Trend Vision One™ –

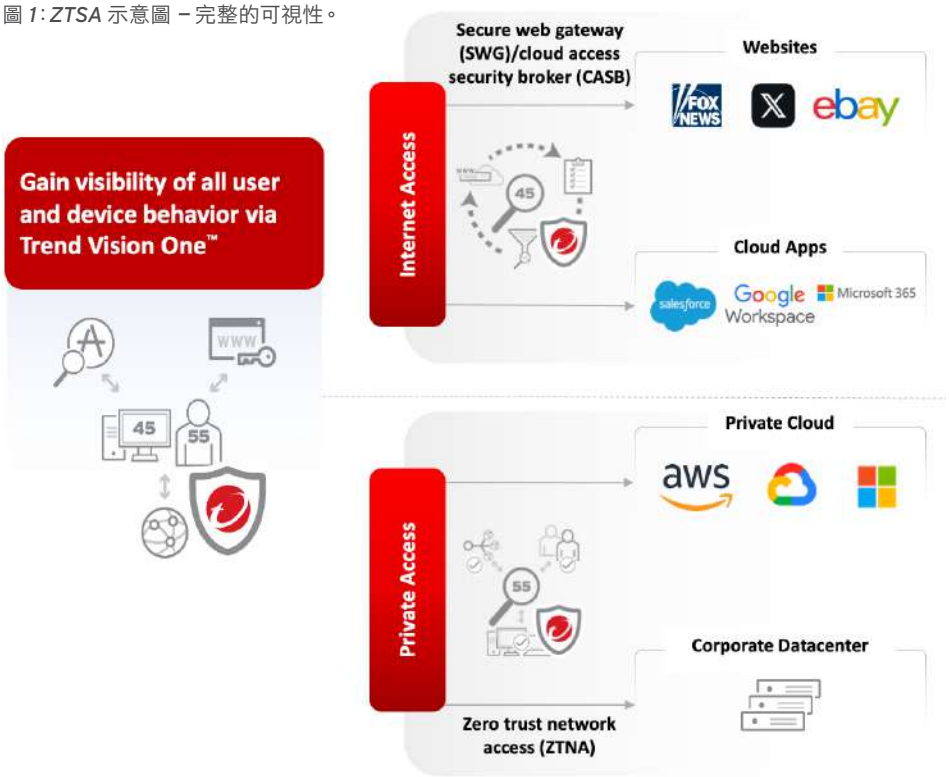
Zero Trust Secure Access (ZTSA)

藉由集中式數位防護管理來整合所有的政策、風險回應以及可視性

在今日無時無刻不連上網路的世界，許多企業都在轉換或已經轉換至混合或遠端作業模式。但隨著數位攻擊面的擴大，資安風險也跟著升高，因此過去那種「原則上信任、但要先驗證」的作法再也不切實際。面對今日隱匿又狡猾的駭客以及持續演變的威脅情勢，預設普遍信任的方法與實務作法再也不足以保障您的營運安全，您需要有效的驗證機制來協助您降低資安風險。

您可採用 Trend Vision One™ – Zero Trust Secure Access (ZTSA) 來安全地連接使用者、裝置和應用程式，不論他們位於何處，或者需要存取什麼。透過靈活的存取控管來強化您的防護措施，提供精細的可視性、更好的安全性，以及持續的風險評估。保護您使用者的存取過程以及與生成式 AI (GenAI) 的互動，驅動零信任架構來支援您的業務目標。

圖 *1*: *ZTSA* 示意圖 – 完整的可視性。



與我們 AI 驅動的 Trend Vision One 平台整合

Trend Vision One 整合了 ZTSA 以及我們專門的攻擊面風險管理 (ASRM) 與延伸式偵測及回應 (XDR) 功能。有了 Trend Vision One，您將擁有持續的適應性風險與資安評估來強化和支援您的防護策略。相對於安全服務邊緣 (SSE)，ZTSA 為您提供了 SWG、CASB 與 ZTNA 功能，使您能夠全面保護使用者和裝置，涵蓋網路、網站、雲端、私有應用程式以及 AI 服務。

