DELL Technologies

APEX Data Storage Services – Security Best Practices

Dell Corporate Security & Resiliency Organization • Version 1.1 • Last Updated 08-18-2022

Executive Summary

IT organizations continue to face challenges in their technology transformation journeys, such as:

- Over / under-provisioning
- Capital budget constraints
- Lengthy procurement cycles
- Complexity in infrastructure migration
- The rapid pace of technology change
- Limited IT staffing resources and skillsets

IT leaders are looking for a much simpler and more agile experience. APEX Data Storage Services is an as-a-Service portfolio of scalable and elastic storage resources designed for OpEx treatment.[1] This offer enables you to optimize for simplicity by reducing over and under-provisioning as well as complex procurement and migration cycles. You can easily manage your as-as-Service experience through a single interface — the APEX Console.

This paper draws on secured development strategies, which are foundational for designing and developing applications and programs at Dell. The focus of the white paper is an on-premises APEX Data Storage Services deployment scenario.

This white paper reviews:

1. Security risks organizations should consider.
2. Responsibilities associated with securing information through the Shared Responsibility Matrix.
3. How APEX Data Storage Services security strategies and measures protect the security and integrity of your data.

APEX Data Storage Services Security Considerations

Organizations should be sure to consider the potential risks associated with integrating third party infrastructure into the data center environment. Some key security considerations for organizations currently using or planning to use storage delivered in an as-a-Service model include:

- **Security governance:** Security governance is critical because it delineates the respective responsibilities of the service provider and the customer. Dell has its own security governance that is mapped to several industry important frameworks and controls. These can be found later in this document in Security and Compliance section.
- **Data protection considerations:** Storing highly sensitive data and information on third party storage systems presents additional risk to customers. A breach of sensitive data could lead to both tangible and intangible losses, such as business reputation, which may have a direct impact on organizational profitability and may also culminate in potential regulatory issues. Therefore, as-a-Service customers need assurance about data protection, including but not limited to confirming that the service provider has risk mitigating controls in place.
- **Legal/Compliance:** Organizations considering private or public storage services should be sure to understand the legal implications associated with the types of data that can be stored with the storage

[1] OpEx treatment is subject to customer internal accounting review and policies.

provider. Among other things, applicable law (e.g., GDPR and CCPA) and the sensitivity of the stored data may have a significant impact on the implicated risks associated with your approach to data storage.

Risks that Dell will mitigate are associated with security of the service offer and the supporting infrastructure. It is the responsibility of the customer to manage the risks related to the operation of the data, systems, and applications within the cloud.

APEX Data Storage Services Customer and Dell responsibilities

In addition to the option for Dell-managed Block and File services, customers have the flexibility and control to choose who performs day-to-day management operations. With Dell-managed, you maintain operational control of workloads and applications while Dell manages and maintains the on-premises infrastructure. Alternatively, IT organizations seeking even more control over the as-a-Service experience may choose the Customer-managed option, designed to empower you with ownership of tasks such as monitoring capacity utilization, infrastructure management and resource optimization.

A shared responsibilities model has been developed which clearly delineates the respective roles between the customer and Dell on a function-by-function basis, as well as shared levels of responsibility. It spotlights an application delivery strategy that allows customer teams to focus on day-to-day operations without the necessity of worrying about the underlying infrastructure for the service.

For a detailed overview of roles and responsibilities, please review the documentation located here: https://www.dell.com/support/home/en-us/product-support/product/apex-data-storage-service/docs

Category	Service Activity	Customer managed		Dell managed	
		Customer	Dell	Customer	Dell
Deploy	Power, space, HVAC, access to customer data and management network*	✓		✓	
	Remote connectivity – providing access to telemetry for usage and health monitoring*	✓	✓	✓	✓
	Installation and initial provisioning		✓		✓
Monitor	System performance, capacity and availability	✓			✓
	Configuration changes to maintain performance and uptime commitment	✓			✓
Operate	Implement firmware and system software updates (system maintenance)**	✓			✓
	Define and maintain data protection, sync and snap policies	✓		✓	
	Manage data access - volumes, NFS exports and SMB shares	✓		✓	
Optimize	Performance and configuration recommendations	✓			✓
	Proactive capacity expansion and buffer management	✓			✓
Support	24x7 proactive hardware and system software support and onsite parts replacement		✓		✓
	Operational how-to guidance		✓		✓
Decommission	Onsite data sanitization and asset recovery with customer coordination		✓		✓

