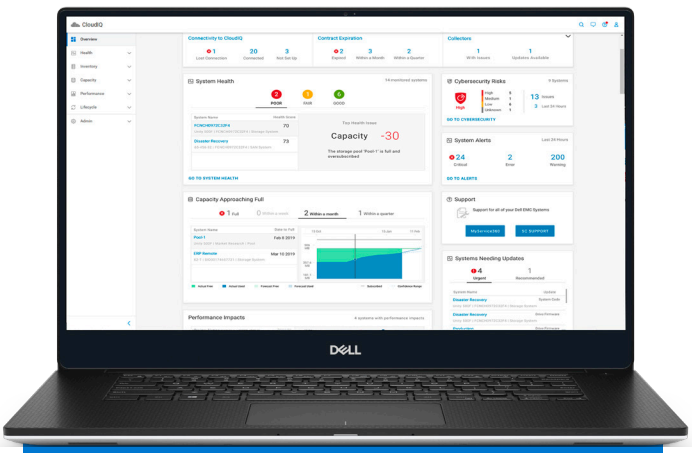
CloudIQ - 인프라스트럭처 사이버 보안

사전 예방적 사이버 보안 진단과 신속한 문제 해결을 통해 인프라스트럭처를 안전하게 유지



CloudIQ 지능적인 사이버 보안 분석 정보 제공

간략한 소개

- **위험 완화** – 시스템 사이버 보안 시각화와 사전 예방적 알림을 통해 위험을 정확히 파악하고 신속한 해결을 위한 권장 조치 확인
- **정책 관리** – 사용이 간편한 인터페이스로 예약된 진단을 위한 인프라스트럭처 보안 정책을 맞춤 구성
- **생산성 향상** - 클라우드 기반 애플리케이션으로 인프라스트럭처 사이버 보안, 상태, 성능 및 용량을 함께 편리하게 모니터링

인프라스트럭처 구성이 잘못되면 조직이 사이버 침입에 취약해지고 데이터 보안이 위험해집니다. 스마트한 최신 솔루션이 없는 경우 전담 직원을 배정하여 운영 환경의 모든 인프라스트럭처 요소에 대한 보안 구성을 수동으로 진단하거나 임시방편적 위험 진단을 실시해야 하며, 두 가지 방법 모두 실용적이거나 경제적이거나 효과적이지 않습니다.

CloudIQ는 시스템 관리자가 인프라스트럭처 상태, 용량 및 성능 문제를 모니터링하고 해결하기 위해 일상적으로 사용하는 애플리케이션에서 인프라스트럭처 보안 위험을 사전 예방적으로 알려 이러한 딜레마를 극복하는 최신 솔루션입니다.

CloudIQ는 Dell 인프라스트럭처 제품 포트폴리오에 대한 클라우드 및 AI/ML 기반의 사전 예방적 모니터링 및 예측 분석 애플리케이션으로, 인간 지능과 머신 인텔리전스를 결합해 사전 예방적이고 효율적으로 비즈니스 요구를 충족하도록 IT 인프라스트럭처의 상태를 유지하는 데 도움이 되는 분석 정보를 제공합니다.

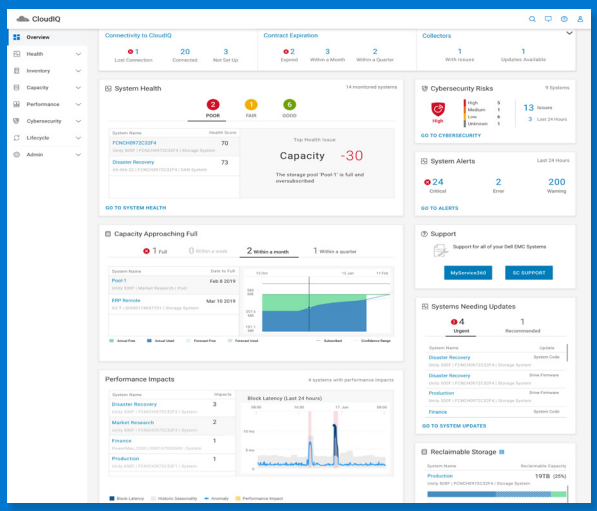
인프라스트럭처 상태, 성능 및 용량 문제를 해결하는 데 소요되는 시간을 평균 2배에서 10배까지 단축[1]하는 것으로 입증된 CloudIQ를 통해 더 적은 노력으로 IT 환경의 보안 태세를 개선할 수 있습니다.