建置強大又涵蓋您整個企業的存取權限控管來強化您的整體資安狀況，全部透過單一整合平台來完成。

主要效益：

- 掌控使用者與裝置的網路存取。
- 建置管理嚴格的存取權限控管來保護使用者和資料。
- 提高您的風險韌性，同時簡化資安與網路團隊的作業。
- 透過持續的風險評估洞見來改善可視性與回應時間。
- 有自信地在您的企業內擁抱 AI 並保護使用者的存取過程。

何謂零信任？

零信任資安模型改變了企業架設及維護網路的方式。

零信任不再預設信任從某些網路位置存取資源的使用者，而是假設任何異於常態的存取方式都有可能是駭客入侵。因此，所有使用者、裝置與資產之間的連線都必須先經過檢查來加以授權和認證。

不僅如此，還必須對裝置進行完整的評估來判斷其風險與資安狀況之後，才允許它連上您的網路。

圖 2：*Trend Vision One™– Zero Trust Secure Access (ZTSA) – AI Service Access* 示意圖。

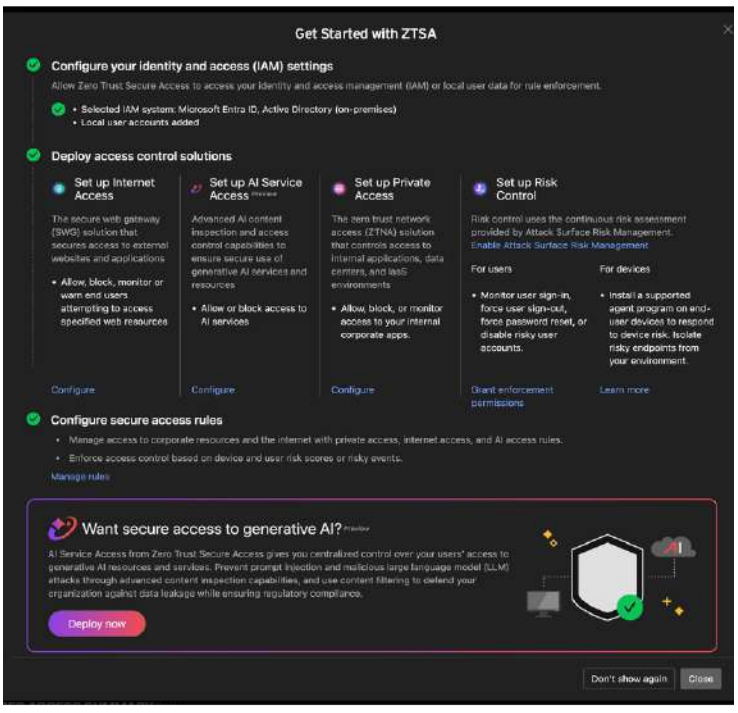
消除 GenAI 服務與安全存取之間的鴻溝

企業既可將 AI 應用在業務與資安營運當中，同時又能防止 AI 遭到惡意濫用。在存取公有或私有 GenAI 服務時，可透過零信任原則來強制實施存取控管。

ZTSA – AI Service Access 能控管 AI 的使用情況並檢查 GenAI 的提示與回應內容，它可偵測、過濾及分析內容以避免公有雲和/或私有雲環境內可能發生的機密資料外洩，或不安全的輸出。提高可視性以便更有效監控及管理您企業的 AI **使用情況，在使用者存取的過程中利用提示注入偵測來協助您防止潛在的資料外洩和攻擊。如此便可降低** GenAI 服務遭駭客操弄所帶來的潛在風險。

有了 ZTSA – AI Service Access，您將擁有更好的防護來保護使用者的存取過程並簡化操作，讓使用者與 GenAI 的互動更安全、更流暢，同時還確保符合法規。改善您的整體資安狀況、業務韌性、擴充性、卓越營運，以及使用者體驗。

圖 3：*ZTSA* 新手指南。



Trend Vision One　ZTSA

雲端原生且具備風險感應能力的 Trend Vision One 讓您在單一平台當中同時擁有 ASRM、XDR、ZTSA 以及多層式資安功能。藉由更好的可視性與更廣泛的風險感應能力來支援您的網路與資安團隊，協助他們專注於策略性資安措施，而非管理複雜的基礎架構。

