ivanti

DATASHEET

Ivanti Neurons for Zero Trust Access

Everywhere Workplace 的安全存取

Ivanti Neurons for Zero Trust Access (nZTA) 建立從 設備到本地和雲端中的網路應用程式的安全連接，提高了安全性、生產力和合規性，同時大幅改善行政管理和 終端使用者體驗。

無處不在的零信任存取

獲得持續的使用者和設備驗證，以及對本地、資料中心及私有雲和 公有雲上的企業應用程式的 長期持續保護存取。

根據靈活而精細的限制自動驗證和授權使用者、設備和應用程式的連接，確保自適應控制、微分段能力和減少攻擊面。

更高的可視性和分析能力

存取即時狀態和歷史趨勢，並利用 nZTA 學到的用法和行為資料（例如，使用者從何處登入、他們經常使用的設備及他們經常存取的設備），先發制人地採取行動並降低安全風險。

提高業務生產力和敏捷性

安全地執行新服務並更快速地進行精細分層的政策更改。nZTA 消除了流量髮夾現象，並透過直接存取應用程式改善了使用者體驗。使用單一客戶端進行本地、遠端和直接到雲端的存取，毫無障礙地加速您的零信任工作。

選擇和靈活性：精細分層的政策和閘道配置 閘道配置

將閘道器放置在您想要的位置。每個指定使用者最多可以支援五台設備，並增加數量可隨時改變的閘道來確保您的最佳安全環境。

舒緩網路流量壅塞與資料通行費

使用 nZTA，您的資料絕對不會通過我們的平台，如此一來可以減少公司頻寬的壓力並消除 SWG 和 CASB 上的資料費用。

整合 VPN

整合 nZTA 與現有的 VPN，提高生產力並避免冗長的基礎設施或軟體實施時間。輕鬆快速地提供對新應用程式的安全存取、整合新事業單位或促進併購活動。

整合CASB和SWG

通過增加核心CASB（雲端存取資安代理）和SWG（安全網頁閘道），來確保連接到SaaS平台和互聯網應用的請求，支持DLP（資料外洩防護），EDRM（企業數位版權管理），OCR（光學字元辨識）的威脅檢測

