Dell Managed Service for Machine Learning Operations – Security Overview

September 2023

H19718

White Paper

Abstract

This paper describes the shared security responsibilities between Dell Technologies and the customer. Dell Technologies has designed and implemented internal security controls, including suggested best practices and recommendations, to guide customers who use the Machine Learning Operations service.

DELL Technologies

Copyright

Contents

Executive summary

Overview

Dell is expanding its managed services offers to include Machine Learning Operations (the “Service”). The urgency for leveraging data to achieve competitive advantage is driving demand for data science capabilities. In the digital era, businesses must move quickly and drive projects to production. Artificial Intelligence (AI) and Machine Learning (ML) are rapidly gaining momentum to help achieve these objectives. However, rising costs system complexity, operational inefficiencies, and the decentralization of the public cloud create massive roadblocks to success. Maintaining the confidentiality, integrity, and availability of 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.

The Service provides a complete, fully tested, validated, and centralized platform for ML workloads, managing the infrastructure, platform, and model life cycle for business. Improved operational efficiencies enable data teams to get models to production and focus more on innovation.

This document describes the security measures used by Dell, designed to secure remote management of the Service. Furthermore, this document defines the shared responsibilities between Dell and the customer as it relates to the Service.

At Dell, cybersecurity is of great importance to us. Our approach to addressing cyber threats and risks is based on an adversary’s perspective. We use the MITRE ATT@CK™ framework, a knowledge base, and model for observed cyber adversary behavior. This framework reflects 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 attack vectors in the most effective way to secure the Service.

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

Revisions

Date	Part number/ revision	Description
September 2023	H19718	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 on this topic, see Managed Services for MLOps

Managed Services For Machine Learning Operation Overview

Overview

The Service is a comprehensive solution used to develop, deploy, and monitor ML models. The main service users are Data Architect/IT Administrators and Data Engineer/Scientists.

The Architect/IT Administrator designs the ML infrastructure, selects and manages ML tools, and the integration of hardware and software. The Data Engineer/Scientist manages the ML model life cycle, instead of on-model development and continuous learning. As a result, many models that are developed are never deployed into production.

The Service includes:

- Continuous life cycle management for ML hardware and software deployed at the customer data center
- Complex data science platform on a validated, tested, and scaled infrastructure
- Monitoring and management of infrastructure and data science platforms
- 24/7 availability and performance monitoring
- Management of day-to-day activities to maintain the health of the environment

Shared Responsibility Model

The Service is a shared responsibility between Dell and the customer. Dell is responsible for logically securing the management stack for the remote service and the infrastructure on which it is hosted. The customer is responsible for the physical security of all solution components deployed within their location, including the management stack infrastructure. 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 responsible for the security of the data that is transported, stored, analyzed, and sent to and from the ML platform, including models, algorithms, raw/analyzed data, and more.

The customer is also responsible for the network security in this Service, including the connectivity between Dell backend-managed services sites to the ML platform residing at the customer facility.

Additional customer security is for user management life cycle, access, privileges, actions, and auditing to and at the ML platform.

The overall security of this Service is achieved through the shared responsibilities of Dell and its customers. When consuming these Services, some responsibilities are transferred from the customer to Dell. The following figure illustrates the areas of responsibility between Dell and its customers.

