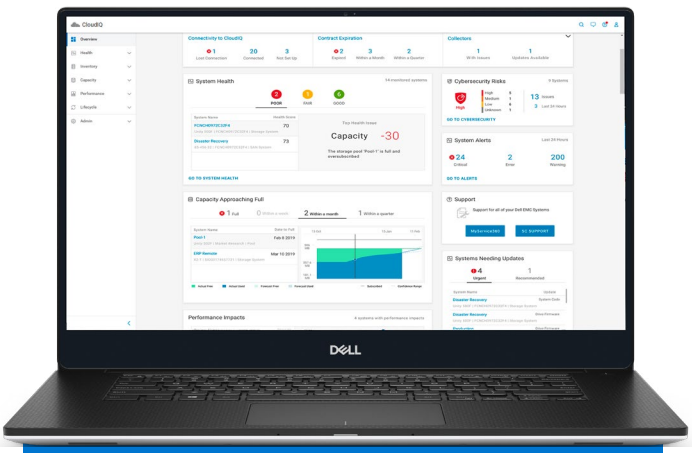
CloudIQ – インフラストラクチャ サイバーセキュリティ

プロアクティブなサイバーセキュリティ評価と迅速な修復により、インフラストラクチャを安全に保つ



インフラストラクチャの構成ミスにより、組織はサイバー侵入を受けやすくなり、データ セキュリティの大きな脅威となります。スマートな最新ソリューションがなければ、専任スタッフが環境内のすべてのインフラストラクチャ要素のセキュリティ構成を手動で評価したり、そのたびにリスク評価したりする必要があります。このようなオプションは現実的ではなく、経済的でも効果的でもありません。

CloudIQは、このジレンマを克服する最新のソリューションです。インフラストラクチャの正常性、容量、パフォーマンスの問題を監視して解決するために日頃から使用している同じアプリケーションで、インフラストラクチャのセキュリティ リスクに関する通知が、システム管理者にプロアクティブに送信されます。

CloudIQは、Dellインフラストラクチャの製品ポートフォリオ向けの、クラウドベースおよびAI/MLベースのプロアクティブなモニタリングおよび予測分析のアプリケーションです。人とマシンのインテリジェンスを組み合わせてインサイトを提供し、プロアクティブで効率的な方法で、ITインフラストラクチャの状態がビジネス ニーズを満たすようにします。

インフラストラクチャの正常性、パフォーマンス、容量に関する問題解決に要する時間を、平均で2分の1～10分の1に短縮することが実証されているCloudIQは[1]、IT環境のセキュリティ体制強化を少ない労力で実現します。

CloudIQのインテリジェントなサイバーセキュリティ インサイト

基本

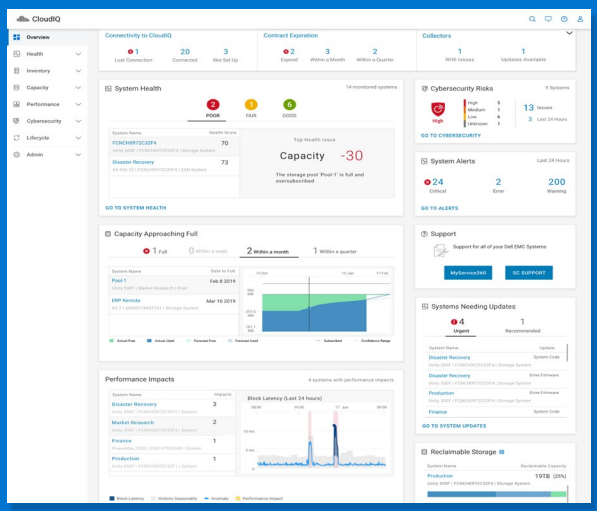
- リスクの低減 – システムのサイバーセキュリティを可視化してプロアクティブに通知することで、リスクを特定し、迅速な解決のためのアクションを推奨
- ポリシーの管理 – 使いやすいインターフェイスでインフラストラクチャのセキュリティ ポリシーをカスタマイズして、評価をスケジュール設定
- 生産性の向上 – インフラストラクチャのサイバーセキュリティ、正常性、パフォーマンス、容量をまとめて手軽に監視できるクラウドベースのアプリケーションを使用

