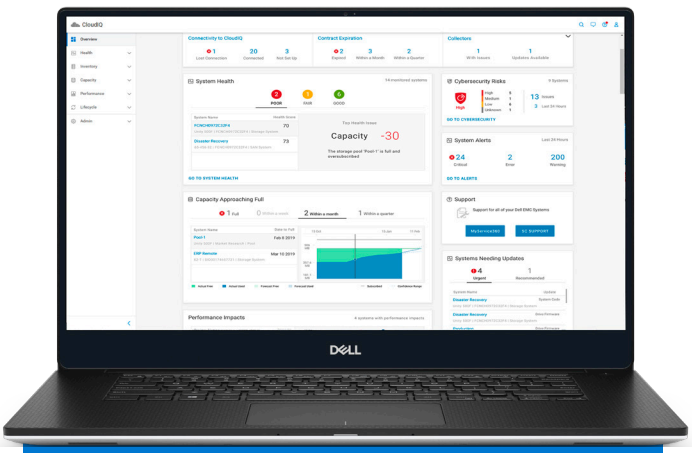
CloudIQ — 基础架构网络安全

通过主动评估网络安全状况和快速采取补救措施，确保基础架构安全



CloudIQ 智能网络安全见解

概要

- **降低风险** — 通过直观呈现系统网络安全状态，并主动提供风险识别和操作建议通知，快速解决问题
- **管理策略** — 通过简单易用的界面，为计划评估自定义基础架构安全策略。
- **提高工作效率** — 使用基于云的应用程序，可方便地同时监视基础架构网络安全、运行状况、性能和容量

基础架构配置错误会让您的组织面临网络入侵的风险，并且是数据安全方面的主要威胁。如果没有智能的现代解决方案，您就必须专门安排员工手动评估您环境中的每个基础架构元素的安全配置，或进行临时风险评估。但这两种方法都不实用，不仅成本高昂，而且效果欠佳。

CloudIQ 是一款可破解这一难题的现代解决方案。它可以集成到系统管理员用于日常监视和解决基础架构运行状况、容量和性能问题的同一应用程序中，主动通知系统管理员基础架构所面临的安全风险。

CloudIQ 是基于云和 AI/ML 的主动监视和预测性分析应用程序，适用于戴尔基础架构产品组合。它将人类智能和机器智能相结合来为您提供见解，帮助您主动、高效地确保 IT 基础架构的状态满足您的业务需求。

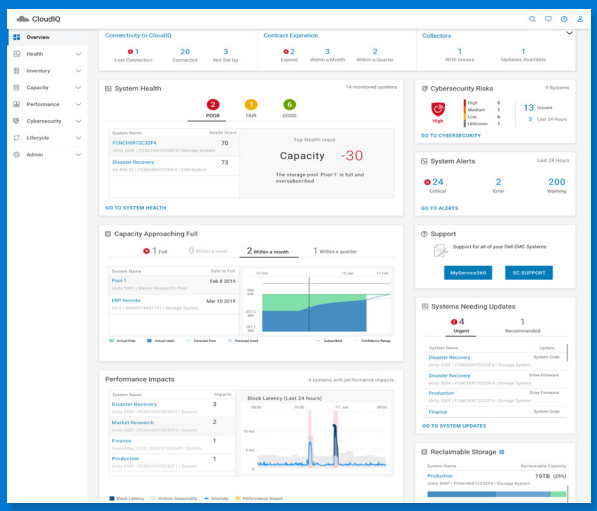
实践证明，CloudIQ 可将基础架构运行状况、性能和容量问题的解决速度平均加快 2 倍到 10 倍[1]，进而使您能够轻松提升 IT 环境的安全态势。

