Pulse Secure®

销售策略 #1：混合 IT 的安全访问

市场概览

85%

85% 的企业在混合 IT 环境中运营

根据 Gartner 的调查，端点、应用程序和服务在传统界限之外运行，更加强调“零信任”方法。监控远程网络访问的技术专业人员正在考虑多种远程安全产品，具体取决于法规要求和用例。

主要用例：

- 不间断访问
- BYOD
- 按需访问
- 网关整合

混合 IT 现实

当组织将工作负载分布到多个位置时，用户必须能够透明地连接所有这些位置。必须能够从用户使用的任何设备、任何位置到托管数据的任何位置（无论是内部还是云）进行连接。

混合 IT 访问（不包括 SDP/ZTNA）：

- 对于端点，与 IPsec 相比 TLS vpn 提供了最灵活、最可靠的方法
- TLS 隧道的拆分隧道为混合或多云环境提供了更好的用户体验，还支持从不间断到按需 VPN 的转变，并减少了互联网访问的延迟。如果法规或合规性要求允许，可以使用拆分隧道从分支提供按需云访问。
- 在连接到网络之前和期间，进行用户身份和端点合规性检查。
- 云服务用户和设备的快速应用程序访问。
- 端点类型和位置是选择解决方案的一个重要因素 - 对于云，从端点到应用程序的直接连接更有效。对于 IoT，可能需要无代理。对于云，按需 VPN 更具成本效益。

解决方案：混合 IT 的安全访问

Pulse 为混合 IT 提供领先的零信任访问解决方案，为数据中心和 SaaS/云融合了卓越的用户体验和兼容访问。

Pulse 混合访问解决方案：

- Pulse Connect Secure
- Essentials Suite（混合 IT 捆绑包）

安全访问的多个用例

支持以下任何用例：同类最佳 TLS VPN、针对合规性的带锁定模式的不间断 VPN、针对按需安全的 Web/云访问的基于域的拆分隧道。

出色的用户体验

具有多通道功能的统一客户端极大地简化了用户体验并提高了用户生产力。

针对混合 IT 的 SSO 和自适应 MFA

用于数据中心和 SaaS/云的单点登录和自适应多因素 (MFA) 身份验证。

端点/BYOD 合规性

强制实施设备合规性；通过持续评估应用身份和访问控制，以确保只有授权用户才能访问数据。

集中的访问管理

集中配置和管理访问服务，以便于部署和维护。

针对混合 IT 访问的关键功能

功能	优势
专为高性能、高容量物理或虚拟混合环境设计	随着添加更多的用户、设备和云用例便利地扩展
基于域的拆分隧道和按需或不间断锁定模式 VPN，始终处于启动状态或仅在需要时出现（可按应用程序配置）	有助于满足混合访问的合规性或法规要求，并确保移动用户连接到 Web/云
单点登录 (SSO) 云应用	用户友好并且比专用 SSO 解决方案更有成本效益
内置一次性密码 (TOTP) 解决方案以及自适应多因素身份验证	防止未经授权的访问和凭据失窃；灵活地支持内置和第 3 方身份验证源
广泛的应用程序支持，包括 SaaS、Web、经典数据中心、原生 VDI、HTML5、自定义应用（L2 到 L7）	广泛的资源和应用程序访问覆盖范围 - 有助于标准和自定义应用的合规性
稳健的主机检查器提供设备安全态势检查	确保对托管和非托管设备（公司所有，BYOD）的设备兼容性访问
连接前后设备态势评估	在整个交互过程中验证安全态势，应用行为分析并根据需要进行补救
集中的策略配置和管理	易于配置；自动化以减少错误；使 IT 人员从日常的重复性任务中解放出来

发现问题

您是否使用 Office 365、Salesforce、Box 或其他 SaaS 应用?	**Pulse Cloud Secure** 通过将现有的设备合规性和用户身份的数据中心保护措施扩展到云/SaaS 中的应用程序和服务，简化了云/SaaS 的采用。
您在使用什么云平台?	如果客户使用超过 1 个公共云（AWS、Azure、Google、阿里云），请参阅销售策略 #2（多云访问）
在允许访问您的数据之前，您是否强制实施设备合规性?	**Pulse Secure** 解决方案通过执行彻底的设备态势检查来帮助满足公司标准，并防止非托管设备访问数据中心或云/SaaS 中的资源。
您是否使用第 3 方身份提供商（Ping、Okta、AD FS）?	**Pulse Secure** 解决方案有内置的 SSO（单点登录）和 MFA（多因素身份验证），但也支持第三方身份提供商，如 Ping、Okta 和其他采用 SAML 2.0 的提供商。
您需要将安全的外部访问与网络内部的精细网络访问控制结合起来吗?	解决方案是 Enterprise Suite 或 Pulse Policy Secure 和 Pulse Connect Secure。请参阅销售策略 #3（零信任网络访问控制）或销售策略 #4（端到端零信任安全）
在冬季或自然灾害期间，您是否担心用户在家工作时失去远程访问连接?	**Pulse Secure ICE（紧急情况）**许可证可确保您在紧急情况下激活（设备的）最大数目远程访问许可证，这样您的用户就不会丢失连接，并且可以不间断地工作。
所有应用程序都有一个单一访问点吗?	**Pulse vADC Traffic Manager 的 OGS** 功能通过最近的 PCS 网关提供一个单一访问点。它自动确定最近的网关，优化性能并简化用户体验。

竞争力比较

混合 IT 访问功能	Pulse Secure	Cisco AnyConnect	Palo Alto Networks	Microsoft	Zscaler ZPA
无缝用户体验，无需考虑位置即可访问应用程序	✓	有限	有限	有限	X
数据中心和云的采用 SSO 和条件访问的丰富多因素身份验证	✓	✓	有限	✓	X
广泛的连接前和连接后端点安全态势评估和实施	✓	有限	X	X	有限
广泛的应用程序支持：SaaS、Web、原生 VDI、HTML5、VoIP、SIP、P2P、自定义应用	✓	有限	有限	有限	有限
可按应用程序配置的 VPN，具有基于域的拆分隧道	✓	有限	X	X	X
针对用户目录、第三方身份验证来源的开放平台支持	✓	X	X	有限	有限
便于配置和管理	✓	X	✓	有限	有限