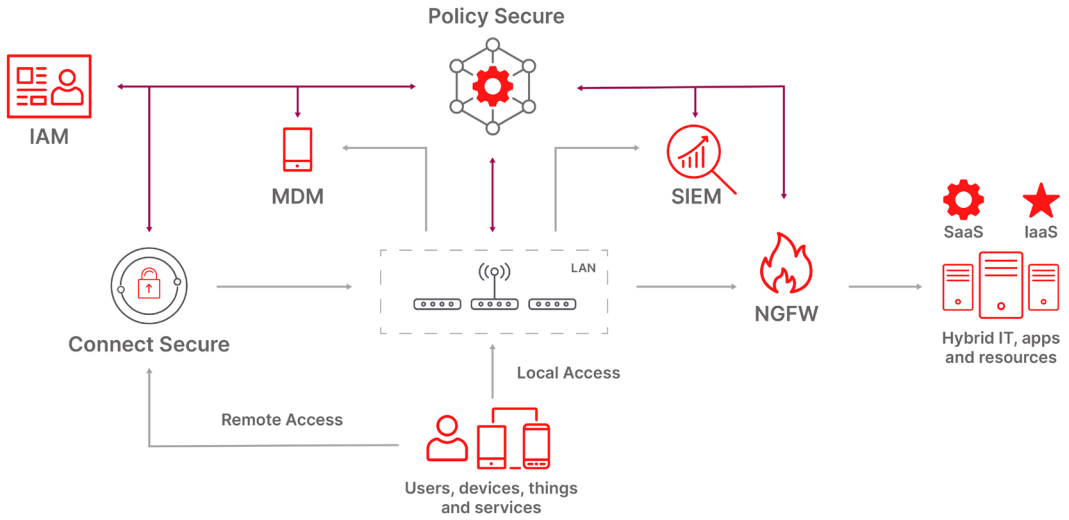
Policy Secure集成威胁防御

概要

为了保护数据和资源，企业安全人员使用各种解决方案，包括用于控制访问和监测流量的下一代防火墙（NGFW）和用于分析和建立互相关事件的安全信息和事件管理（SIEM）工具。问题是：这些解决方案仅限于发送警报，或对经过它们的流量执行政策。在传统上，网络访问控制（NAC）解决方案会对端点强制执行安全态势，然后才准予连接到网络。

如果与安全生态系统双向整合，NAC便能在收到其他安全解决方案发出的警报后对端点连接采取补救措施，从而提高整体安全效能。结合NAC的自动安全执行的优势包括：

- 缩短威胁响应时间
- 简化安全操作
- 限制威胁的横向扩散
- 自动安全合规和更轻松的审计
- 基于情境信息的更细化的策略



除交换机、无线控制器和下一代防火墙（NGFW）等网络和安全基础架构设备外，Policy Secure也可与身份和访问管理（IAM）、SIEM、高级威胁防护（ATP）和企业移动管理（EMM）等解决方案整合。Policy Secure能够根据身份、安全态势和地理位置等情境数据做出自动化、可操作的准入访问决定。Policy Secure建于零信任访问框架之上，能在端点的连接周期内持续执行相应信任级别，并在检测到行为异常时将其隔离。

持续信任评估集成

网络接入

零信任的原则是：永远验证。Policy Secure 首先会根据策略验证用户及其设备。然后，Policy Secure 把设备连接到与用户角色相符的访问架构。动态网络分段限制了威胁在不同物联网设备和用户分级之间的横向扩散。PPS使用通用的802.1X标准或SNMP与行业领先的交换和Wi-Fi解决方案整合，包括思科、Juniper、Mist、Aruba、华为和Ruckus等。

动态网络周界配置进一步增强了访问控制。NGFW策略可以利用额外的情境信息，如用户身份或位置。PPS可集成Palo Alto Networks、Checkpoint、Juniper和Fortinet等NGFW解决方案，以提供此类端点情境信息

端点合规

端点需要使用各种各样的软件，包括操作系统、安全工具（如反病毒软件）和用户级应用程序。所有这些软件都会定期更新，以增强功能和修复安全问题。主机检查器功能持续验证软件更新历史和活跃的应用程序，对设备的安全态势作出评估。在准许用户和/或设备访问网络后，Policy Secure会在整个连接周期内持续监控其安全态势。如果安全态势发生变化，例如用户启动了违反策略的影子IT应用，Policy Secure会立刻把端点转移到一个受限的网络环境中。

