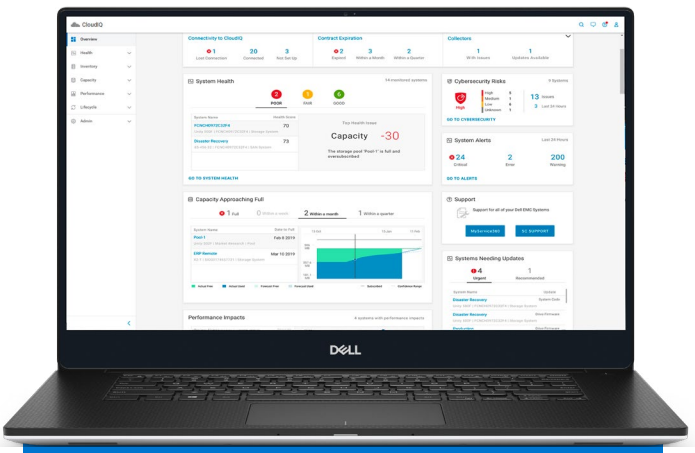
CloudIQ - Infrastructuurbeveiliging

Houd de infrastructuur veilig met proactieve evaluaties van cyberbeveiliging en snelle probleemoplossing



CloudIQ Intelligente inzichten in cyberbeveiliging

Belangrijkste punten

- **Minder risico's** – met visualisatie van systeemcyberbeveiliging en proactieve notificaties die risico's aangeven en acties aanbevelen voor snelle probleemoplossing
- **Beleid beheren** – met een gebruiksvriendelijke interface voor het instellen van beleidsregels voor infrastructuurbeveiligingsbeleid voor geplande evaluaties
- **Verbeter de productiviteit** – met een cloudgebaseerde applicatie die infrastructuurbeveiliging, systeemstatus, prestaties en capaciteit samen controleert

Een verkeerde configuratie van de infrastructuur opent uw organisatie voor cyberinbraken en vormt een belangrijke bedreiging voor databeveiliging. Zonder een slimme, moderne oplossing moet u personeel inzetten om de beveiligingsconfiguratie van elk infrastructuurelement in uw omgeving handmatig te beoordelen of ad-hocrisicobeoordelingen uit te voeren. Geen van beide opties is praktisch, betaalbaar of effectief.

CloudIQ is een moderne oplossing die dit dilemma overwint door uw systeembeheerders proactief te informeren over risico's op het gebied van infrastructuurbeveiliging in dezelfde applicatie die ze dagelijks gebruiken om de status, capaciteit en prestatieproblemen van de infrastructuur te controleren en op te lossen.

CloudIQ is de cloud- en AI/ML-gebaseerde applicatie voor proactieve monitoring en voorspellende analyse binnen de Dell infrastructuurproductportfolio. Het combineert menselijke intelligentie en machine-intelligentie en biedt u inzichten om er proactief en efficiënt voor te zorgen dat de status van de IT-infrastructuur aan de eisen van uw bedrijf voldoet.

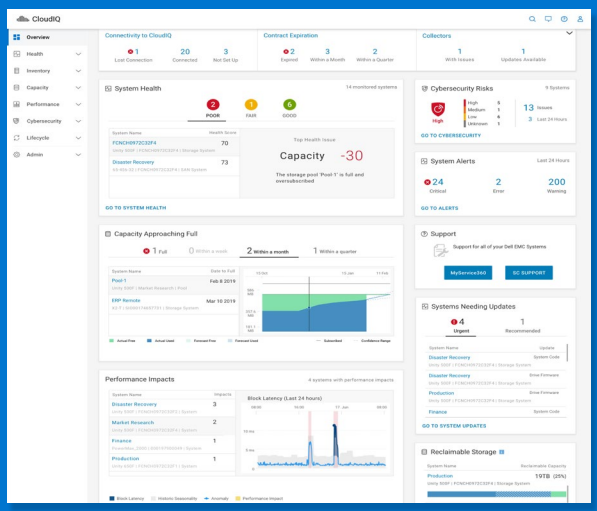
Het is bewezen dat CloudIQ de time-to-resolution van infrastructuurstatus, prestaties en capaciteitsproblemen gemiddeld 2x tot 10x verbetert[1]. CloudIQ staat ervoor om de beveiligingshouding van uw IT-omgeving met minder inspanning te verbeteren.

