Ivanti Neurons for MDM (前身為 MobileIron Cloud)

挑戰

組織需要安全存取與輕鬆管理他們的員工、承包商和第一線工作人員使用的任何端點上的企業資料。

今天的無所不在的工作場所包括使用多元的端點，例如 iOS、macOS、Android、Windows 裝置，以及其他沈浸式與堅固的裝置，例如 HoloLens、Oculus、Zebra 等。

管理隱私與符合性，以及最小化風險必須分隔與保護企業應用程式與其使用者的端點裝置的個人應用程式。安全、統一的端點管理解決方案 需要可以同時提供卓越的使用者體驗。

關鍵使用案例

確保組織中的隱私與合規性，主要與保護敏感資料有關：
保護任何端點上的企業資料安全，並分隔各個端點上的企業和個人資料

可從單一主控台管理多個裝置、多個作業系統和個應用程式：
組織擁有結合了 iPhone、iPad、Mac、Android 裝置、Windows 筆記型電腦和個人電腦、Zebra、Oculus 等配備的混合式裝置環境。統一管理這些有不同作業系統和應用程式的裝置是最優先要務。

授權給第一線工作人員
支援衛生保健、運輸、製造等其他行業中使用堅固裝置或資訊站模式中的裝置的現場、主力和第一線工作人員。

提供更好的終端使用者
選擇和愉快的使用者體驗：當使用者選擇和終端使用者體驗至關緊要時，Ivanti Neurons for MDM 提供改善使用者生產力的最簡易加入和卓越的裝置體驗。

資安標準和認證*

- CSA STAR
- FedRAMP Moderate Authority
- SOC 2 Type II

如需更多與認證有關的資訊，請瀏覽此處：
ivanti.com/resources/security-compliance

Ivanti Neurons for MDM 在無所不在的工作場所中保護和管理您的裝置。

Ivanti Neurons for MDM 可安全存取和保護您無所不在的工作場所的資料。Ivanti 的安全方式驗證裝置，確保只有獲得授權的使用者、裝置、應用程式和服務可以用企業資源。您實現了跨任何端點的愉快、原生的使用者體驗。

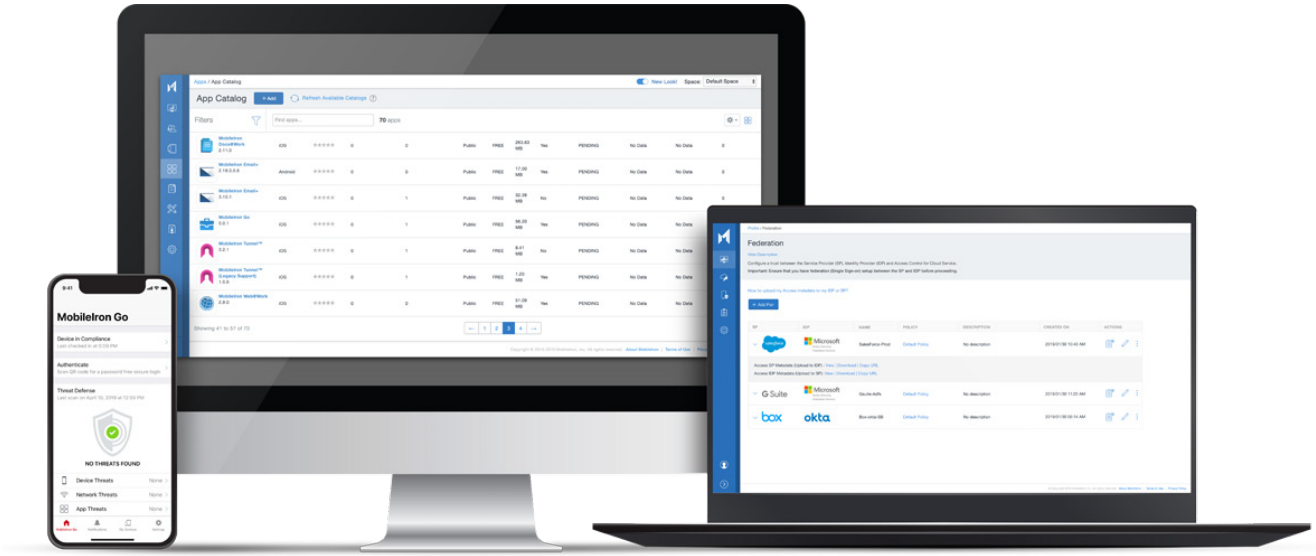
Ivanti Neurons for MDM 以企業行動安全性為您企業的中心，並允許您以去除密碼的技術 (零登入 (ZSO)) 建置確保使用者驗證 (多重要素驗證 (MFA)) 和偵測與緩解端點安全威脅 (行動威脅防禦 (MTD))。

全面的安全性

Ivanti 的 Neurons for MDM 提供保護、管理和監控存取重要企業資料的任何企業或個人擁有的行動裝置或桌上型設備所需的可見度和 IT 控制功能。除了允許組織保護組織內正使用的大量 BYO 裝置外，同時也管理端點的整個生命週期，包括：