只需几分钟即可快速确保 IT 基础架构的安全

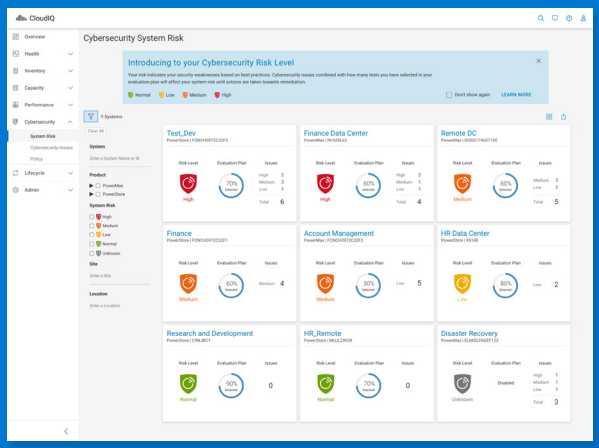
CloudIQ 托管在安全的 Dell IT 云中且具有与您 IT 环境的安全网络连接，首次设置仅需几分钟即可完成。只需单击一下基础架构系统的 Element Manager 应用程序（例如 Unisphere for PowerMax 存储系统），即可启动 CloudIQ 以收集和分析您系统的运行状况、性能和容量遥测。要启用网络安全支持功能，只需完成两个简单的后续步骤：首先启动安全遥测收集，然后使用简单的网络安全评估计划编辑器来设置您的安全策略计划，这样系统就会开始评估数据并检测安全配置错误。

