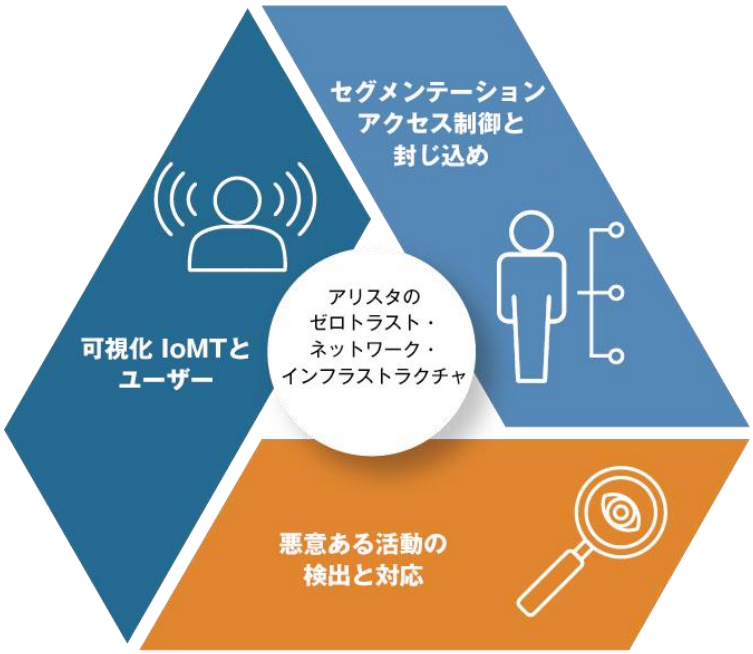
健全な病院インフラストラクチャの基本原則

健全な病院を構築する際には、患者データのセキュリティを基本的考慮事項とすることがこれまで以上に必要となっています。ランサムウェアの大規模感染、患者情報の盗難、医療診断機器の改ざんが最近急増していることが示すように、従来の設計とアーキテクチャはもはや十分ではなくなっています。健全な病院インフラストラクチャは、すべてのアセットとユーザーの可視化、セグメンテーションによるデータの封じ込め、悪意ある活動の継続的な監視を提供する必要があります。医療費が高いことは世界的な関心事であるため、健全なホスピタル・ネットワーク・アーキテクチャでは、セキュリティだけでなく、運用コストと簡素性も考慮することが必要です。

病院がコネクテッド・デジタル・テクノロジーを活用することで、医療分野のモノのインターネット（IoMT）が生まれました。IoMTには、ナース・ステーション、ビルディング・オートメーション・システム、医療機器、セキュリティ・システム、テレビ、電話などが含まれ、すべてがホスピタル・ネットワークに接続されます。ユーザー、アプリケーション、サプライチェーン・パートナー、契約業者が皆、ネットワーク・アクセスを持つことになるため、これを制御する必要があります。ホスピタル・ネットワークはユビキタス、つまり、広範で、耐障害性に優れ、常に利用でき、容量無制限である必要があります。



