IoT Threat Defense for Healthcare

利点

Cisco® IoT Threat Defense for Healthcare は、病院のコネクテッド医療機器とネットワークを管理して保護する方法を変革します。シンプルかつオープンな自動化ソリューションにより脅威を軽減して、医療機関における高セキュリティのデジタル変革を実現します。

- 業務や患者ケアに影響が及ぶ前に、セキュリティ違反を迅速に特定して阻止します。
- 個別のネットワークを管理することなく、医療機器とネットワークのセキュリティを改善します。
- ネットワークを監視してネットワーク ポリシーおよびデバイス ポリシーを適用する機能を強化します。
- サイバーセキュリティの専門家とテクニカル サービスが、リスクの評価と管理を支援します。

IoT 脅威の軽減により医療ネットワークを保護

かつての医療には、時間と場所の制限がありました。今、医療施設、特に命を守るために使用される機器において、コネクテッド化がかつてないほど進んでいます。デジタル変革は、新たな可能性の世界を開き、より多くの患者が高品質の医療を利用できるようにするとともに、コストも削減します。このようなコネクテッド化のあらゆるケースにおいて必要とされるのが、患者とデータを保護する強力な脅威防御です。

ほとんどの医療機器は有線および無線のネットワークで使用される設計になっていますが、多くの場合、その保護は十分ではありません。このような機器が侵害を受けると、カルテや財務情報といった機密データへの進入口になるおそれがあります。Cisco IoT Threat Defense for Healthcare は、医療機器およびそのサポートティング システムの保護を支援します。そして、ネットワークのセキュリティ インフラストラクチャ全体とシームレスに統合し、シンプルかつオープンな自動化セキュリティを提供します。

シスコが選ばれる理由

シスコは、25 年超にわたってネットワークの設計、導入、保護に携わってきました。シスコが構築する機器、考案するテクノロジー、策定する規格は、インターネットの実現に寄与してきました。そして今後も創造を続けます。

シスコの IoT Threat Defense の特徴：

- デバイス、ネットワーク全体、クラウドの脅威を検出してブロックする一連の統合テクノロジーおよびサービスをベースにしたサイバーセキュリティアーキテクチャです。
- ポリシーに基づいてネットワーク全体に適用される、拡張可能でスケーラブルな自動セグメンテーションを使用して医療機器を保護します。
- どんなに離れた場所でも拠点間の通信を保護し、第三者のアクセスを制御します。それにより、ベンダーに高度にセキュアなデバイス アクセスを提供すると同時に、アクセスの対象を彼らのサポートを必要とするデバイスのみに制限することが可能です。
- エキスパートが主導するプロフェッショナル サービスと技術サービスで、セキュアな IoT ソリューションの評価、設計、導入を支援し、サイバーセキュリティ リスク管理能力を向上させます。

関連情報

IoT Threat Defense for Healthcare の詳細については、Cisco Healthcare セキュリティおよびコンプライアンス [英語] を参照してください。

C45-739006-00 06/17