

SECURITY SOLUTIONS FOR EMC ISILON SCALE-OUT NAS

Vormetric File-Based Encryption and Key Management

ESSENTIALS

Key Features and Benefits Include:

- Automatic encryption of any sensitive file, anywhere in the enterprise
- Centralized key and policy management
- Strong separation of duties model that encrypts files and leaves associated metadata in the clear so system administrators can perform their jobs
- Enforcement of role and user based decryption and data integrity policies
- Granular auditing of data access policy supports monitoring and regulatory compliance initiatives

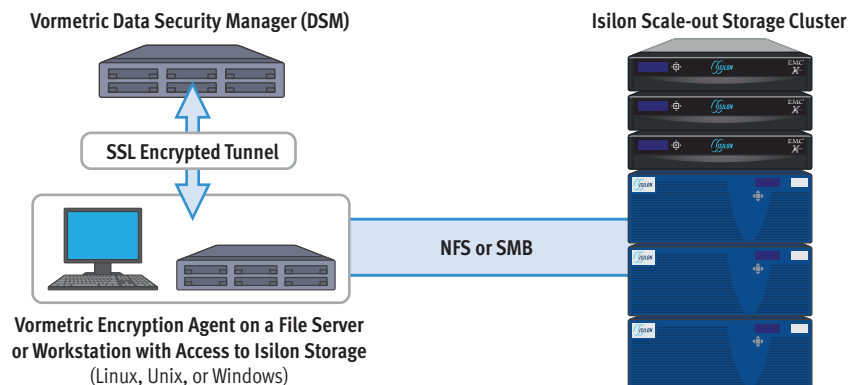
MEETING THE SECURITY CHALLENGE

Internal data governance requirements and external compliance regimes frequently require enterprises to safeguard sensitive data. Requirements for data security arise from a variety of sources including executive mandates to secure intellectual property to external compliance rules such as:

- The Payment Card Industry Data Security Standard (PCI DSS)
- The Sarbanes-Oxley Act
- The Health Information Technology for Economic and Clinical Health (HITECH) Act
- The European Union Data Protection Directive and other EU Data Privacy laws
- Various U.S. State data protection and breach disclosure laws

To address the need for data security, many enterprises take a number of steps including securing data at rest with encryption, controlling access to data and reporting on access to satisfy auditors, regulatory compliance regimes, business partners and customer concerns around data security.

To meet these demanding security requirements, EMC Isilon and Vormetric have teamed to deliver a highly scalable clustered NAS solution with encryption and key management capabilities. This solution protects sensitive information and facilitates compliance with a variety of security requirements.



Vormetric security technologies incorporated into this solution include a host-based software agent and the Data Security Manager appliance. These are described in more detail below:

Vormetric Encryption Expert Agent – resides between database, application or user layer and file system to transparently encrypt/decrypt data. Vormetric agents are installed on each server where data requires protection. The agents are specific to the OS platform and transparent to applications and file systems. Vormetric supports the most commonly deployed operating systems including Linux, Unix (Solaris, IBM AIX, and HP-UX) and Windows.

The agents evaluate any attempt to access the protected data and apply predetermined policies to either grant or deny such attempts. The agents maintain a strong separation of duties model on the server by encrypting files and leaving their metadata in the clear so IT administrators can perform their jobs without directly accessing the information.

Vormetric Data Security Manager – integrates key management, data security policy management and event log collection into a centrally managed appliance that provides high availability and scalability to thousands of software agents. The Data Security Manager stores the data security policies, encryption keys, and audit logs in a FIPS 140-2 certified appliance that is physically separated from the Encryption Expert Agents. The Data Security Manager functions as the central point for creating, distributing and managing data encryption keys, policies, and host data security configurations.

These encryption and key management solutions for EMC Isilon scale-out NAS can be used to address a number of important security needs:

ENCRYPTION OF UNSTRUCTURED DATA

Enterprises typically need to secure a variety of unstructured data including pdf documents, spreadsheets, computer-aided design documents, audio files, graphics images and video files. Unauthorized data access can occur either with data-at-rest (stored on the hard-drive of the Isilon cluster) or data-in-transit (when data is transmitted from the client to server and vice versa). Vormetric encryption and key management technology provides rigorous data security for both of these cases. Sensitive data files are automatically encrypted and access is strictly governed via policies established at the Vormetric Data Security Manager appliance. For example, a policy can allow privileged users (example: root, system administrators) to manage data while not having the ability to decrypt the data, thus enabling a rigorous separation of duties model.

DATABASE ENCRYPTION

Databases contain the information live blood of today's enterprises and frequently require encryption to comply with internal governance or external compliance mandates. Vormetric's file-based technology provides encryption for the most commonly deployed databases in Linux, Unix and Windows environments. Vormetric's external approach also secures files surrounding the database such as Extract-Transform-Load (ETL) files, logs, script files and reports.

DATA SEGREGATION

Enterprises using EMC Isilon scale-out network attached storage (NAS) as a central repository for data from numbers of internal or external entities often need to securely segregate data. In these cases, Vormetric enables each entity to encrypt data with its own encryption key so adjacent entities or administrators cannot view encrypted data.

DIGITAL SHREDDING

For organizations that need to securely remove classified information from a non-classified storage cluster, Vormetric Data Security provides a simple and easy way to ensure that the data is never recoverable even after it has been deleted. Digital shredding enables enterprises to securely repurpose storage or to sell off assets, including storage hardware when those assets are no longer useful to the organization. When a file or folder on a non-classified Isilon cluster becomes classified and needs to be securely deleted, an administrator can encrypt that file or folder using the easy to use Vormetric web interface. A server with access to the Isilon cluster, running the Vormetric Encryption Agent performs the encryption. The encryption keys to that file could then be deleted from the Vormetric Data Security Manager rendering the file contents irrecoverable.

CONTACT US

To learn more about how EMC 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

EMC², EMC, and the EMC logo, are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. © Copyright 2012 EMC Corporation. All rights reserved. Published in the USA. 01/12 Solution Overview H8324