Datasheet

NetApp SolidFire Element OS Full Disk Encryption

Comprehensive data security and compliance protection

Key Benefits

High Security

Securely protect data from unauthorized access while in use and during the decommissioning of disk drives with the AES-256 encryption standard.

Simple Administration

Enable easy administration of self-encrypting drives with transparent protection of all data from multiple applications.

High Performance

Efficiently encrypt data for exceptional data security with no performance impact.

The Challenge

Data is a company's most valuable asset. Organizations must protect their sensitive customer information, intellectual property, and proprietary data or risk lost revenue, legal implications, and tarnished reputations. At the same time, data security risks are on the rise. Data at rest is especially vulnerable to loss or attack as disk drives leave the data center for retirement, relocation, or maintenance.

The negative impacts of data security breaches can include:

- Loss of customers and revenue
- Unplanned expenses
- Legal implications, penalties, and fines
- Negative press and tarnished reputation
- Lost goodwill and undermining of other corporate relationships
- Expense of risk remediation services for exposed customers

The Solution

NetApp® SolidFire® Element® OS full disk encryption (FDE) provides comprehensive security for data at rest without sacrificing storage system performance or ease of use. The system uses a 256-bit password distributed across all the nodes in the system and prevents administrator access to the keys.

With Element OS FDE, data management is as simple and robust as the data protection it provides. Element OS FDE combines local key management with self-encrypting drives, effectively protecting data from unauthorized access or modification resulting from theft, loss, or repurposing of disk drives. Simple and intuitive configuration makes the solution easy to manage.

High Security

By embedding the intelligent management of self-encrypting drives in the software, Element OS FDE eliminates the day-to-day administrative tasks of managing disk security without allowing administrator access to the keys. Element OS FDE supports Advanced Encryption Standard (AES-256) algorithms approved by the U.S. government for protecting secret-level classified information. Element OS FDE provides strong protection against unauthorized data access during the routine activities of servicing, repurposing, and decommissioning of drives.

Protecting Against Theft

For additional peace of mind, Element OS FDE encrypts the cluster-wide password, which is used to secure access to each drive. The system then stores the password across multiple nodes in the cluster. At least two nodes are required to assemble the password to unlock the drives; three nodes are required to bring the cluster back online and access data.

The cluster-wide password used to lock drives is unique to each cluster. If any number of drives are removed from the system, the password is not present on the drives, and all data is encrypted. Therefore, a drive or a node removed ungracefully from a cluster cannot be accessed until it is securely erased or returned to its original cluster.

Simple Administration

Element OS FDE makes self-encrypting drives as easy to manage as traditional drives with transparent key management. As an administrator, you can set security authorizations and apply them to all self-encrypting drives within the cluster. Doing so enables you to eliminate complexity and easily manage system communication without modifying host operating systems or applications. This powerful yet easy-to-administer storage feature enables you to seamlessly manage all applications with high security requirements.

There is also no need for administrators to recreate keys. Keys, both drive-level and cluster-level, are automatically regenerated when a drive is removed from the system. For example, the system might regenerate keys if a drive fails or a storage node is returned to a factory default setting.

High-Performance Encryption

With Element OS FDE, the self-encrypting drives enable data security with no performance impact. Other encryption methods that take place at the software or host level might negatively affect processing resources. Using simplified drive encryption management, Element OS FDE does not take CPU cycles from the host or interrupt the transfer of I/O to the hosts.

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit www.netapp.com. #DataDriven