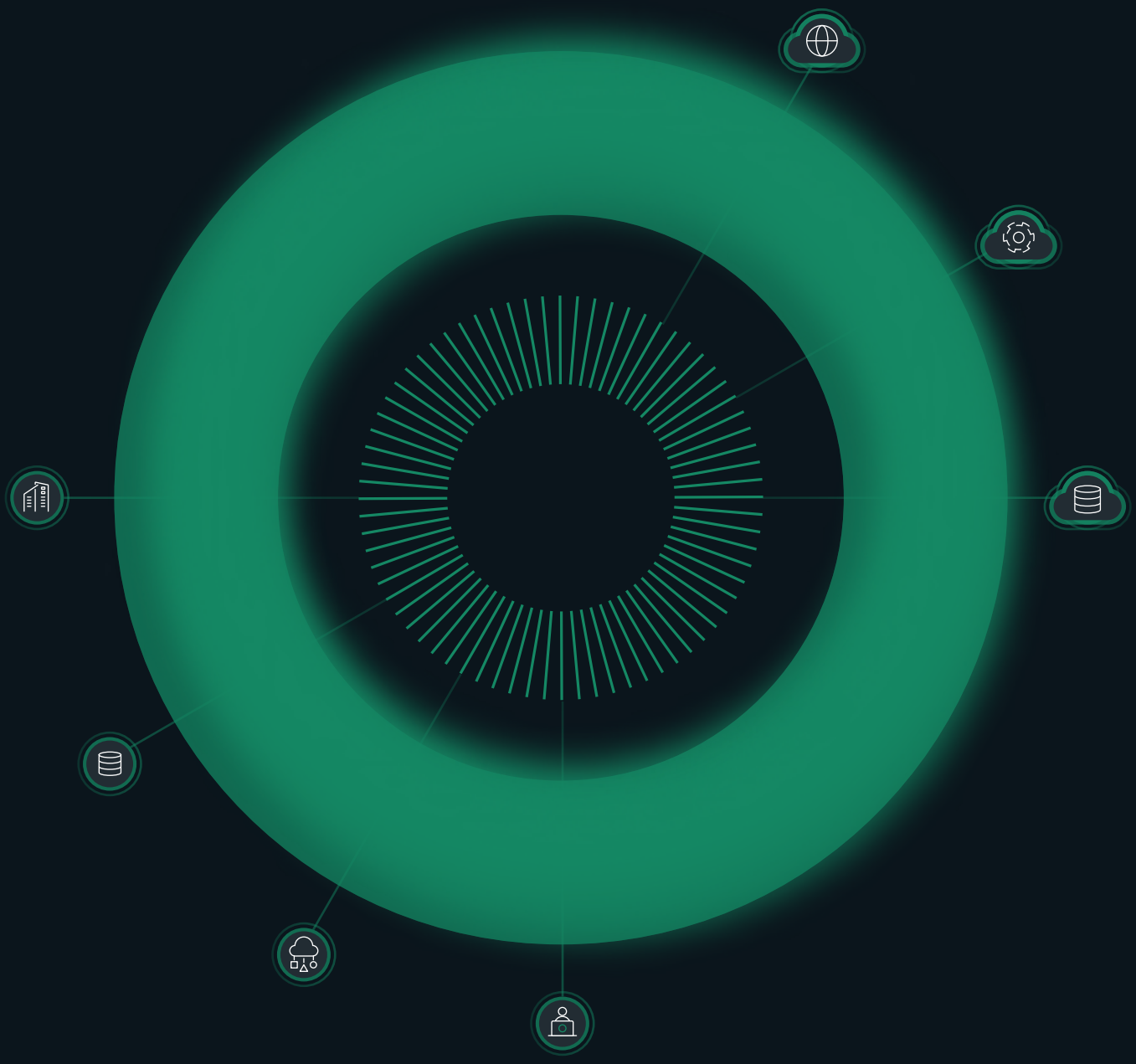
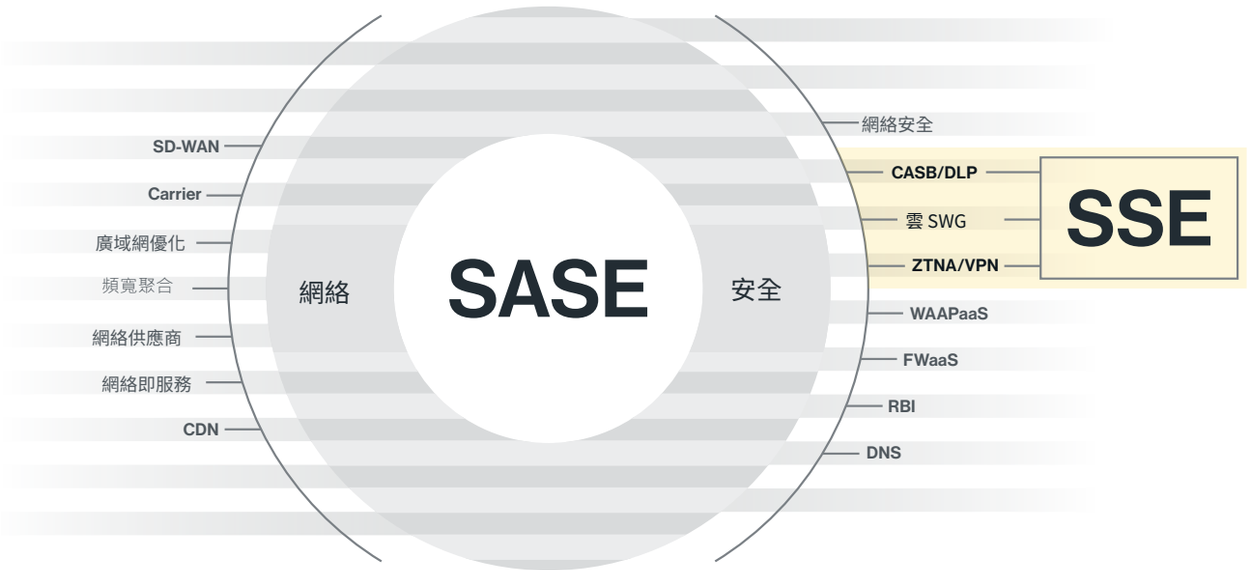
CATO
NETWORKS

