Dell APEX Cyber Recovery Services – Security Guide

November 2022

H19310

White Paper

Abstract

This paper describes the internal security controls, and suggested best practices and recommendations, to guide customers who use Dell APEX Cyber Recovery Services. It also describes the shared security responsibilities between Dell Technologies and the customer.

Dell Technologies

Copyright

Published in the USA November 2022 H19310.

Contents

Executive summary

Overview

Dell Technologies is expanding its available Cyber Recovery offerings to include the APEX Cyber Recovery Services solution (the “Service”). The importance of having an on-premises, isolated, immutable cyber vault that protects critical data is now empowered by a Dell Technologies managed service. As customers embrace as-a-Service consumption models, such as APEX, cybersecurity is a top priority.

Maintaining the availability of customer’s data within the Service is paramount and a core priority for Dell. Importantly, the overall security of this Service is a shared responsibility between Dell and the customer.

This paper describes the security measures in use by Dell designed to secure remote management of the Service. This paper also defines the shared responsibilities between Dell and the customer as it relates to the Service.

Cybersecurity approach – from attacker perspective to a secured solution

In Dell services, cybersecurity is of great importance to us. Our approach to address cyber threats and risks is based on the attacker point of view. We use the MITRE ATT@CK framework, a knowledge base and model for observed cyber adversary behavior, reflecting the various phases of an adversary’s attack life cycle and the platforms they are known to target. Through this approach, we identify what an adversary can do and define how to protect against the veritable attack vectors in the most effective way to secure the Service by design.

Layered security is a supplementary approach we use to ensure that a security system will leverage the protection in multiple layers, to slow, block, delay, or hinder a threat until it can be completely neutralized.

Revisions

Date	Description
November 2022	Initial release

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Eyal Haver

Note: For links to other documentation for this topic, see the Data Protection Info Hub.

APEX Cyber Recovery Services

Overview

APEX Cyber Recovery Services is a fully managed solution that isolates critical data and is designed to help defend against cyberattacks and ransomware. This Service simplifies recovery operations and speeds recovery after a cyberattack by having Dell manage day-to-day cyber recovery vault operations and assist with recovery activities. With expertise from more than 1,100 isolated, immutable, intelligent vault solutions deployed globally, Dell works with customers to apply templated recovery runbooks to assist customers in their recovery. The Service helps with the recovery of business operations with standardized configurations and simplified Dell-assisted recovery options, allowing for better control over growing cyber threats. However, it should be noted that the Service is not a replacement for a customer's real-time security tools and applications. Customers are responsible for implementation and use of security tools and applications within their environment.

The Service includes:

- Standard hardware configurations with Small (100-200 TB), Medium (150-300 TB), or Large (300-600 TB) vault capacity options
- Dell-assisted recovery options
- One or three year subscription terms
- A Dell-managed cyber recovery vault deployed in the customer's on-premises data center
- Intelligence with CyberSense to detect anomalies in the data protected in the vault
- Regular recovery testing to mature recovery processes
- A Customer Success Manager serving as a trusted advisor and primary contact throughout the Service

Shared responsibility model

The security of APEX Cyber Recovery Services is a shared responsibility between Dell and the customer. Dell is responsible for logically securing the infrastructure; the customer is responsible for the physical security for all solution components deployed within their location. The customer is also responsible for any other security functions, compliance with internal and external processes, policies and regulations, and industry best practices.

The customer is also responsible for the security of the data that is transported to and from the vault and for identifying the data to be protected within the vault itself.

Lastly, the customer is responsible for the network security to and from the vault, and for identity management of customer users connecting to the vault.

The overall security of APEX Cyber Recovery Services is achieved through the shared responsibilities of Dell and customers. When consuming the Service, some responsibilities are transferred from the customer to Dell. Figure 1 illustrates the areas of responsibility between Dell and customers.

