CloudIQ Security

Dell Corporate Security & Resiliency Organization • Version 1.0 • Last Updated 06-10-2022

Executive Summary

Using proactive monitoring, machine learning and predictive analytics, Dell's CloudIQ AIOps application delivers 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, CloudIQ 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 CloudIQ 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 CloudIQ 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

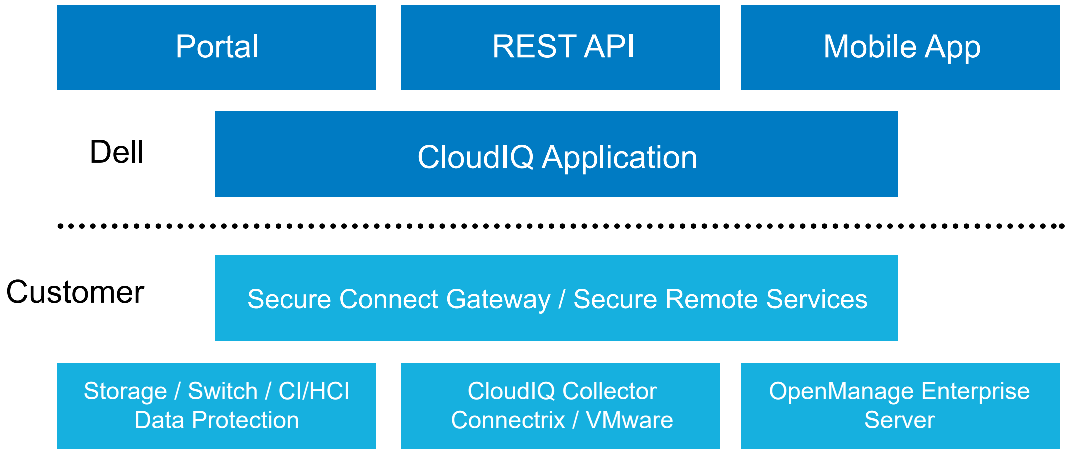
The target audience for this white paper includes current or prospective customers interested in learning more about CloudIQ application security. This paper and the security topics covered are targeted to customer roles including IT security, IT Operations as well as IT infrastructure administrators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

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



- Secure Remote Services (SRS): SRS is a secure remote connection between Dell and the customer site that enables remote communication and delivery of telemetry from the customer's Dell devices to secure Dell IT infrastructure and CloudIQ.
- Secure Connect Gateway is Dell's newest version of secure connectivity technology. As with SRS, it provides a secure remote connection between Dell and the customer site. System telemetry from the customer's Dell devices is sent securely over Secure Connect Gateway to secure Dell IT infrastructure and CloudIQ.
- Direct Connection: Some Dell products support an embedded SRS or Secure Connect Gateway service within the management platform which eliminates the need for an external gateway.
- Customer endpoints: CloudIQ Portal, CloudIQ REST API and Webhooks, CloudIQ Mobile App
- Dell Infrastructure: CloudIQ Application and Database
- Dell Gateways: Secure Connect Gateway/Secure Remote Services (SRS) Gateway
- CloudIQ Collector: Collects VMware and Connectrix data and sends to CloudIQ through SRS or Secure Connect Gateway.
- OpenManage Enterprise: Collects server data and sends to CloudIQ through a secure connection.

Identity and Trust Verification

CloudIQ utilizes a secure industry standard approach for web application and API authentication. The CloudIQ portal utilizes a username and password approach to authenticate users and grant access to the portal. The portal also provides single sign on (SSO) across Dell sites including Dell MyService360 and the Developer Portal.

CloudIQ is moving to 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 CloudIQ.

API and Webhook

The CloudIQ API utilizes an OAuth2 client ID and secret to grant access to the REST API and functionality within CloudIQ. The CloudIQ Webhook uses HMAC-SHA256 secrets to sign the messages sent to remote Webhook endpoints. All Webhook calls come from a limited numbers of static IP addresses that Dell can communicate to customers.

Access and Authorization

Authentication

CloudIQ access is granted to a user based on valid Dell Support Account credentials. Customers use their existing support account credentials to log in to CloudIQ. Authentication is handled by Dell's SSO infrastructure.

Asset Visibility

Each user's support account is mapped to available assets based on the mapping between user and Site ID. Assets that a user can access in MyService360 are the same assets that are visible in CloudIQ, assuming those assets have been onboarded to CloudIQ.

Access Groups

CloudIQ supports Access Groups as defined by Company Administrators. Access Groups have improved security by providing additional control to Administrators who set the visibility of sites and assets for their employees. Groups of users are mapped to an Access Group by a Company Administrator who determines which sites 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).

Role Based Access Controls (RBAC)

RBAC enables users to have different privileges when logged in to CloudIQ. For example, access to view API keys and Webhooks requires the CloudIQ DevOps role. Access to Cybersecurity features requires a Cybersecurity related role. Only users with the CloudIQ Admin role can manage role access. CloudIQ 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 CloudIQ. Note that even CloudIQ Admins must assign themselves additional roles such as CloudIQ DevOps or Cybersecurity Admin to access these additional features.