Cato SSE 360

對所有流量、用戶和應用程序的全面可調性和控制



SSE、SASE 和 IT 融合之路



2019 年，Gartner 推出了安全訪問服務邊緣 (SASE) 類別。 SASE 定義了將 WAN 邊緣 (SD-WAN) 和網絡安全這兩個不同的技術市場融合到一個全球雲服務中，該服務可以為任何用戶、任何位置和任何應用程序提供安全和優化的訪問。 SASE 的安全支柱包括安全 Web 網關 (SWG)、具有數據丟失防護 (DLP) 的雲訪問安全代理 (CASB)、零信任網絡訪問 (ZTNA) 以及作為雲服務提供的防火牆即服務 (FWaaS)。

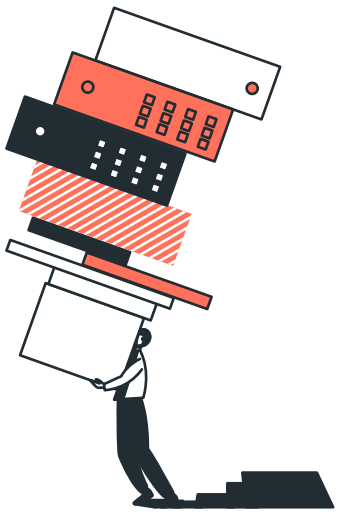
兩年後，Gartner 推出了一個名為安全服務邊緣 (SSE) 的新類別，以描述專注於網絡安全的更有限的融合範圍。 SSE 將三個安全組件 SWG、CASB/DLP 和 ZTNA 融合到一個雲服務中。 SSE 提供對應用程序的安全訪問，而無需直接解決該訪問的端點到端點優化網絡連接和東西向 WAN 安全方面的問題。 這些仍然是獨立技術堆棧的一部分，包括 SD-WAN、下一代防火牆 (NGFW) 和全球網絡主幹等技術。