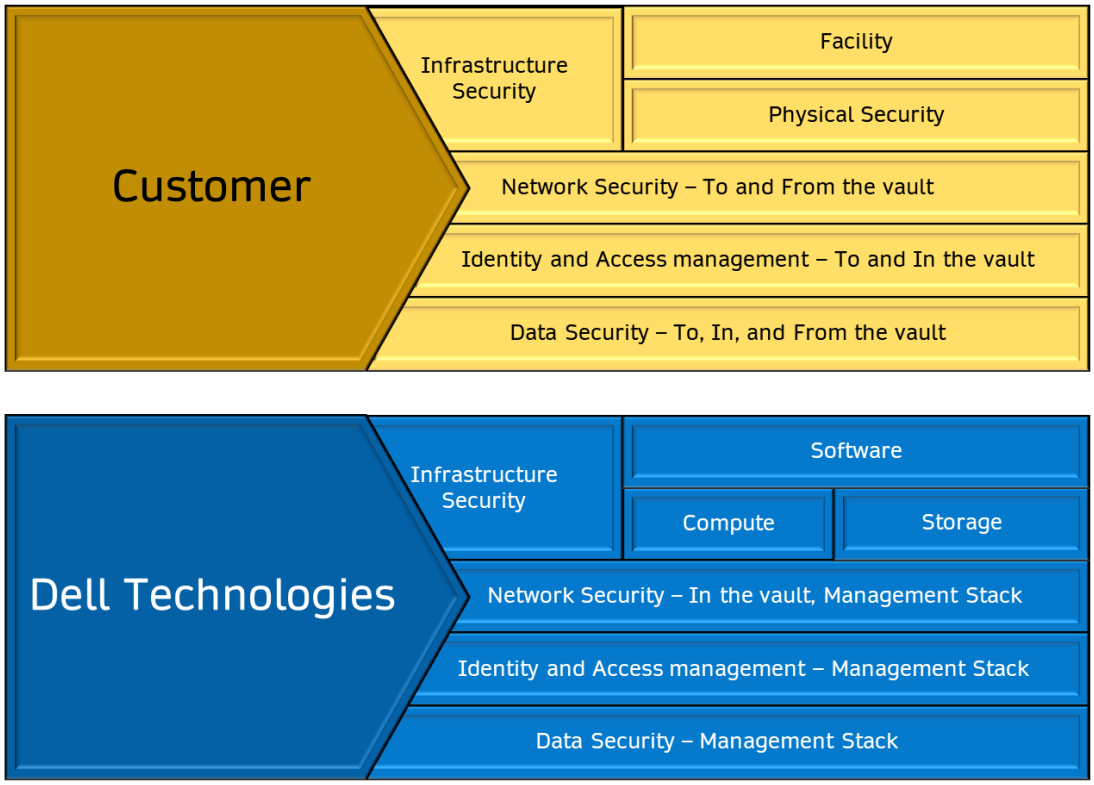

Figure 1. Shared responsibility model for APEX Cyber Recovery Services

Architecture

The Service contains several different architectural components and zones that constitute the security capabilities as illustrated in Figure 2.

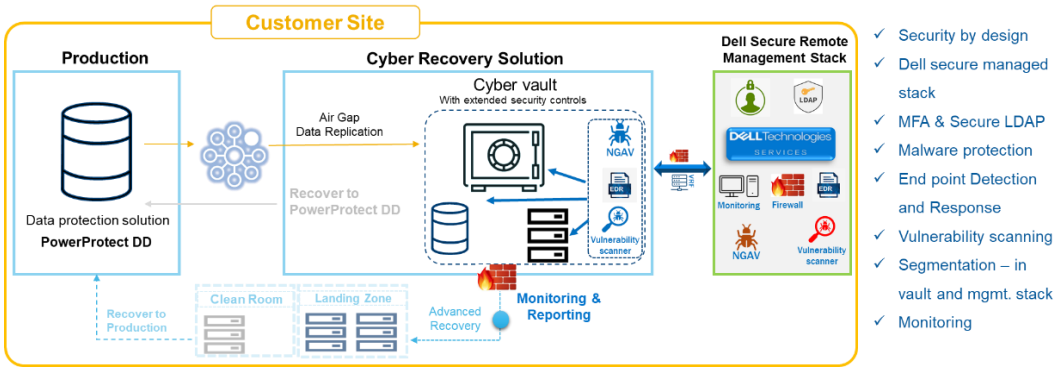

Figure 2. Service design

Dell data centers host the Cloud Management Services Platform (CMSP) backend management systems. The Services also have a secure portal for Dell engineering teams to manage and monitor the solution using Dell's onsite management stack.

