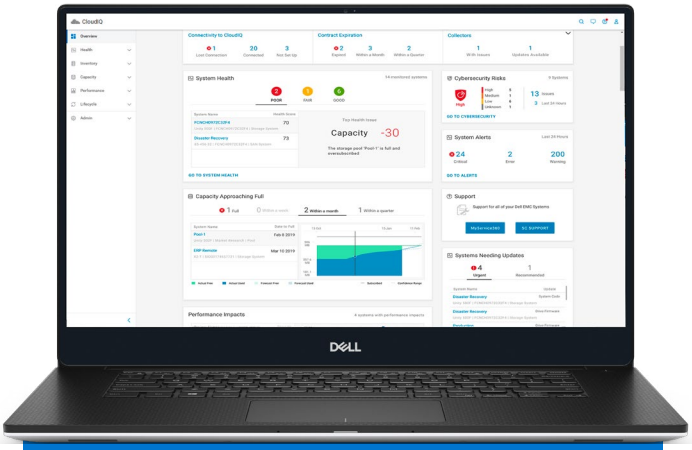
CloudIQ – Infrastruktur-Cybersicherheit

Schutz der Infrastruktur mit proaktiven Cybersicherheitsbewertungen und schnellen Korrekturmaßnahmen



CloudIQ – Intelligente Erkenntnisse zur Cybersicherheit

Wesentliche Punkte

- **Risiken reduzieren** – mit Cybersicherheitsvisualisierung des Systems und proaktiven Benachrichtigungen, die Risiken ermitteln und Maßnahmen für eine schnelle Lösung empfehlen
- **Policies managen** – mit einer benutzerfreundlichen Oberfläche für die Anpassung von Infrastruktursicherheitsrichtlinien für geplante Bewertungen
- **Produktivität steigern** – mit einer Cloud-basierten Anwendung, die die Cybersicherheit, Integrität, Leistung und Kapazität der Infrastruktur bequem zusammen überwacht

Eine Fehlkonfiguration der Infrastruktur setzt Ihr Unternehmen möglichen Cyberangriffen aus und stellt eine der führenden Bedrohungen für die Datensicherheit dar. Ohne eine intelligente, moderne Lösung müssen Sie Mitarbeiter einsetzen, um die Sicherheitskonfiguration jedes Infrastrukturelements in Ihrer Umgebung manuell zu prüfen oder Ad-hoc-Risikobewertungen durchzuführen. Keine der beiden Optionen ist praktisch, kostengünstig oder effektiv.

CloudIQ ist eine moderne Lösung, die dieses Dilemma überwindet, indem sie Ihre Systemadministratoren proaktiv über Infrastruktursicherheitsrisiken in derselben Anwendung informiert, die sie täglich zur Überwachung und Behebung von Infrastrukturintegritäts-, Kapazitäts- und Performanceproblemen verwenden.

CloudIQ ist die Cloud- und KI-/ML-basierte Anwendung für proaktives Monitoring und vorausschauende Analysen für das Dell Infrastruktur-Produktportfolio. Sie kombiniert menschliche und maschinelle Intelligenz, um Ihnen die Möglichkeit zu geben, proaktiv und effizient sicherzustellen, dass der Status der IT-Infrastruktur die Anforderungen Ihres Unternehmens erfüllt.

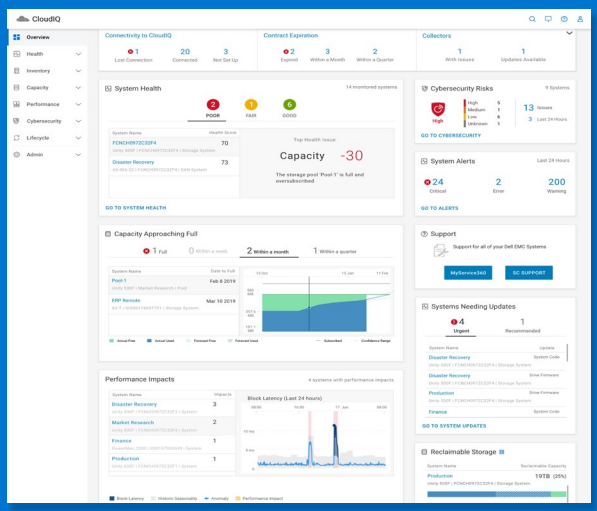
CloudIQ hat gezeigt, dass es die Zeit bis zur Behebung von Infrastrukturintegritäts-, Performance- und Kapazitätsproblemen im Durchschnitt um das 2-Fache bis 10-Fache verbessern kann[1]. CloudIQ kann die Sicherheitslage Ihrer IT-Umgebung mit weniger Aufwand verbessern.