客戶現在面臨如何處理其 IT 基礎架構的“融合未來”的決定。 一些組織將從一開始就尋求完全的 SASE 融合。 其他人將通過多個步驟來實現完全 SASE 融合，首先是在現有網絡基礎設施之上由 SSE 驅動的安全轉型，然後在後期階段進行網絡轉型項目的 SASE。 對於大多數企業來說，使用單一供應商 SASE 保持這條完整的轉型路徑是開放的，是一項戰略決策。 總而言之，融合越深入，可見性、安全狀況、操作簡單性、成本節約和業務敏捷性就越好。

在本文中，我們將探討 Cato SSE 360 涵蓋的功能、優勢和用例、Cato 的 SSE 實施以及全面 SASE 轉型的路徑。

傳統安全架構影響敏捷性、風險、資源和技能

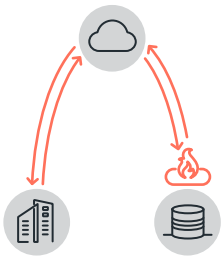
當今的企業依賴於日益混合的勞動力對本地和雲中的應用程序和數據進行優化和安全的全球訪問。使用脫節的單點解決方案和設備構建的剛性安全架構，無法適應新興的業務和技術要求以及不斷變化的威脅形勢。導致業務敏捷性降低，並且由於缺乏資源、稀缺的網絡安全技能和高昂的外包支持成本而使風險增加。



傳統架構造成的數字化轉型的主要障礙

傳統網絡是圍繞實體公司位置構建的

這種設計模式迫使網絡重新架構，以支持物理和雲數據中心的內部應用程序、公共雲應用程序以及用戶隨時隨地的安全訪問。



集中式（backhauling）安全模式減慢了安全的雲訪問速度

隨著互聯網和雲綁定流量的增加，驅動所有流量通過數據中心防火牆不再有意義。 必須在每個位置啟用直接安全 Internet，直至單個遠程用戶，以便在不影響用戶體驗的情況下擴展對所有應用程序訪問的完全可見性和控制。