The Dell onsite management stack is a physical component (hardware and software) deployed within the customer's data center. Once deployed and provisioned by Dell teams, the management stack provides the following:

- Telemetry Collection: Handles telemetry data, events, logs, and other data points
- Connectivity functions: Provides secure connectivity for transferring telemetry (file and message) between customer on-premises and the Dell CMSP platform using secured protocols
- Support Functions: Provides configuration management, remote takeover, troubleshooting, COTS/3rd party integrations, and ticketing automation
- Orchestration and control: Execution tasks against assets as defined in the Service
- Individual product APIs or element managers: Intent, declarative, or outcome configuration, direct/imperative for direct configuration, policy settings, and so on
- Local intelligence: Error detection with automated remediation, configuration integrity and drift, and Service optimization tuning
- Connectivity between Dell's data center and the customer on-premises data center is solely a responsibility of the customer

Infrastructure security

Infrastructure security is the foundation for all the Service components built on top of it. Infrastructure security encompasses the lowest layers of security, from physical facilities to configuring and implementing security of the compute, storage, and networking hardware and software used to deliver the Service.

Facility security

The customer is responsible for the physical security of the facility hosting this Service. It is recommended to include:

- Access controls to limit physical access to the locking cabinets only to authorized personnel and biometric, proximity cards, or similar technologies to restrict access to the cabinets
- CCTV to monitor physical access to the vault and the onsite management stack
- Support of on-site UPS systems and backup generators to ensure Service availability if there is a power failure
- Data center is protected against damage from human or natural disasters

Compute, storage, and network security

Dell is responsible for the security of the services solely within Dell's control. Dell installs and maintains the infrastructure according to its policies, including:

- Host security hardening configurations
- Anti-malware protection
- Endpoint detection and response
- Maintaining up-to-date device firmware
- Performing regular security tests and vulnerability scanning

Software security

Dell software solutions are developed according to industry security standards. A Secure Development Lifecycle (SDL) methodology prevents software vulnerabilities and design weaknesses from being introduced into Dell products and applications while they are built.

Dell is also responsible for periodic vulnerability scanning and updating of other software used in the managed infrastructure, such as compute, storage, and network. Dell neither monitors, nor accesses, customer data.

If a customer requires additional redundancy in the Service, engage your Dell sales team for further discussions.

Logging and monitoring

The Service includes logging and monitoring of security events. Dell monitors all Dell-controlled Service components 24x7, including racks, power, environment, and networking up to the top-of-rack (ToR) switch. Incident management is also performed 24x7.

Penetration testing

Dell has performed a third-party external penetration test on the Service's infrastructure.

Network security

Network security is defined as the process of protecting resources from unauthorized access or attack by applying controls to network traffic. The goal is to ensure that only legitimate and authorized traffic is allowed. Network security is a shared responsibility between Dell and its customers. The Service relies on layers of network security.

Separation and isolation

The Service has a designated rack containing both the vault and the management stack deployed in the customer's data center. The vault has separation and isolation capabilities that are achieved with dedicated hardware and software. The vault is secured from the customer's production infrastructure through a logical air gap, and from the Dell CMSP backend management system through designated hardware and software security controls.

Network security controls include the use of secure connectivity between the onsite management stack to the vault, using VRFs, VLANs, and encrypted communication. These controls enforce and maintain separation and isolation of the vault to prevent customer telemetry and data from becoming visible to unauthorized users.

The APEX Cyber Recovery vault and the PowerProtect DD in the customer data center are isolated on separate networks. An operational logical air gap separates the networks between the source PowerProtect DD at the customer data center and the PowerProtect DD in the vault. This communication is closed until the Cyber Recovery Manager instance inside the vault turns on the communication port for a replication request. After the replication is completed, the physical communication port on the PowerProtect DD in the vault is turned off again.