Sichern Sie Ihre IT-Infrastruktur in wenigen Minuten

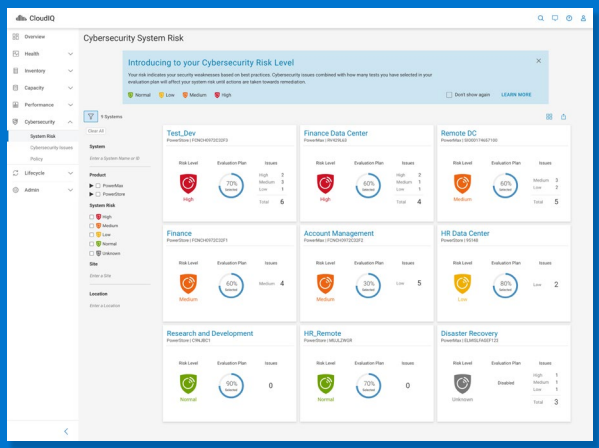
CloudIQ wird in der sicheren Dell IT-Cloud mit einer sicheren Netzwerkverbindung zu Ihrer IT-Umgebung gehostet und benötigt nur wenige Minuten für eine Ersteinrichtung. Ein einziger Klick in der Anwendung Element Manager Ihrer Infrastruktursysteme (z. B. Unisphere für PowerMax-Storage-Systeme) initiiert CloudIQ, um die Integrität, Performance und Kapazitätstelemetrie Ihrer Systeme zu erfassen und zu analysieren. Die Cybersicherheitsunterstützung wurde mit zwei einfachen Nachbereitungsschritten entwickelt: zunächst die Erfassung von Sicherheitstelemetrie initiieren, dann einen einfachen Planeditor für Cybersicherheitsbewertung verwenden, um Ihren Sicherheitsrichtlinienplan einzurichten, und das System beginnt, die Daten zu bewerten und Sicherheitsfehlkonfigurationen zu erkennen.

Das ist wirklich so einfach und wird sicher durch rollenbasierten Zugriff gemanagt.

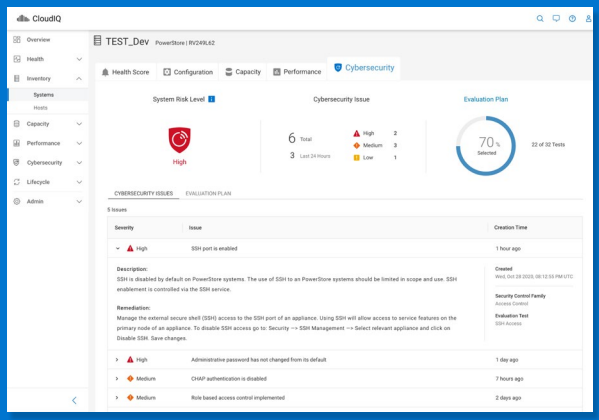
Erkenntnisse und Maßnahmen zur Cybersicherheit



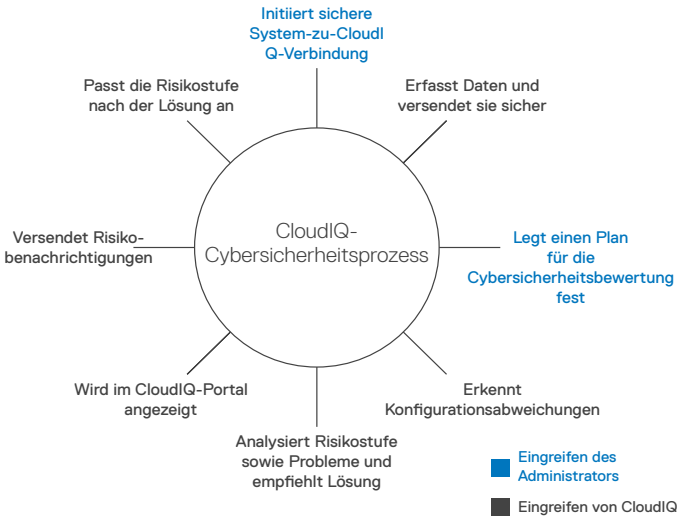
CloudIQ-Übersicht mit Cybersicherheit



Cybersicherheitsrisikostufen



Details und Empfehlungen zu Cybersicherheitsrisiken

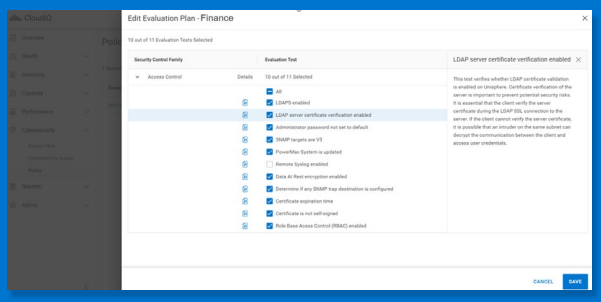


CloudIQ ermöglicht einen effizienten, geschlossenen Prozess für eine umfassende 24x7-Cybersicherheitsbewertung und -korrektur der Infrastruktur.

Weniger Risiken

Mithilfe des sicheren Dell Technologies Netzwerks, das in der sicheren Dell IT-Cloud gehostet wird, erfasst, speichert und bewertet CloudIQ Sicherheitskonfigurationsinformationen von Ihren Systemen in Ihrer gesamten IT-Umgebung, einschließlich primärer und sekundärer Rechenzentren und Edge-Standorte.