Begin binnen enkele minuten met de beveiliging van uw IT-infrastructuur

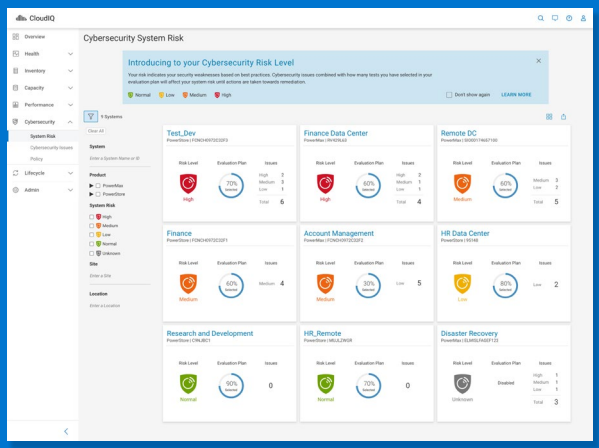
CloudIQ wordt gehost in de veilige Dell IT-cloud met een beveiligde netwerkverbinding naar uw IT-omgeving. Het duurt slechts enkele minuten om CloudIQ voor de eerste keer in te stellen. Met één klik in de beheerapplicatie van uw infrastructuursystemen (bijv. Unisphere voor PowerMax storagesystemen) wordt CloudIQ gestart om de status, prestaties en capaciteitstelemetrie van uw systemen te verzamelen en te analyseren. Cyberbeveiliging vindt plaats via twee eenvoudige vervolgstappen: start eerst de verzameling van beveiligingstelemetrie en gebruik vervolgens een eenvoudige editor voor het plannen van de evaluatie van de cyberbeveiliging. Hiermee kunt u uw beveiligingsbeleidsplan opzetten. Vervolgens begint het systeem met het evalueren van de data en het detecteren van onjuiste beveiligingsconfiguraties. Vervolgens begint het systeem met het evalueren van de data en het detecteren van onjuiste beveiligingsconfiguraties.

Zo eenvoudig is het, en beheer vindt plaats via op rollen gebaseerde toegang.

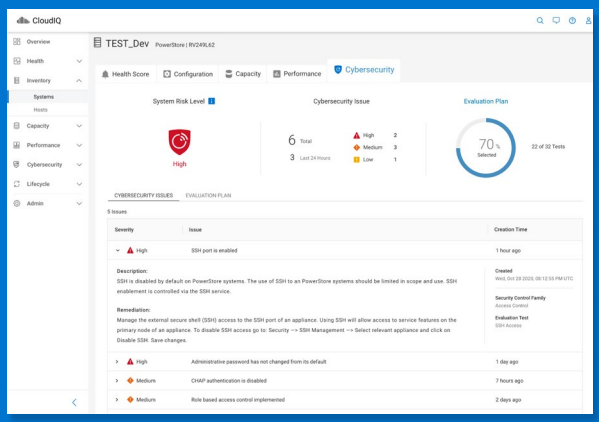
Inzichten en acties op het gebied van cyberbeveiliging



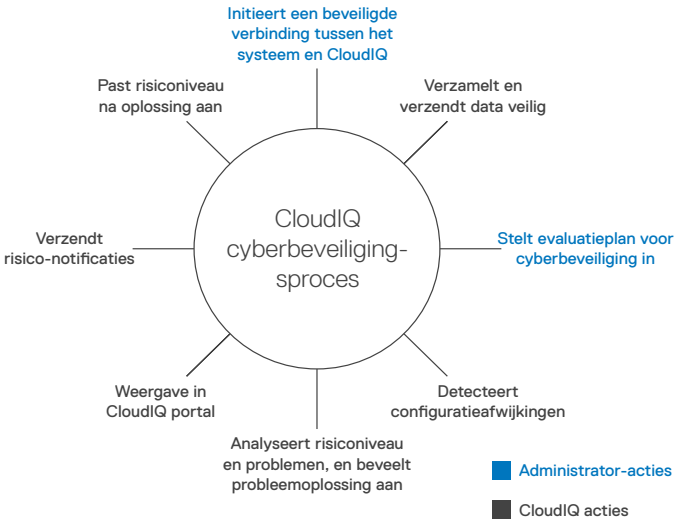
CloudIQ overzicht met cyberbeveiliging



Risiconiveaus voor cyberbeveiliging



Informatie en aanbevelingen over cyberbeveiligingsrisico's

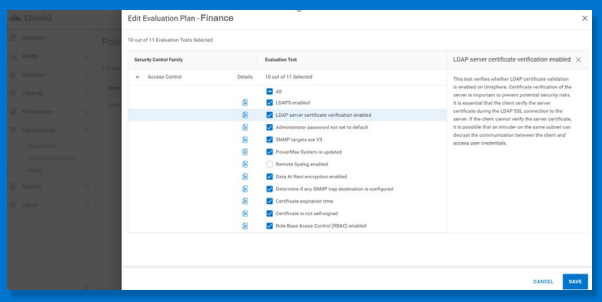


CloudIQ maakt een efficiënt, gesloten proces mogelijk voor uitgebreide, 24x7 evaluatie en herstel van infrastructuurbeveiliging.