Network connectivity security

Security of the network connectivity between the different zones of the Service, as illustrated in Figure 1, is a shared responsibility between Dell and customer.

Dell owns, and is responsible for, the security of the communication channel from the onsite management stack to the vault. Traffic to and from the Service is encrypted using TLS v1.2/v1.3 and separated through a dedicated firewall.

The customer is responsible for configuring network firewall rules for the traffic between the CMSP and the Service. Dell is responsible for securing and separating the remote management using designated Dell-managed network security.

Dell provides an additional network security layer to secure the communication between CMSP and the Service. The measures to secure this network are combined technologies that include VRF defined at top of rack (ToR), VLANs, and encryption communication through a designated firewall.

Secure remote access

Excluding physical security, which is a customer responsibility, Dell has end-to-end responsibility for the security of the onsite management stack, including:

- Infrastructure Security (Compute, Storage, and Network Security): Dell installs and maintains the infrastructure according to its policies. These include host security hardening configurations, anti-malware protection, maintaining up-to-date device firmware, and performing regular vulnerability scanning.
- Software Security: The logical security of the onsite management stack and its APIs are owned, operated, and maintained by Dell, and contain Endpoint Security Suite (EPS) and Endpoint Detection and Response (EDR).
- Other security capabilities of the management stack include vulnerability scanning, logging, monitoring, hardening, and updating security patches.
- All security capabilities of the management stack are installed, operated, and monitored by Dell.
- Only approved and certified Dell support engineers can operate the management stack.

Logging and monitoring

Actions performed on the Service are logged and monitored. The logs are collected and securely forwarded to Dell's centralized system for ongoing monitoring and analysis. The logging and monitoring capabilities are configured, managed, and operated by Dell, and as previously noted, Dell does not collect, analyze, or monitor customer data.

Identity and access management

Identity and access management are shared responsibilities within the vault. The customer is responsible for identity and access management (IAM) of users accessing the vault. IAM includes identification, authentication, and authorizations (including access management) to the vault and the data that resides in it. The customer controls who can do what within the vault.

Dell is responsible for managing IAM to the onsite management stack, based on Dell policies. Only authorized service engineers can access the management stack and perform necessary actions.

Direct data access

Direct data access is the data path in which data flows between the customer's production environment (the source PowerProtect DD) and the APEX Cyber Recovery vault.

There is no direct connection between the customer production area to the Service and the vault except for in the following use cases:

1. Replication connection is the only regular connection from the customer production environment (the source PowerProtect DD) to the vault. The default connection is "normally closed," and only at times of replications it is opened, until replication is completed. Opening this connection is Dell's responsibility and controlled only from inside the vault by Dell.
2. Reverse-Replication connection: When needed only, and in urgent and extreme cases, Dell Technologies will operate a reverse replication directly to the customer-designated PowerProtect DD in the customer's production environment. Opening this connection is Dell's responsibility.
3. Temporary and ad hoc connection from the customer production location to the backup application and analytics tool in the Service for specific file recovery. If needed, and based on customer request, an ad hoc and time-limited secured connection will be established. This connection enables the customer to connect the backup application or analytic tool, or both, in the vault and to choose specific files and directories for recovery.

The customer owns the security of these data access paths and networks. Access should be locked down and denied by default. Strong data and network routing controls such as Layer 3 and Layer 4 firewall rules and ACLs should be in place to minimize attack surfaces and vectors.

During data transmission to and from the Service, the customer must ensure data integrity, confidentiality, and availability to prevent interruption, replication, tampering, forgery, interception, and monitoring. The customer should implement security controls for these activities to secure the data ingress and egress to and from the Service.

Data security

Customers keep control and ownership of their data and are solely responsible for their data stored in the Service. Customers control what data is going into and out of the Service. Sensitive data must be protected, and risks of data leakage and damage must be minimized. Security best practices should be followed for all phases of the Data Security Lifecycle, as illustrated in Figure 3.

