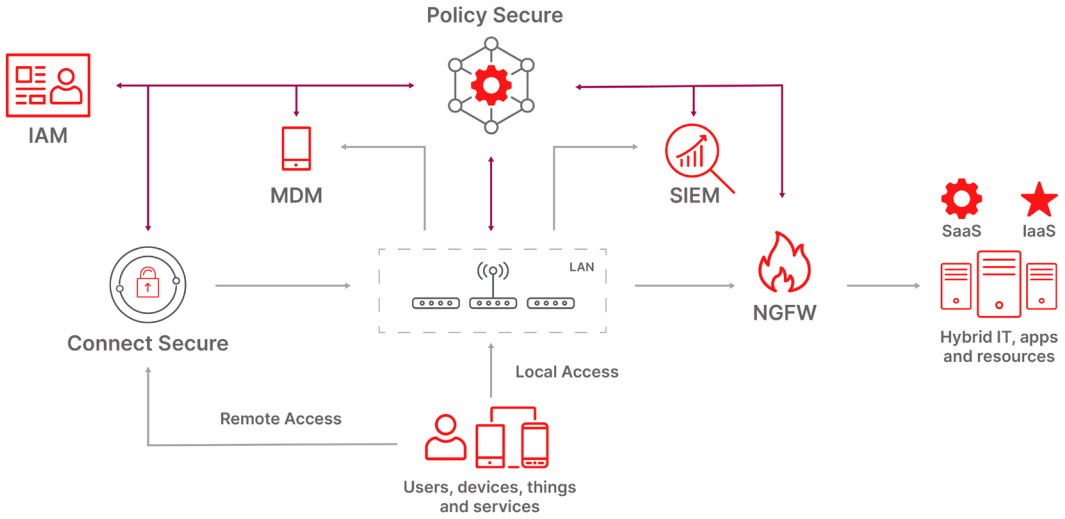
Defensa integrada contra amenazas con Policy Secure

Visión general

Para proteger los datos y los recursos, el personal de seguridad de la empresa utiliza soluciones como los cortafuegos de nueva generación (NGFW) para controlar el acceso y flujos de tráfico, y gestores de información y eventos de seguridad (SIEM) para analizar y correlacionar los eventos. El problema: estas soluciones se limitan a enviar alertas, o a aplicar políticas sobre el tráfico que pasa a través de ellas. Las soluciones de control de acceso a la red (NAC), tradicionalmente han reforzado la postura de seguridad de un punto final antes de conectarse a la red. La integración bidireccional con el ecosistema de seguridad permite a un NAC aumentar la eficacia general de la seguridad al tomar medidas correctivas en la conectividad de un punto final después de recibir alertas de otras soluciones de seguridad. La aplicación automatizada de la seguridad con un NAC proporciona ventajas como:

- Reducción del tiempo de respuesta a las amenazas.
- Agilización de las operaciones de seguridad.
- Limitación de la propagación lateral de las amenazas.
- Cumplimiento de la seguridad automatizado y auditorías más sencillas.
- Políticas más detalladas con información contextual.



Policy Secure se integra con dispositivos de infraestructura de red y seguridad como conmutadores, controladores inalámbricos y cortafuegos de nueva generación (NGFW), pero también con soluciones como la gestión de identidades y accesos (IAM), SIEM, Protección avanzada contra amenazas (Advanced Threat Protection, ATP) y la gestión de la movilidad empresarial (EMM). Policy Secure permite tomar decisiones de acceso automatizadas y procesables basadas en datos contextuales como la identidad, la postura de seguridad y la ubicación. Basado en un marco de acceso de confianza cero, Policy Secure aplica continuamente el nivel de confianza de un punto final durante su ciclo de vida de conectividad y lo pone en cuarentena cuando se detecta una anomalía de comportamiento.

Integraciones para la evaluación continua de la confianza

Acceso a la red

El principio de la confianza cero: verificar siempre. Policy Secure primero valida el usuario y el dispositivo con respecto a la política. A continuación, Policy Secure conecta el dispositivo con la infraestructura de acceso de acuerdo con la función de ese usuario. Esta segmentación dinámica de la red limita la propagación lateral de las amenazas entre las diferentes clases de dispositivos y usuarios del IoT.

PPS se integra con las principales soluciones de conmutación y Wi-Fi de proveedores como Cisco, Juniper, Mist, Aruba, Huawei y Ruckus utilizando el estándar común 802.1X, o SNMP.

El aprovisionamiento dinámico del perímetro de la red proporciona otra capa de control de acceso. Las políticas de NGFW pueden aprovechar información contextual adicional, como la identidad o la ubicación del usuario. PPS se integra con soluciones NGFW como Palo Alto Networks, Checkpoint, Juniper y Fortinet, para proporcionar esta información contextual sobre el punto final.

