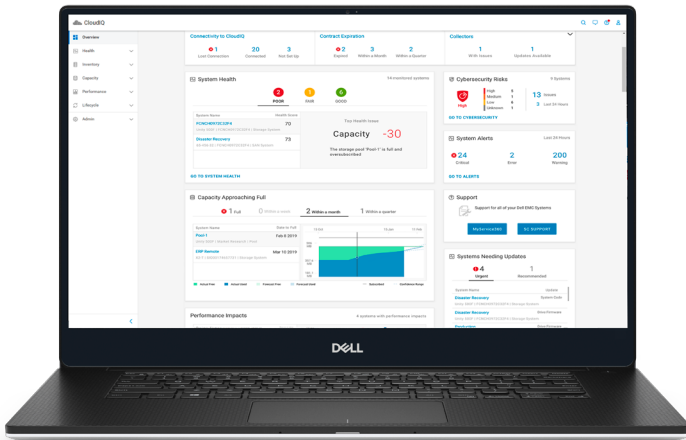


# CloudIQ - Infrastructure Cybersecurity

Keep infrastructure safe with proactive cybersecurity assessments and fast remediation



## CloudIQ Intelligent Cybersecurity Insights

### Essentials

- **Reduce Risk** – with system cybersecurity visualization and proactive notifications that pinpoint risk and recommend actions for fast resolution
- **Manage Policy** – with an easy-to-use interface for customizing infrastructure security policy for scheduled assessments
- **Improve Productivity** – with a cloud-based application that conveniently monitors infrastructure cybersecurity, health, performance, and capacity together

Infrastructure misconfiguration opens your organization to cyber-intrusion and is a leading threat to data security. Without a smart, modern solution, you must dedicate staff to manually assess security configuration of every infrastructure element in your environment or make ad hoc risk assessments. Neither option is practical, affordable, or effective.

CloudIQ is a modern solution that overcomes this dilemma by proactively notifying your system administrators about infrastructure security risks in the same application they use daily to monitor and resolve infrastructure health, capacity, and performance issues.

CloudIQ is the cloud- and AI/ML-based proactive monitoring and predictive analytics application for the Dell infrastructure product portfolio. It combines human and machine intelligence to provide you with the insight to proactively and efficiently assure that the state of IT infrastructure will meet your business' demands.

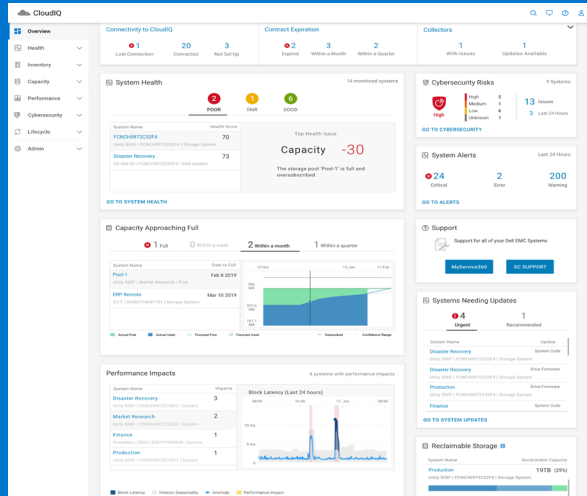
Proven to improve time-to-resolution of infrastructure health, performance, and capacity issues by 2X to 10X on average<sup>1</sup>, CloudIQ stands to improve the security posture of your IT environment with less effort.

