DELL Technologies

Dell AIOps Security

Dell Corporate Security & Resiliency Organization • Version 3.0 • Last Updated 08-19-2025

Executive Summary

Using proactive monitoring, machine learning and predictive analytics, Dell Technologies' Dell AIOps intelligent insights for simplifying and proactively managing on-premises infrastructure and data protection in the cloud. As a cloud-native software as a service (SaaS) application, Dell AIOps supports Dell's broad portfolio of server, storage, network, data protection, hyperconverged, and converged system products.

This white paper describes the security controls and policies that Dell AIOps employs to deliver a secure and modern cloud service. This paper is intended to proactively address the security concerns many companies raise when adopting a new cloud-hosted application.

This white paper reviews:

1. Dell AIOps security strategy.

2. Architecture overview and security controls.

3. How Dell Technologies' security measures protect the security and integrity of your data.

4. Responsibilities associated with securing information through the Shared Responsibility Matrix.

Target Audience

The target audience for this white paper includes current or prospective customers interested in learning more about Dell AIOps application security. This paper and the security topics covered are targeted to customer roles including IT security, IT Operations, and IT infrastructure administrators and architects.

Dell's Security Assurance

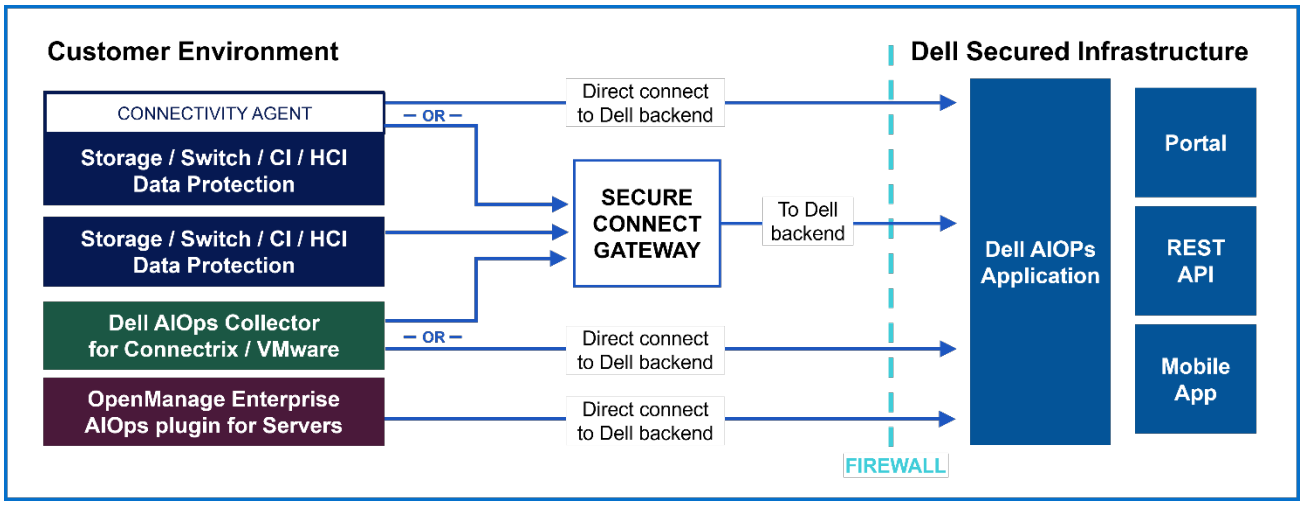
Dell Technologies has taken steps to ensure its program and application development teams follow a consistent methodology using an internal Secure Development Lifecycle (SDL) process. Dell's SDL integrates standards from a variety of data sources and is aligned with the principles outlined in NIST's Secure Software Development Framework (SSDF) and ISO/IEC 27034 information technology, security techniques and application security. Dell AIOps has also achieved SOC2 Type 2 certification and ISO 27001 certification and complies with EU Data Act.

The SDL is a common reference for Dell product organizations to benchmark their secure development activities against market expectations and industry best practices. It defines controls that Dell product teams must adopt while developing new features and functionality. The SDL includes both analysis activities and prescriptive proactive controls around key risk areas.

The analysis includes activities such as threat modeling, static code analysis, scanning and security testing, which are intended to discover and address security defects throughout the development lifecycle.

