EMC ISILON SmartLock

Protect critical data from unauthorized deletion or alteration

ESSENTIALS

- WORM data protection to prevent accidental or malicious alteration or deletion
- Flexible retention times that can be customized for specific files or datasets
- Certified to meet stringent SEC 17a-4 requirements for business data protection

RELIABLE AND SECURE DATA PROTECTION AND RETENTION

Protecting critical data from accidental deletion or alteration of critical data is a key business imperative for most organizations today. For example, loss of vital data such as engineering design or research and development data could result in significant productivity losses that negatively impact business operations. Securely safeguarding financial data and business records is another critical need for many organizations today to help ensure that they meet necessary regulatory and governance requirements.

Malicious alteration or deletion of critical data is less frequent, but still a concern and many companies have created policies requiring systems to have safeguards in place to protect against such potential attacks. Many organizations also have a need to provide secure, long-term protection for specific classes of data. The final digital master of a movie; historic releases of a software product; design data for a high-rise building are all examples of data assets with a long-term useful life that organizations will want to protect.

EMC® Isilon® SmartLock™ is designed specifically to help you protect your critical data against accidental, premature or malicious alteration or deletion. Because SmartLock is a software-based approach to Write Once Read Many (WORM) data protection, you can store SmartLock-protected data alongside other data types in your Isilon scale-out storage environment with no effect on performance or availability and without the added cost of purchasing and maintaining specialty WORM-capable hardware.

SmartLock operates in either one of two modes—in an Enterprise mode or in a Compliance mode. The Isilon storage administrator must choose the desired mode of operation during the initial cluster configuration. The major difference between the two modes is that in the Compliance mode, login by the root user is disabled, providing the extra level of protection against malicious modification of data required to meet regulatory requirements. This difference is reflected in a side-by-side comparison in Table 1. With Compliance mode, SmartLock can help you to meet regulatory compliance requirements to provide absolute retention and protection of business critical data—including the most stringent SEC 17a-4 requirements.

Data protected with SmartLock cannot be altered by anyone—this includes file data as well as the associated metadata. In the Enterprise mode, this data can be deleted by an authorized administrator. Retention times set under SmartLock are absolute, elapsed time and thereby preclude the impact of potential time zones changes, leap years or other time and calendar-related events which might occur during the retention period.

FLEXIBLE AND EFFICIENT DATA PROTECTION OPTIONS

With SmartLock, you can protect your data at the directory-level and thereby eliminate the wasted space and complexity of managing WORM protections across multiple devices or volumes. SmartLock also offers you the flexibility to set customized default retention times on a directory-level basis. You can also set customized retention times for specific files.

SmartLock is tightly integrated with the Isilon OneFS® operating system and provides a highly efficient storage environment for your WORM data. SmartLock is easy to use and works seamlessly with other Isilon data protection and management software including Isilon SmartPools™ software for automated storage tiering, Isilon SnapshotIQ™ for efficient data backup and recovery and Isilon SyncIQ™ for remote data replication and disaster recovery protection.

A summary of key SmartLock features is provided in Table 1.

Feature	EMC Isilon SmartLock Enterprise Mode	EMC Isilon SmartLock Compliance Mode
Data is Deletion Protected	Yes	Yes
Data is Tamper Protected	Yes	Yes
Privileged delete by Administrator	Yes	No
SEC 17a-4 Compliance	No	Yes
Directory vs. Volume	Directory	Directory
Customized Retention Times for Specific Files	Yes	Yes
Default Retention	Yes	Yes
Customized Retention Time	Yes	Yes
Minimum Retention Period	Unlimited	Unlimited
Maximum Retention Period	Unlimited	Unlimited
Litigation Hold	Yes	Yes
Auto-Delete on Expiration	No	No

Table 1. Summary of EMC Isilon SmartLock Features in Enterprise and Compliance Modes

SmartLock provides secure, highly flexible, policy-based data protection and retention for your critical business data. SmartLock is also certified to help you meet strict SEC 17a-4 compliance requirements and safeguard your data from accidental or malicious alteration or deletion.

CONTACT US

To learn more about how EMC Isilon products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller—or visit us at www.EMC.com/Isilon

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

EMC Isilon Storage Division
Seattle, Washington 98104
1-206-315-7500
www.EMC.com/Isilon