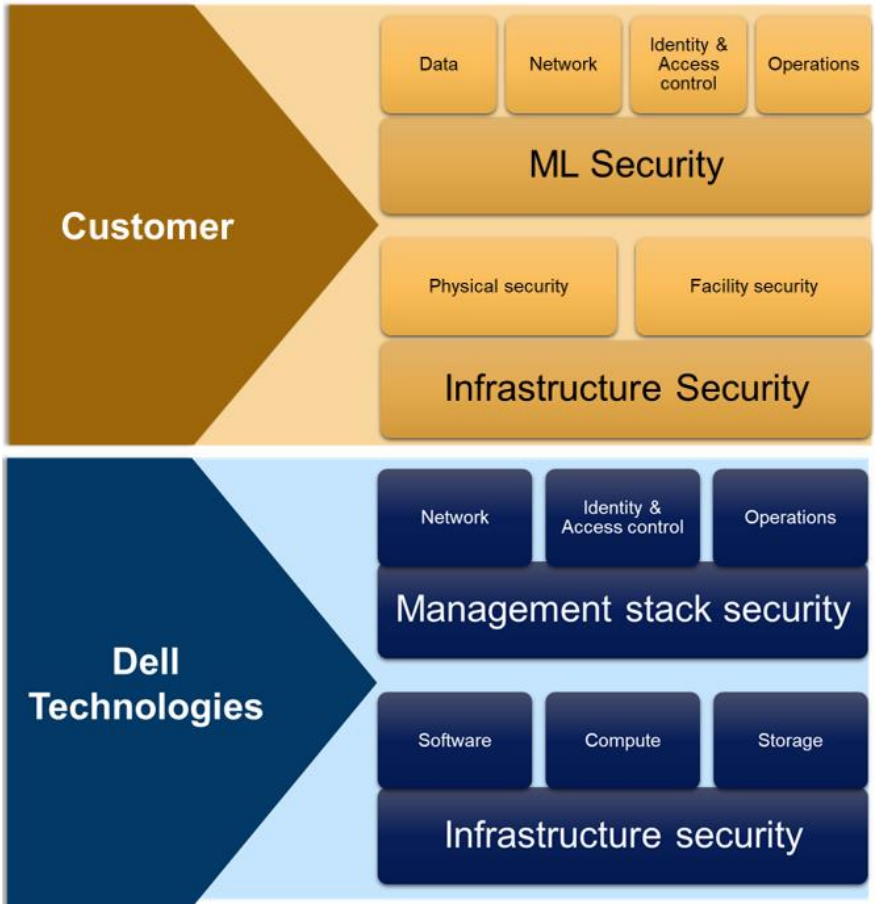

Figure 1. Shared responsibility model for the service

The Services require the customer to procure their own software licenses to enable Dell to deliver the Services ("third-party software"). Customer may use a "bring your own license" (BYOL) model or, in some instances, procure the third-party software through the Dell reseller program (the latter assuming Dell can resell the applicable third-party software). The customer must also ensure that Dell has the necessary rights to manage and access the third-party software on behalf of the customer. Dell assumes no license rights, obligations, or liabilities associated with the third-party software.

Architecture

The Services contain several different architectural components and zones as illustrated in the following figure.

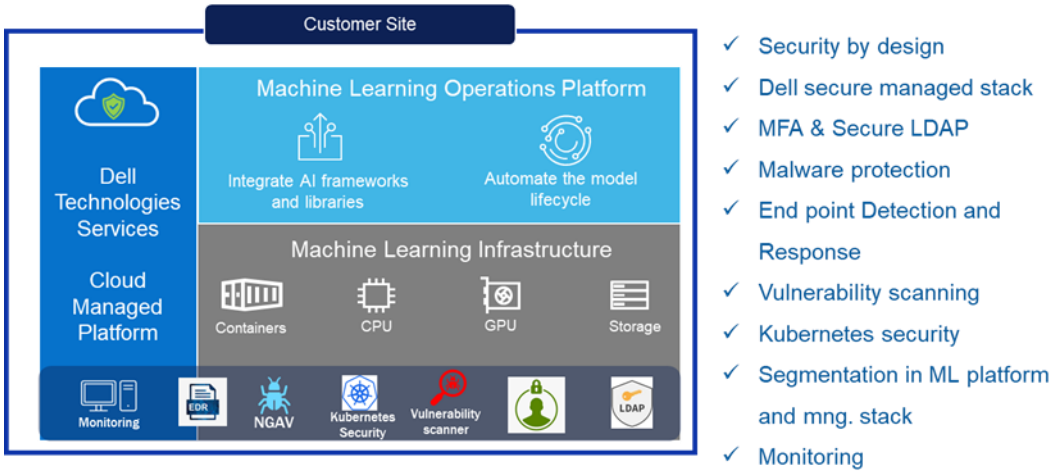

Figure 2. Services design

Dell's hosted Cloud Management Services Platform (CMSP) is used for backend management of 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 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:

1. Telemetry collection: Handles telemetry data, events, logs, and other data points
2. Connectivity functions: Provides secure connectivity for transferring telemetry (file and message) data between customer on-premises and Dell platforms using secured protocols
3. Support functions: Provide configuration management, remote access, troubleshooting, COTS/3rd party integrations, and ticketing automation
4. Orchestration and control: Execution tasks against assets as defined in the Services
5. Individual product APIs or element managers: Intent, declarative, or outcome configuration, direct/imperative for direct configuration, and policy settings
6. Local intelligence: Error detection with automated remediation, configuration integrity and drift, and Services optimization tuning
7. Internet connectivity between Dell's data center and the customer's on-premises data center is solely the responsibility of the customer. Dell does not monitor, nor access, to customer data.

Infrastructure Security

Infrastructure security encompasses the lowest layers of security, from physical facilities to configuring and implementing security of the Dell-owned or Dell-licensed 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. Recommended measures include (but are not limited to):

- Access controls to limit physical access to the locking cabinets only to authorized personnel. Biometrics, proximity cards, or similar technologies to restrict access to the cabinets.
- CCTV to monitor physical access to the data center of the Service stack (Dell management stack and ML platform).
- Support of on-site UPS systems and backup generators to ensure Service availability if there is a power failure.
- The 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 its control, which is the Cloud Management Support Platform and the onsite infrastructure hosting the management stack. In the latter case, Dell is only responsible for the logical security of the management stack infrastructure. Dell installs and maintains the infrastructure according to its policies, including, and not limited to:

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

Software Security

Dell software solutions are developed per industry security standards. A secure development life cycle methodology is designed to help prevent software vulnerabilities and design weaknesses from being introduced into Dell products and applications during development.

Dell is also responsible for periodic vulnerability scanning and updating of other Dell-owned or Dell-licensed software used in the managed infrastructure (such as compute, storage, and network).

Logging and Monitoring

The Services include logging and monitoring of security events on Dell-controlled infrastructure. Dell monitors all Dell-controlled Services components 24/7, including racks, power, environment, and networking up to the top-of-rack (ToR) switch. Incident management is also performed 24x7.

Penetration Testing

Dell performs penetration tests on the Dell-owned and managed infrastructure and the ML platform.

Network Security

Network security is the process of protecting resources from unauthorized access or attacks by applying controls to network traffic and infrastructure. 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 Segmentation

The Service contains a designated rack containing the ML tools and the management stack deployed in the customer's data center. The ML tool has networking security capabilities achieved through designated Kubernetes security configuration and Kubernetes Network Security Policy. The ML tool can be secured from the customer's production infrastructure through the customer firewall and customer's access management controls. Dell defines a designated Kubernetes namespace for the customers to communicate, manage, and operate for their needs in this service. Dell also secures and separates the backend management system through designated network security controls.

Network Connectivity Security

The customer is responsible for configuring the network firewall rules for the traffic between the Dell management components and the ML platform in the Service. Dell is responsible for securing and separating the remote management using a designated Dell-managed network security capability.

Dell provides an additional network security layer to secure the communication between the management platform and the Service. The measures to secure this network are combined technologies that include L3 segmentation at the ToR, VLANs, and an access-list-defined in different network elements. At the Kubernetes layer for the management stack and the ML platform, there is a strict network security policy at the namespace and pod layers for ingress and egress traffic.

These controls enforce and maintain communication segmentation in different layers to help prevent customer data from becoming visible to unauthorized users.