讓 ZTSA 來協助您保護網際網路、軟體服務 (SaaS) 應用程式以及/或是 GenAI 工具的存取。運用 XDR 輔助的進階數據分析以及 ASRM 驅動的持續性風險評估，根據使用者風險狀態的改變來動態允許 (或撤銷) 存取權限。

> 一套簡化、整合的方案，並採用單一代理程式來提供 XDR　CASB 和 ZTSA 功能，再加上簡單明瞭的定價方式，將協助客戶避免部署 SASE 時經常面臨的複雜性。
>
> 451 Research
> S&P Global
> Market Intelligence

取得洞見、提升管控、降低風險

導入持續性風險評估

風險隨時都在變化，因此必須被持續評估才能形成一種有助於提升資安狀況的機制。為此，我們的 Trend Vision One™ – Attack Surface Risk Management (ASRM) 解決方案為 ZTSA 提供了持續性風險評估。ASRM 會利用我們的端點代理程式與網路工具來蒐集監測數據和資料並自動做出判斷。

來自 ASRM 的風險評分資料，可依規律的間隔或動態即時產生來評估您當前使用者、裝置與應用程式之間的連線。假使風險評分超過了自訂的門檻，連線就會被切斷以避免您的網路曝露於風險。當風險回到容許範圍時，就能重新建立連線，讓您安全地繼續作業。

圖 *4*：使用者存取過程示意圖。

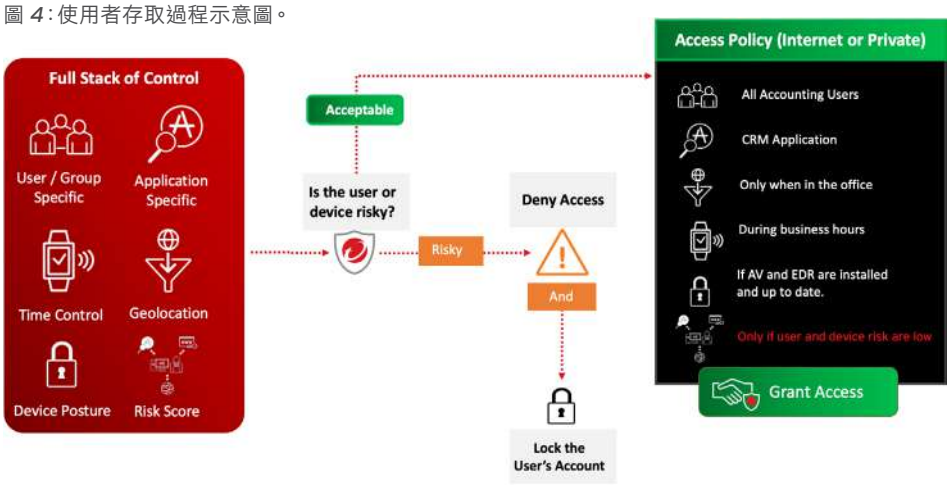
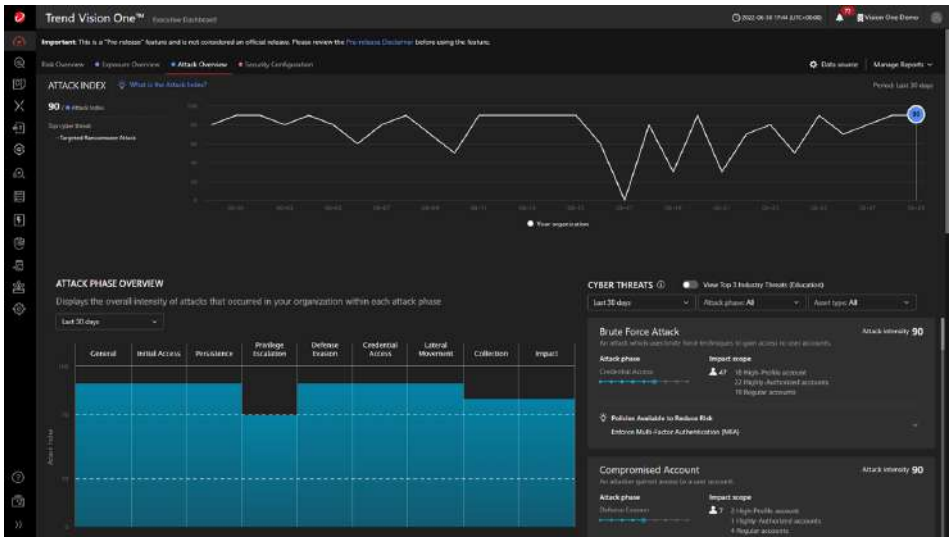