ITインフラストラクチャの保護を数分で開始

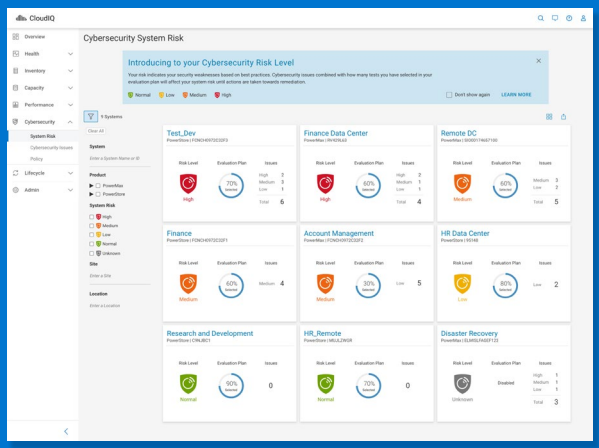
CloudIQは、IT環境への安全なネットワーク接続を備えたセキュアなDell IT Cloudでホストされているため、初めてセットアップするのにかかる時間はわずか数分です。インフラストラクチャ システムのエレメント マネージャー アプリケーション（Unisphere for PowerMaxストレージ システムなど）で1回クリックするだけで、CloudIQが開始され、システムから正常性、パフォーマンス、容量のテレメトリーが収集されて分析されます。サイバーセキュリティの実現は、2つの簡単なフォローアップ手順で行なうよう設計されています。まず、セキュリティ テレメトリーの収集を開始し、次に、シンプルなサイバーセキュリティ評価プラン エディターを使用してセキュリティ ポリシー プランを設定すると、システムがデータの評価とセキュリティ構成ミスの検出を開始します。

いたって簡単で、ロール ベースのアクセスにより安全に管理されます。

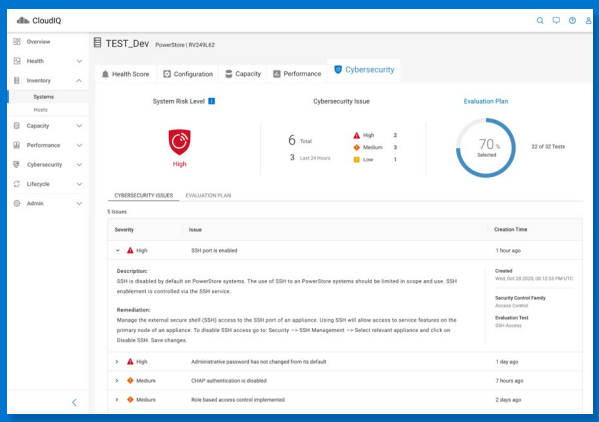
サイバーセキュリティに関するインサイトとアクション



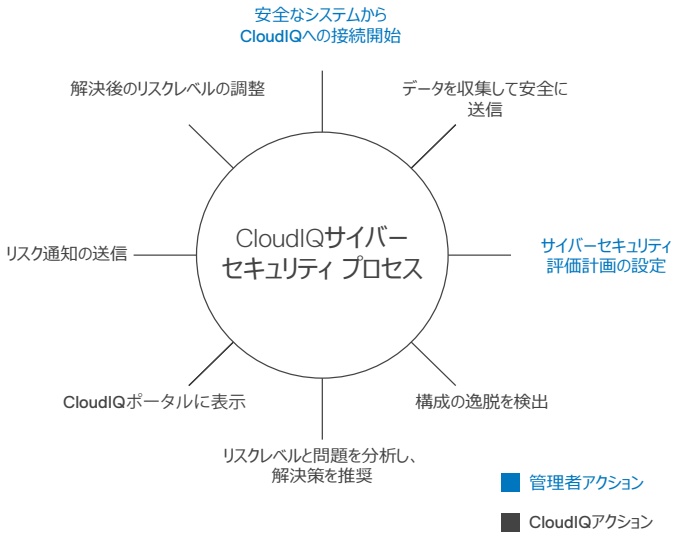
サイバーセキュリティに関するCloudIQの概要



サイバーセキュリティのリスク レベル



サイバーセキュリティ リスクの詳細と推奨事項

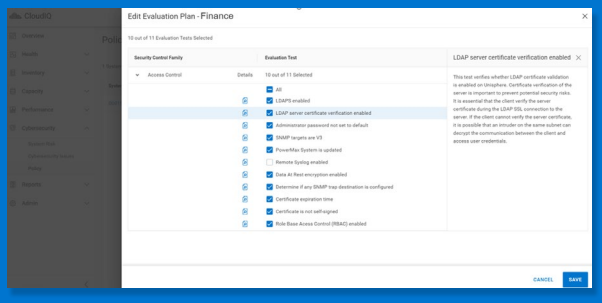


CloudIQは、効率的なクローズドループ プロセスを実現しており、インフラストラクチャ サイバーセキュリティの包括的な評価と修復に24時間365日対応します。

リスクの低減

デル・テクノロジーズの安全なネットワークを使用し、セキュアなDell IT CloudでホストされているCloudIQは、セキュリティ構成情報を、プライマリー データ センター、セカンダリー データ センター、エッジ ロケーションなど、IT環境全体にわたって、システムから収集して、保存し、評価します。