몇 분 안에 IT 인프라스트럭처 보호 시작

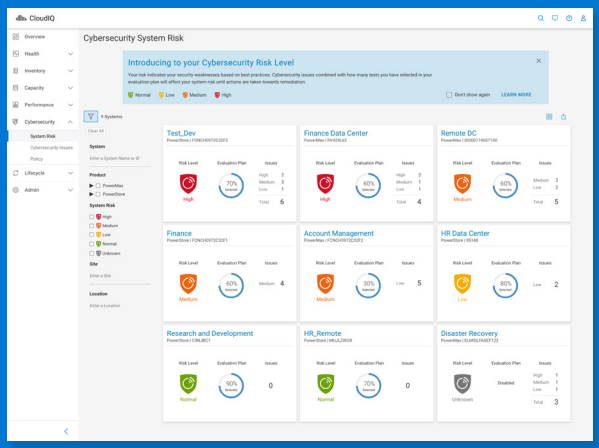
IT 환경에 대한 보안 네트워크 연결을 통해 안전한 Dell IT Cloud에서 호스팅되는 CloudIQ는 처음 설정하는 데 몇 분밖에 걸리지 않습니다. 인프라스트럭처 시스템의 Element Manager 애플리케이션(예: PowerMax 스토리지 시스템용 Unisphere)에서 한 번 클릭하면 CloudIQ가 시스템에서 상태, 성능 및 용량 텔레메트리를 수집하고 분석하기 시작합니다. 사이버 보안은 두 가지 손쉬운 후속 단계를 통해 구현됩니다. 보안 텔레메트리 수집을 시작한 후 간단한 사이버 보안 평가 계획 편집기를 사용해 보안 정책 계획을 설정하면 시스템이 데이터를 평가하고 보안 구성 오류를 탐지하기 시작합니다.

이처럼 매우 용이하게 사이버 보안이 구현되며 역할 기반 액세스를 통해 안전하게 관리됩니다.

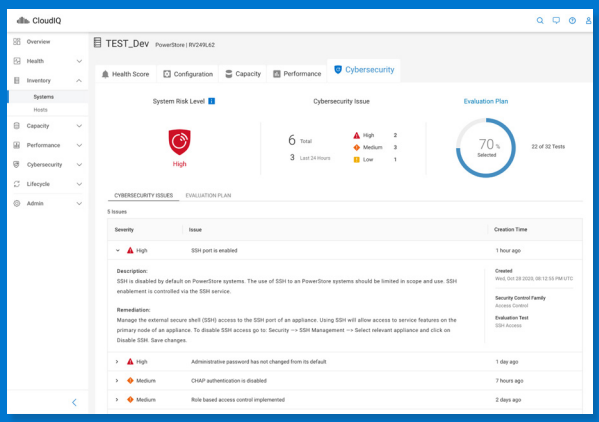
사이버 보안 분석 정보 및 조치



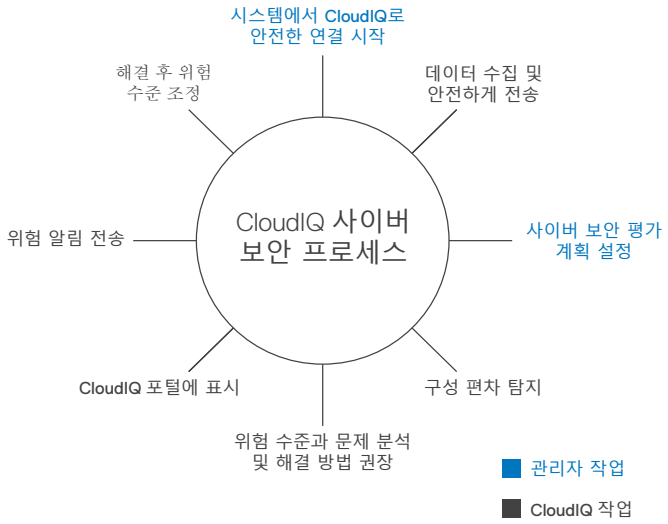
CloudIQ의 사이버 보안 개요



사이버 보안 위험 수준



사이버 보안 위험 세부 정보 및 권장 사항

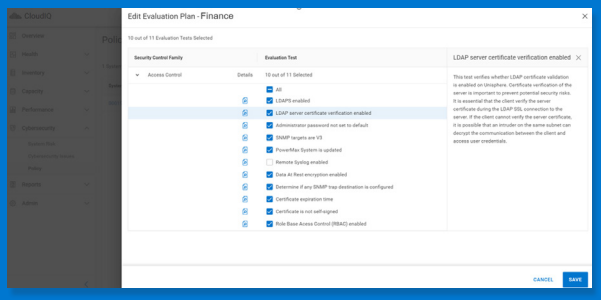


CloudIQ는 효율적인 순환형 프로세스를 통해 포괄적인 **24x7** 인프라스트럭처 사이버 보안 진단 및 문제 해결을 지원합니다.

