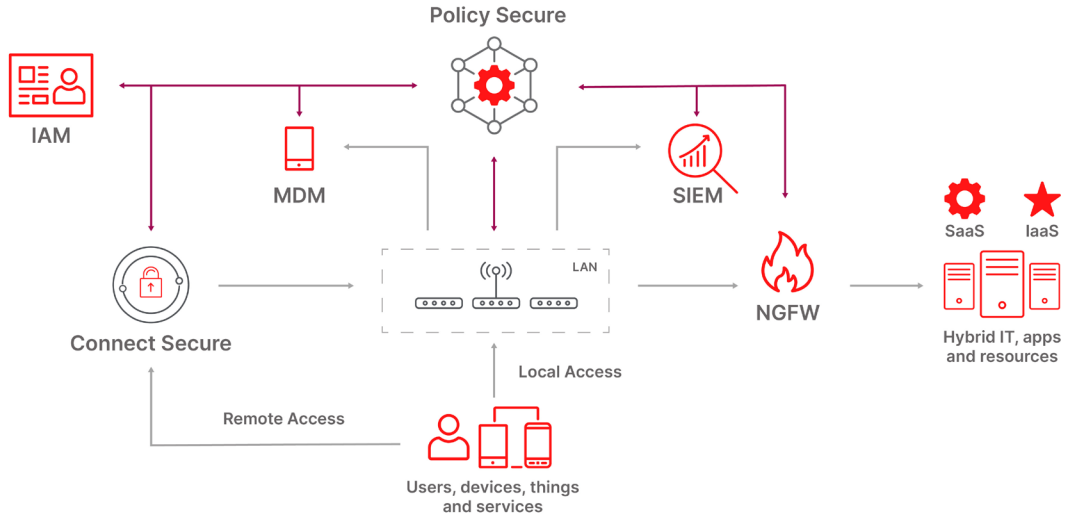
Integrated Threat Defense with Policy Secure

Overview

To protect data and resources, enterprise security personnel use solutions such as Next-Generation Firewalls (NGFWs) to control access and monitor traffic flows, and Security Information and Event Managers (SIEMs) to analyze and cross-correlate events. The problem: these solutions are limited to sending alerts, or enforcing policies on the traffic that passes through them. Network Access Control (NAC) solutions have traditionally enforced an endpoint's security posture before connecting to the network. Bidirectional integration with the security ecosystem enables an NAC to increase overall security efficacy by taking remedial action on an endpoint's connectivity after receiving alerts from other security solutions. Automated security enforcement with an NAC provides benefits including:



- Reduced threat response time.
- Streamlined security operations.
- Limited lateral spread of threats.
- Automated security compliance and easier audits.
- More granular policies with contextual information.

Policy Secure integrates with network and security infrastructure devices such as switches, wireless controllers and next-generation firewalls (NGFW), but also with solutions such as identity and access management (IAM), SIEM, Advanced Threat Protection (ATP) and Enterprise Mobility Management (EMM). Policy Secure enables automated, actionable access decisions based on contextual data such as identity, security posture and location. Based on a zero trust access framework, Policy Secure continuously enforces the trust level of an endpoint during its connectivity lifecycle and quarantines it when a behavioral anomaly is detected.

Integrations for continuous trust assessment

Network access

The principle of zero trust: always verify. Policy Secure first validates the user and the device against the policy. Then, Policy Secure connects the device with the access infrastructure in line with that user's role. This dynamic network segmentation limits the lateral spread of threats between different classes of IoT devices and users. PPS integrates with leading switching and Wi-Fi solutions from vendors such as Cisco, Juniper, Mist, Aruba, Huawei and Ruckus using the common 802.1X standard, or SNMP.

Dynamic network perimeter provisioning provides another layer of access control. NGFW policies can leverage additional contextual information such as the user's identity or location. PPS integrates with NGFW solutions like Palo Alto Networks, Checkpoint, Juniper and Fortinet, to provide this contextual information about the endpoint.

