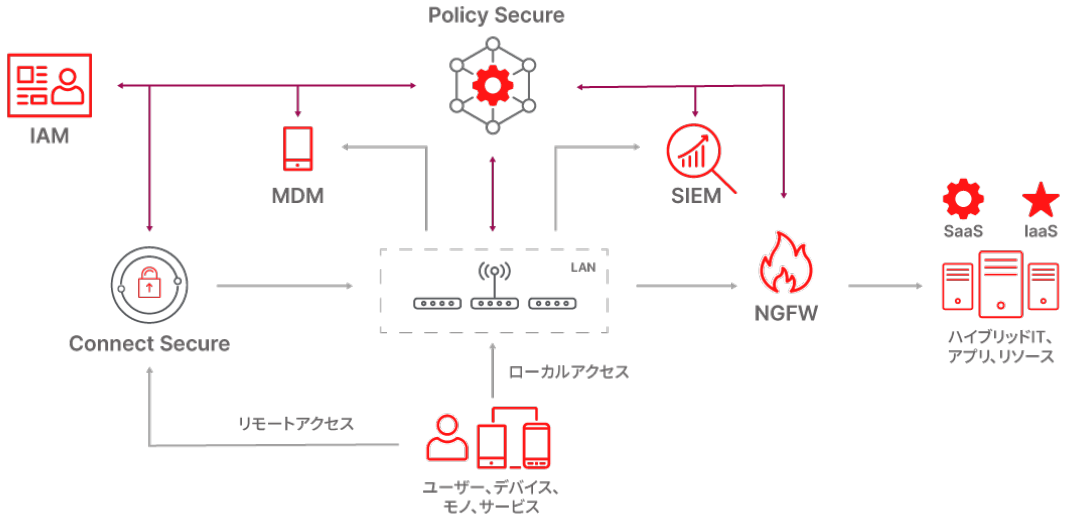
Policy Secureによる統合された脅威防御

概要

データとリソースを保護するために、企業のセキュリティ担当 は、次世代ファイアウォール NGFW などのソリューションを使用してアクセスを制御し、トラフィックフローをモニタリングします。また、セキュリティ情報イベント管理 SIEM を使用してイベントを分析し、相互に 連付けます。問題は、これらのソリューションはアラートの 信、またはファイアウォールを 過するトラフィックにポリシーを適用することしかできないという点です。Network Access Control NAC ソリューションは、従来、ネットワーク接続前のエンドポイントのセキュリティポスチャに適用されてきました。セキュリティエコシステムとの双方向の統合により、NACは他のセキュリティソリューションからアラートを受信するとエンドポイントの接続に対して修復措置を じ、全体的なセキュリティ効果を めることができます。NACによる 動セキュリティ適用には、次のようなメリットがあります。



- 脅威への対応時間の短縮
- セキュリティ運用の合理化
- 脅威の横方向への拡散を抑制
- セキュリティコンプライアンスの自動化と監査の簡素化
- コンテキスト情報を使用したより詳細なポリシー

Policy Secureは、スイッチ、ワイヤレスコントローラ、次世代ファイアウォール（NGFW）などのネットワークおよびセキュリティインフラストラクチャデバイスをはじめ、IDおよびアクセス管理（IAM）、SIEM、Advanced Threat Protection（ATP）、Enterprise Mobility Management（EMM）などのソリューションとも統合できます。

Policy Secureは、ID、セキュリティポスチャ、場所などのコンテキストデータに基づき、実行可能なアクセス決定を自動化できます。Policy Secureは、ゼロトラストアクセスのフレームワークに基づいて、接続ライフサイクルの間エンドポイントの信頼レベルを継続的に実行し、異常な動作が検出された場合には隔離を行います。

継続的な信頼評価のための統合

ネットワークアクセス

ゼロトラストの原則は、常に検証を行うということです。Policy Secureは、まずポリシーに対してユーザーとデバイスを検証します。次に、そのユーザーの役割に従ってデバイスをアクセスするインフラストラクチャに接続します。この動的なネットワーク・セグメンテーションは、さまざまなクラスのIoTデバイスとユーザー間における脅威の横方向への拡散を抑制します。PPSは、Cisco、Juniper、Mist、Aruba、Huawei、Ruckusなどのベンダーの主要なスイッチングおよびWi-Fiソリューションと、共通の802.1X標準、または SNMPを使用して統合されます。

動的なネットワーク境界のプロビジョニングにより、アクセス制御にもう1つのレイヤを加えられます。NGFWポリシーでは、ユーザーのIDや場所などの追加のコンテキスト情報を活用できます。PPSは、Palo Alto Networks、Checkpoint、Juniper、FortinetなどのNGFWソリューションと統合して、エンドポイントに関するコンテキスト情報を提供します。

