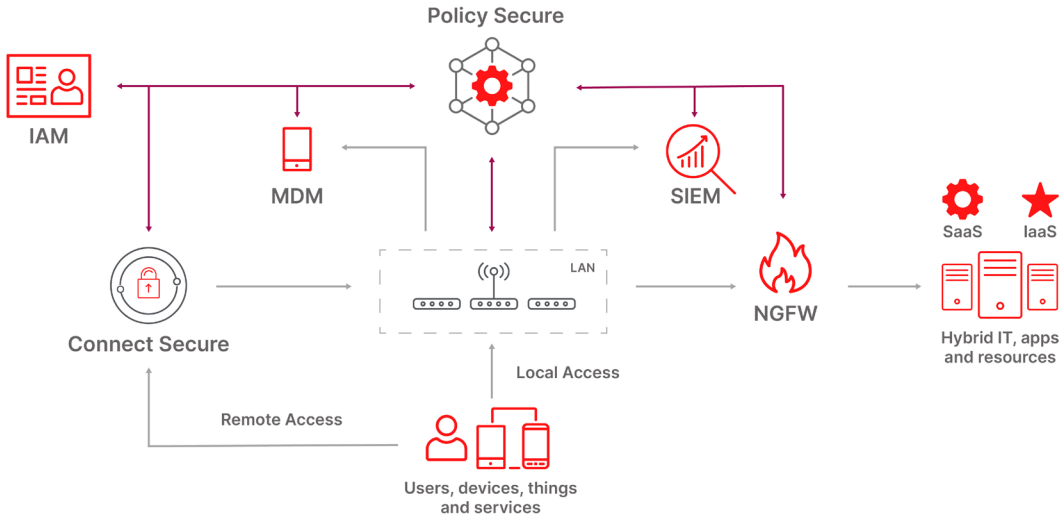
Prévention intégrée des menaces avec Policy Secure

Vue d'ensemble

Pour protéger les données et les ressources, le personnel de sécurité des entreprises utilise des solutions comme les pare-feux nouvelle génération (NGFW) pour contrôler les accès et surveiller les flux de trafic, et des gestionnaires d'événements et d'informations de sécurité (SIEM) pour analyser et relier les événements. Problème : ces solutions se limitent à l'envoi d'alerte ou à l'application de stratégies au trafic qui les traversent. Traditionnellement, les solutions de contrôle des accès réseau (NAC) mettaient en place des mesures de sécurité sur le poste client avant de se connecter au réseau. L'intégration bidirectionnelle avec l'écosystème de sécurité permet au NAC de renforcer l'efficacité de la sécurité globale en appliquant une opération de correction aux connexions d'un poste client, après avoir reçu une alerte de la part d'autres solutions de sécurité. La mise en place d'une sécurité automatisée avec une solution NAC offre notamment les avantages suivants :

- Réduction du délai de réaction aux menaces
- Fluidification des opérations complexes
- Limitation de la dispersion latérale des menaces
- Mise en conformité automatisée de la sécurité et facilitation des audits
- Stratégies plus détaillées avec des informations contextuelles



Policy Secure s'intègre aux périphériques de l'infrastructure réseau et de sécurité, notamment les commutateurs, les contrôleurs sans fil et les pare-feux nouvelle génération (NGFW), mais aussi aux solutions telles que les outils de gestion des identités et des accès (IAM), le SIEM, la protection avancée contre les menaces (ATP) et la gestion de la mobilité d'entreprise (EMM). Policy Secure permet de prendre automatiquement des décisions d'accès utiles, sur la base de données contextuelles comme l'identité, l'état de sécurisation et l'emplacement géographique. Basé sur une structure d'accès Zero Trust, Policy Secure renforce en continu le niveau de confiance d'un poste client, tant qu'il reste connecté, et le met en quarantaine si un comportement anormal est détecté.

Intégration pour une évaluation constante du niveau de confiance

Accès réseau

Principe essentiel du Zero Trust : toujours tout vérifier. Policy Secure valide d'abord l'utilisateur et le périphérique par rapport à la stratégie. Ensuite, Policy Secure connecte le périphérique à l'infrastructure d'accès, en fonction du rôle de l'utilisateur. Cette segmentation dynamique du réseau limite la dispersion latérale des menaces entre les différentes classes de périphériques IoT et d'utilisateurs. PPS s'intègre aux principales solutions de commutation et de Wi-Fi de différents fournisseurs, notamment Cisco, Juniper, Mist, Aruba, Huawei et Ruckus, en utilisant la norme 802.1X courante ou le SNMP.

Le provisioning dynamique du périmètre réseau fournit une couche supplémentaire de contrôle des accès. Les stratégies NGFW peuvent exploiter des informations contextuelles supplémentaires, comme l'identité ou l'emplacement géographique de l'utilisateur. PPS s'intègre à des solutions NGFW comme Palo Alto Networks, Checkpoint, Juniper et Fortinet, pour fournir ces informations contextuelles concernant le poste client.

