Ivanti Neurons 神经元零信任访问功能

安全访问无处不在的工作空间

Ivanti Neurons 神经元零信任访问功能（nZTA）为设备访问基于网络的企业本地和云端应用程序建立安全连接，从而提升安全性、生产力和合规性，同时大幅改善管理和 终端用户体验。

无处不在的零信任访问

获得持续的用户和设备认证以及始终受保护的连接，从而安全访问本地、数据中心以及私有云和公共云上的企业应用程序。

根据灵活细化的约束条件自动验证和授权用户、设备 和应用程序的连接，确保自适应控制、微分段隔离能力和缩小攻击面。

更强的可视性和分析能力

查看实时状态和历史趋势，利用nZTA学习的使用和行为信息（例如用户从哪里登录、通常使用什么设备、通常访问什么设备）来主动采取行动，降低安全风险。

提高业务效率和应变能力

安全实施新服务，更快执行细化政策变更。nZTA消除了发卡流量，通过直接到应用程序的访问改善用户体验。此外，通过一个单一客户端实现本地、远程和直接到云的访问，快速顺利地完成您的零信任进程。

选择与灵活：细化策略和网关位置

把网关放在任何地方。每个命名用户最多支持五台设备，并可灵活增加网关数量，确保最佳的安全环境。

缓解网络流量拥堵和数据收费支出

有了nZTA，您的数据永远无需经过我们的平台，在减少企业带宽的压力的同时免除了SWG和CASB的数据费用。

与VPN整合

整合nZTA和现有VPN，提高工作效率，节省漫长的基础架构或软件实施时间。轻松快速地为新应用程序提供安全访问，整合新的业务单位，或促进并购活动。

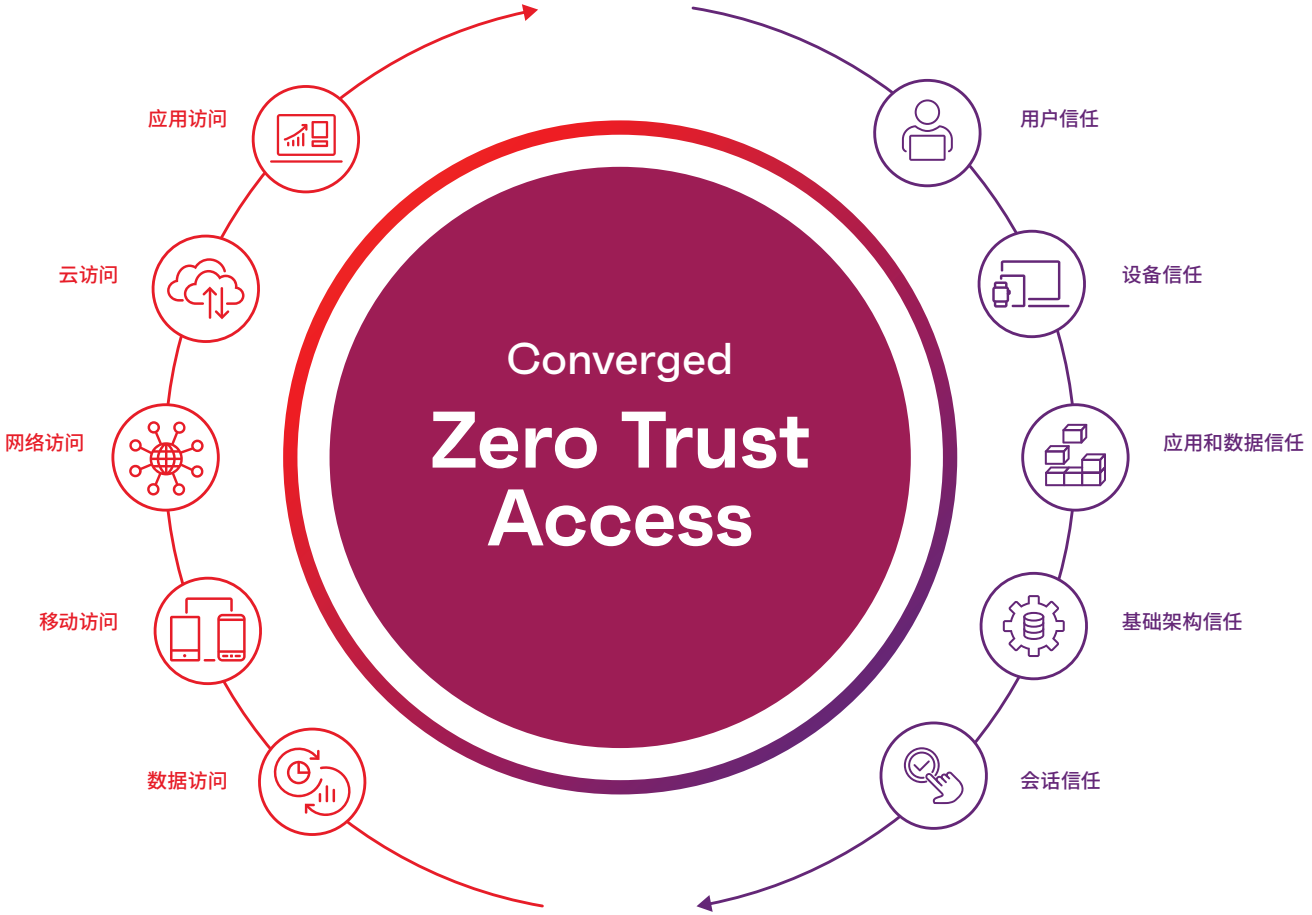
原理

nZTA是一个以“软件即服务”形式交付的零信任网络访问解决方案，其目的是与您的VPN解决方案或云优先企业共同协作。

nZTA对用户身份和设备安全态势进行认证和授权，在确保合规后才建立会话。nZTA通过集中部署管理的策略来管辖每个访问请求和会话，并通过内置的用户实体行为分(UEBA)来增强有关策略，每次会话的属性都会得到监控和评估。我们专有的风险评分能够识别不合规定、恶意和异常的活动，从而加速威胁缓解操作。

nZTA网关可以灵活地部署在您选择的地方，无论是在本地还是在您的云应用程序附近。这样的近距离能够优化用户体验、减少延迟并推动大规模的混合IT部署。控制器验证设备和网关的访问策略，创建安全的MTLS隧道，消除nZTA控制器的任何数据交互。

nZTA能够为任何地方的应用部署提供部署灵活性和联贯的策略管理，同时为纯多云环境的企业提供全面的安全访问能力。



功能特性	优势
端到端访问策略	为每一个资源定义端到端访问策略，消除远程用户和本地用户之间的差异。
暗云	只有经过认证和授权的用户和设备才能访问隐藏的应用程序。
单一视窗的可视性	一体化可视性和合规性报告，涵盖整个企业的用户、设备、应用程序和基础架构。
控制平面和数据平面的分离	用户和应用流量直接在用户和指定网关之间发送，降低数据丢失的风险，提升用户体验。
自适应性SSO	通过SAML 2.0整合提供SSO，支持SaaS和第三方应用程序。
端点合规性	用户和设备在获得访问权限之前会根据细化政策通过认证，降低恶意软件和其他威胁的可能。
用户行为分析	利用分析数据降低安全风险、检测异常情况、优化用户体验和适应远程工作需求。
数据隐私和主权	客户端和网关之间的所有用户和应用程序数据完全加密，nZTA从不与客户数据互动。
本地和混合云	网关可部署于公共云、私有云或客户数据中心。

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