本ホワイトペーパーでは、健全な病院アーキテクチャの 3 つの基本原則について解説します。

- 接続されている IoMT およびユーザーの可視化
- アクセス制御と封じ込めのためのセグメンテーション
- 悪意ある活動の検出と対応

また、医療機関がこれらの基本原則を実現する上で、アリスタのゼロ・トラスト・ネットワーク戦略がどのように役立つかについても説明します。

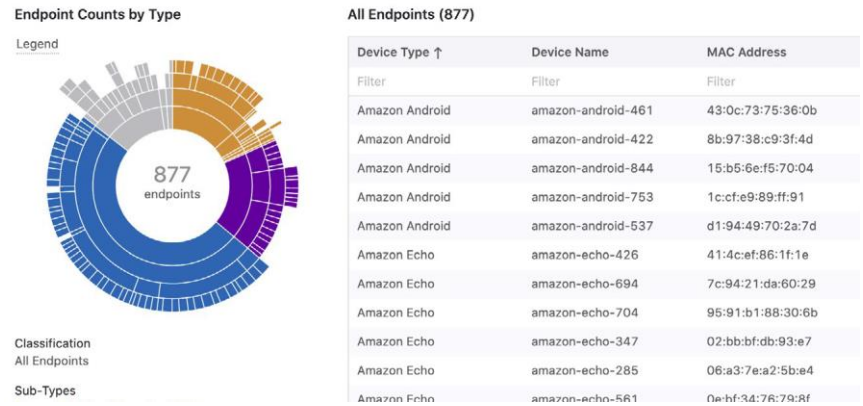
接続されている IoMT およびユーザーの可視化

健全な病院の確保は、IoMT、IoT、ユーザー、ネットワーク・インフラストラクチャなど、接続されているすべてのリソースの可視化から始まります。各リソースの状態データには、ソフトウェア・バージョン、ロケーション、日時、観測された振舞い、デバイス分析などを含めることができます。また、業界標準の PSIRT（製品セキュリティ・インシデント対応チーム）の報告で特定されたソフトウェアの既知の不具合や脆弱性によってネットワーク機器が侵害されていないことを確認するために、スイッチやルーターなどのネットワーク・インフラストラクチャを可視化することも必要です。セキュリティは可視化から始まります。リソースを可視化することが、デバイスやユーザーの通信の許可と不許可を規制する適用ポリシーを推進するからです。後述するように、接続されているすべてのリソースの可視化は、マルウェアや悪意のあるユーザーによる悪意ある活動を特定するための基礎となります。接続されているすべてのリソースを把握するために、アリスタはさまざまな可視化技術を提供し、オープン標準を通じて他のベンダーと戦略的パートナーシップを結ぶことで相互運用性も確保しています。

ネットワーク・インフラストラクチャ可視化のための Arista CloudVision

Arista CloudVision と Arista NDR は、接続されているリソースを把握するための豊富な可視化情報を提供します。

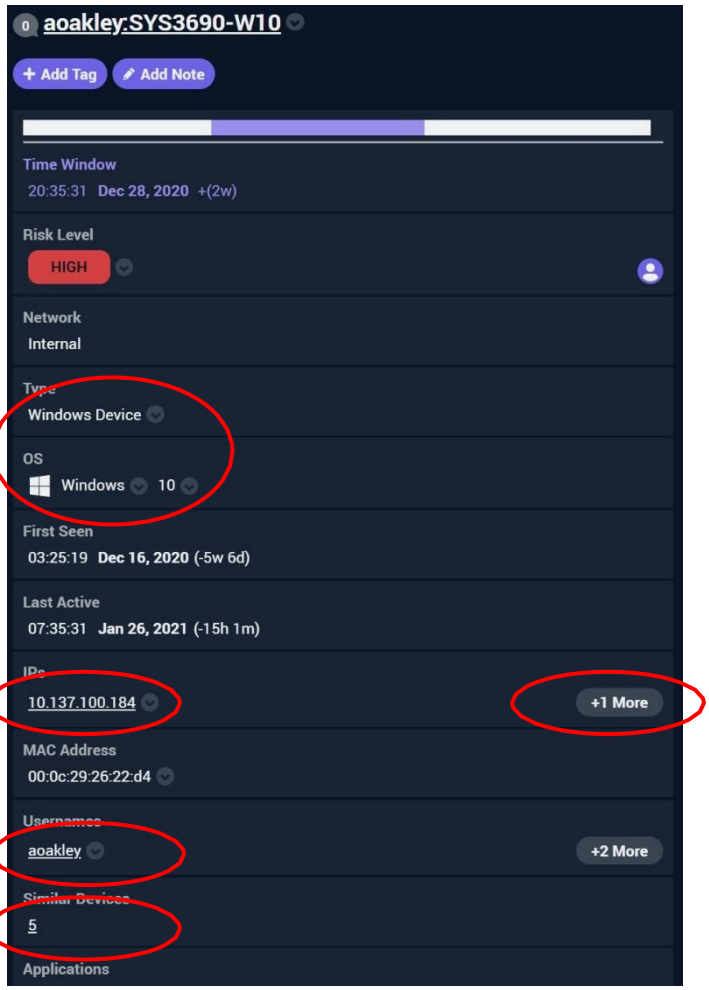
CloudVision のコンプライアンス・ダッシュボードは、PSIRT の対象になりやすくなったり、既知のソフトウェアの不具合の影響を受けやすくなったりしているすべての Arista スイッチについて、一元化されたレポートを提供します。