圖 *5*：*Trend Vision One* 高階主管儀表板 *(Executive Dashboard)* 中的攻擊階段總覽。



> 企業對於自己的網路架構往往都有一種『自然而然的信任感』，零信任可以防止駭客利用這種信任感。

Eric Skinner
市場策略副總裁，趨勢科技

重新思考您對企業內部的信任

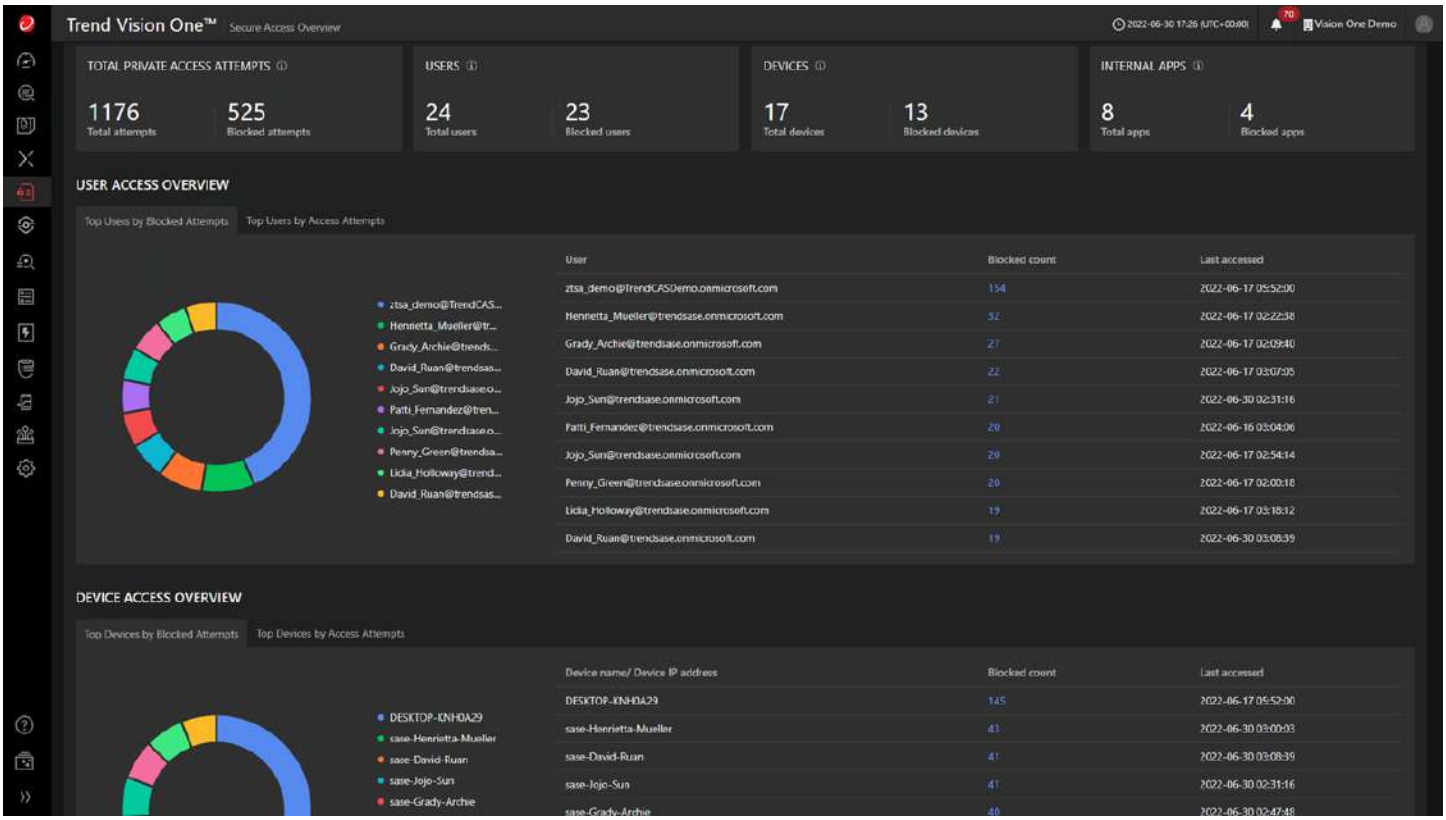
在許多企業中，預設信任是標準常態。但這會讓您的企業曝露於嚴重的風險當中，因為只要有一個使用者帳號遭到入侵，駭客就能對您的環境造成破壞，並且在您的網路內部四處遊走。