- 自動化的加入
- 原則配置和執行
- 應用程式發佈和管理
- 管理和安全監控
- 除役和退役

Ivanti Neurons for MDM 可在有靈活部署選項的經證實、安全、可擴充、企業架構的平台上運作，在重視使用者體驗的同時保持著最高品質的安全標準。



Ivanti Sentry 作為電子郵件和內容的內嵌閘道，可管理、加密和保護行動點與後端企業系統之間的流量安全。Ivanti Tunnel 是一款多作業系統應用 VPN 解決方案，組織可以運用其授權給特定的行動應用程式使用防火牆背後的企業資源，但不需要使用者進行任何互動。

以行動裝置和雲端自信與安全的管理您的企業並使其成長

組織和使用者控制：Ivanti Neurons for MDM 允許組織實施個人化的移動性和安全策略，依其自己的進度滿足業務需求。我們也確保使用者個人資料的隱私，同時保護企業資料 - 提供類似的資訊控制能力給使用者和系統管理員。

自由選擇：Ivanti Neurons for MDM 與作業系統和裝置無關。系統管理員可以根據預算選擇雲端或內部部署，員工可以使用他們最喜愛的端點進行工作。

經驗帶動的採用：Ivanti Neurons for MDM 支援跨運作中的生產力應用程式的原生使用者體驗來協助推動採用。這簡化了合規性，同時緩解了安全威脅與影子 IT。使用者採用率越高，IT 就越能加速跨組織的生產力和成長。

提供企業恢復力：我們的安全平台在不侵入使用者的情況下預防業務中斷。在您的企業穩步前進時，無形和自動化的安全確保符合性。

關鍵特點和功能

裝置管理和安全

安全和管理 – 保護和管理執行 Apple 的 iOS、macOS、iPadOS 和 Google 的 Android 與 Microsoft 的 Windows 作業系統的端點。可用於內部部署和作為雲端服務。

行動應用程式管理 (MAM) - 安全的企業應用程式結合承包商和員工裝置上的 Ivanti AppStation，不需要裝置管理。

輕鬆加入 - Apple Business Manager (ABM)、Google Zero-Touch Enrollment 和 Windows AutoPilot 等調整服務，提供自動化的裝置註冊給使用者。

安全的電子郵件閘道 - Ivanti Sentry 是一種內嵌閘道，可管理、加密和保護行動端點與後端企業系統之間的流量安全。

應用程式發佈和配置 - Apps@Work 是一種企業應用程式，結合 Apple Volume Purchase Program (VPP) 可安全發佈行動應用程式。此外，iOS Managed Apps 和 Android Enterprise 可輕鬆配置應用程式級設定和安全原則。

安全生產

安全的電子郵件和個人資料管理 (PIM) 應用程式 - Ivanti Email+ 是一款跨平台，適用於 iOS 和 Android 系統的安全 PIM 應用程式。安全控制，包括政府級加密、基於憑證的驗證、S/MIME、應用程式級加密和密碼強制實施。

安全的網頁瀏覽 - Web@Work 透過保護傳輸中的資料和儲存中的資料，提供安全的網頁瀏覽。自訂書籤和安全通道確保使用者可以快速和安全存取企業資訊。

安全的內容協作 - Docs@Work 允許使用者安全的存取、建立、編輯、標示和分享來自 SharePoint、Box、Google Drive 等存放庫的內容。

行動應用程式容器化 – 部署 AppConnect SDK 或應用程式包裝函式，為您的內部行動應用程式提供額外的安全層，或從我們的 AppConnect i整合應用程式的生態系統中選擇。

衍生的認證 – 支援使用通用存取卡 (CAC) 和個人身分驗證 (PIV) 的雙重驗證。

安全連線

Per app VPN – Ivanti Tunnel 是一款多作業系統應用 VPN 解決方案，組織可以運用其授權給特定的行動應用程式使用防火牆背後的企業資源，但不需要使用者進行任何互動。調整 IT 運作

服務台工具

在使用者許可的情況下， Help@Work 讓 IT 人員可以在遠端檢視和控制使用者的畫面，協助有效率的疑難排解和解決問題。

報告- 透過自訂報告和自動化的修復行動，取得跨所有管理裝置的深入可見度和控制。

條件式存取

Trust Engine – 結合使用者、裝置、應用程式、網域、地理區域等各種訊號，提供適應性存取控制。

無密碼使用者驗證 – 對單一雲端或內部部署應用程式使用作為身分的裝置的無密碼多重要素驗證。

關於 Ivanti

Ivanti 讓 Everywhere Workplace 成為可能 在 Everywhere Workplace，員工使用五花八門的裝置存取 IT 網路、應用程式和資料，以在任何地方工作時保持工作效率。Ivanti 自動化平台將公司領先業界的統一端點管理、零信任安全和企業服務管理解決方案連接起來，為企業提供單一管理平台，使裝置能夠自我修復和自我保護，終端使用者能夠自助服務。超過 40,000 個客戶 (包括財星雜誌百大企業中的 78 間企業) 選擇 Ivanti 來搜尋、管理、保護和服務從雲端到邊緣的 IT 資產，並為員工提供卓越的終端使用者體驗，無論他們在哪裏工作，以何種方式工作。如需更多資訊，請瀏覽 Ivanti.com.cn

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