エンドポイントのコンプライアンス

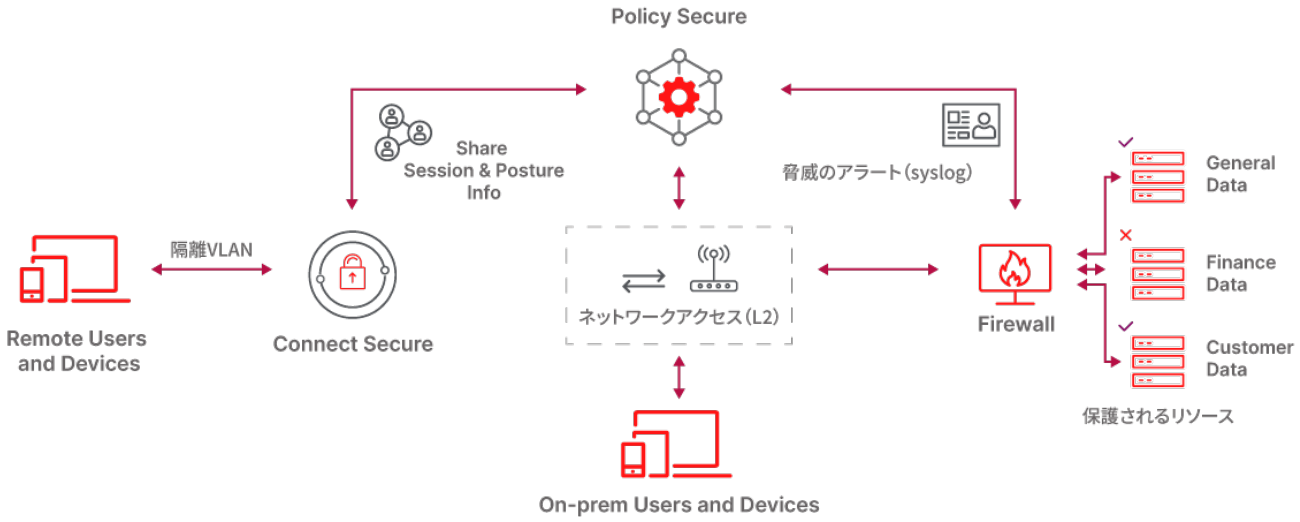
エンドポイントでは、オペレーティングシステム、アンチウイルスなどのセキュリティユーティリティ、ユーザーレベルのアプリケーションなど、さまざまなソフトウェアが使用されます。こうしたソフトウェアはすべて、機能拡張およびセキュリティ修正の定期的な更新を受信します。

ホストチェッカー機能は、ソフトウェアアップデート履歴とアクティブなアプリを検証することで、デバイスのセキュリティポスチャを継続的に評価します。Policy Secureは、ユーザーやデバイスへのネットワークアクセスを許可すると、すべての接続ライフサイクルの間、セキュリティポスチャを継続的にモニタリングします。たとえば、ポリシーに違反するシャドーITアプリをユーザーが起動したなどの理由でセキュリティポスチャが変更された場合、Policy Secureはエンドポイントをただちに制限付きネットワーク環境に移動します。

Policy Secureは、エンドポイントのコンプライアンスを自動的に実行することで、組織のリスクを最小限に抑えることができます。ホストチェッカーは、Windows Management Instrumentation、Windows Defender、Microsoft Security Essentials、またはIvantiのConnect Secure VPNクライアントと相互に作用してさらにきめ細かいチェックを行うことができます。

IDおよびアクセス管理（IAM）

認証メカニズムは、ユーザーのIDを検証し、役割を定義します。システムは、時間、地理的位置、または動作に基づいてコンテキスト情報を活用できます。たとえば、認証されたセッションがすでに別の地理的位置に存在する場合、ユーザーに二要素認証（2FA）など追加の認証方式を要求できます。Policy Secureは、SAML（Ping、Okta、Duoなど）、ActiveDirectory（Microsoft）、RADIUS/TACACS+、LDAPforなどのプロトコルを使用してIAMソリューションと統合し、より分離された環境を実現します。Policy SecureにはRADIUSサービスが組み込まれています。



セキュリティイベント

強固な階層型セキュリティ戦略では、次世代ファイアウォール(NGFW)、セキュリティ情報およびイベント管理(SIEM)、Advanced Threat Detection(ATD)などのソリューションを使用して、ネットワークフローとイベントを継続的に分析する必要があります。

Policy Secureとの双方向の統合により、ネットワークアクセスレベルで実行可能な自動応答が適用され、全体的なセキュリティ効果が向上します。セキュリティ侵害インジケーター(IOC)への自動応答により、修復時間を短縮し、管理リソースを合理化します。

PPSは、Palo Alto Networks、Checkpoint、Juniper、Fortinetなどの主要なNGFWや、IBM QRadar、SplunkなどのSIEMソリューションと統合できます。

ユースケース:NGFWアラート

NGFWが脅威を検出すると、標準のsyslogを使用してPolicy Secureにアラートを送信します。Policy Secureは、疑わしいデバイスを制限付きアクセス環境に隔離して問題を修正し、脅威の横方向への拡散を防止します。

ivanti.com
1 800 982 2130
sales@ivanti.com