- サイバーセキュリティ評価：システムのセキュリティ構成が、ポリシーから逸脱していないかを判断します。これには、ロール ベースのアクセス制御、デフォルトの管理パスワード、静止データ暗号化の有効化、NFSセキュリティ レベルなどが含まれます。CloudIQがこの逸脱性を継続的に評価するので、構成ごとの手動チェックが必要なくなり、常にリスクを確実に認識できます。
- サイバーセキュリティ リスクの概要：同じダッシュボードで、セキュリティ リスク（高、中、低）があるシステムの数を確認でき、システムの正常性スコア、関連する容量、パフォーマンス分析が一目でわかります。これにより、アクションに優先順位を素早く付けて、問題解決にかかる時間を短縮できます。
- サイバーセキュリティのリスク レベル：1つのダッシュボードを使用して、リスクのあるすべてのシステムを特定でき、それぞれのカードには、サイバーセキュリティ リスク レベルの値が表示されます。このようなシステムは、リスクのレベルに応じてトップダウンで表示され、アクションをさらに優先付けるのに役立ちます。
- サイバーセキュリティの詳細と修復：各システムのリスクの詳細がわかり、逸脱したセキュリティ構成を安全な状態に戻すために、推奨されるアクションを確認できます。各システムのエレメント マネージャーをCloudIQから直接起動して、すぐに対応処置をとることができます。



サイバーセキュリティ評価プラン エディター

管理

シンプルなツールを使用して、インフラストラクチャ セキュリティ構成の評価ポリシーを策定できます。CloudIQはそのポリシーを使用してサイバーセキュリティ リスクを評価します。

- プランニング ツール：テンプレート駆動型のサイバーセキュリティ評価プラン エディターを使用して、セキュリティ構成を選択します。CloudIQは、その構成をシステムの実際の構成と比較します。このエディターでは、各評価テストの有効または無効をクリックで指定し、お好みのセキュリティ ポリシーに設定できます。
- セキュリティ標準：セキュリティ構成のベースとなっているのは、NIST 800-53 r5およびNIST 800-209の標準のほか、数千人のユーザーをサポートしてきたエンジニアの長年の経験から引き出された、特定のインフラストラクチャ製品ごとのデル・テクノロジーズのベスト プラクティスです。

生産性を向上

ユーザー アンケートによると、CloudIQは、IT部門の時間を週平均9時間[2]節約しています。

- オールインワン モニタリング：同じツールを使用して、インフラストラクチャ システムの正常性とサイバーセキュリティ問題の監視やトラブルシューティングを行うので、インフラストラクチャに最も近い人々、つまりシステム管理者の最優先事項にセキュリティを位置づけておくことができます。
- プロアクティブな通知と情報共有：CloudIQは、システムの正常性とサイバーセキュリティに関する通知を、オプトインEメールでプロアクティブに送信します。これにより、問題解決のための詳細と推奨事項を確認できます。自分やチーム、関係者にとって重要な、システム グループと場所に関するレポートのカスタマイズ、スケジュール設定、共有もできます。
- 自動化ワークフローの統合：CloudIQの通知とデータを、WebhookおよびREST APIを介してサード パーティー アプリケーションに送信し、ITプロセスを迅速化できます。たとえば、ServiceNow（チケット発行）やSlack（DevOps通知）、Microsoft Teams（エスカレーション）のほか、Ansible、VMware vRealize（インフラストラクチャでの対応処置の自動化）などがあります。

CloudIQの技術情報、デモンストレーション ビデオ、サード パーティーによるレビュー、導入事例については、次のリンクをご参照ください。

dell.com.cloudiq

[1]2021年5月～6月に実施されたCloudIQユーザーに対するデル・テクノロジーズの調査に基づきます。実際の結果は異なる場合があります。CLM-000884
[2]2021年5～6月に実施されたCloudIQユーザーに対するデル・テクノロジーズの調査に基づきます。実際の結果は異なる場合があります。CLM-003872