DELL Technologies

APEX Data Storage Services Security

November, 2021

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. Dell Technologies 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 eliminating 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 Dell Technologies' 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.
- **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:** 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 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.

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

APEX Data Storage Services Customer and Dell responsibilities

APEX Data Storage Services is customer operated with infrastructure that is owned and maintained by Dell Technologies.

A shared responsibilities model has been developed which clearly delineates the respective roles as between 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 Dell Technologies and customer roles and responsibilities, please consult the Service Offering Description located on https://www.dell.com/learn/us/en/uscorp1/apex-terms.

Category	Service Activity	Customer operated	Dell maintained
Deploy	Ensure site readiness - power, space, HVAC, customer data and management network	✓	
	Remote connectivity - providing access to telemetry for usage and health monitoring (VPN)	✓	
	Installation and initial provisioning		✓
Monitor	System performance, capacity, health status and availability		✓
	Configuration changes to maintain performance and uptime commitment		✓
Operate	Implement firmware, system SW updates and HW upgrades		✓
	Define and maintain data protection, sync (business continuity), and snap (data loss prevention) policies	✓	
	Manage data access - volumes, NFS exports and SMB shares	✓	
Optimize	Monthly performance and configuration recommendations		✓
	Proactive capacity expansion and buffer management		✓
Support	24x7 proactive HW and system SW support		✓
	Operational how-to guidance		✓
Decommission	Onsite data sanitization and asset recovery with client-side coordination		✓

How Information is Secured

APEX Console

The self-service IT management console reduces complexity to make it easier to identify, configure, 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. The console provides security through ensuring customers have visibility into the services they are using. Attempts to make unauthorized changes can be quickly noticed from the Console dashboard when an administrator logs into the system.

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 map to numerous industry-accepted security standards, regulations, and control frameworks, including but not limited to:

ISO 27001/27002/27017/27018: The International Standard Organization (ISO) specification for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system within the context of the business activities of the organization and the risks it faces. These standards also offer collection of commonly accepted information security control objectives and controls and includes guidelines for implementing these controls.

NIST SP 800-53 revision 4: A publication of policies and framework for the protection of information systems against insider threats, application security, supply chain risks, advanced persistent threats, and the trustworthiness, assurance, and resilience of information systems.

AICPA TSC: Published criteria to be used for evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the systems at an entity or organization.

ENISA Information Assurance Framework: set of assurance criteria that organizations can review with cloud service providers (CSPs) to ensure they have sufficient protections in place for customer data. The IAF is intended to assess the risk of cloud adoption and reduce burden on CSPs.

German BSI C5: A publication developed by the German Federal Office for Information Security (BSI) as a mechanism for assessing the information security of cloud services.

PCI DSS: Publication and development of security standards for securing payment data and information.

GDPR: The governing regulation in the European Economic Area (EEA) addressing privacy and the protection of personal data. One of main objectives of the law is to ensure personal data are protected inside and outside of the EEA. Companies are held to strict standards in the protection of data.

By leveraging these mapped industry standards, APEX incorporates industry best practices in cybersecurity, product development, privacy, enterprise resiliency and compliance. More information about information security from some of the respected industry standards are listed here:

- NIST Security and Privacy Controls for Federal Information Systems and Organizations
- The Payment Card Industry Data Security Standard
- COBIT | Control Objectives for Information Technologies
- ISO 27000 Information Security Management Systems
- ENISA Information Assurance Framework
- GDPR

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 and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, separation of duties, emergency access, large-scale provisioning or geographically distributed deployments and personnel redundancy for critical systems)
- Identity trust verification, service-to-service application (API) and information processing interoperability (e.g., SSO and federation)
- Account credential lifecycle management from instantiation through revocation
- Account credential and/or identity store minimization when feasible
- Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions

All access must have an audit trail that includes request, approval, creation, modification, recertification, and removals.

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 vulnerability scans and penetration testing.
3. System configurations are monitored and compared to a user configurable evaluation plan at which point a risk level is assigned to each system.

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 not supported
- Data in transit and at rest, due to their classification and protocol used may be encrypted
- Customers are responsible for their key management for their cryptographic infrastructure
- 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:

- Triaging and logging the incident
- Escalation procedures
- Documentation of the incident
- Defined methodology for engagement with impacted customer(s)

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 at least annually 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 Remote Connectivity

Connectivity between customer infrastructure and APEX Data Storage Services is supported through Virtual Private Network services. Establishing Virtual Private Networks (VPNs) ensures that data is secured in transit and that only authorized users and devices can access it. Customers connect over site-to-site IPSEC-based VPN tunnels so that data can be shared bi-directionally in a secured manner.

Customer is responsible for internet services, VPN network equipment and management at their service locations. Dell is responsible for the management server equipment and the management platform at the customer site. The network design for remote connectivity requires a highly secure protocol to be adhered to by both Dell and the customer. Customers must adhere to Dell’s standard protocol configuration as advised during deployment, and as updated by Dell from time to time. Future updates of APEX will review the connectivity through VPN.

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.

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
VPN	Virtual Private Network
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