Cumplimiento del punto final

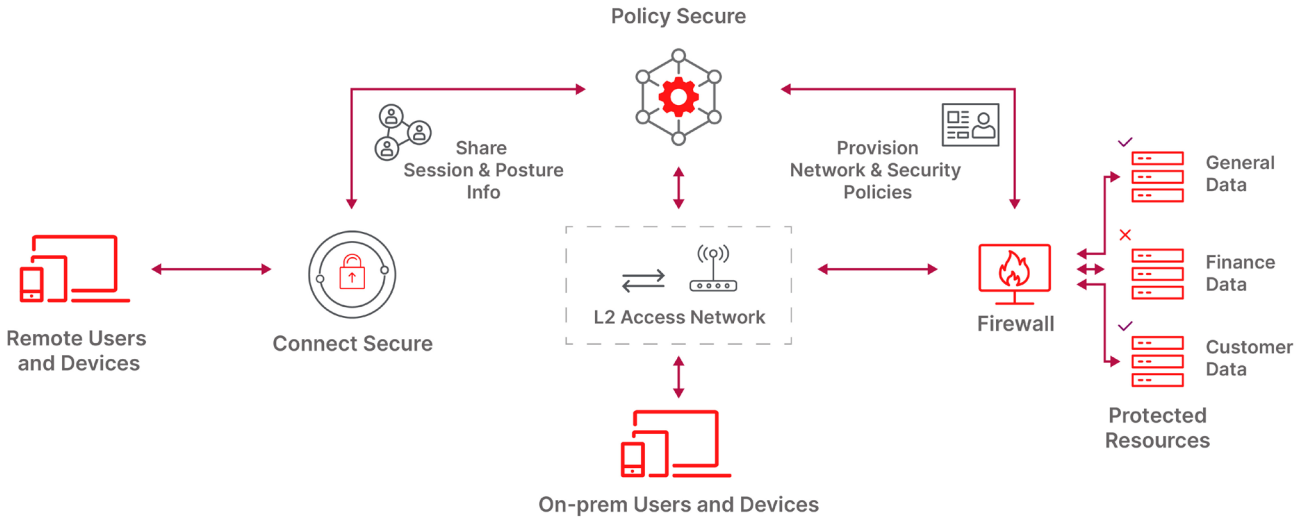
Los puntos finales utilizan una amplia variedad de software que incluye el sistema operativo, utilidades de seguridad como el antivirus, además de aplicaciones a nivel de usuario. Todo este software se actualiza periódicamente para mejorar las funciones y corregir la seguridad. La función de comprobación del host evalúa continuamente la postura de seguridad del dispositivo validando el historial de actualizaciones de software y las aplicaciones activas. Una vez que Policy Secure concede el acceso a la red a un usuario y/o dispositivo, supervisa continuamente la postura de seguridad durante todo el ciclo de vida de la conectividad.

Si la postura de seguridad cambia, por ejemplo porque el usuario lanza una aplicación de TI en la sombra que viola la política, Policy Secure mueve inmediatamente el punto final a un entorno de red restringido.

Policy Secure ayuda a las organizaciones a minimizar el riesgo al imponer automáticamente el cumplimiento de los puntos finales. El comprobador de hosts puede interactuar con Windows Management Instrumentation, Windows Defender, Microsoft Security Essentials o el cliente VPN Connect Secure de Ivanti para obtener una mayor granularidad.

Gestión de la identidad y acceso (IAM)

El mecanismo de autenticación valida la identidad de un usuario y define sus funciones. El sistema puede aprovechar la información contextual basada en el tiempo, la geolocalización o el comportamiento. Por ejemplo, si ya existen sesiones autenticadas en una geolocalización diferente, el usuario puede ser sometido a métodos de autenticación adicionales, como la autenticación de dos factores (2FA). Policy Secure se integra con soluciones IAM que utilizan protocolos como SAML(Ping, Okta, Duo, etc.), Active Directory (Microsoft), o incluso RADIUS/TACACS) o LDAP para entornos más aislados. Policy Secure viene con un servicio RADIUS integrado.



Eventos de seguridad

Una estrategia de seguridad sólida y por capas requiere el análisis continuo de los flujos y eventos de la red, utilizando soluciones como los cortafuegos de nueva generación (NGFW), la gestión de información y eventos de seguridad(SIEM) o la detección avanzada de amenazas (ATD). La integración bidireccional con Policy Secure mejora la eficacia general de la seguridad con respuestas procesables y automatizadas aplicadas en el nivel de acceso a la red. Las respuestas automatizadas a los Indicadores de Compromiso (IoC) reducen el tiempo de remediación y agilizan los recursos administrativos. PPS se integra con los principales NGFW, como Palo Alto Networks, Checkpoint, Juniper y Fortinet, así como con soluciones SIEM como IBM QRadar y Splunk.

Caso de uso: Alerta NGFW

Cuando un NGFW descubre una amenaza, alerta a Policy Secure, utilizando el syslog estándar. Policy Secure puede poner en cuarentena el dispositivo sospechoso en un entorno de acceso restringido para solucionar el problema y evitar la propagación lateral de la amenaza.

ivanti

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