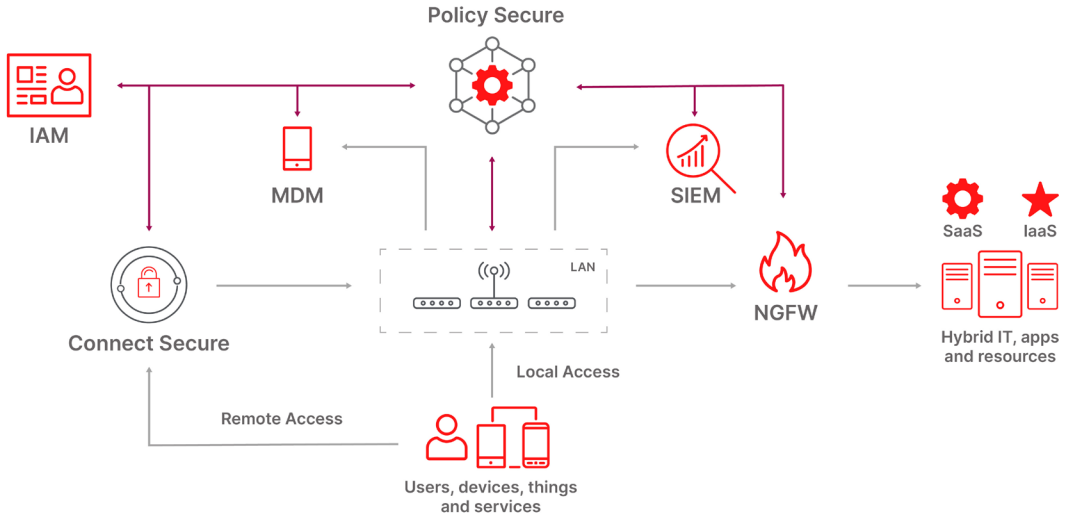
Integrierte Bedrohungsabwehr mit Policy Secure

Übersicht

Um Daten und Ressourcen zu schützen, verwendet das Sicherheitspersonal in Unternehmen Lösungen wie Next-Generation Firewalls (NGFWs), um den Zugriff zu kontrollieren und den Datenverkehr zu überwachen, sowie Security Information and Event Manager (SIEMs), um Ereignisse zu analysieren und zu korrelieren. Das Problem: Diese Lösungen beschränken sich auf das Versenden von Warnungen oder das Durchsetzen von Richtlinien für den Datenverkehr, der sie durchläuft. Network Access Control (NAC)-Lösungen haben traditionell die Sicherheitslage eines Endpunkts durchgesetzt, bevor er sich mit dem Netzwerk verbindet. Durch die bidirektionale Integration in das Sicherheits-Ökosystem kann ein NAC die Gesamtwirksamkeit der Sicherheit erhöhen, indem es nach dem Empfang von Warnungen von anderen Sicherheitslösungen Abhilfemaßnahmen für die Verbindung eines Endpunkts ergreift. Die automatisierte Sicherheitsdurchsetzung mit einem NAC bietet unter anderem folgende Vorteile:

- Verkürzte Reaktionszeit auf Bedrohungen.
- Rationalisierte Sicherheitsabläufe.
- Begrenzte laterale Ausbreitung von Bedrohungen.
- Automatisierte Sicherheits-Compliance und einfachere Audits.
- Granularere Richtlinien mit kontextbezogenen Informationen.



Policy Secure lässt sich in Netzwerk- und Sicherheitsinfrastrukturgeräte wie Switches, Wireless-Controller und Firewalls der nächsten Generation (NGFW) integrieren, aber auch in Lösungen wie Identitäts- und Zugriffsmanagement (IAM), SIEM, Advanced Threat Protection (ATP) und Enterprise Mobility Management (EMM). Policy Secure ermöglicht automatisierte, umsetzbare Zugriffsentscheidungen, die auf kontextbezogenen Daten wie Identität, Sicherheitsstatus und Standort basieren. Basierend auf einem Zero-Trust-Zugriffs-Framework erzwingt Policy Secure kontinuierlich die Vertrauensstufe eines Endpunkts während des Lebenszyklus seiner Verbindung und stellt ihn unter Quarantäne, wenn eine Verhaltensanomalie erkannt wird.

Integrationen zur kontinuierlichen Vertrauensbewertung

Netzwerkzugriff

Das Prinzip von Zero Trust: immer verifizieren. Policy Secure validiert zunächst den Benutzer und das Gerät anhand der Richtlinie. Dann verbindet Policy Secure das Gerät mit der Zugriffsinfrastruktur, die der Rolle des Benutzers entspricht. Diese dynamische Netzwerksegmentierung begrenzt die laterale Ausbreitung von Bedrohungen zwischen verschiedenen Klassen von IoT-Geräten und Benutzern. PPS lässt sich mit führenden Switching- und Wi-Fi-Lösungen von Anbietern wie Cisco, Juniper, Mist, Aruba, Huawei und Ruckus über den gemeinsamen Standard 802.1X oder SNMP integrieren.

Die dynamische Bereitstellung des Netzwerkperimeters bietet eine weitere Ebene der Zugriffskontrolle. NGFW-Richtlinien können zusätzliche kontextbezogene Informationen wie die Identität oder den Standort des Benutzers nutzen. PPS lässt sich in NGFW-Lösungen wie Palo Alto Networks, Checkpoint, Juniper und Fortinet integrieren, um diese kontextbezogenen Informationen über den Endpunkt bereitzustellen.

