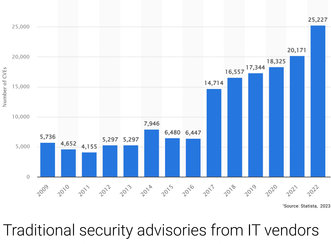
Protect your IT environment from vulnerabilities with AIOps-powered security advisories

Common IT Security Vulnerabilities and Exposures Worldwide

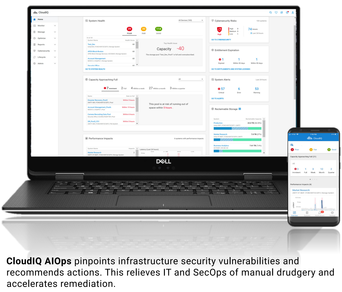


*Source: Statista, 2023

Traditional security advisories from IT vendors and across the industry require too much manual investigation before you can respond.

It can take hours to days to review advisories, documentation and recommendations and manually verify systems' hardware, firmware and software to determine risk – before you're even ready to take recommended actions.

CloudIQ AIOps: Intelligence for closing the vulnerability gap

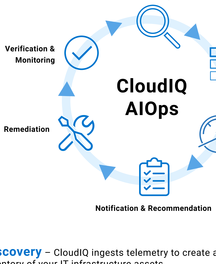


CloudIQ AIOps pinpoints infrastructure security vulnerabilities and recommends actions. This relieves IT and SecOps of manual drudgery and accelerates remediation.

CloudIQ AIOps also simplifies IT infrastructure health, cybersecurity and sustainability management, speeds resolution up to 10X[2] and saves IT a day per week on average.[2]

Continuous Vulnerability Management

Machine intelligence provides real-time updates, insights and recommendations about security advisories that enable quick response to shrink the vulnerability window and eliminate threats.



Discovery – CloudIQ ingests telemetry to create a detailed, metadata-rich inventory of your IT infrastructure assets

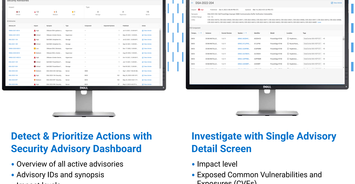
Prioritization – You can label your IT assets' business sensitivity to help prioritize your response

Assessment – CloudIQ maps Dell Security Advisories to your assets and profiles each risk's severity and business sensitivity

Notification & Recommendation – CloudIQ sends notifications and recommendations, such as change configuration or download a patch

Remediation – Now you can prioritize your response and follow recommendations

Verification – CloudIQ displays resolved and active vulnerabilities



Detect & Prioritize Actions with Security Advisory Dashboard

- Overview of all active advisories
- Advisory IDs and synopsis
- Impact levels
- Number and type of impacted systems
- Advisory articles/recommendations

Investigate with Single Advisory Detail Screen

- Impact level
- Exposed Common Vulnerabilities and Exposures (CVEs)
- CVSSv3 score range (vulnerability severity ranking)
- Affected systems and components
- Advisory article/recommendation
- Location of system

Quickly Respond and Reduce Risk with Advisory Article

- Advisory ID and synopsis
- Impact level
- Third-party components and CVEs
- Affect system version levels
- Link to software/firmware patch for remediation
- Workarounds

CloudIQ comes with Dell ProSupport and ProSupport Plus Services at no additional cost.

See a CloudIQ Cybersecurity Demo.

See more demos, data sheets and white papers:

www.dell.com/cloudiq

[1]"Common IT Vulnerabilities and Exposures Worldwide 2009-2023," Statista, 2023

[2]Dell Technologies survey of CloudIQ users conducted May through June 2021. Actual results may vary.