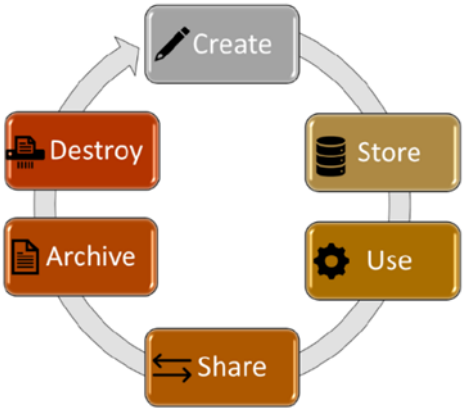

Figure 3. Data security lifecycle

Data handling and controls should ideally reflect internal standards and policies. Major considerations include data classification, data retention, and data disposal.

Dell does not inspect, approve, or monitor the data that customers deploy to the vault. Dell does not claim data ownership over any customer information that is stored in the Service.

Data security in transit

PowerProtect DD series encryption software enables customers to enhance the security of the data that resides on PowerProtect DD series appliances using industry-standard encryption algorithms. PowerProtect DD series encryption software protects backup and archive data stored on PowerProtect DD series appliances with data encryption that is performed inline before the data is written to disk.

It is the customer's responsibility and decision to encrypt or not to encrypt the data in-flight to and from the vault. Data encryption is designed to protect customer data if the protection system is stolen or if the physical storage media is lost during transit. It also eliminates accidental exposure of a failed drive if it is replaced. When data enters the protection system using any of the supported protocols (NFS, CIFS, DDVTL, DD Boost, and NDMP tape server), the stream is segmented, fingerprinted, and deduplicated (global compression). Then, the data is grouped into multisegmented compression regions, locally compressed, and encrypted before being stored to disk. When data encryption is enabled, the PowerProtect DD Encryption feature encrypts all data entering the appliance.

Customers should consider implementing PowerProtect DD series encryption for highly classified and sensitive data. Encryption of data in-flight encrypts data that is being transferred using DD Replicator between two PowerProtect DD series appliances. It uses AES 256-bit encryption to encapsulate the replicated data over the wire. The encryption-encapsulation layer is immediately removed when it transfers to the destination system. Data within the payload can also be encrypted using PowerProtect DD Encryption.

PowerProtect DD Replicator provides automated, policy-based, network-efficient replication for disaster recovery, remote-office data protection, and multisite tape consolidation. DD Replicator software asynchronously replicates only the compressed, deduplicated data over the WAN or LAN during the backup process, making network-based replication fast, reliable, and cost-effective. PowerProtect DD Replicator can

securely encapsulate its replication payload over SSL with AES 256-bit encryption. This ability enables secure transmission over the wire, a process also known as encrypting data in flight.

Encryption of data in-flight over NFS, NFSv3, and NFSv4 support Kerberos v5 protocol with integrity checking using checksums (krb5i) and with privacy service (krb5p) for integrity and privacy, respectively. However, there are performance penalties for encryption.

Data replication to the vault

The customer is exclusively responsible for the data backups content, including:

- Identification of critical data to protect: Not to include Personally Identifiable Information (PII)[1]
- Definition of replication policies
- Duration of retention policies
- Defining recovery operations

Dell neither backs up nor archives customer data that resides in the Service. Dell does not accept any liability for data that is lost, corrupted, stolen, or damaged.

Storage media data sanitation

If the Service is terminated, it is recommended that the customer purge the data. After customer data migration, Dell will retrieve Service hardware and complete a sanitization process to purge customer data from the Service. Malfunction of a Service offer component will trigger the Return Material Authorization (RMA) process to replace the component. The component will be sanitized before reuse or destructed when repair is not possible.

[1] Personally Identifiable Information (PII) is information that organizations can use to identify, contact, or locate a single person, or to identify an individual in context.

References

Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- APEX Cyber Recovery Services Overview
- APEX Cyber Recovery Services Resource Page
- Dell PowerProtect Cyber Recovery Configuration Guide
- Dell PowerProtect Cyber Recovery Product Guide
- Dell PowerProtect Cyber Recovery Solution Guide
- Dell PowerProtect Data Manager Cyber Recovery User Guide

Other documentation

See also the following useful documentation.

- https://attack.mitre.org/