Conformité du poste client

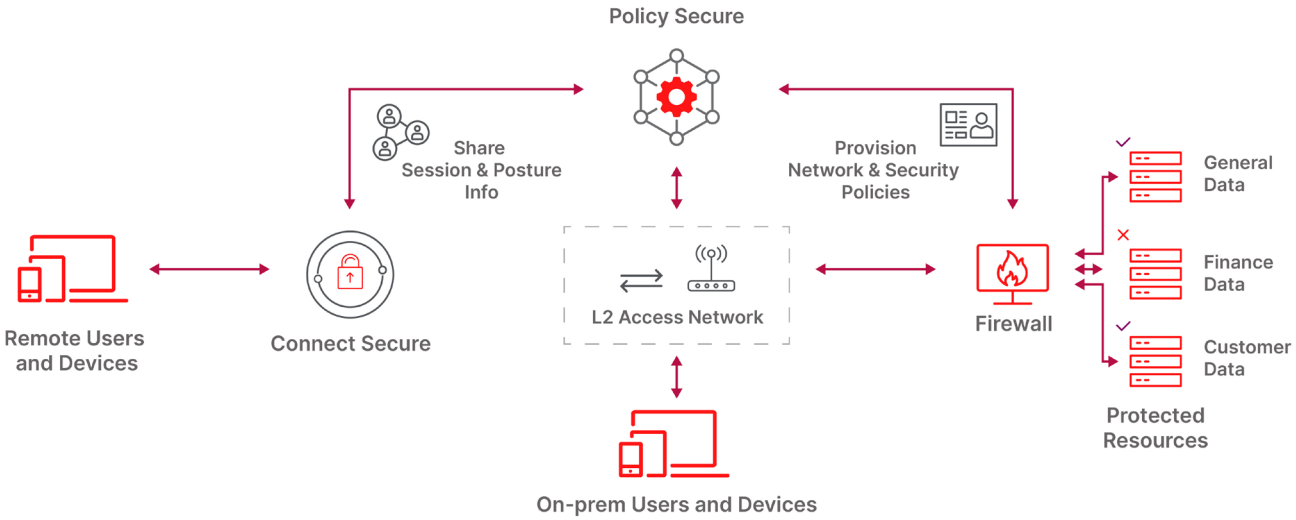
Les postes client utilisent toute une variété de logiciels, y compris le système d'exploitation, des utilitaires de sécurité comme l'antivirus et des applis de niveau utilisateur. Tous ces logiciels bénéficient de mises à jour périodiques qui améliorent les fonctions et corrigent la sécurité.

La fonction de vérification de l'hôte évalue en continu l'état de sécurisation du périphérique, en contrôlant l'historique de mise à jour des logiciels et les applis actives. Une fois que Policy Secure autorise l'accès réseau d'un utilisateur et/ou d'un périphérique, il surveille en continu l'état de sécurisation, tout au long du cycle de vie de la connexion. Si l'état de sécurisation change, par exemple parce que l'utilisateur lance une appli de Shadow IT qui viole la stratégie, Policy Secure déplace immédiatement le poste client vers un environnement réseau restreint.

Policy Secure aide les entreprises à limiter les risques en assurant automatiquement la conformité du poste client. L'outil de vérification de l'hôte peut interagir avec Windows Management Instrumentation (WIM), Windows Defender, Microsoft Security Essentials ou le client VPN Ivanti Connect Secure pour encore plus de granularité.

Solutions de gestion des identités et des accès (IAM)

Le mécanisme d'authentification vérifie l'identité de l'utilisateur et définit des rôles. Le système peut exploiter des informations contextuelles basées sur l'heure, l'emplacement géographique ou le comportement. Par exemple, si des sessions authentifiées existent déjà à un autre emplacement géographique, l'utilisateur peut être soumis à des contraintes d'authentification supplémentaires, comme l'authentification à deux facteurs (2FA). Policy Secure s'intègre aux solutions d'IAM à l'aide de protocoles de type SAML (Ping, Okta, Duo etc.), Active Directory (Microsoft), ou même RADIUS/TACACS+ ou LDAP dans les environnements les plus isolés. Policy Secure est livré avec un service RADIUS intégré.



Événements de sécurité

Une stratégie de sécurité multiniveau solide nécessite une analyse en continu des flux et événements réseau, à l'aide de solutions comme les pare-feux nouvelle génération (NGFW), les outils de gestion des informations et événements de sécurité (SIEM), ou les outils de détection des menaces avancées (ATD). L'intégration bidirectionnelle avec Policy Secure renforce la sécurité globale, grâce à des réponses automatisées utiles appliquées au niveau des accès réseau. Ces réponses automatisées aux indicateurs de compromission (IoC) réduisent les délais de correction des problèmes et fluidifient les ressources administratives. PPS s'intègre avec les principaux pare-feux nouvelle génération (NGFW), comme Palo Alto Networks, Checkpoint, Juniper et Fortinet, ainsi qu'avec des solutions SIEM comme IBM QRadar et Splunk.

Scénario d'utilisation : Alerte NGFW

Lorsqu'un pare-feu nouvelle génération (NGFW) détecte une menace, il alerte Policy Secure via le journal système (syslog) standard. Policy Secure peut mettre le périphérique suspect en quarantaine dans un environnement d'accès restreint afin de résoudre le problème et d'empêcher toute dispersion latérale de la menace.

ivanti

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