Role Name	Description	Notes Standard
CloudIQ Admin	Admin role for CloudIQ functionality	Managed by MyService360
CloudIQ Standard	Default role for CloudIQ Users	Default role – cannot be managed.
CloudIQ DevOps	DevOps role for automation related functionality such as REST API and Webhooks	Assigned by CloudIQ Admin
Cybersecurity Admin	Admin role for cybersecurity feature	Assigned by CloudIQ Admin
Cybersecurity Viewer	Viewer role for cybersecurity feature	Assigned by CloudIQ Admin

Dell Advisors and Partners

Customers can grant Dell Advisors and Partners access to CloudIQ for the purpose of providing assistance and recommendations that optimize Dell infrastructure. Dell employees and partners must explicitly be provided access to CloudIQ 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 CloudIQ REST API uses the OAuth2 protocol for authentication and authorization. Only users with the CloudIQ DevOps role can manage API keys needed to access the CloudIQ REST API. Once the API client credentials are generated, the user will be provided 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 utilize 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 CloudIQ REST API.

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

Audit Logs

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

- CloudIQ 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

CloudIQ only collects system metadata such as logs, alerts, health, capacity, performance and configuration information. The data is transmitted securely over Dell's secure remote connectivity technology such as Dell Secure Remote Services, Dell Phone Home services, and Dell Secure Connect Gateway. No customer data is sent, only data generated by the customer's systems. Customers control which systems send information over these channels. See the Secure Connect Gateway security white paper for additional details: (https://www.delltechnologies.com/asset/en-us/services/support/industry-market/secure-connect-gateway-security-wp.pdf.external).

All data arriving through those channels is protected in transit by industry-standard best practices. Both channels use digital certificates and customer-controlled access policies to establish point-to-point encryption and ensure all data is securely transported to the Dell IT-managed infrastructure. Connection and access is performed over secured transport and presentation protocols – TCP, TLS 1.2, SSH and HTTPS. In addition, Secure Connect Gateway provides for dedicated VPN and multifactor authentication. Once the data arrives, CloudIQ stores data relating to those systems which have CloudIQ management enabled in its own Dell IT-managed infrastructure.

Data at Rest

Dell Technologies hosts CloudIQ data in a US-based data center designed to maintain high levels of availability and security. CloudIQ 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, industry-leading anti-virus 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; 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, to ensure that they undergo the appropriate reviews, approvals, and are communicated to users.

Threat/Vulnerability Assessments

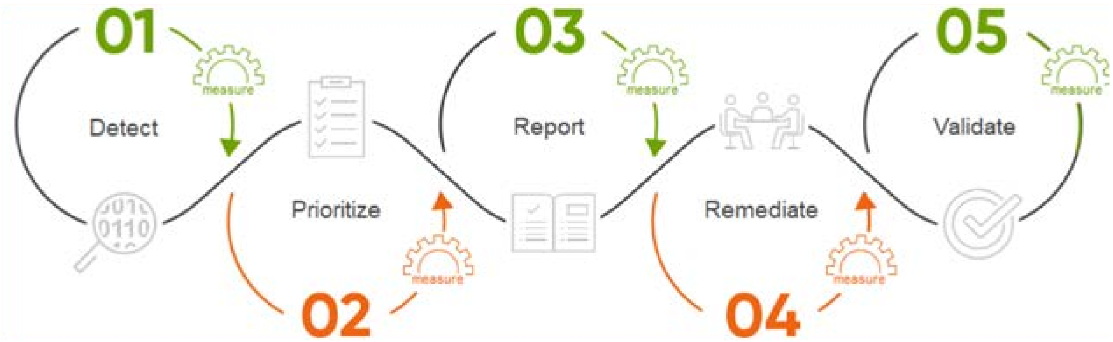
CloudIQ supports threat and vulnerability management strategies to ensure the infrastructure, software components and source code are protected against identified risks and vulnerabilities. These threat and vulnerability management strategies are drawn from methodologies used in Dell's Secure Development 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.

CloudIQ 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



CloudIQ Customer and Dell responsibilities

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

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

Security and Compliance

CloudIQ 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 established frameworks and regulations to help ensure that appropriate security principles and requirements are reflected in the development lifecycle. The security measures that protect CloudIQ 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

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 CloudIQ customers.

Glossary

Term	Definition
AIOPS	Artificial Intelligence for IT Operations
SaaS	Software-as-as-Service
SDL	Secure Development Lifecycle
RBAC	Role Based-Access Control
SSO	Single Sign-On
SRS	Secure Remote Services
NIST	National Institute of Standards and Technology
SRS	Secure Remote Service

NOTICE

This whitepaper is for informational purposes only and represents current Dell practices, which are subject to change without notice. It does not create any commitments or assurances from Dell and its affiliates, suppliers or licensors. Dell's responsibilities and liabilities to its customers are controlled by Dell agreements which are neither a part of, nor modified by this whitepaper. Customers are solely responsible for making their own independent assessment of the information provided in this whitepaper.