如同數位轉型一樣，邁向零信任是一個漸進的過程，而非一套解決方案。視您企業最迫切需要解決的風險以及您目前的資安狀況而定，您一開始可先從四個重要步驟著手。當然，企業在邁向零信任架構的過程中還會出現更多其他應用情境，但您一開始可採取的步驟包括：

1. SWG：利用即時的洞見來保護網際網路存取

- 提供「有代理程式」和「無代理程式」的防護來保障網站瀏覽安全，防止存取未經核准的應用程式。
- 為 Trend Vision One 提供豐富的情境資料以提升可視性。
- 提供網際網路存取與網頁瀏覽可視性，讓企業重新掌握資安與政策的控制權。
- 同時保護企業裝置與個人自備裝置 (BYOD)。
- 原生整合至 Trend Vision One 當中
- 擁有趨勢科技網站信譽評等服務、Trend™ Research 以及 ASRM 在背後支援。

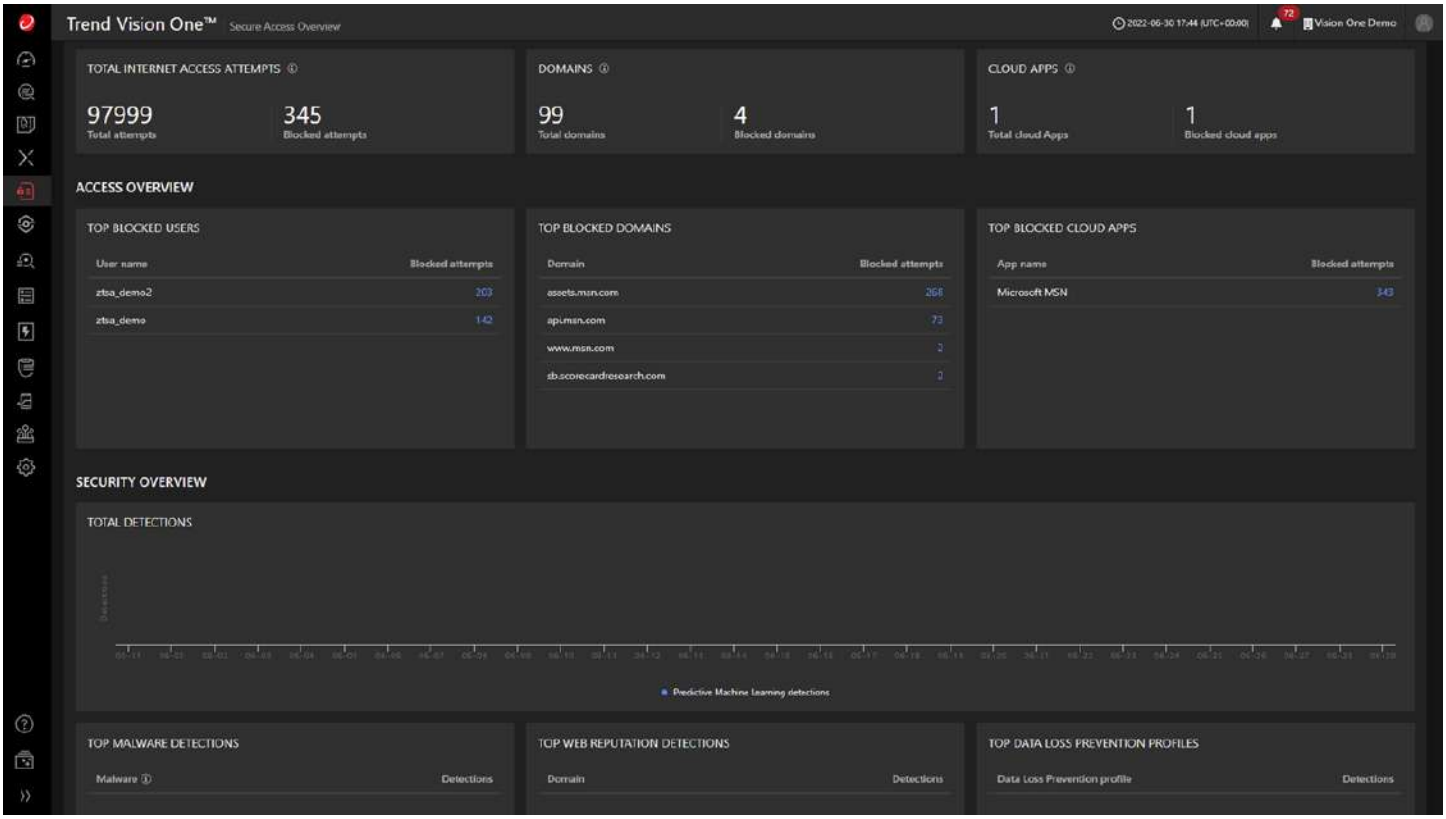
圖 6：*Trend Vision One* 內的 *ZTSA*。



2. CASB：安全的雲端應用程式存取與控管

- 為經過核准的 SaaS 應用程式提供有代理程式和無代理程式的防護。
- 提供安全的 SaaS 應用程式存取，檢查是否有違反政策的情況以及資安風險。
- 降低資料與關鍵資訊遭未經授權存取的風險。
- 透過精細的雲端應用程式動作控管來監控應用程式活動。
- 運用 ASRM 來提供持續的風險評估。
- 在 Trend Vision One 當中提供一套容易管理的介面。