CloudVision デバイス・アナライザ機能は、接続されているすべてのエンドポイントを識別し、分類します。また、誰と誰が対話しているかを示すフロー・レコードと、トラフィック量を示すパケット・データも提供します。

可視化のための Arista EntityIQ

Arista EntityIQ は AI ベースのセキュリティ・ナレッジ・グラフを使用して、振舞いに基づくデバイス識別を行います。このグラフでは、エンタープライズ・ネットワーク上のデバイス、ユーザー、アプリケーションの識別、プロファイリング、追跡を行うことができます。デバイスは共通の振舞いに基づいてピア・グループに分類され、ネットワークをまたいで移動したときや、IP アドレスが変更されたときにも追跡されます。以下のスクリーンショットに示すように、EntityIQ は、IP アドレスが変更されても、このデバイスを実際に追跡しています。

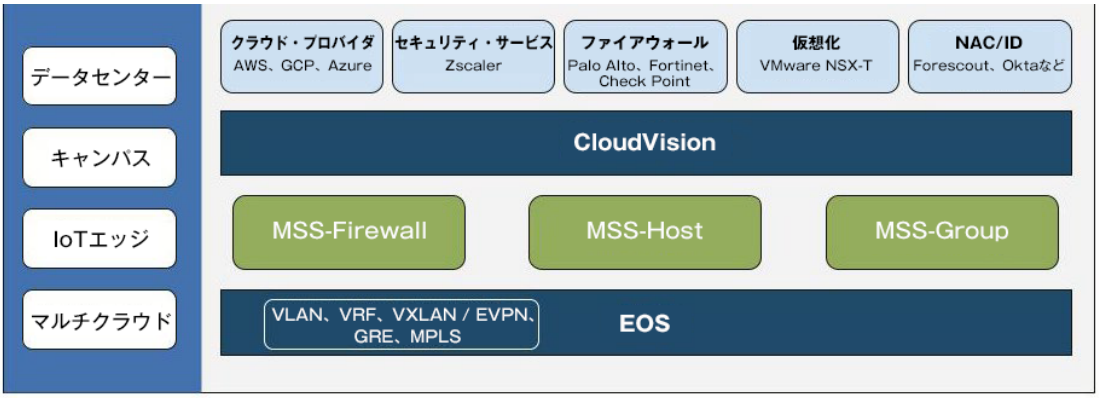


可視化のためのサードパーティ・インテグレーション

CloudVision は、すべての主要 NAC プロバイダと統合されます。たとえば、Forescout と統合すると、IoMT デバイスのきめ細かなテレメトリを含むようにネットワークの可視化が拡張されます。

アクセス制御と封じ込めのためのセグメンテーション

健全な病院の確保に必要な 2 つ目の側面は、デバイスとユーザーが、関連するビジネス成果の実現に必要なリソースにのみアクセスできるように、アクセス制御を実装することです。ネットワークのセグメンテーションは、アクセス制御を規制するためだけでなく、大規模感染の発生時に影響を受けるデバイスを限定して封じ込めるためにも重要です。アリスタは、さまざまなセグメンテーション・コントロールをサポートしています。現在、ACL、VLAN、VRF などの旧来の手法が広く使用されていますが、今の多くの病院には、よりきめ細かく動的なセグメンテーション・アプローチが必要です。