傳統安全解決方案無法擴展並支持在任何地方的工作

支持多分公司需要一個靈活且可擴展的安全架構，該架構可以保護整個企業員工，無論他們在哪里工作：辦公室、路上和家裡。

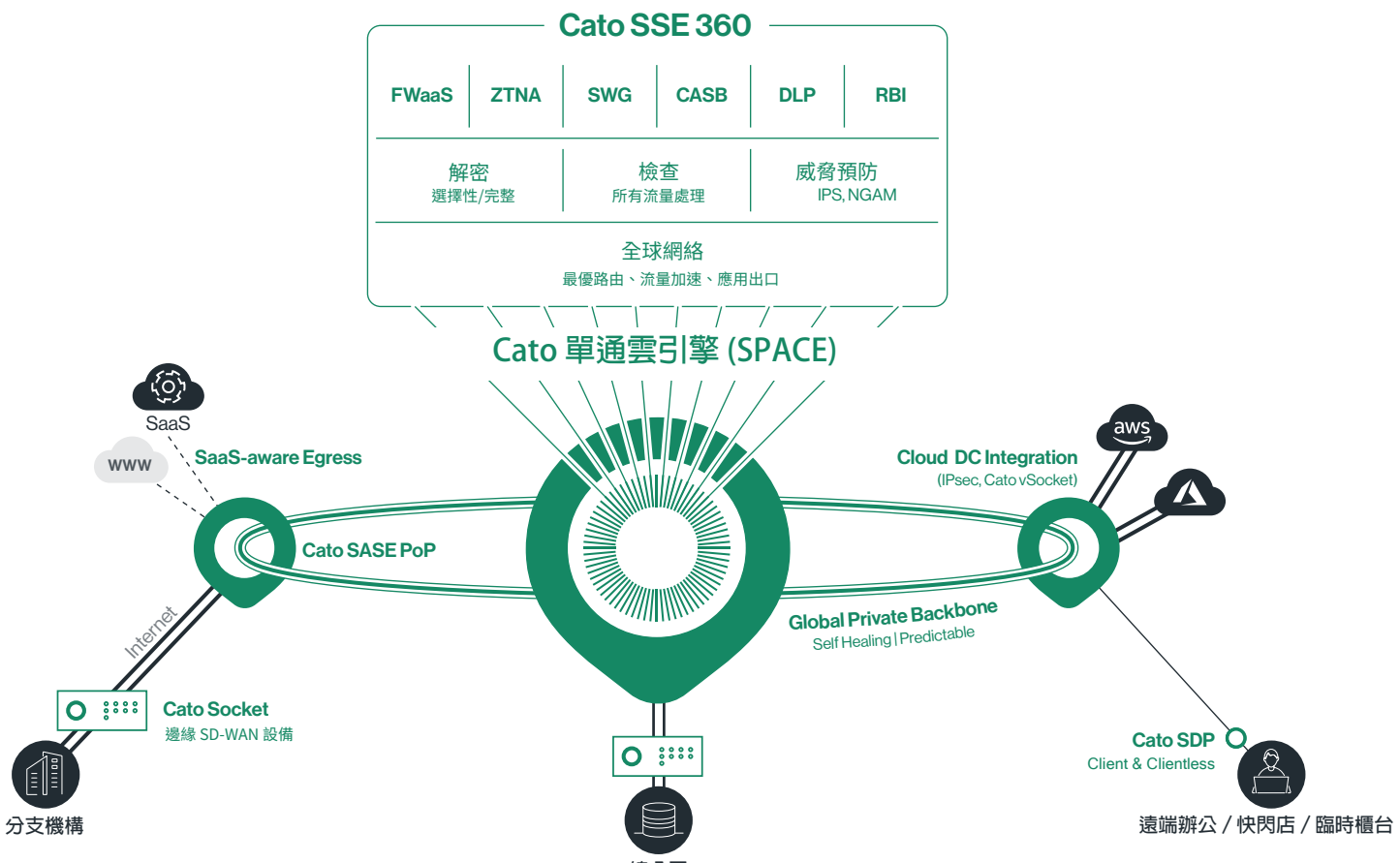
脫節的解決方案引入了碎片化和復雜的管理

雲中的安全整合和架構融合，減少了 IT 部門保持安全基礎設施，正常運行並處於最佳安全狀態所需的工作。 隨著工作轉移到為所有客戶運行雲平台的專家團隊，因工作量而出現錯誤或疏忽的可能性降低了。

這些都是架構和結構問題，另一種解決方案無法解決的話。 企業應考慮使用正確的安全服務邊緣 (SSE) 架構進行安全轉型來解決這些問題。

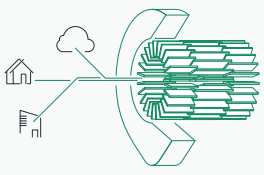
Cato SSE 360:
超越 Gartner 的 SSE

安全服務邊緣 (SSE) 使企業能夠從僵化和脫節的 IT 架構轉向作為雲服務交付的融合安全平台。 借助 SSE，企業 IT 可以快速滿足新的業務和安全要求，例如雲遷移、採用公共雲應用程序以及在任何地方工作。 SSE 的融合架構通過單一管理平台、自我修復基礎架構和可無縫緩解新興威脅的自動演進防禦，通過簡單的管理降低了成本和復雜性。 客戶可以選擇自己管理他們的基礎設施，也可以與他們首選的合作夥伴共同管理。