*For Dell-managed colocation facilities, Dell holds primary responsibility for these activities

**For Customer-managed option, the customer is responsible for initiating semiannual system maintenance. For Dell-managed option, system maintenance is provided ongoing as needed

How Information is Secured

For Customer-managed solutions it is the customer's responsibility to implement, maintain and support all security configurations and activities affecting infrastructure deployed to customer location for security and compliance, access control, threat and vulnerability management, data encryption, and incident response.

APEX Console

The self-service IT management console reduces complexity to make it easier to identify, deploy, monitor, and expand solutions quickly, so you can meet business requirements while reducing operational risk. The reduction in complexities and operational risks through the console provides a simple yet secured way for managing the services.

Security and Compliance

APEX Data Storage Services protects Dell and customer data utilizing policies and strategies from established frameworks. This can assist customers to meet their own compliance program requirements. Where applicable, application and product development at Dell utilizes mappings to these established frameworks and regulations to help ensure that appropriate security principles and requirements are reflected in the development lifecycle. The security measures that protect APEX are inspired by CCM, ISO, and NIST standards, regulations, and control frameworks to ensure security assurance.

- NIST Security and Privacy Controls for Federal Information Systems and Organizations
- ISO 27000 Information Security Management Systems
- CCM Cloud Control Matrix

Access Controls

Access to information stored in the underlying infrastructure of APEX Data Storage Services must be protected against unauthorized access, disclosure, and modification. The following access control practices help to maintain security for data access:

- Business case considerations for higher levels of assurance
- Identity trust verification and information processing interoperability (e.g., SSO)
- Permissions and supporting capabilities for customer controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions

Threat and Vulnerability Management

APEX Data Storage Services supports threat and vulnerability management strategies to ensure the infrastructure is protected against identified risks and vulnerabilities. These threat and vulnerability management strategies are drawn from methodologies used in Dell's secure development lifecycle, including:

1. Consistency in patching the underlying infrastructure ensures the most current and updated features and security gaps are implemented. Dell uses a regulated methodology for scanning the underlying infrastructure for APEX Data Storage Services.
2. Methods to identify security risks/vulnerabilities are deployed as a component of APEX Data Storage Systems. These methods include both security scans and security testing.

Note: Customers retain the responsibility to ensure that the applications connected to APEX Data Storage Services infrastructure are consistently managed and updated to prevent them from being used as attack vectors.

Encryption

APEX Data Storage Services has the ability to encrypt data using NIST approved algorithms defined per NIST Special Publications 800-131Ar2. NIST Crypto Algorithms defines the use of cryptographic algorithms and key lengths. Here are standards Dell uses for consideration on Public Key Infrastructure to protect assets and information:

