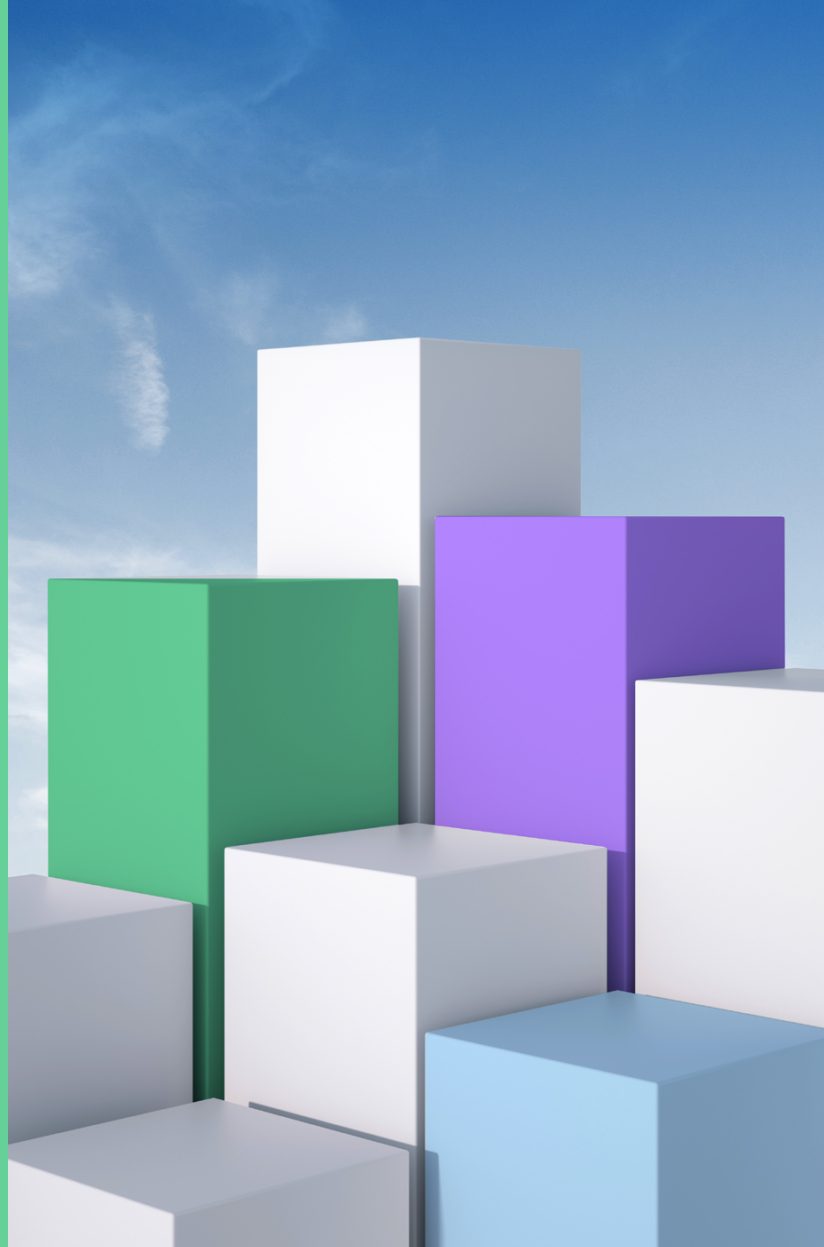


DATASHEET

# Element Software security designed for multitenancy

Element software powers  
NetApp SolidFire to build  
secure automated, scalable,  
and predictable private clouds.



As cloud architects search for new ways to consolidate workloads, automate their environments, and simplify their infrastructure, more and more organizations are building private clouds. NetApp® Element®, the software behind NetApp SolidFire®, is designed to scale for environments that handle diverse workloads for a variety of customers.

To ensure the security of each customer's data, the Element scale-out storage system offers a mix of features to manage access for the right users and the right volumes, in addition to encryption and network security.

### **The Challenge**

Securely managing access to data in a multitenant environment can be complicated, especially in a large-scale private cloud with a diverse array of workloads and customers sharing a general-purpose infrastructure.

### **The Solution**

Designed to consolidate workloads and guarantee performance in multitenant environments, Element software offers a collection of features to simplify managing data security.

The Element API allows architects to automate security for their storage infrastructure, from user and volume access to enabling drive encryption and securing data at the network level.

### **Element on NetApp SolidFire**

NetApp Element software on SolidFire delivers agile automation of your storage infrastructure through scale-out flexibility and guaranteed application performance so you can build clouds to accelerate new services:

- Achieve nondisruptive system expansion with instant resource availability.
- Deliver predictable performance to hundreds of applications on a single platform.
- Drive your business forward with automated operational simplicity.
- Provide flexible deployment models to fit the needs of your next-generation data center.

**Keep your consolidated workloads secure at every level.**

#### **User Security**

Authorize and authenticate users to your system and grant access with centralized user management.

#### **Volume Security**

Manage access to volumes in a diverse environment with multiple tenants.

#### **Data Security**

Multiple drive encryption options ensure security at the hardware level.

#### **Network Security**




Isolate traffic in flight to prevent volume visibility between different tenants' data.

---

### **About NetApp**

In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services and applications to the right people—anytime, anywhere. [www.netapp.com](http://www.netapp.com)

		
Software or feature	Function	Impact
LDAP/Active Directory	User authentication	Centralized user management
CHAP and Access Group	Storage client access management	Manage and enforce storage client access to volumes
VLAN	Network traffic isolation	Isolate tenant data in flight to ensure that tenants have visibility only to their own data over the network
Logging	Identify and maintain record of user activity	Quickly identify sources of potential security threats by connecting users to their activities
Encryption	Hardware and software level data security	Secure data at rest to protect drives from being accessed by bad actors
Secure Erase	Cryptographically wipe data at rest	Provable data erasure for the entire drive
FIPS 140-2	Third-party-certified encryption standards	External validation of encryption practices for customers who require certain levels of security compliance
External key management	Use third-party key manager	Centralized and replicated encryption key management ensures control and high availability—never lose your key availability
Multifactor authentication	SAML-based user authentication	Centralized multifactor user authentication
TLS	TLS 1.2 used for secure UI and API communication	Ensures that all management traffic is protected by strong cryptography
Onboard key manager	Self-contained encryption key manager for data at rest	Drive encryption can be managed through Element software without a third-party service
Login and message of the day	Login banners are printed in the output before authentication	These banners enable organizations and administrators to communicate with system users
Role-based access control	User-level authorization	Defines different types of access based on different categories of users
Secure Volume Access	Client access and network isolation	Isolate client data access via preferred virtual networks