平台概述

Cato SSE 360 是 Cato 的 SSE 實施，它使 SSE 超出了 Gartner 定義的範圍。 它具有以下組件：



雲原生安全服務邊緣

Cato SSE 360 使用 Cato 單通道雲引擎 (SPACE) 架構構建，該架構是 Cato 全球融合雲原生服務的基礎。 當前的融合功能不僅包括 SWG、ZTNA 和 CASB/DLP，還包括具有高級威脅預防（IPS、下一代反惡意軟件）的完整防火牆即服務 (FWaaS)。 將 FWaaS 與其他融合功能結合使用，Cato 能夠將全套 SSE 控制應用於所有流量。

Cato 全球私有骨幹

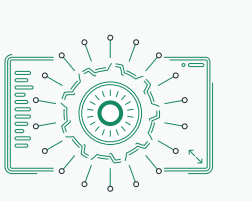
一個由 70 多個 PoP 組成的全球性、地理分佈、SLA 支持的網絡，由多個一級運營商和互聯網交換所互連，與 500 多個網絡和服務提供商對等。 每個 PoP 運行全套 Cato SSE 360 功能，以確保連接的用戶和位置的延遲最小。 此外，骨幹網還提供全局路由優化、自我修復功能、WAN 和雲優化，以實現最大的端到端流量和完全加密。

Cato SDP 客戶

輕量級客戶端將用戶設備連接到 Cato SSE 360，以優化和安全地訪問 Internet、內部應用程序、本地和雲中以及全球公共雲應用程序。 Cato 提供為筆記本電腦、智能手機和平板電腦的客戶端，以及無客戶端瀏覽器訪問選項。

支持 IPsec 的設備和 Cato Socket SD-WAN 位置

物理和雲位置使用任何支持 IPsec 的第三方設備或 Cato Socket SD-WAN 設備連接到 Cato SSE 360。 Cato Socket 提供最後一英里的彈性和服務質量 (QoS)，並使用基於應用程序的動態路徑選擇和數據包丟失緩解來克服停電和斷電。



綜合管理應用程序分析和策略配置

Cato 為客戶提供用於安全和網絡分析的管理應用程序，以及完整的細粒度策略配置。 如果適用，Cato 或其合作夥伴提供託管服務選項，包括站點部署、智能最後一英里監控、網絡配置和安全策略更改以及託管檢測和響應 (MDR)。

關鍵用例、功能和優勢

通過使用 Cato SSE 360，企業可以解決廣泛的用例並獲得多種戰略能力。
這些包括：

可擴展的混合工作

Cato 使用 Cato SDP 客戶端、Cato Socket 或無客戶端訪問，為世界各地的所有用戶、位置和應用程序提供安全和優化的訪問。 所有流量均受 Cato SSE 360 保護，並使用全球私有骨幹網進行優化。 Cato 的全球足跡和彈性雲原生架構支持訪問模式的巨大轉變，用戶可以在辦公室、旅行和家中自由漫遊。 因此，Cato SSE 360 克服了基於設備的 VPN 和安全解決方案的物理限制。 客戶使用 Cato 來消除單點解決方案的成本和復雜性，包括設備和基於雲的安全服務，例如 VPN、防火牆、CASB 和安全 Web 網關。

逐步雲遷移

Cato 可以輕鬆地將物理和雲數據中心連接到 Cato SSE 360，並優化對公共雲應用程序的訪問。 流量由 Cato SSE 360 檢查，並使用“中間一英里”的全球私有骨幹網進行優化。 這是通過“smart egress”功能實現的，該功能允許客戶定義應用程序級規則，以在最接近為組織服務的目標實例的指定 PoP 處退出特定應用程序流量。 借助 Cato，客戶可以消除 AWS DirectConnect 和 Microsoft ExpressRoute 等高級雲連接解決方案。