圖 7：*Trend Vision One* 當中的 *ZTSA* 網際網路存取控管。

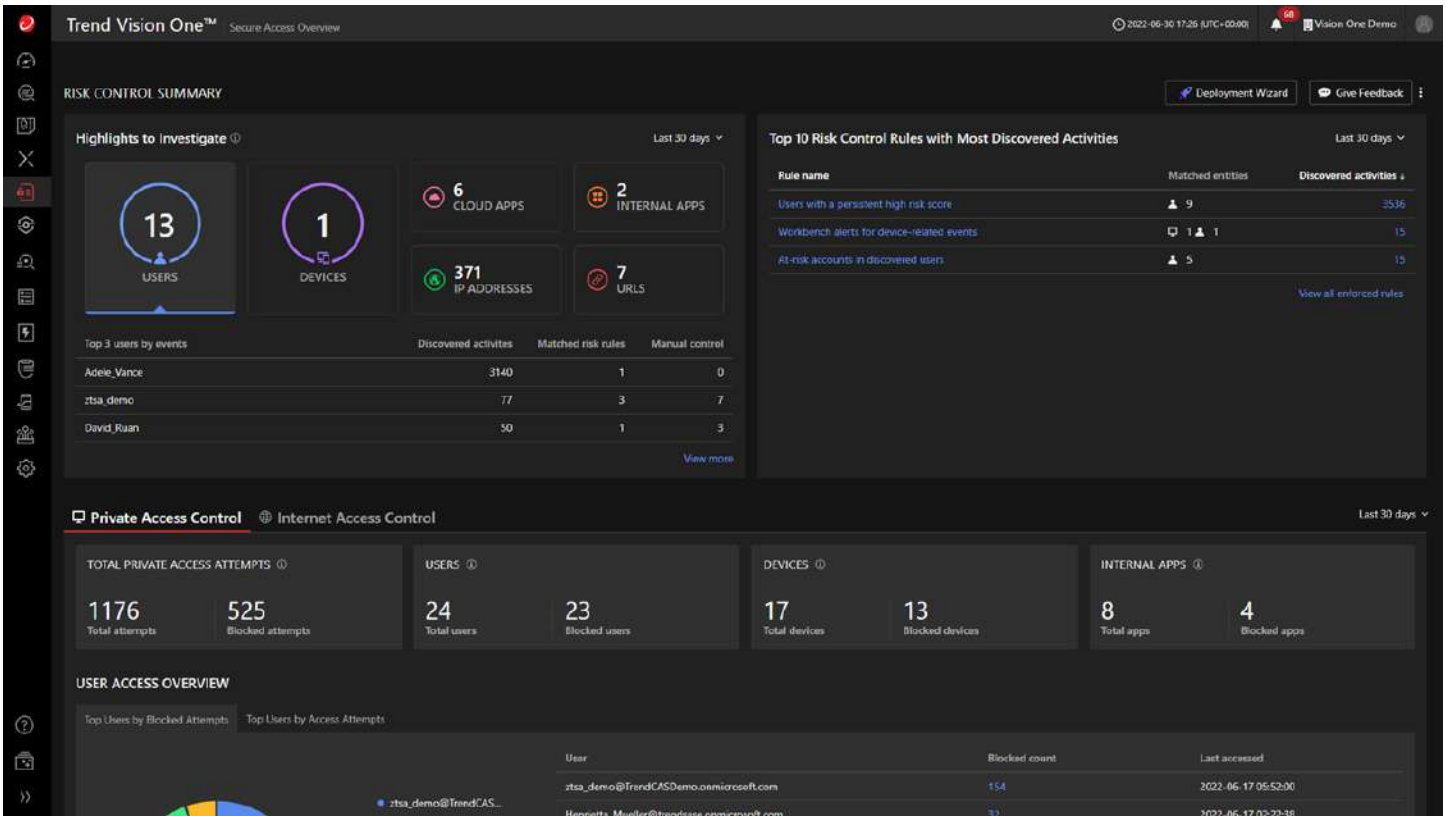


3. ZTNA：利用現代化方法來保護營業關鍵資源的存取

- 提供有代理程式與無代理程式的存取控管，透過精細的控管選項讓使用者輕鬆存取應用程式和資源。
- 縮減虛擬私人網路 (VPN) 的預設信任以改善風險評估。
- 提供通過認證、安全、即時 (just-in-time) 的應用程式與資源存取來提升防護。
- 縮小衝擊範圍，萬一遭駭客入侵可限制駭客只能存取某部分的網路。
- 運用 ASRM 來提供持續的風險評估。
- 藉由持續的風險評估來控管應用程式與資源的連線，隨風險程度的變化而動態允許或撤銷存取。

有別於 VPN 會提供整個網路的存取權限，ZTSA 提供的只是一個存取特定應用程式與資源的閘道，任何其他不相干的網路資源都無法存取。如此一來，萬一有合法使用者的登入憑證遭到竊取，也能控制駭客可存取的企業資源，這等於限制了任何攻擊的衝擊範圍。

圖 *8*：*Trend Vision One* 當中的 *ZTSA* 私人存取控管。



4. ZTSA – AI Service Access：保護使用者存取 GenAI 服務的過程

- 管控 AI 應用程式的使用情況，套用持續的風險導向存取規則，並掌握精細的可視性。
- 檢查 GenAI 服務的提示和回應以避免潛在的資料外洩和不預期的回應。
- 偵測提示注入攻擊來降低 GenAI 服務被操弄所帶來的潛在風險。
- 避免私有模型的阻斷服務威脅。
- 提供安全的 GenAI 應用程式存取，檢查是否有違反政策的情況以及資安風險。
- 降低資料與關鍵資訊遭未經授權存取的風險。

