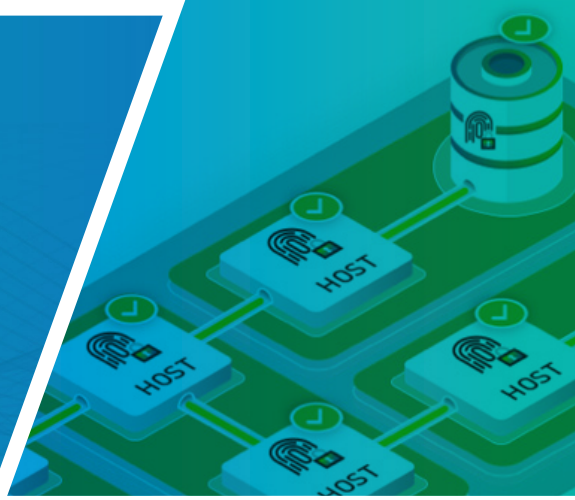
資料表

ZSCALER工作負載分段

一鍵零信任

公共雲和資料中心的自動微分段



微分段極其簡單

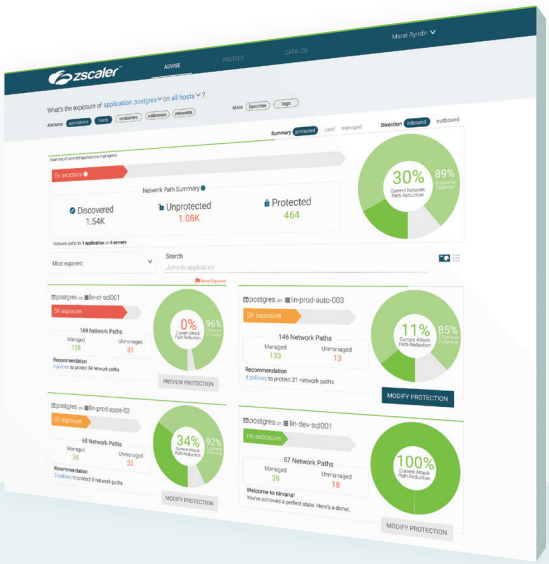
網路威脅需要攻擊路徑才能到達易受攻擊的目標。減少網路攻擊面的最有效方法是分段，專家們認為微分段是工作負載的核心保護策略。但是，在過去，實施分段所需的時間、複雜性和成本超過了安全受益。

但現在不是了。

Zscaler工作負載分段是對環境進行微分段的一種新方法。它非常簡單，只需點選一下即可。透過允許 Zscaler工作負載分段來揭示風險並將基於身份的保護應用於您的工作負載，就可以降低風險，免除任何操作，並且無需對網路進行任何架構更改，也無需進行重啟。Zscaler的工作負載分段軟體基於身份的模型透過自動適應其運行環境的政策來提供無間隙保護。消除網路攻擊面從未如此簡單。

Zscaler工作負載分段價值

- 提供東西向網路通信的全面可視性
- 基於身份的專利政策可以適應您的動態環境
- 基於代理的保護可以最大程度地提高安全和性能
- 毫不費力地優化降低風險和簡化運營政策
- 可證的安全投資回報



> “...在某個時候，Zscaler工作負載分段可以部署在世界各地的每家公司。”
>
> goulston&storrs

應用感知控制的好處

雲和資料中心網路中充滿了資料，極易引來網路犯罪分子的攻擊。儘管您的邊界控制功能強大，但網路犯罪分子仍可以透過網路釣魚或其他形式的社會工程來存取您的網路。如果使用傳統的基於網路的安全性原則，一旦攻擊者竊取了憑據或利用漏洞獲取網路的存取權，他們就可以“依靠這片土地維持生活”—引入惡意軟體並在可信的網路通信路徑內橫向移動來獲取關鍵應用的未經授權的存取權限。網路折衷可能會造成極大的破壞，造成深遠的財務、聲譽和運營損失。為了防止未經授權的東西向通信，組織需要以 已批准應用程式的驗證身份為中心的安全控制措施。