保護敏感數據

Cato SSE 360 的 CASB 和 DLP 可實現對敏感數據的全面可見性和控制。 Cato 對來自公司和 BYOD 設備的數據訪問實施細粒度策略，根據設備狀態和所需的訪問級別限制訪問，並控制跨應用程序的數據共享。 借助 Cato，客戶可以降低敏感數據丟失和聲譽影響的風險，並更好地遵守法規要求。

即時部署安全能力

現在和未來的所有安全功能都融合到 Cato SSE 360 中，並且可以通過“輕按開關”進行部署，無需複雜的集成、容量規劃和多個管理控制台。 所有安全策略和分析均通過單一管理平台進行管理，並保證在當前部署定義的地理位置、容量和彈性下工作，無需進一步規劃。 客戶使用 Cato 來消除單點解決方案的成本和復雜性，包括設備和基於雲的安全服務，例如 VPN、防火牆、CASB 和安全 Web 網關。

面向未來和零維護的安全性

Cato SSE 360 是自我維護、自我進化和自我修復的。 Cato 消除了與維護本地基礎設施相關的繁重工作，並使用尖端的安全專家團隊來保持 Cato SSE 360 的最佳安全態勢以應對新出現的威脅。 Cato MDR 通過持續搜尋和修復網絡上的常駐威脅進一步增強了客戶資源和技能。

Cato SSE 360 如何擴展 SSE

Cato SSE 360 通過提供對所有流量的完全可見性和控制、在不依賴公共 Internet 的情況下優化全球應用程序訪問以及實現完全單一供應商 SASE 部署的無縫路徑來擴展 SSE。

Cato SSE 360 提供對所有流量的全面可見性和控制

大多數 SSE 平台基於 Web 代理架構，僅用於檢查 Internet 和公共雲應用程序流量。 SSE 無法檢查非 Web 流量以及通過應用程序連接器支持的 ZTNA 流量。 因此，它無法解決與威脅相關的風險，例如跨 WAN 的惡意軟件傳播以及與非人為產生的流量相關的威脅。

相比之下，Cato 的基於網絡的架構將所有企業資源連接到一個安全的雲網絡中。 Cato 旨在檢查通過 Cato 雲網絡的所有端口和協議的所有流量。 因此，無論來源（用戶、設備、機器、應用程序等）或目的地（內部或外部應用程序，在本地或在雲中）。 Cato 基於網絡的架構將我們的安全研究和機器學習算法可用的可見性和控制擴展到更廣泛的實時流量，並提高了 Cato 檢測和預防數據洩露風險的能力。

Cato SSE 360 優化全球應用程序訪問

Cato SSE 360 利用 Cato 的全球私有骨幹網來優化來自世界任何地方的本地或雲中的應用程序訪問。 骨幹網是一個全球性的、地理分佈的、由 75 多個 PoP 支持的 SLA 網絡，由多個一級運營商和與 500 多個網絡和服務提供商對等的互聯網交換互連。 每個 PoP 運行全套 Cato SSE 360 功能，以確保連接的用戶和位置的延遲最小。 此外，骨幹網還提供全局路由優化、自我修復功能、WAN 和雲優化，以實現最大的端點到端點流量和完全加密。 與典型的 SSE 不同，Cato SSE 360 可以跨主幹網（“中間一英里”）運行應用程序流量，而不是將其丟棄 Internet，以確保優化用戶體驗。

Cato SSE 360 支持通往完整單一供應商 SASE 的無縫路徑

客戶可以通過部署 Cato SSE 360 進行安全轉型，利用現有的 WAN 邊緣設備實現 Cato SSE 360 連接，開始他們的 SASE 之旅。通過將部署擴展到 Cato Socket SD-WAN 設備，Cato 可以消除分支機構和數據中心 WAN 設備，例如路由器、防火牆、第三方 SD-WAN 和 WAN 優化。 此擴展支持將網絡功能和策略整合到 Cato SASE 雲中，包括頻寬管理、最後一英里彈性和監控以及應用程序服務質量 (QoS) 管理。基於雲的安全性和 WAN 邊緣的融合推動了成本、複雜性和管理開銷的大幅降低，同時提高了彈性和端點到端點的可見性。