Minder risico's

Met behulp van het beveiligde Dell Technologies netwerk en gehost in de beveiligde Dell IT-cloud, verzamelt en bewaart CloudIQ beveiligingsconfiguratiegegevens van uw systemen en beoordeelt deze binnen uw gehele IT-omgeving, inclusief primaire en secundaire datacenters en edge-locaties.

- **Evaluatie van cyberbeveiliging:** Bepaalt of configuraties voor systeembeveiliging afwijken van uw beleidsregels. Dit omvat op rollen gebaseerde toegangscontrole, standaard administratorwachtwoord, ingeschakelde versleuteling van data-at-rest, NFS-beveiligingsniveau en meer. CloudIQ beoordeelt voortdurend afwijkingen en zorgt ervoor dat u elke configuratie handmatig kunt controleren en dat u zich altijd bewust bent van de risico's.
- **Overzicht van cyberbeveiligingsrisico's:** Bekijk het aantal systemen met hoge, gemiddelde en lage beveiligingsrisico's op hetzelfde dashboard dat u een overzicht geeft van de systeemstatusscores en gerelateerde capaciteits- en prestatieanalyses. Dit helpt u snel prioriteit te geven aan acties en de time-to-resolution te bekorten.
- **Risiconiveaus voor cyberbeveiliging:** Gebruik één dashboard om elk systeem te identificeren dat risico loopt, elk op zijn eigen kaart met een cyberbeveiligingsrisicoscore. Systemen worden top-down weergegeven op basis van het risiconiveau om u te helpen bij het verder prioriteren van acties.
- **Informatie over cyberbeveiliging en herstel:** Raadpleeg de details van de risico's van elk systeem en bekijk de aanbevolen actie om de afwijkende beveiligingsconfiguratie terug te brengen naar een veilige staat. U kunt de elementbeheerapplicatie van elk systeem rechtstreeks vanuit CloudIQ starten om snel corrigerende maatregelen te nemen.



Editor voor het plannen van de evaluatie van de cyberbeveiliging

Beleidsregels beheren

Met behulp van een eenvoudige tool kunt u de beleidsregels voor evaluatie van uw infrastructuurbeveiligingsconfiguratie instellen die CloudIQ zal gebruiken om de risico's op het gebied van cyberbeveiliging te beoordelen.

- **Planningstool:** Gebruik een sjabloongestuurde editor voor het plannen van de evaluatie van de cyberbeveiliging om beveiligingsconfiguraties te selecteren die CloudIQ zal vergelijken met de werkelijke configuraties van uw systemen. Met de editor kunt u elke evaluatietest voor uw gewenste beveiligingsbeleid in- of uitschakelen.
- **Beveiligingsstandaarden:** Beveiligingsconfiguraties zijn gebaseerd op NIST 800-53 r5 en NIST 800- 209 standaarden, evenals best practices van Dell Technologies voor elk specifiek infrastructuurproduct op basis van de jarenlange ervaring van onze technici bij het ondersteunen van duizenden gebruikers.

Productiviteit verbeteren

Volgens gebruikersonderzoek bespaart CloudIQ de IT-afdeling gemiddeld 9 uur per week[2].

- **Alles-in-één controle:** Door gebruik van dezelfde tool voor het controleren van de systeemstatus van de infrastructuur en het oplossen van cyberbeveiligingsproblemen blijft beveiliging prioriteit voor de mensen die het dichtst bij de infrastructuur staan: systeemadministrators.
- **Proactieve notificaties en delen van informatie:** CloudIQ stuurt proactief notificaties over systeemstatus en cyberbeveiliging via opt-in-e-mails en deze leiden u naar meer informatie en aanbevelingen voor probleemoplossing. U kunt ook rapporten aanpassen, plannen en delen over groepen systemen en locaties die voor u, uw team en uw belanghebbenden belangrijk zijn.
- **Integratie voor geautomatiseerde workflow:** Verzend CloudIQ-notificaties en -data naar applicaties van derden via Webhook en REST API om IT-processen te versnellen. Voorbeelden zijn ServiceNow (voor ticketing), Slack (voor DevOps-meldingen); Microsoft Teams (voor escalatie), plus Ansible en VMware vRealize (voor het automatiseren van corrigerende acties in de infrastructuur).

Ga voor technische informatie over CloudIQ, demonstratievideo's, beoordelingen van derden en casestudy's naar:

dell.com.cloudiq

[1]Gebaseerd op een onderzoek van Dell Technologies onder CloudIQ gebruikers, uitgevoerd in mei t/m juni 2021. De werkelijke resultaten kunnen variëren. CLM-000884

[2]Gebaseerd op een onderzoek van Dell Technologies onder CloudIQ gebruikers, uitgevoerd in mei t/m juni 2021. De werkelijke resultaten kunnen variëren. CLM-003872