entire e-record archive
- Provable data integrity and protection
- Software-controlled disk to implement write once, read many (WORM) files that are non-rewritable and non-erasable
- Mandatory enforcement disk volumes configurable to meet stringent requirements (e.g. SEC 240 17-a4)
- Advisory enforcement volumes configurable for less stringent requirements (e.g. business governance)
- Easy-to-view WORM-protected audit logs available to qualified users
- Configuration possible for no single point of failure
- Remote data mirroring support
- Integration with leading enterprise content management applications
- Optional WORM tape support

Businesses are now required to retain and quickly retrieve fixed content, and demonstrate it has not been altered or accessed by anyone other than an authorized user, in order to comply with the laws and regulations mandating records retention. On occasion, these records may defend the company in the event of an audit, investigation, or lawsuit. As a result, the ability to demonstrate the trustworthiness of the records produced becomes imperative.

The Sun StorEdge™ Compliance Archiving System couples the Sun StorEdge NAS Appliance with Sun StorEdge Compliance Archiving Software to provide compliance-enabling features for authenticity, integrity, ready access, and security. The compliance archiving software was designed from the ground up in consultation with information-management-compliance and enterprise-content-management industry experts to help address the most stringent requirements for electronic storage media retention and protection.

The software is available across the entire NAS product line. Flexible configurations include the choice of Fibre Channel, SCSI or serial ATA disk, single- or dual-NAS heads and RAID controller units, or providing file services to a storage area network (SAN), matching your needs for availability, capacity, performance, and cost.

When the Compliance Archiving Software is licensed on the Sun StorEdge NAS Appliance, administrators can create compliance-enabled volumes. It is possible to have multiple volumes on a single Sun StorEdge NAS Appliance, only some of which are compliance-enabled. When each volume is created the administrator can choose to enable compliance with “mandatory” or “advisory” enforcement. Mandatory enforcement is the most stringent form, with features designed to meet strict regulations including the U.S. Securities and Exchange Commission (SEC) Rule 240 17a-4. Advisory enforcement is less stringent and allows a trusted administrator to do certain activities, including reducing the retention time of a file or removing WORM-protected files. Compliance auditing provides an immutable audit trail of all successful and unsuccessful attempts to modify retention times or to modify and delete data that resides on both mandatory enforcement and advisory enforcement compliance-enabled volumes.

Regulatory compliance is about mitigating risk. By focusing on risk management and security as an integral part of its products and services, Sun along with its ecosystem of software and service partners, provides a solid foundation for minimizing risk, from the desktop application through to the back-end archive.

Sun StorEdge™ Compliance Archiving Software and Sun StorEdge Compliance Archiving System features and benefits

Per-file retention period

A file's retention-period specifies how long the file must be preserved on non-rewritable, non-erasable disk. Retention periods may be extended (for legal hold situations or change in fiduciary responsibilities). They may only be decreased on "advisory enforcement" volumes (this allows a file to be removed and is required to satisfy some countries' privacy rules.) The action is captured in the audit log. A new retention-period may be assigned to a file whose previous retention period has expired.

Per-file WORM protection

On "mandatory enforcement" volumes WORM files cannot be modified, extended, or renamed, regardless of the identity or privileges of the user or client attempting the operation. In addition, the critical metadata attributes of WORM files cannot be changed. On "advisory enforcement" volumes, a trusted administrator can shorten retention times and remove files. Actions are captured in the audit log. NAS Gateway system configurations only support compliance with advisory enforcement.

Option for non-WORM file archive

You get the flexibility to set up areas where you can store information you are not yet ready to WORM protect.

Secure clock

A secure clock helps prevent changes to the externally visible system clock from affecting the retention periods of WORM files.

Audit system

An audit system captures and preserves successful and attempted retention-related actions in a WORM-protected log that is easily viewable by authorized users.

Data mirroring

The ability to remotely mirror files to another Sun StorEdge NAS Appliance running the Sun StorEdge Compliance Archiving Software provides for dual copies of all WORM files (and indexes to those files) on non-erasable, non-rewritable media.

Integrity checks for data quality and accuracy

Checks are provided for all data paths through the system, and all places where data can reside, even temporarily. These include a mechanism to automatically verify data correctness — and to automatically detect and correct data corruption.

Integrates seamlessly

Open, standard protocols provide integrated support for Windows and UNIX® clients, plus easy integration with existing information and records management applications.

Graphical user interface

A GUI makes it easy for administrators to set security and network configurations and to perform administrative tasks.

Empty folder rename

An empty folder on a compliance-enabled volume can be renamed. This is beneficial to Windows clients where new folder directories require new names in order to be meaningful.

Administrative security controls

Administrative functions cannot be used to circumvent the guarantees made by WORM files and retention periods.

Lightweight directory access protocol (LDAP) and Windows Active Directory

Lightweight directory access protocol (LDAP) and Windows Active Directory enable integrated authorization and authentication

services between the application and the Sun StorEdge Compliance Archiving System.

Advanced access controls

Only authorized users can gain access to your archived e-records. Mechanisms to enforce this include: Windows access control lists (ACLs) and access tokens; UNIX credentials and permissions; credential mapping, approve lists, trusted host lists, netgroups; cross-platform file locking; and cross-platform authentication.

Antivirus protection

Antivirus software running on a client machine can be used to scan the disks to help identify and eliminate infected files.

Supports a variety of name services

Name services supported include: Active Directory Service (ADS), Windows Internet Naming Service (WINS), Domain Name System (DNS), Network Information Service (NIS), Network Information Service Plus (NIS+), and LDAP to help provide identity and security among systems interoperating with the system.

Multi-client support

Content applications archiving to the system can run on UNIX or Windows clients, enabling you to choose the platform or platforms that work best for your infrastructure.

Cabinet or rack mountable

The appliance and software support integration into an existing, secured data center, or can be purchased inside a lockable cabinet.

Tape backup support

The software can integrate into existing backup schemes using NDMP backup clients offered by popular vendors.