Secure Remote Access

Along with physical security and firewalls, the rules for secure remote connection are the customer's responsibility, coordinated with Dell. Dell is responsible for the following security components of the onsite management stack:

- Infrastructure Security (compute, storage, and network security): Dell installs and maintains the infrastructure according to its policies which 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.

Logging and Monitoring

Actions performed on the management stack and infrastructure 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., Dell does not collect, analyze, or monitor customer data, and only approved Dell personnel can operate the management stack.

Identity and Access Management

Identity and access management are shared responsibilities between the customer and Dell within the Service. The customer is responsible for identity and access management (IAM) of users accessing the ML platform. IAM includes identification, authentication, and authorizations (including access management) to the ML platform and the data that resides within it. The customer controls permissions within the ML platform.

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

Data Access

Data access is the path in which data flows to create, read, write, or delete permissions between the customer's data center and/or external data repositories from their production environment to the ML platform.

The customer owns the security of the data access paths and networks. Access should be managed and audited at all times. Strong data and network routing controls such as Layer 3 and Layer 4 firewall rules (customer firewall) and access lists 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, analyzed, and operated in the Service. Customers control the inbound and outbound data within the Service. Sensitive data should be protected, and the risks of data leakage and damage should be minimized. Security best practices should be followed for all phases of the data security life cycle, as illustrated in the following figure.

Figure 3. Data Security Lifecycle

Data handling and controls should 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 Service. Dell does not claim data ownership over any customer information that is stored in the Services.

Data Security in Transit

It is the customer's responsibility and decision to encrypt or not to encrypt the data in-flight to and from the ML platform. Data encryption at rest protects customer data if the 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.

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. However, there are performance impacts that result from such encryption.

Dell does not back up or archive customer data that resides in the Services. 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 should purge the data. After customer data migration, Dell retrieves Service hardware and completes a sanitization process to purge customer data from the Services. A malfunction of a Services offer component triggers the Return Material Authorization (RMA) process to replace the component. The component is sanitized before reuse or destroyed when a repair is not possible.

Kubernetes Security

This Service uses an infrastructure Kubernetes solution. The ML platform uses several Kubernetes components.

Kubernetes security is a shared responsibility within this Service. Dell is responsible for the security of the Kubernetes control plane, while the customer is responsible for the security of the pods at the ML platform. The customer is subjected to Dell Kubernetes security policy and must comply with adequate security measures at the Kubernetes layer of the ML platform.

Kubernetes network security

Dell defines Kubernetes Network Policies in this Service to control traffic between namespaces, pods, and external sources. Network Policies enable administrators to define ingress and egress traffic rules, restricting communication based on namespace, source IP, destination IP, ports, or other criteria.

Kubernetes Authentication & Authorization

The Service supports various Kubernetes authentication mechanisms, such as client certificates, bearer tokens, and usernames and passwords at the infrastructure level. The customer is also required to implement a proper authentication that ensures only authorized users can access the ML platform. Once a user is authenticated to the ML platform, the customer must employ the Kubernetes authorization mechanism to

determine the actions they are allowed to perform based on Role-Based Access Controls (RBAC).

Kubernetes POD and Image Security

Container images used in Kubernetes should be scanned for vulnerabilities and known security issues. Dell performs timely vulnerability scanning to ensure the integrity and safety of the images being deployed. The customer is responsible for performing vulnerability assessment, findings analysis, and quantification on the ML platform. Remediation planning is based on the customer's instructions and the execution is Dell's responsibility. Pod Security Policies (PSPs) define a set of security-related constraints that pods must adhere to. They enforce policies including restricting the use of privileged containers, host namespace sharing, and controlling pod-level security contexts.

References

Dell Technologies documentation

The following 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.

- Managed services for Machine Learning operations Home
- Managed services for Machine Learning operations Service Overview

MITRE documentation

- https://attack.mitre.org/

Microsoft documentation

- Threat Modeling AI/ML Systems and Dependencies