The prescriptive controls are intended to ensure development teams code defensively to prevent specific prevalent security issues, including those found in the OWASP Top 10 or SANS Top 25. Many of these activities are automated as part of the company's DevOps strategy to drive enforcement of SDL at scale.

Architecture Overview



- **Connectivity Software Platform:** Dell's next-gen secure connect gateway technology provides a single connectivity solution for managing your Dell infrastructure. It is a scalable solution that adapts to a wide range of IT environments and operational needs. Choose the right configuration for your Dell AIOps needs—a gateway or direct connect option—from the flexible installation options. These are customer installable and upgradeable.

  Dell's technology establishes a secure, end-to-end encrypted communication channel between the customer site and Dell, enabling the reliable and protected transmission of telemetry data from monitored Dell devices to Dell's secure IT infrastructure and AIOps platform. This built-in capability ensures that data in transit remains safeguarded.

  When configured as:

  Gateway technology: Dell's gateway software sits external to the products within the customer environment and is ideal for mixed IP environments, making it possible to connect multiple Dell systems to the gateway to communicate back to Dell Technologies. This configuration simplifies the firewall/networking setup so only the gateway connects outbound over the internet.

  Direct connect: In certain Dell product models, the connectivity technology is integrated into the product operating environment. The connectivity agent running on the product behaves as a mini-gateway and allows for direct connection to the Dell backend. This option is ideal for smaller customers and non-traditional customers who prefer to avoid setting up additional software. Direct connect enabled products can be switched to connect via a gateway.

- **Customer endpoints**: Dell AIOps Portal, Dell AIOps REST API and Webhooks, and Dell AIOps App which includes support for MFA and SSO.
- **Dell Infrastructure**: Dell AIOps Application and Database.
- **Dell AIOps Collector**: Collects VMware, Connectrix, and PowerSwitch data and sends it to Dell AIOps through secure connect gateway technology.
- **OpenManage Enterprise AIOps plugin for Servers**: Collects server data and sends it to Dell AIOps by enabling a secure connection—based on secure connect gateway technology—through the AIOps plugin.

Access and Authorization

Authentication

Dell AIOps access is granted to a user based on valid Dell Support Account credentials. Customers use their existing support account credentials to log in to Dell AIOps. Authentication is handled by Dell's Single Sign-On (SSO) and Multifactor Authentication (MFA) infrastructure. For customers that leverage the Dell AIOps optional federated identity management model, Authentication for the Dell Support Account is handled by the customers' Identity Provider.

Asset Visibility

Each user's support account is mapped to available assets based on the mapping between user and location ID. Assets that a user can access in the MyService360 analytics dashboard at the Dell Support site are the same assets that are visible in Dell AIOps, assuming those assets have been onboarded to Dell AIOps and are sending telemetry.

Access Groups

Dell AIOps supports Access Groups as defined by Company Administrators. Access Groups have improved security by providing additional control to Administrators who set up the visibility of locations and assets for their employees. Groups of users are mapped to an Access Group by a Company Administrator who determines which locations and assets the associated users can view. Additional details on how to manage Access Groups can be found in KB #000179622 (https://www.dell.com/support/kbdoc/en-us/000179622).

Federated Accounts

Dell AIOps provides an optional federated identity management model, enabling customers to have a common set of policies, practices, and protocols in place to manage the identity and trust for users and devices across corporate customer environments and external SaaS solutions, such as Dell AIOps.

The Administrators can also now leverage Federated Groups in a new Groups tab on the Identity Management page. A Federated Group can be mapped directly to one or more Dell AIOps roles by creating a 'Group To Role' mapping. The Roles Tab now shows groups information in the Details pane, along with the existing permissions and assigned users' information.

Role-Based Access Controls (RBAC)

RBAC enables users to have different privileges when logged in to Dell AIOps. For example, access to view API keys and Webhooks requires the DevOps role. Access to Cybersecurity features requires a Cybersecurity related role. Only users with the Admin role can manage role access. Dell AIOps Admins are automatically assigned that role based on the Company Admin role as defined in MyService360. Users can determine their Company Admins by referring to KB #000191817 (https://www.dell.com/support/kbdoc/en-us/000191817).