它如此简单且可通过基于角色的访问权限，以安全方式对其进行管理。

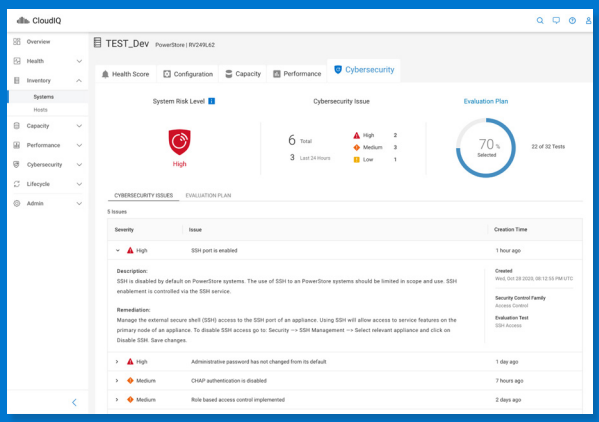
网络安全见解和措施



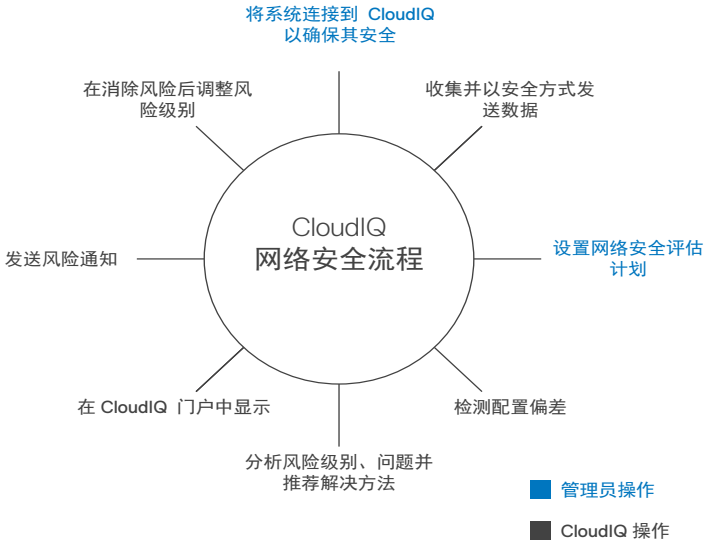
CloudIQ 网络安全概览



网络安全风险级别



网络安全风险详细信息和建议

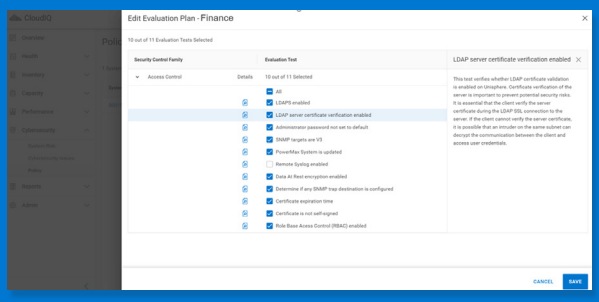


CloudIQ 支持高效的闭环流程，可实现全方位、全天候基础架构网络安全评估和补救。

降低风险

CloudIQ 使用安全的 Dell Technologies 网络，并托管在安全的 Dell IT 云中，可收集、存储和评估整个 IT 环境（包括主数据中心和辅助数据中心以及边缘位置）中的安全配置信息。

- **网络安全评估**：确定系统安全配置是否违反您的策略，包括基于角色的访问控制、默认管理密码、启用静态数据加密、NFS 安全级别等。CloudIQ 可以持续评估偏差，以使您不必手动检查每个配置，并确保您能始终了解风险。
- **网络安全风险概览**：在同一个控制面板中查看具有高、中和低安全风险的系统数量，让您对系统运行状况评分以及相关容量和性能分析数据全部一目了然。这有助于您快速确定各项措施的轻重缓急，并缩短解决问题所需的时间。
- **网络安全风险级别**：使用单个控制面板即可识别所有存在风险的系统，而且每个此类系统都以单独的卡片显示，并具有网络安全风险级别值。这些系统将按风险级别从高到低的顺序自上而下排列，以便您进一步确定应优先采取的措施。
- **网络安全详细信息和补救措施**：了解各个系统所面临的风险的详细信息，并查看将偏离的安全配置恢复到安全状态的操作建议。您可以直接从 CloudIQ 启动每个系统的 Element Manager，以快速采取纠正措施。



网络安全评估计划编辑器

管理策略

您可以使用简单的工具来规划基础架构安全配置评估策略，CloudIQ 将根据此策略评估网络安全风险。

- **规划工具**：使用模板驱动的网络安全评估计划编辑器选择安全配置，CloudIQ 会将您所选择的配置与系统的实际配置进行比较。借助该编辑器，您可以单击启用或禁用所需安全策略的每个评估测试。
- **安全标准**：安全配置基于 NIST 800-53 r5 和 NIST 800-209 标准，以及 Dell Technologies 针对每个特定基础架构产品的最佳实践，这些实践是根据我们的工程师多年来为数千名用户提供支持的经验总结而来。

提高工作效率

根据用户调查，CloudIQ 可让 IT 部门每周平均节省 9 小时时间[2]。

- **一体化监视**：使用同一工具即可监视基础架构系统运行状况和网络安全问题并进行故障处理，这让最接近基础架构的人员（系统管理员）能够始终将安全放在第一位。
- **主动通知和信息共享**：CloudIQ 可通过电子邮件（需选择加入此功能）主动发送系统运行状况和网络安全通知，从而为您提供详细信息和问题解决建议。您还可以自定义、计划和共享有关对您、您的团队和利益相关者至关重要的系统和位置组的报告。
- **用于自动化工作流的集成**：通过 Webhook 和 REST API 将 CloudIQ 通知和数据发送到第三方应用程序，从而加快 IT 流程。第三方应用程序示例包括 ServiceNow（用于开票）、Slack（用于 DevOps 通知）、Microsoft Teams（用于上报），以及 Ansible 和 VMware vRealize（用于在基础架构中自动执行纠正措施）。

要查看 CloudIQ 技术信息、演示视频、第三方评论和案例分析，请访问：

dell.com.cloudiq

[1]基于 Dell Technologies 于 2021 年 5 月到 6 月对 CloudIQ 用户进行的调查。实际结果可能有所不同。CLM-000884
[2]基于 Dell Technologies 于 2021 年 5 月到 6 月对 CloudIQ 用户进行的调查。实际结果可能有所不同。CLM-003872