위험 완화

CloudIQ는 안전한 Dell Technologies 네트워크를 사용하며 안전한 Dell IT Cloud에서 호스팅되어 운영 데이터 센터와 보조 데이터 센터, 엣지 위치를 포함한 전체 IT 환경의 시스템에서 보안 구성 정보를 수집, 저장, 진단합니다.

- **사이버 보안 진단**: 시스템 보안 구성이 정책에서 벗어났는지 확인합니다. 여기에는 역할 기반 액세스 제어, 기본 관리 비밀번호, 저장 상태 데이터 암호화 활성화, NFS 보안 수준 등이 포함됩니다. CloudIQ는 지속적으로 편차를 진단하므로 각 구성을 수동으로 확인할 필요가 없으며 위험을 항상 인식할 수 있습니다.
- **사이버 보안 위험 개요**: 시스템 상태 점수와 관련 용량 및 성능 분석 정보를 한눈에 파악할 수 있는 대시보드에 보안 위험이 높은/중간/낮은 수준인 시스템 수도 표시됩니다. 이를 통해 조치 우선 순위를 빠르게 지정하여 문제 해결 시간을 단축할 수 있습니다.
- **사이버 보안 위험 수준**: 단일 대시보드에서 위험에 처한 모든 시스템을 파악하고 각각 자체 카드에서 사이버 보안 위험 수준 값을 확인할 수 있습니다. 위험 수준이 높은 시스템부터 순서대로 표시되므로 조치 우선 순위를 정하는 데 도움이 됩니다.
- **사이버 보안 세부 정보 및 문제 해결**: 각 시스템의 위험에 대한 세부 정보와 정책에서 벗어난 보안 구성을 안전한 상태로 되돌리기 위한 권장 조치가 표시됩니다. CloudIQ에서 직접 각 시스템의 Element Manager를 실행하여 신속하게 개선 조치를 취할 수 있습니다.



사이버 보안 평가 계획 편집기

정책 관리

CloudIQ가 사이버 보안 위험을 진단하는 데 사용할 인프라스트럭처 보안 구성 진단 정책을 간단한 툴로 계획할 수 있습니다.

- **계획 툴:** 템플릿 기반 사이버 보안 평가 계획 편집기를 사용하여 CloudIQ가 시스템의 실제 구성과 비교할 보안 구성을 선택합니다. 편집기에서 원하는 보안 정책에 대한 각 평가 테스트를 클릭하여 활성화하거나 비활성화할 수 있습니다.
- **보안 표준:** 보안 구성은 다년간 수천 명의 사용자를 지원한 엔지니어 경험에 입각해 각 특정 인프라스트럭처 제품에 대해 구축된 Dell Technologies 모범 사례와 NIST 800-53 r5 및 NIST 800 – 209 표준을 기반으로 합니다.

생산성 향상

사용자 설문조사에 따르면 CloudIQ는 IT 부서의 작업 시간을 주당 평균 9시간 절감[2]할 수 있도록 지원합니다.

- **올인원 모니터링:** 하나의 툴로 인프라스트럭처 시스템 상태와 사이버 보안 문제를 모니터링하고 문제를 해결함으로써 인프라스트럭처를 밀접하게 다루는 시스템 관리자가 항상 보안을 최우선으로 고려할 수 있습니다.
- **사전 예방적 알림 및 정보 공유:** CloudIQ는 옵트인 이메일을 통해 시스템 상태 및 사이버 보안 알림을 사전 예방적으로 전송하므로 문제 해결을 위한 세부 정보와 권장 사항을 확인할 수 있습니다. 또한 사용자, 소속 팀, 이해 관계자에게 중요한 여러 시스템 및 위치에 대한 보고서를 맞춤 구성하고 예약하며 공유할 수 있습니다.
- **자동화된 워크플로를 위한 통합:** Webhook 및 REST API를 통해 타사 애플리케이션에 CloudIQ 알림 및 데이터를 전송하여 IT 프로세스를 가속화합니다. 이러한 애플리케이션의 예로는 ServiceNow(티켓팅용), Slack(DevOps 알림용), Microsoft Teams(에스컬레이션용), Ansible 및 VMware vRealize(인프라스트럭처에서의 개선 조치 자동화용)를 들 수 있습니다.

CloudIQ 기술 정보, 데모 비디오, 타사 리뷰 및 사례 연구를 보려면 다음 사이트를 방문하십시오.

dell.com.cloudiq

[1]2021년 5월부터 6월까지 CloudIQ 사용자를 대상으로 실시한 Dell Technologies 설문조사 기준. 실제 결과는 달라질 수 있습니다. CLM-000884
[2]2021년 5월부터 6월까지 CloudIQ 사용자를 대상으로 실시한 Dell Technologies 설문조사 기준. 실제 결과는 달라질 수 있습니다. CLM-003872