The following chart shows which roles exist today in Dell AIOps. Note that even Dell AIOps Admins must assign themselves additional roles such as DevOps or Cybersecurity Admin to access these additional features.

Role Name	Description
Admin	Admin role for Dell AIOps functionality
Advisor	Advisor role for Dell AIOps consultants
APM Admin	Admin role for access to APM Instana
APM Viewer	Viewer role for access to APM Instana
Cybersecurity Admin	Admin role for Cybersecurity feature
Cybersecurity DevOps	DevOps role for cybersecurity functionality
Cybersecurity Operator	Operator role for Cybersecurity functionality
Cybersecurity Viewer	Viewer role for Cybersecurity feature
DevOps	DevOps role for automation related functionality such as REST API and Webhooks
Incident Management Admin	Role granting access to AIOps Incident Management related features and to configure the instance
Incident Management Operator	Role granting access to AIOps Incident Management related features and to manage alerts and incidents
Incident Management Owner	Role granting access to AIOps Incident Management related features and to manage its licenses
Server Admin	Admin role for remote server management
Standard	Default role for Dell AIOps Users

Dell Advisors and Partners

Customers can grant Dell Advisors and Partners access to Dell AIOps for the purpose of providing assistance and recommendations that optimize Dell infrastructure. Dell employees and partners must explicitly be provided access to Dell AIOps from the customer. Advisors and partners have a read-only role and cannot grant or revoke access for other users. See KB # 000020659 for additional information: (https://www.dell.com/support/kbdoc/000020659).

REST API and Webhook

The Dell AIOps REST API uses the OAuth2 protocol for authentication and authorization. Only users with the DevOps role can manage API keys needed to access the Dell AIOps REST API. Once the API client credentials are generated, the user will be provided with the Client ID and Client Secret. The client must then authenticate to a specific API endpoint to obtain an Access Token using these credentials. Once the Access Token is granted, the client can use it to make the desired REST API calls. The access token is available for one hour, and client credentials have a lifetime of one year. Users can refer to https:// developer.dell.com/apis for additional documentation on the Dell AIOps REST API.

The Dell AIOps Webhook uses HMAC-SHA256 secrets to sign the messages sent to remote Webhook endpoints. All Webhook calls come from a limited number of static IP addresses that Dell uses to communicate with customers.

Audit Logs

Dell AIOps provides audit logging to track operations performed by Dell AIOps users. Only users with the Admin role have visibility to the Dell AIOps Audit Log features. Examples of operations tracked by audit logging include:

- Dell AIOps RBAC changes
- VxRail RBAC changes
- Cybersecurity operations
- Code staging and update operations
- REST API operations
- Webhook operations
- Custom label operations

Data Security/Protection

Data In Transit

Dell AIOps only collects system metadata such as logs, alerts, health, capacity, performance, and configuration information. All communications between the customer and Dell backend infrastructure is initiated outbound by secure connect gateway technology from the customer site. It creates a secure end-to-end communication tunnel using industry standard Transport Layer Security (TLS) 1.3 encryption over the Internet, and digital certificate authentication signed by Dell Technologies Services. No customer data is sent—only data generated by the customer's systems. Customers control which systems send information over these channels.

Read the security paper to learn how secure connect gateway technology integrates privacy, data protection and threat prevention into its security architecture: (https://www.delltechnologies.com/asset/en-us/services/support/industry- market/secure-connect-gateway-security-wp.pdf.external).

Once the data arrives, Dell AIOps stores data relating to those systems with Dell AIOps management enabled in its own Dell IT-managed infrastructure.

Data at Rest

Dell Technologies hosts Dell AIOps data in a US-based data center designed to maintain high levels of availability and security. Dell AIOps data is stored on Dell infrastructure, which is highly available, fault tolerant and provides a 4-hour Disaster Recovery service level objective. Dell's Global Security Organization (GSO), led by a Chief Information Security Officer, is responsible for security and protection of Dell's information technology infrastructure. This is accomplished by using an established set of governing security policies and procedures, and enforcement of information security control. This includes measures such as multi-layered firewalls, intrusion detection systems, and industry-leading antivirus and malware protection.

The Dell Cybersecurity team is involved in running continuous vulnerability scans on the application and underlying environment. Any required remediation is handled through an ongoing vulnerability remediation program such as software upgrades, patches, or configuration changes.

