

# AxiomONE SecureWORMfs Software

## Pillar Axiom™ Storage System



### AxiomONE™ SecureWORMfs Advantages

**Simplify** – Organizations can simplify storage management and securely store archive and compliance data without deploying special-purpose appliance solutions

**Consolidate** – Multi-tier storage capabilities of the Axiom platform allows consistent policy-based management of primary business applications alongside archive and compliance storage on one Axiom platform

**Save** – Reduced deployment time, management and training costs, and integrated WORM capability save time and money over managing many dedicated systems

### Enabling Digital Lockdown

Good business practices and governmental regulation are driving growth in the amount and types of data that need unalterable storage in secure archives. Good business practices require long-term digital storage with guaranteed integrity of intellectual property, source code, and specified documents. Regulatory compliance initiatives require similar digital storage methods that guarantee document immutability for a pre-set retention period. Organizations seeking to comply with regulatory requirements need digital storage technologies that enable them to prove to auditors and other interested parties that such data cannot be and is not altered throughout the retention period. Modification or loss of archived data can result in expensive litigation or liability that can damage an organization's reputation.

Tape and optical media are proving unsuitable for these types of archive, which may need to remain available for immediate access. Tape is notoriously unreliable as an archive medium. Both tape and optical archive are complicated and cumbersome to manage, presenting slow restore times and difficulty locating specific files and content. Disk drives are much more reliable, but easy to alter.

Write Once, Read Many (WORM) technology for disk drives provides a software-based data "lockdown" mechanism that guarantees file integrity for long-term archive storage that also remains readily accessible to users. Through its AxiomONE SecureWORMfs software, Pillar Data Systems™ delivers two levels of WORM capability for Pillar Axiom™ NAS storage systems: Compliance and Standard.

In conjunction with content management and archiving applications, SecureWORMfs software allows organizations to establish policy-based, fixed-content archive solutions. It enables time-based retention of non-erasable, non-rewriteable storage for file-based data.

### Capabilities Overview

- **Flexible, centralized policy management** – As with standard filesystems, administrators can provision SecureWORMfs filesystems as needed and set them to grow automatically based on policies.
  - **Complete security and data protection** – Generates digital fingerprints with each file or record to provide proof of immutability. This fingerprint is immediately verified per SEC 17a-4 regulations to guarantee that content is properly stored.
  - **Interoperability with third party applications** – Through its application-programmable interface (API), SecureWORMfs interoperates with popular third party archiving and content management applications. Administrators can set and extend retention and compliance attributes with standard XML. Alternatively, where application integration is not feasible, an auto-protection capability protects content with pre-set retention periods without administrator intervention.
  - **Reliability** – The highly available Axiom platform delivers built-in reliability with redundant components, no single point of failure, and rapid failover and recovery.
  - **Scalability** – SecureWORMfs can store billions of objects, scalable to 384TB per system.
  - **Performance** – The high-performance Axiom platform enables a robust storage repository system, with efficient content management and use of archive space.
  - **Ease of access** – Files are stored in native format, remaining accessible through standard CIFS and NFS protocols.
- **Data migration** – Any open systems backup/recovery application can back up and recover data, and securely migrate data to another storage repository at the end of the useful life of the current Axiom system.
  - **Disaster recovery** – AxiomONE File Replicator (AFR) can provide encrypted replication to remote SecureWORMfs storage to support disaster recovery plans.

### AxiomONE SecureWORMfs Versions

AxiomONE SecureWORMfs software is available in two versions to meet a variety of archive and compliance requirements:

#### Compliance

SecureWORMfs Compliance edition is used to store critical business data stipulated by industry regulations such as Sarbanes-Oxley, HIPAA, the UK Data Protection Act, or SEC Rule 17-a4. Data is retained on the filesystem for a fixed period of time that is specified by file level retention settings and remains unalterable. While storing protected files with unexpired retention settings, SecureWORMfs Compliance enforces that no one can delete files in that storage space.

#### Standard

SecureWORMfs Standard is used to protect stored content that should be non-rewritable to comply with corporate governance initiatives. The SecureWORMfs filesystem retains data in an unalterable state for a fixed period of time specified by file-level retention settings; however, SecureWORMfs Standard allows an authorized storage administrator to reclaim storage space by allowing the deletion of the entire filesystem even if files have unexpired retention settings.

#### System Requirements

Pillar Axiom storage system with AxiomONE Software Release 2.0 or higher