Policy Secure通过自动执行端点合规性，帮助企业将风险降至最低。主机检查器能够与Windows Management Instrumentation、Windows Defender、Microsoft Security Essentials或Ivanti的Connect Secure VPN客户端进行交互，以达到更高的细化程度。

身份和访问管理（IAM）

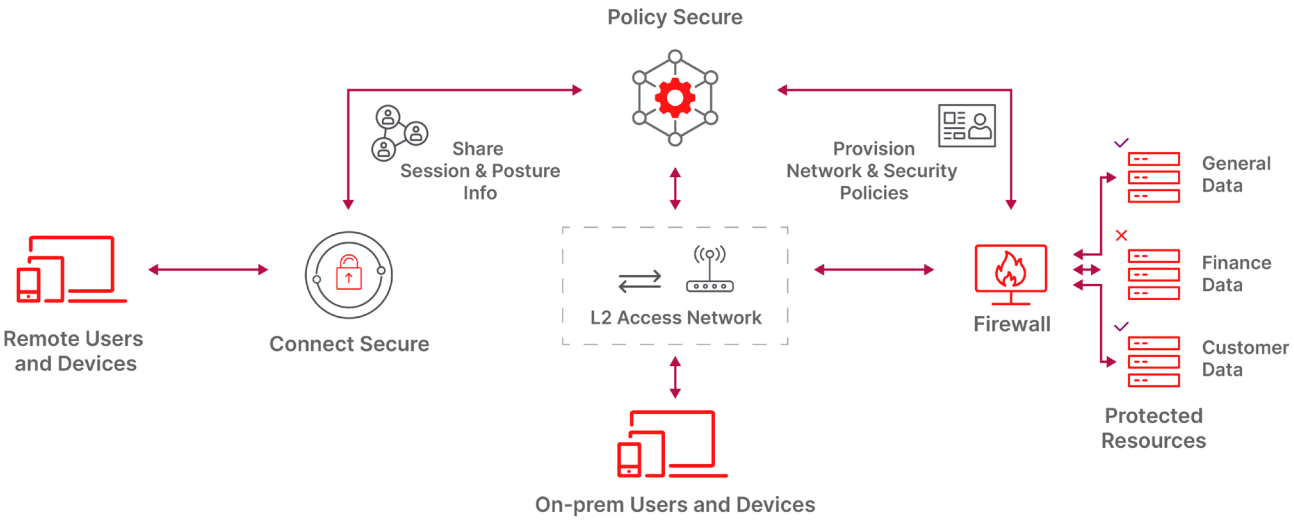
验证机制对用户身份进行验证并定义角色。该系统可以利用时间、地理位置或行为等情境信息。例如，如果验证会话已在另一地理位置存在，用户则需要采取额外验证，如双因素验证（2FA）。Policy Secure可集成使用SAML（Ping、Okta、Duo等）、Active Directory（Microsoft）以及RADIUS/TACACS+或LDAP等协议的IAM解决方案，以创造更孤立的环境。Policy Secure内置RADIUS服务。

安全事件

一个可靠的分层安全战略需要使用下一代防火墙（NGFW）、安全信息和事件管理（SIEM）或高级威胁检测（ATD）等解决方案对网络流量和事件进行持续分析。Policy Secure的双向集成在网络访问层面上执行可操作的自动响应，从而提高了整体安全效率。通过对失陷指标（IoC）作出自动响应，减少了修复时间，并精简了管理资源。PPS可与多种业界领先的NGFW（如Palo Alto Networks、Checkpoint、Juniper和Fortinet）和SIEM（如IBM Qradar和Splunk）解决方案集成。

用例：NGFW警报

当NGFW发现威胁时，它会使用标准系统日志向Policy Secure发出警报。Policy Secure能够将可疑设备隔离到受限访问环境中，对问题作出补救并防止威胁横向扩散。



关于Ivanti

Ivanti让无处不在的工作空间成为可能。在“无 处不在的工作空间”，员工可能会在任何地方 工作，并使用多种设备来访问IT网络、应用 程序和数据，以保证工作效率。Ivanti自动化 平台集成了业内领先的统一端点管理、零信 任安全和企业服务管理解决方案，通过一站 式平台实现为企业实现自我修复和自我安全，并为终端用户提供自我服务。已经有4万多位 客户，包括78家《财富》百强企业，选择了 Ivanti为他们检测、管理、保护和维护从云端 到边缘的IT资产，同时为员工提供卓越的终 端用户体验，无论他们在哪里、使用何种方 式工作。更多信息请访问ivanti.com.cn

ivanti

ivanti.com.cn
+86 (0)10 85412999
ContactChina@ivanti.com