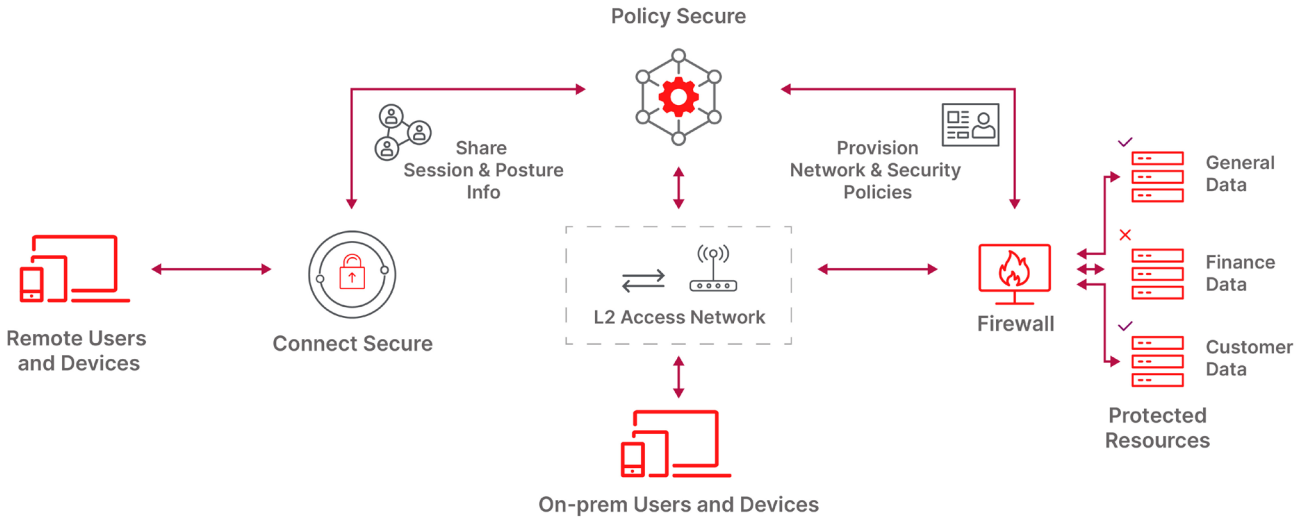
Endpunkt-Compliance

Endgeräte verwenden eine Vielzahl von Software, darunter das Betriebssystem, Sicherheitsprogramme wie Anti-Virus-Software und Anwendungen auf Benutzerebene. All diese Software erhält regelmäßige Updates für Funktionsverbesserungen und Sicherheitsbehebungen. Die Funktion „Host-Checker“ prüft kontinuierlich die Sicherheitslage des Geräts durch Validierung der Software-Update-Historie und der aktiven Apps. Sobald Policy Secure einem Benutzer und/oder Gerät den Netzwerkzugriff gewährt, überwacht es kontinuierlich die Sicherheitslage während des gesamten Verbindungslebenszyklus. Wenn sich die Sicherheitslage ändert, zum Beispiel weil der Benutzer eine zweifelhafte IT-App startet, die gegen die Richtlinie verstößt, verschiebt Policy Secure den Endpunkt sofort in eine eingeschränkte Netzwerkumgebung.

Policy Secure hilft Unternehmen, Risiken zu minimieren, indem es automatisch die Compliance von Endpunkten durchsetzt. Der Host-Checker kann mit Windows Management Instrumentation, Windows Defender, Microsoft Security Essentials oder dem Connect Secure VPN-Client von Ivanti interagieren, um noch mehr Granularität zu erreichen.

Identitäts- und Zugriffsmanagement (IAM, Identity and Access Management)

Der Authentifizierungsmechanismus validiert die Identität eines Benutzers und definiert Rollen. Das System kann kontextbezogene Informationen basierend auf Zeit, Geolocation oder Verhalten nutzen. Wenn beispielsweise bereits authentifizierte Sitzungen in einer anderen Geolocation existieren, kann der Benutzer zusätzlichen Authentifizierungsmethoden wie der Zwei-Faktor-Authentifizierung (2FA) unterzogen werden. Policy Secure lässt sich mit IAM-Lösungen integrieren, die Protokolle wie SAML (Ping, Okta, Duo usw.), Active Directory (Microsoft) oder sogar RADIUS/TACACS+ oder LDAP für isoliertere Umgebungen verwenden. Policy Secure verfügt über einen integrierten RADIUS-Dienst.



Sicherheitsereignisse

Eine solide, mehrschichtige Sicherheitsstrategie erfordert die kontinuierliche Analyse von Netzwerkflüssen und - ereignissen mithilfe von Lösungen wie Next-Generation Firewalls (NGFWs), Security Information and Event Management (SIEM) oder Advanced Threat Detection (ATD). Die bidirektionale Integration mit Policy Secure verbessert die allgemeine Sicherheitseffizienz durch umsetzbare, automatisierte Reaktionen, die auf der Netzwerkzugangsebene durchgesetzt werden. Automatische Reaktionen auf „Indicators of Compromise“ (IoC) verkürzen die Zeit für die Behebung und rationalisieren die administrativen Ressourcen. PPS lässt sich mit führenden NGFWs wie Palo Alto Networks, Checkpoint, Juniper und Fortinet Lösungen wie IBM QRadar und Splunk integrieren.

Anwendungsfall: NGFW-Alarm

Wenn eine NGFW eine Bedrohung entdeckt, alarmiert sie Policy Secure über das Standard-Syslog. Policy Secure kann das verdächtige Gerät in einer Umgebung mit eingeschränktem Zugriff unter Quarantäne stellen, um das Problem zu beheben und eine laterale Ausbreitung der Bedrohung zu verhindern.

ivanti

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