圖 *9*：*Trend Vision One* 當中的 *ZTSA – AI Service Access*。

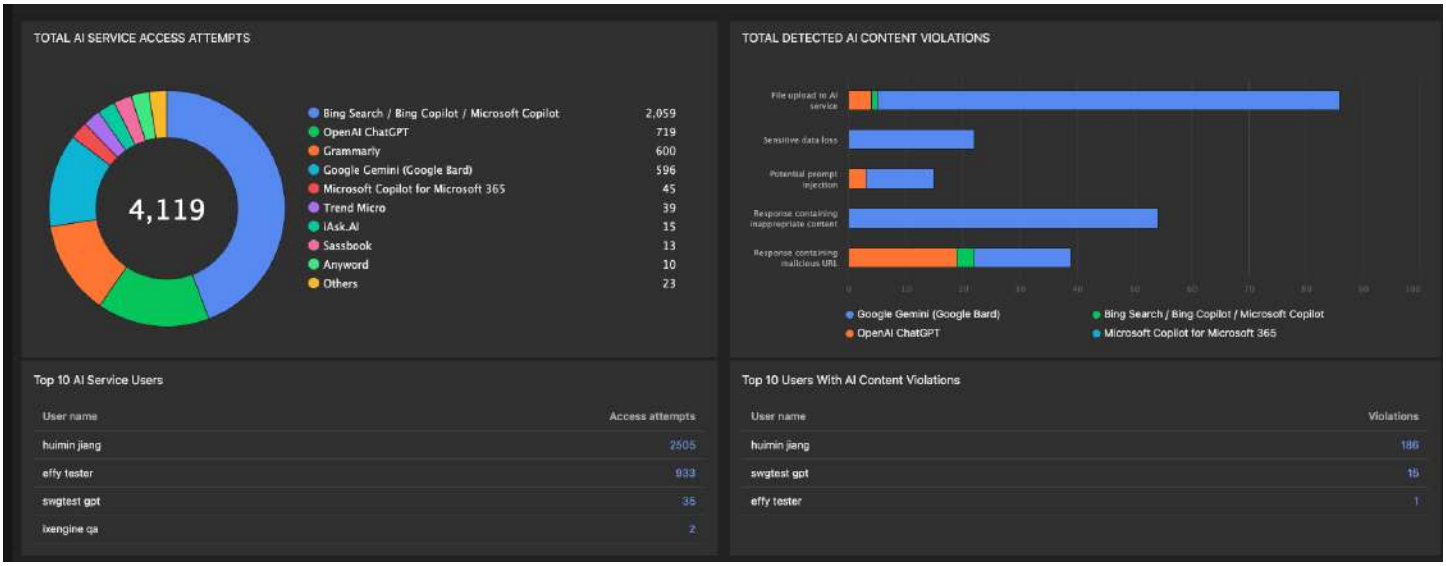
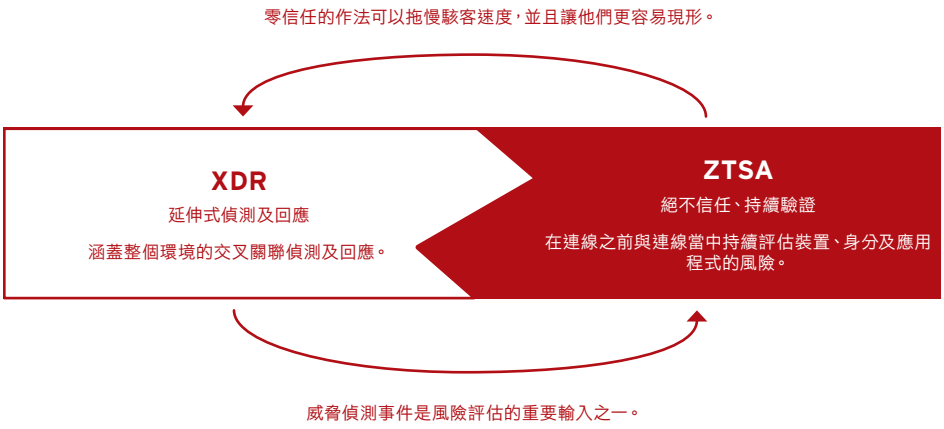


圖 *10*：使用 *ZTSA* 時 *XDR* 與 *SSE* 之間的關聯。



› 取得平台試用