MSS-Group

アリスタは、多くの病院やキャンパスの健全なネットワークに求められる新しいセグメンテーション要件に対応するため、MSS-Group（グループ単位のマクロ・セグメンテーション・サービス）という革新的なアプローチを考案しました。MSS-Group には、以下のような利点があります。

- デバイスの IP アドレスまたはサブネットとは無関係に、セグメント化されたグループを作成できます。
- このソリューションは、他のベンダーのスイッチング機器でも動作し、シンプルに導入および運用できます。
- 管理者は、ACL に関連するスケーラビリティの問題、新しい VLAN 追加のためのネットワークの一部への IP の再割り当て、単一メーカーでのみ動作する独自のタギング・ソリューション、複雑さを増すオーバーレイ・ネットワークを心配する必要がありません。

たとえば、スマート・ベッドは、ナース・ステーションと医師ネットワークとのみ通信できるようにする必要があります。セキュリティ監視カメラは、ビデオ・レコーダー機器とセキュリティ・チームとのみ通信する必要があります。監視カメラ間の通信はマルウェア拡散の原因になることが多いため、監視カメラ間の通信も禁止する必要があります。アリスタの MSS-Group 方式は、このような課題へのソリューションを提供します。

悪意ある活動の検出と対応

近年、病院内のデータ保護対策はますます複雑化しています。デバイスをグループごとに細かくセグメント化することは、アクセス制御ポリシーの実装と、大規模感染発生時の封じ込めのために重要ですが、悪意ある活動を検出するには、それ以外の対策も必要です。悪意ある活動の動機には、内部ユーザーによる金銭的利益の追求、患者の個人記録の収集、国家主導の混乱など、さまざまなものが考えられます。ネットワークを悪用するメカニズムは高度に巧妙化しており、従来のマルウェア検出メカニズムでは検出できなくなっています。

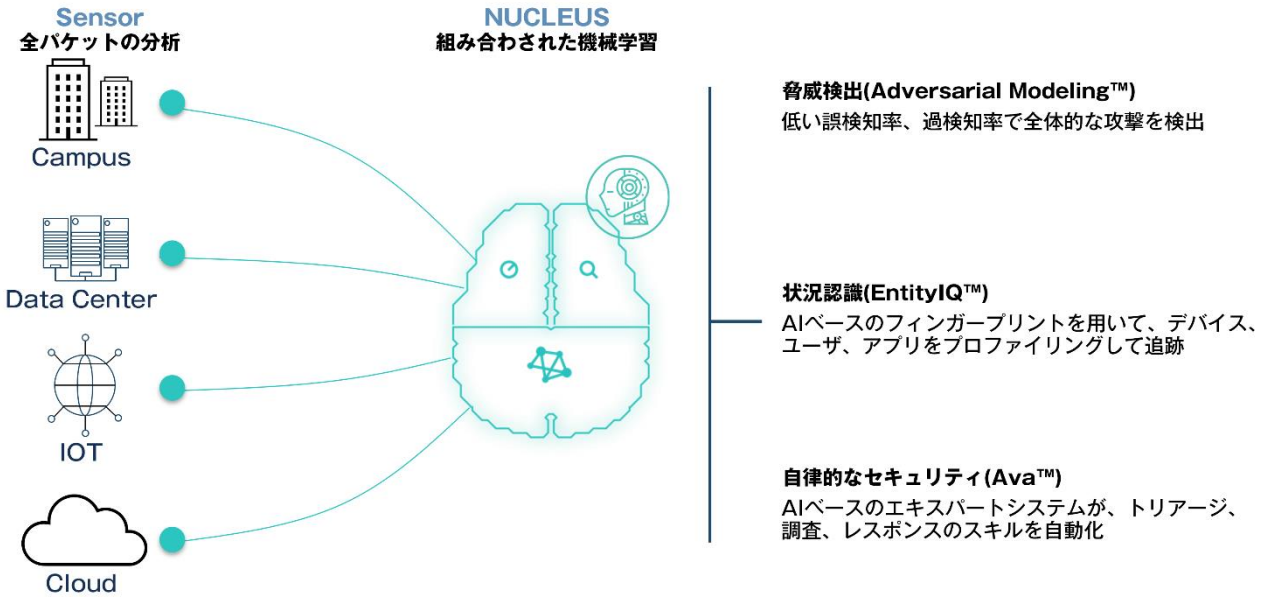
アリスタの経験では、多くの組織において 50%以上、場合によっては 70%のデバイスが管理対象外であり、エンドポイント・エージェントがなく、ログのエクスポート/アグリゲーションも行われていません。特定の OS とソフトウェアのバージョンの有無の認定検査を行う多くの IoMT 機器に、セキュリティ・エージェントをインストールできないのは明らかです。そのようなデバイスはロックダウンされており、たとえ技術的に可能でも、エージェントを追加することは許可されていません。もう 1 つの傾向として、攻撃が進化し、侵害の 50%以上がマルウェアの痕跡を示していませんが、既存のセキュリティ・ツールのほとんどは、マルウェアの特定に重点を置いています。攻撃者は、正当なユーザー、契約業者、アプリケーションの認証情報を奪い、“内部関係者”として活動します。その活動は、“通常”の医療機関において一般的な“正当な業務”の活動に紛れ込んでいます。最後に、暗号化の利用の増加が、従来のネットワーク・セキュリティ・ツールの有効性に影響を及ぼしています。Gartner は、現在、悪意ある活動の 70%以上が TLS/SSL のような暗号化プロトコルの背後に隠れていると推定しています。