Cato SSE 360 vs. SSE: 選擇正確的解決方案

Cato SSE 360 通過提供對所有流量的完全可見性和控制、在不依賴公共 Internet 的情況下優化全球應用程序訪問以及實現完全單一供應商 SASE 部署的無縫路徑來擴展 SSE。

	SSE	Cato SSE 360
核心能力		
ZTNA零信任	●	●
• 客戶端和無客戶端	●	●
• 設備勢態	●	●
• 多重認證	●	●
• 針對威脅的持續流量檢查	○	●
SWG	●	●
CASB/DLP	●	●
• Inline	●	●
• SaaS API	●	●
具有全面威脅預防的 FWaaS	○	●
所有功能的統一架構	○	●
管理		
與啟用 IPSec 的設備或 SD-WAN 設備連接	●	●
“單一窗口”管理	●	●
自維護平台	●	●
自我修復平台（雲可用性）	◑	●
經驗證可快速適應不斷變化的威脅	◑	●
流量能見度		
互聯網：網站	●	●
互聯網：公共雲應用程序 (Office 365)		
WAN：雲 DC 應用程序（AWS、Azure、GCP）	● 特定於應用程序的連接器	●
WAN：物理 DC 應用	● 特定於應用程序的連接器	●
所有端口和通訊協定	○	●
流量控制		
SSL解密	●	●
互聯網流量	●	●
廣域網流量檢測	●	●
帶解密和全面檢查的最大吞吐量	1gbps	3gbps
預防威脅		
進入 **(Web)**	●	●
外出 **(Web)**	●	●
廣域網傳遞	○	●
所有端口和通訊協定	○	●
威脅檢測		
安全事件收集	●	●
報告導出的安全事件	●	●
託管檢測和響應	○	●
優化全球訪問		
帶“中間一英里”控制的全球私有骨幹網	○	●
雲應用訪問優化	● peering	● egress
廣域網應用流量優化	○	●
SASE 融合之路		
無縫擴展至單一供應商 SASE	○	●
SD-WAN, FW, Routers, Wan Opt 的設備消除	○	●
支持 SD-WAN	○ 夥伴	●

全面 SASE 轉型之旅始於 Cato SSE 360

安全服務邊緣 (SSE) 正在改變分散的安全堆棧，這正在減緩許多企業的數字化轉型。 ZTNA、SWG 和 CASB 的融合是應對這一挑戰的正確步驟。 然而，SSE 本身是建立在傳統技術之上的，這些技術旨在保護基於 Web 的應用程序。 因此，典型的 SSE 產品對來自網絡設備、物聯網和應用程序的非 Web 流量和非人工流量視而不見，並且對保護對內部應用程序的訪問的支持有限。 此外，他們忽略了訪問的性能方面，主要依賴不可預測的公共互聯網作為應用程序訪問傳輸。

Cato SSE 360 通過全面的流量可見性和控制擴展了 SSE 功能。 簡而言之，Cato SSE 360 “sees”所有端口、協議、源和目的地的所有流量，並將其全方位的訪問控制、威脅預防和數據保護功能應用於該流量。 建立在全球私有主幹上，應用程序訪問通過可預測和可靠的傳輸進行了全面優化，該傳輸同樣適用於物理數據中心、雲數據中心和公共雲中的應用程序。

Cato SSE 360 為客戶在單一供應商平台上無縫完成其完整的 SASE 轉換奠定了良好的基礎。 通過擴展 Cato SSE 360 實施 Cato Edge SD-WAN，客戶可以替換第 3 方路由器、防火牆、SD-WAN 和 WAN 優化設備。 這種安全和網絡的融合進一步降低了成本、複雜性、風險和管理開銷。

SD-WAN. SSE 360. SASE. 隨心所欲。

聯繫我們