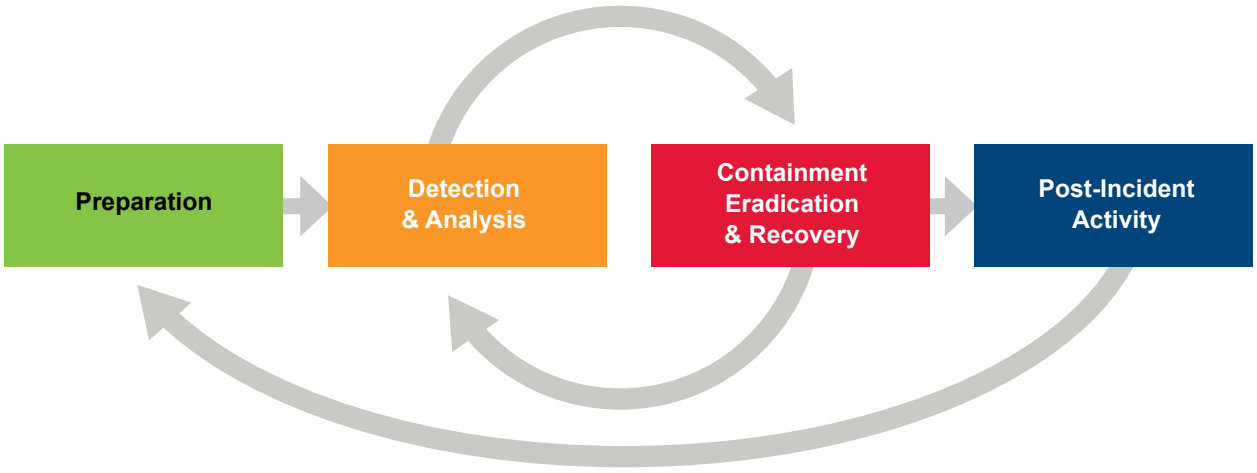
- Deprecated cryptographic algorithms are disabled by default
- Data classified as sensitive while in transit and at rest, can and should be encrypted
- Key length for symmetric keys must be at minimum 256 bits
- Key length for asymmetric keys must be at minimum 2048 bits for RSA and DSA and 256 bits for Elliptical Curve (EC) algorithms
- TRIPLE DES (3DES) must be strengthened to AES 256-bit baseline for all applications

Incident Response

Dell addresses security incidents and events pursuant to a documented methodology for reporting and management. This process ensures customers are timely notified where necessary and that appropriate steps are taken to resolve the incident.

Dell follows the following process for incident response:

- Preparation
- Detect/Analysis
- Containment/Eradication
- Recover
- Report



System Auditing and Accountability

APEX Data Storage Services leverage compliance and assurance processes to continuously assess the effectiveness of the security controls in place for protecting data and information on the platform. This includes periodic audits and assessments to identify and remediate non-compliance.

Independent reviews and assessments are performed by Dell to ensure APEX, which builds on established frameworks such as the Cloud Security Alliance's CCM, conforms to established industry policies and standards.

The assessment will include:

- Host Assessment
- Web Application Assessment
- Web Services Assessment
- Mobile Assessment
- Binary Assessments (where applicable)

Secure Connect Gateway

Secure Connect Gateway is a secure, two-way connection between APEX Data Storage Services and customer infrastructure. Establishing the Secure Connect Gateway tool will create a secured transfer of data and use by only authorized users/devices. This solution provides proactive wellness monitoring and issue prevention.

The customer is responsible for maintaining users, their corresponding attributes, and building their connections within their own infrastructure. Dell will be responsible for management of the supporting servers and networks that will support the communication. The services require highly secured protocols from Dell and the customer for all communications. Dell will also provide configuration guides during deployment.

Conclusion

APEX Data Storage Services will be an enabler for your transformation journeys with the capability to demand and scale storage needs with this powerful Storage as-a-Service solution. Customers can be assured of Dell's commitment to providing a reliable, private, and secure experience for the collection, communication, transportation, use and storage of data within the APEX Data Storage Services infrastructure.

For more information on APEX Data Storage Services, please visit Dell.com/APEX-Storage

Glossary

Term	Definition
APEX	APEX is a portfolio of Dell Technologies as-a-Service offerings that simplify digital transformation by increasing IT agility and control.
NIST	National Institute of Standards and Technology
EC	Elliptical Curve
RSA	Rivest–Shamir–Adleman
AAA	Authentication, Authorization, and Accounting
CCM	Cloud Control Matrix
DSA	Digital Signature Algorithm
SSO	Single Sign On
OpEx	Operating Expenditure
GDPR	General Data Protection Regulation
CCPA	California Consumer Privacy Act
AICPA	American Institute of Certified Public Accountants
PCI DSS	Payment Card Industry Data Security Standard
CSP	Cloud Service Provider