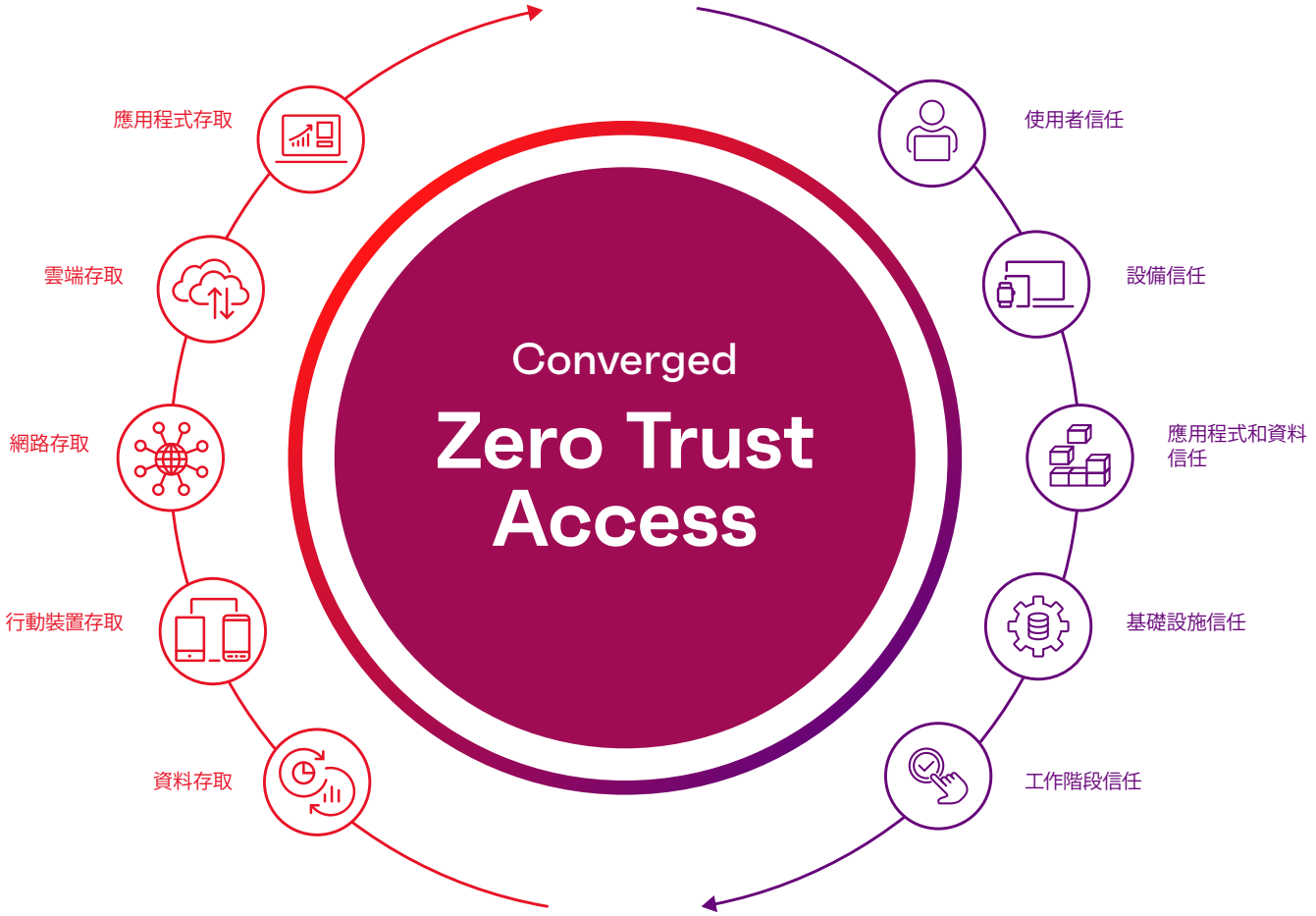
工作原理：

nZTA 是一種 SaaS 交付的零信任網路存取解決方案，旨在與您的 VPN 解決方案或雲端優先組織一起工作。

nZTA 會在建立工作階段之前驗證和授權使用者身份和設備安全狀態以確保符合規定。nZTA 透過集中部署和管理的政策來管理每個存取要求和工作階段，並使用內建的User and Entity Behavior Analytics（UEBA）來強化這些政策，其中每個工作階段的屬性都受到監控和評估。專有風險評分可識別不合規範、惡意和異常活動，進而加速威脅緩解措施。

nZTA 閘道器可以靈活地部署在您想要的位置，無論是在本地還是在您的雲端應用程式附近。這種鄰近性優化了使用者體驗，減少延遲，並且支援大規模混合 IT 部署。控制器可驗證設備和閘道上的存取政策，打造安全的 MTLS 通道，消除任何與 nZTA 控制器的資料交互運用。

nZTA 為在任何地方部署應用程式提供了部署靈活性和統一的政策管理，同時還為那些擁有純多重雲端環境的組織提供全面的安全存取能力。



功能	優勢
端到端存取政策	為每個資源定義端到端存取政策，消除遠端使用者和本地使用者之間的區別。
Dark Cloud	只有在使用者和設備通過身份驗證和授權後，才能存取不可見的應用程式。
單一虛擬管理平台可視性	全企業使用者、設備、應用程式和基礎設施的全面可視性和合規性報告。
控制權和資料層分離	使用者和應用程式流量直接在使用者和指定的閘道之間發送，降低資料外洩的風險，並改善使用者體驗。
自適應 SSO	通過 SAML 2.0 整合，為受支援的 SaaS 和第三方應用程式提供 SSO。
端點合規性	在授予存取權限之前，使用者和設備已根據精細分層的政策進行身份驗證，降低了惡意軟體和其他威脅的可能性。
使用者行為分析	利用分析資料來降低安全風險、檢測異常、優化使用者體驗並適應行動工作人員。
資料隱私權和主權	nZTA 從不與客戶資料交互運用，所有使用者和應用程式資料在客戶端和閘道之間都是完全加密的。
本地雲和混合雲	閘道可以部署在公有雲、私有雲或客戶資料中心。

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