Arista NDR は、これらの課題への対処を支援します。このプラットフォームは、今日の最先端のホスピタル・ネットワーク上にある何千もの IT デバイスと IoMT デバイスを監視し、分析します。アリスタは、人工知能ドリブン型のアプローチを採用し、信頼されている内部関係者と外部の攻撃者のどちらが原因であるかにかかわらず、悪意ある活動を検出します。このアプローチは、ランサムウェアからサプライチェーンの脅威までの各種攻撃と、特に医療機器を標的とする攻撃を軽減することができます。

アリスタのソリューションは、AVA（Autonomous Virtual Assist）と呼ばれる技術を通じて、最先端の AI インテリジェンス技術を活用しています。AVA は、時間をまたぐ点と点を結び、関係するデバイスと観測された活動を特定することで、既存のセキュリティ・チームを強化します。AVA は、個別の症状より根本的な状態の特定に重点を置いているため、人間のアナリストが、意味のないことの多い個別のセキュリティ・アラートに基づくトリアージと診断のために面倒な手作業を行う手間を省くことができます。代わりに、AVA が提供する意思決定サポート・システムは、攻撃の全容を自動的に検出し、調査と修復のオプションを 1 つの画面で表示します。

Arista NDR は、セキュリティ・エージェントがプリインストールされたシステムだけでなく、ホスピタル・ネットワーク上のすべてのシステムのセキュリティを監視することで、医療スタッフに必要なデバイスが必要なときに利用でき、正しく動作するようにします。また、脅威を検出し、影響を受ける可能性のあるデバイスとリアルタイムで関連付けることで、セキュリティ・チームはリスクと最悪の影響を軽減できます。