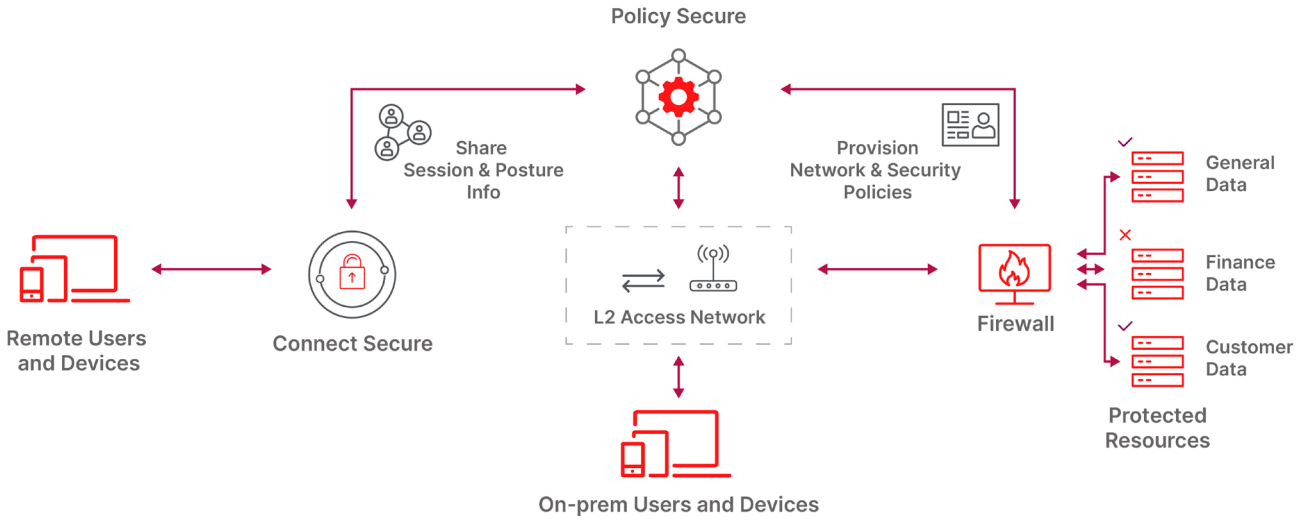
Endpoint compliance

Endpoints use a wide variety of software including the operating system, security utilities like anti-virus, plus user-level apps. All this software receives periodic updates for feature enhancements and security fixes. The host checker feature continuously assesses the security posture of the device by validating the software update history and active apps. Once Policy Secure grants network access to a user and/or device, it continuously monitors the security posture throughout the connectivity lifecycle. If the security posture changes, for example because the user launches a shadow IT app that violates the policy, Policy Secure immediately moves the endpoint into a restricted network environment.

Policy Secure helps organizations to minimize risk by automatically enforcing endpoint compliance. The host checker can interact with Windows Management Instrumentation, Windows Defender, Microsoft Security Essentials or Ivanti's Connect Secure VPN client for even more granularity.

Identity and Access Management (IAM)

The authentication mechanism validates a user's identity and defines roles. The system can leverage contextual information based on time, geolocation or behavior. For example, if authenticated sessions already exist in a different geolocation, the user can be subjected to additional authentication methods such as two-factor authentication (2FA). Policy Secure integrates with IAM solutions using protocols such as SAML (Ping, Okta, Duo etc.), Active Directory (Microsoft), or even RADIUS/TACACS+ or LDAP for more isolated environments. Policy Secure comes with a built-in RADIUS service.



Security events

A solid, layered security strategy requires the continuous analytics of network flows and events, using solutions such as Next-Generation Firewalls (NGFWs), Security Information and Event Management (SIEM), or Advanced Threat Detection (ATD). Bidirectional integration with Policy Secure improves overall security efficacy with actionable, automated responses enforced at the network access level. Automated responses to Indicators of Compromise (IoC) reduces remediation time and streamlines administrative resources.

PPS integrates with leading NGFWs, such as Palo Alto Networks, Checkpoint, Juniper and Fortinet, as well as SIEM solutions such as IBM QRadar and Splunk.

Use case: NGFW alert

When an NGFW discovers a threat, it alerts Policy Secure, using standard syslog. Policy Secure can quarantine the suspect device to a restricted access environment to remediate the problem and prevent lateral spread of the threat.

ivanti

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