## Start securing your IT infrastructure in minutes

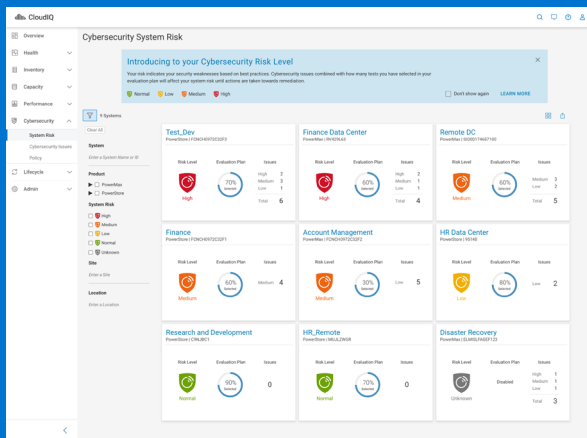
Hosted in the secure Dell IT Cloud with a secure network connection to your IT environment, CloudIQ only takes minutes to set up for the first time. A single click in your infrastructure systems' element manager application (e.g., Unisphere for PowerMax storage systems) will initiate CloudIQ to collect and analyze health, performance, and capacity telemetry from your systems. Cybersecurity enablement is designed with two easy follow-up steps: first initiate security telemetry collection, then use a simple Cybersecurity Evaluation Plan Editor to set up your security policy plan, and the system starts to evaluate the data and detect security misconfiguration.

It's that easy and is managed securely through role-based access.

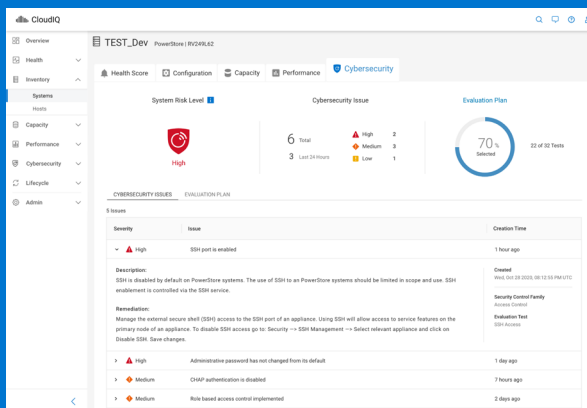
# Cybersecurity Insights and Actions



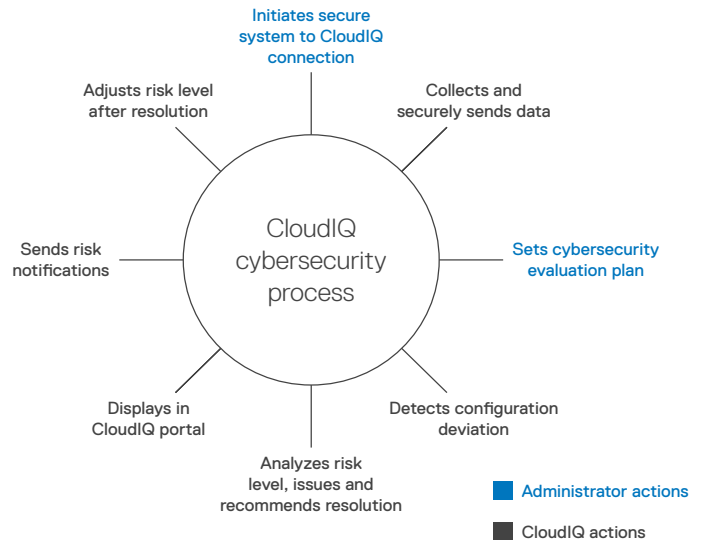
CloudIQ Overview with Cybersecurity



Cybersecurity Risk Levels



Cybersecurity Risk Details and Recommendations



CloudIQ enables an efficient, closed-loop process for comprehensive, 24x7 infrastructure cybersecurity assessment and remediation.