Arista NDR 新しいAIドリブン型セキュリティ

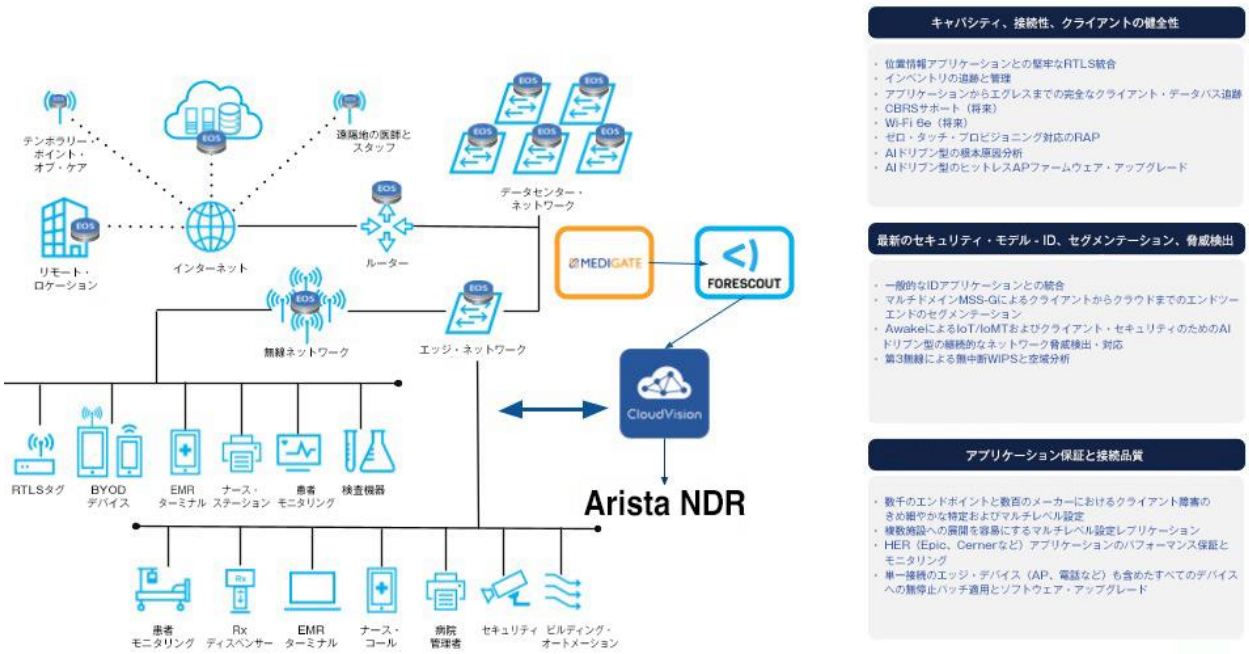


ゼロトラスト・セキュア・ネットワーキングのためのアリスタのインフラストラクチャ

2008 年、アリスタは、ネットワークの構築方法に新機軸のアプローチを採用してデータセンターのネットワーク・アーキテクチャに革命を起こす事業を開始しました。Microsoft、Facebook、Google などの大手クラウド企業が大規模なクラウドベース・ネットワークを構築しており、従来型のベンダーでは実現できない新しいレベルのスケール、品質、管理性が求められていました。アリスタは、このような要件を満たすために設立されました。アリスタの最優先事項は今でも、品質、可用性、管理性、パフォーマンスです。俊敏性の高いネットワークに質の高い自己回復型のアーキテクチャを提供することは、健全な病院の基本要件です。単純な冗長性を提供するだけの従来のアーキテクチャは、大手クラウド企業にとっても、健全な病院にとっても十分ではなくなりました。

ネットワークの可用性はソフトウェアから始まります。Arista EOS（Extensible Operating System）ソフトウェアは、すべての Arista スイッチで使用される単一のバイナリです。他のベンダーの場合、製品ファミリーごとにソフトウェア・イメージが異なります。製品ファミリーごとに管理システムと機能セットが異なり、冗長性と接続性のアーキテクチャも異なる場合があります。アリスタの場合は、すべてのスイッチが同じバイナリを使用し、同じ管理システムで管理され、同じ基本機能セットを備えています。

