At-A-Glance

Cisco Identity Services Engine

企業ネットワークはもはや四方を壁に囲まれた閉じた存在ではありません。従業員の活動範囲やデータの利用範囲が広がるにつれて、企業ネットワークの範囲も拡大しています。今日の従業員は、企業のネットワークに縛られず、多様なデバイスとネットワークから業務リソースにアクセスしたいと考えるようになっています。モビリティや Internet of Everything（IoE）で、人々の生活や働き方は変化しています。企業は急増する新しいネットワーク対応デバイスをサポートする必要性に迫られており、無数のセキュリティ脅威やデータ侵害に関する多数の報道からも明らかなように、この拡大する企業ネットワークへのアクセスを保護することは非常に重要です。

ネットワークの拡大に伴い、リソースの整理、分散型セキュリティソリューションの管理、およびリスク制御の複雑性も増加しています。IoE のユビキタス接続と、ただでさえ不足している IT リソースのことを考慮すると、セキュリティ脅威を適切に検出、修復できなかった場合に被るであろう被害は甚大なものになると予想されます。

企業のモバイル環境の管理とセキュリティの両方において、異なるアプローチが必要になっているのです。これが Cisco® Identity Services Engine（ISE）です。

利点

- **一元化された安全性の高いアクセス制御**：ビジネス ロールに基づき、有線/無線ネットワークまたは VPN のいずれで接続しているかに関わらず、エンド ユーザに対して一貫したネットワーク アクセス ポリシーを提供できます。
- Cisco® Identity Services Engine（ISE）デバイス プロファイリングおよびデバイス プロファイル フィード サービスにより、**優れた可視性と正確なデバイス認識**が得られ、未知のエンドポイント数を削減できます。
- **ゲスト エクスペリエンスの簡素化**：ブランドごとのカスタマイズ可能なモバイルおよびデスクトップのゲスト ポータルを通じて、ゲストのオンボーディングや管理を容易に行うことができます。これらのポータルは、ゲスト エクスペリエンスを容易に管理できる動的なビジュアル ワークフローを使用して、数分で作成できます。

攻撃対象範囲を絞ってリスクを軽減する

重要なのは、可視性と制御によって予防的な対策を講じることです。たとえば、ネットワークにアクセスするユーザやデバイスに関する高度な可視性を実現し、適切なデバイスを使用する適切なユーザだけが企業サービスにアクセスできるよう、動的に制御します。

再設計された ISE 2.0 により、有線およびワイヤレス マルチベンダー ネットワークとリモート VPN 接続の全体に対して、一貫性のあるセキュアなアクセス制御を簡単に実現できます。広範囲のインテリジェント センサーとプロファイリング機能を備えた Cisco ISE により、ネットワークを詳細に把握でき、リソースにアクセスした人やモノに対する高度な可視性を得られます。Cisco ISE は、重要なコンテキスト データを統合されたエコシステム パートナーと共有し、ソフトウェア定義型セグメンテーションに Cisco TrustSec ポリシーを適用します。それにより、単純なデータの通り道だったネットワークが、ネットワーク上の脅威の検出時間と応答時間を短縮するセキュリティ エンフォーサーへと変わります。

- **企業での BYOD とモビリティの推進**：すぐに使えるセットアップ、セルフサービスでのデバイスのオンボーディングと管理、社内でのデバイス使用許可の管理、さらにオンプレミスとオフプレミスでのデバイス オンボーディングを取り扱う統合エンタープライズ モビリティ管理（EMM）パートナー ソフトウェアによって、モビリティを促進します。
- **ネットワークの脅威を封じ込めるソフトウェア定義型セグメンテーション ポリシーの構築**：Cisco TrustSec® テクノロジーを使用して、ルータやスイッチ レイヤでロールベースのアクセス制御が可能です。複数の VLAN を管理したりネットワークを再設計したりせずに、アクセスを動的にセグメント化できます。
- **豊富なコンテキスト データをパートナー ネットワークやセキュリティ ソリューションと共有**：コンテキスト データを共有することで、全体の効率性を改善し、ネットワーク脅威の検出時間（TTD）と解決時間（TTR）を短縮します。
- **脅威を自動的に封じ込め**：Cisco Firepower Management Center との統合により、ISE は感染したエンドポイントを封じ込めて、修復、監視、または削除できます。

ISE 2.0 では次のような更新と機能強化が行われています。

- Cisco モビリティ サービス エンジン（MSE）との統合により、場所固有のアクセス権を確立して適用するための場所データが得られます。たとえば、医療関係者に対して緊急治療室の医療記録に限定したアクセス権を付与することなどが可能です。
- 特定の ISE エコシステム パートナー向けのオープン アーキテクチャが強化されたため、お客様は既存のセキュリティ ソリューションと ISE を連動させて、ネットワーク内の脅威を特定し、封じ込めと修復を迅速に行うことができます。
- サードパーティのネットワーク アクセス デバイス（NAD）と IPv6 エンドポイントのサポートにより、ISE の到達範囲が拡張され、多様なネットワークでエンドポイントのコンプライアンスが確保されます。
- TACACS+ および RADIUS アクセス機能によるデバイス管理での認証、許可、およびアカウンティング（AAA）の簡素化などの効率的なポリシー管理により、有線ネットワークでのセキュアなアクセス制御ポリシー導入が簡単になります。
- Cisco AnyConnect 4.2 には、新しいネットワーク可視性モジュール（NVM）が含まれています。アプリケーションのトラフィック フローについて、従来のオフプレミスのエンドポイントでは取得できなかった詳細な情報が得られます。

さらに、ISE では Cisco Platform Exchange Grid（pxGrid）[英語] テクノロジーにより、統合されたパートナー エコシステム ソリューションと豊富なコンテキスト データを共有できます。この技術により、拡張ネットワーク全体にわたってセキュリティ脅威を特定、軽減、修復できます。総合的に見て、安全なアクセス制御とは一元化されたシンプルなもので、基幹サービスの安全な提供、インフラ セキュリティの強化、コンプライアンスの保持、サービス運営の合理化を実現します。

優れたセキュリティ情報、イベント管理（SIEM）、脅威防御（TD）ソリューションとの統合、ネットワークの深い可視性、セキュアなアクセス制御機能により、ISE は Cisco Cyber Threat Defense、センサーとしてのネットワーク、およびエンフォーサーとしてのネットワーク ソリューションにおいて不可欠な役割を果たします。最後に、ISE は、企業が攻撃の一連のサイクルにおけるセキュリティを効果的に実装するために必要な可視性、コンテキスト、および動的制御を提供します。具体的には、攻撃前のネットワーク アクセスの管理、攻撃中の脅威の封じ込め、および攻撃後の検出時間（TTD）と応答時間（TTR）の短縮を実現します。

次のステップ

Cisco ISE の詳細については、http://www.cisco.com/jp/go/ise を参照するか、最寄りのシスコ代理店にお問い合わせください。

C45-654884-13 03/16