## Reduce Risk

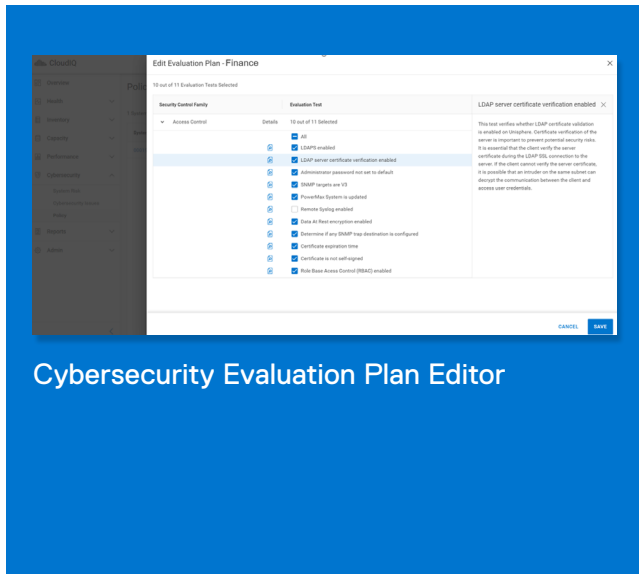
Using the secure Dell Technologies network and hosted in the secure Dell IT Cloud, CloudIQ collects, stores, and assesses security configuration information from your systems across your entire IT environment, including primary and secondary data centers and edge locations.

- Cybersecurity Assessment:** Determines if system security configurations have deviated from your policy. This includes role-based access control, default administrative password, data at rest encryption enabled, NFS security level, and more. CloudIQ continuously assesses deviation to eliminate the need for you to manually check each configuration and to assure your constant awareness of risk.
- Cybersecurity Risk Overview:** See the number of systems with high, medium, and low security risks in the same dashboard that gives you an at-a-glance view of system health scores and related capacity and performance analytics. This helps you quickly prioritize actions and speed time to resolution.
- Cybersecurity Risk Levels:** Use a single dashboard to identify every system that is at risk, each in its own card with a cybersecurity risk level value. Systems are displayed top-down according to level of risk to help you further prioritize actions.
- Cybersecurity Details and Remediation:** Learn the details of each system's risk and see the recommended action to return the deviated security configuration to a secure state. You can launch each system's element manager directly from CloudIQ to take corrective action fast.

## Manage Policy

Using a simple tool, you can plan infrastructure security configuration assessment policy which CloudIQ will use to assess cybersecurity risks.

- **Planning Tool:** Use a template-driven Cybersecurity Evaluation Plan Editor to select security configurations that CloudIQ will compare to your systems' actual configurations. Using the Editor, you can click to enable or disable each evaluation test for your desired security policy.
- **Security Standards:** Security configurations are based on NIST 800-53 r5 and NIST 800 – 209 standards as well as Dell Technologies best practices for each specific infrastructure product based on our engineers' years of experience supporting thousands of users.



Cybersecurity Evaluation Plan Editor

## Improve Productivity

According to user surveys, CloudIQ saves IT an average 9 hours per week<sup>2</sup>.

- **All-in-one monitoring:** Using the same tool for monitoring and troubleshooting infrastructure system health and cybersecurity issues keeps security top-of-mind for the people closest to infrastructure: system administrators.
- **Proactive Notification and Information Sharing:** CloudIQ proactively sends system health and cybersecurity notifications via opt-in emails, and these lead you to further details and recommendations for problem resolution. You can also customize, schedule, and share reports about groups of systems and locations that matter to you, your team, and your stakeholders.
- **Integration for Automated Workflow:** Send CloudIQ notifications and data to third-party applications via Webhook and REST API to accelerate IT processes. Examples include ServiceNow (for ticketing), Slack (for DevOps notifications); Microsoft Teams (for escalation), plus Ansible and VMware vRealize (for automating corrective actions in the infrastructure).

For CloudIQ technical information, demonstration videos, third-party reviews, and case studies, go to:

[dell.com.cloudiq](https://dell.com/cloudiq)

<sup>1</sup>Based on a Dell Technologies survey of CloudIQ users conducted May-June 2021. Actual results may vary. CLM-000884

<sup>2</sup>Based on a Dell Technologies survey of CloudIQ users conducted May-June 2021. Actual results may vary. CLM-003872