- **Cybersicherheitsbewertung:** Ermittelt, ob die Systemsicherheitskonfigurationen von Ihrer Richtlinie abgewichen sind. Dazu gehören rollenbasierte Zugriffskontrolle, standardmäßiges Administratorkennwort, aktivierte Data-at-Rest-Verschlüsselung, NFS-Sicherheitsstufe und mehr. CloudIQ bewertet kontinuierlich Abweichungen, um zu vermeiden, dass Sie jede Konfiguration manuell überprüfen und Ihr ständiges Risikobewusstsein sicherstellen können.
- **Übersicht über Cybersicherheitsrisiken:** Sehen Sie sich die Anzahl der Systeme mit hohen, mittleren und geringen Sicherheitsrisiken im selben Dashboard an, das Ihnen einen Überblick über die Systemintegritätsbewertungen und zugehörige Kapazitäts- und Performanceanalysen bietet. Dies hilft Ihnen, Maßnahmen schnell zu priorisieren und die Problemlösungszeit zu verkürzen.
- **Cybersicherheitsrisikostufen:** Verwenden Sie ein einziges Dashboard, um jedes gefährdete System zu identifizieren, jedes in seiner eigenen Karte mit einem Wert auf Cybersicherheitsrisikoebene. Systeme werden von oben nach unten angezeigt, je nach Risikostufe, um Sie bei der weiteren Priorisierung von Maßnahmen zu unterstützen.
- **Details zur Cybersicherheit und Korrektur:** Erfahren Sie mehr über die Details des Risikos jedes Systems und sehen Sie sich die empfohlene Maßnahme an, um die abweichende Sicherheitskonfiguration in einen sicheren Zustand zurückzuversetzen. Sie können den Element Manager jedes Systems direkt über CloudIQ starten, um schnell Korrekturmaßnahmen zu ergreifen.



Planeditor für Cybersicherheitsbewertung

Policies managen

Mit einem einfachen Tool können Sie die Bewertungsrichtlinie für die Infrastruktursicherheitskonfiguration planen, die CloudIQ zur Bewertung von Cybersicherheitsrisiken verwendet.

- **Planungstool:** Verwenden Sie einen vorlagenbasierten Planeditor für Cybersicherheitsbewertung um Sicherheitskonfigurationen auszuwählen, die CloudIQ mit den tatsächlichen Konfigurationen Ihrer Systeme vergleicht. Mithilfe des Editors können Sie jeden Evaluierungstest für Ihre gewünschte Sicherheitsrichtlinie mit einem Klick aktivieren oder deaktivieren.
- **Sicherheitsstandards:** Sicherheitskonfigurationen basieren auf den 800-53 r5- und NIST 800–209-Standards sowie Best Practices von Dell Technologies für jedes spezifische Infrastrukturprodukt, basierend auf der jahrelangen Erfahrung unserer Ingenieure und Techniker bei der Unterstützung Tausender NutzerInnen.

Mehr Produktivität

Laut Umfragen unter unseren NutzerInnen die IT-Abteilung dank CloudIQ durchschnittlich 9 Stunden pro Woche[2].

- **All-in-one-Monitoring:** Die Verwendung desselben Tools für das Monitoring und Troubleshooting von Problemen mit der Integrität des Infrastruktursystems und der Cybersicherheit sorgt dafür, dass Sicherheit für die Personen, die der Infrastruktur am nächsten sind, oberste Priorität hat: Systemadministratoren.
- **Proaktive Benachrichtigung und Informationsaustausch:** CloudIQ sendet proaktiv Systemintegritäts- und Cybersicherheitsbenachrichtigungen über abonnierte E-Mails, die Sie zu weiteren Details und Empfehlungen zur Problemlösung führen. Sie können auch Berichte über Gruppen von Systemen und Standorten anpassen, planen und teilen, die für Sie, Ihr Team und Ihre Stakeholder wichtig sind.
- **Integration für automatisierten Workflow:** Senden Sie CloudIQ-Benachrichtigungen und -Daten an Drittanbieteranwendungen über Webhook und REST API zur Beschleunigung von IT-Prozessen. Beispiele sind ServiceNow (für Ticketing), Slack (für DevOps-Benachrichtigungen); Microsoft Teams (für Eskalation) sowie Ansible und VMware vRealize (für die Automatisierung von Korrekturmaßnahmen in der Infrastruktur).

Technische Informationen zu CloudIQ, Demonstrationsvideos, Drittanbieterbewertungen und Fallstudien finden Sie unter:

dell.com.cloudiq

[1] Basierend auf einer von Mai bis Juni 2021 durchgeführten Umfrage von Dell Technologies unter CloudIQ-NutzerInnen. Die tatsächlichen Ergebnisse können abweichen. CLM-000884

[2] Basierend auf einer von Mai bis Juni 2021 durchgeführten Umfrage von Dell Technologies unter CloudIQ-NutzerInnen. Die tatsächlichen Ergebnisse können abweichen. CLM-003872