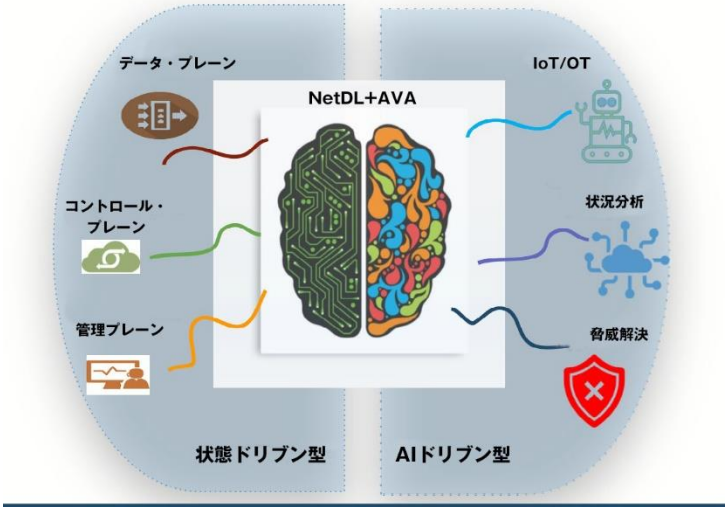
アリスタは、EOS を活用して、病院からリモート・クリニックまでを網羅する単一のユニバーサル・ヘルスケア・ネットワークを構築します。ファブリックには、患者（ゲスト）、医師、管理者、契約業者、あらゆる種類のデバイスが含まれます。このユニバーサル・ヘルスケア・ネットワークは、単一の共通ファブリックを提供することにより、インフラストラクチャ全体の効率と可用性を高め、アクセス・ポリシーと機密性を確保するセキュリティ・コントロールを実現します。オープン標準に基づいているため、管理者は病院のニーズに合った最適な製品を自由に選ぶことができます。アリスタはすべてのスイッチに同じイメージを使用しているため、ホスピタル・ネットワークの管理者は単一のコード・イメージを認定するのみでよくなり、ネットワーク内のすべての場所で同じ設計原則を使用できます。これにより、運用コストが削減されます。



ユニバーサル・ヘルスケア・ネットワークは、共通の管理ソリューションである Arista CloudVision によって管理されます。CloudVision ソリューションは、共通の管理と無停止パッチ適用を提供します。無停止アップグレードは、常時稼働ネットワークの基本要件です。CloudVision により、サービスを中断することなく、非冗長エッジ・スイッチから冗長スパイン・スイッチまで一貫した方法で新機能やパッチを適用できます。前述のように、CloudVision は、運用とトラブルシューティングに必要となる豊富な監視情報を提供し、接続されたエンドポイント、トラフィック・パターン、ネットワーク・テレメトリの把握を支援します。健全な病院にまず必要となるのは、常に利用可能で、耐障害性に優れ、最高品質を備えたネットワーク・インフラストラクチャです。アリスタの高品質のアーキテクチャ的アプローチはこのような要件を満たしており、世界最大規模のネットワークで実証されています。

まとめ

健全な病院の基盤は、円滑な運営を確保して質の高い医療を提供できるようにすることです。健全な病院は、患者と病院のデータのセキュリティを提供し、IoMT デバイスを不正アクセスから保護する必要があります。データをやり取りするコネクテッド IoMT デバイスが増加し、病院はこれまで以上に、患者の医療とプライバシーを脅かす悪意ある活動の影響を受けやすくなっています。このような業界の問題に対処するには、ホスピタル・ネットワークの構築方法に対する新しいアプローチが必要です。新しいアプローチでは、信頼性の高い安全なインフラストラクチャ、すべての接続デバイスの可視化、アクセスを制御するセグメンテーション、あらゆる種類の悪意ある活動の継続的な監視を提供する必要があります。健全なホスピタル・ネットワークに対するアリスタの状態ドリブン型と AI ドリブン型のアプローチにより、組織は信頼性と耐障害性に優れたサービスを提供でき、その結果、患者と医療従事者の成果を向上させることができます。



アリスタネットワークスジャパン合同会社

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル　27F
Tel:03-3242-6401

西日本営業本部
〒530-0001　大阪市北区梅田 2-2　ヒルトンプラザウエストオフィスタワー　19F
Tel: 06-6133-5681

お問い合わせ先

Japan-sales@arista.com

www.arista.com/jp

ARISTA

2021 年 1 月 3 日