Dell's Information Security Policy ensures that all Dell information and resources are properly protected, information owners ensure all resources are accounted for, and each resource has a designated custodian. All infrastructure is located in the core network behind corporate firewalls and is not exposed to external direct access. No individual direct login to the database server and database is allowed, except for the members of System Administrator and Database Administrator teams. Database application accounts are managed using standard database password authentication. Dell has implemented an industry best practice change management process to ensure that Dell production line assets are stable, controlled, and protected. Change management provides the policies, procedures, and tools needed to govern these changes, and to ensure that they undergo the appropriate reviews, approvals, and are communicated to users.

AIOps Cybersecurity

Cybersecurity in Dell AIOps is foundational to add the ability to monitor Dell resources for security risks. Dell AIOps Cybersecurity proactively monitors infrastructure using secure telemetry and applies machine learning to detect potential risks without accessing customer data directly. The Cybersecurity Misconfigurations feature compares configurations and setups to a set of security-related evaluation criteria, notifying users of any deviations from the configured plan. The Cybersecurity Security Advisories feature provides vulnerability awareness by displaying applicable Security Advisories for supported systems. Cybersecurity is supported for PowerMax, PowerStore, PowerEdge Server and Modular Chassis, and PowerProtect DD systems and will continue to expand coverage to other Dell systems.

All Cybersecurity features are role-based, ensuring that only authorized users can view or manage security insights. Cybersecurity insights are securely stored in a protected database, with all data—both in transit and at rest—safeguarded using industry-leading encryption and security best practices.

Ransomware Protection

Cybersecurity also provides ransomware detection capabilities, leveraging abnormal volume activity with encrypted data, which might indicate a potential ransomware or malware attack. Ransomware detection is currently supported on PowerMax storage only.

Threat/Vulnerability Assessments

Dell AIOps supports threat and vulnerability management strategies to ensure the infrastructure, software components, and source code are 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, software components, and source code ensures the most current features and security measures are implemented.

2. Methods to identify security risks/vulnerabilities. These methods include both vulnerability scans and penetration testing.

Dell AIOps undergoes frequent vulnerability assessments as part of Dell's SDL to discover vulnerabilities that are then prioritized and remediated. The vulnerabilities are reported from various activities like threat modeling, static application security scans, third party component scans, penetration tests, and network vulnerability scans.

Proactive Vulnerability Assessment Model

Dell AIOps Customer and Dell responsibilities

Security for Dell AIOps operates under a shared security model. Dell's shared responsibility matrix clearly delineates the respective roles between customer and Dell on a function-by-function basis, as well as shared levels of responsibility. See the table below.

Category	Customer	Dell
Dell AIOps Security		✓
Access & Authorization		✓
Data Security/Protection		✓
Threat and Vulnerability Assessment		✓
Secure Development Lifecycle		✓
User Management	✓	✓
Firewall	✓	
Dell AIOps Collector	✓	✓
Device Onboarding	✓	
Device Maintenance	✓	

Security and Compliance

Dell AIOps protects Dell and Customer data using policies and strategies from established frameworks. This can assist customers in meeting their own compliance program requirements. Where applicable, application and product development at Dell uses mappings to established frameworks and regulations to help ensure that appropriate security principles and requirements are reflected in the development lifecycle. The security measures that protect Dell AIOps map to industry-accepted security standards, regulations, and control frameworks.

- ISO 27001 Information Security Management Systems
- NIST Security and Privacy Controls for Federal Information Systems and Organization
- CSA Cloud Control Matrix
- SOC2 Type 2 Certification

Conclusion

Dell Technologies strives to create a security-aware culture across its entire community. Our internal SDL is a common reference for Dell Technologies' product organizations to benchmark product and application secure development activities against market expectations and industry practices. It defines security controls that product teams should adopt while developing new features and functionality for our programs. Customers can be assured that Dell is committed to providing a reliable, private, and secure experience for Dell AIOps customers.

Glossary

Term	Definition
AIOps	Artificial Intelligence for IT Operations
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
RBAC	Role-Based Access Control
SaaS	Software-as-a-Service
SDL	Secure Development Lifecycle
SSO	Single Sign-On