Zscaler工作負載分段使用基於通信軟體的加密身份的零信任安全控制使企業可以感知應用程式，並保護任何網路免受應用折衷的損害。

採用零信任方法

Zscaler“工作負載分段”零信任、工作負載基於身份的方法放棄了傳統的允許基於可信的 IP位址、埠和協定進行應用程式通信的安全模型。我們的零信任模型將內部通信視為網際網路：暗藏敵意並充滿威脅。只有透過其加密身份驗證的應用程式和服務才被允許發送和接收通信，從而提高了安全性，不論您的應用程式在哪裡，都可以確保其安全。

有專利權的基於身份的自動分段

傳統的微分段涉及多個步驟，可能需要幾個月的時間。Zscaler工作負載分段微分段僅需短短幾分鐘即可完成 – 點選一下即可。從資產清單到映射資料流程再到部署實施政策，我們的微分段既快速又簡單。

Zscaler工作負載分段透過一個全新的控制平面（軟體身份）保護混合雲中的關鍵資料和應用程式。在 Zscaler工作負載分段管理的環境中的所有軟體均使用加密身份屬性的組合進行指紋識別。軟體身份是每個存取控制決策的基礎。根據我們的零信任模型，如果軟體無法透過驗證，則無論以前的許可權如何，它都無法通信。這樣就可確保為您的工作負載提供最強級別的保護，而不論網路發生怎樣的變化。

透過自動重新分段保護新引入的應用程式

雖然自動分段非常適合加快微分段的初始部署，但確保新引入的應用程式也受到保護也同樣重要。這些新應用程式可能具有全新的通信路徑，並且還可能與現有的應用程式服務進行交互，所有這些都需要受到保護。Zscaler工作負載分段透過一次點選即可實現自動重新分段，從而使保護這些新應用程式變得非常簡單。Zscaler工作負載分段以您現有的分段為基礎，並建議新的或修改的政策來覆蓋新的應用程式通信，所有這些操作只需點選一下即可實現。自動分段和自動重新分段一起可以確保始終為您的動態環境提供保護。

這種新的方法論意味著安全控制可以適應任何環境，而且需要管理的政策更少。Zscaler工作負載分段零信任自動分段功能為混合雲提供更強大、更簡單、可擴展的保護，具有以下六個區分屬性：

自動構建政策

透過壓縮政策降低風險

安全結果可證

透過加密屬性驗證軟體身份

分段適應應用程式更新和更改

安全監控工具豐富了應用程式資料

零信任身份

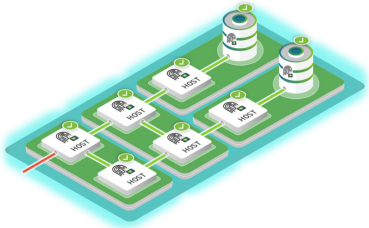
推動 Zscaler工作負載分段自動微分段的技術基於零信任身份 (ZTID)。組成工作負載身份的身份屬性包括SHA256雜湊、模糊雜湊、可執行檔簽名、PE標頭值、UID、CPU序號、配置的主機名稱等等。每個唯一身份都會通知機器學習，該機器學習將構建推薦的政策並用於存取控制決策。由於 Zscaler工作負載分段政策為零信任，因此只有可以透過其 ZTID驗證的軟體才可以在您的網路上進行通信，從而創建一個更安全但運營效率更高的網路。

操作更簡單

一鍵立即對您的環境進行微分段。您的業務應用程式將自動受到保護並可以運行。無需更改網路。無需手動構建或更新單個政策。冗長的部署安排已成為歷史。

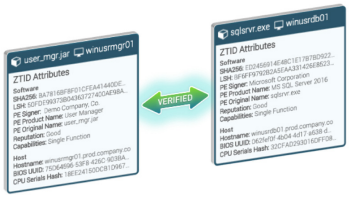
安全性更強

根據通信軟體的相互依賴性 (而不是 IP位址) 定義微分段邊界。透過驗證軟體身份來授權雲和資料中心中的通信，從而防止惡意軟體傳播和濫用管理工具，並確保只有有效的業務應用程式才能通信。



可擴展用於 DevOps

在部署工作負載時，請確保它們始終具有實現平穩業務運營所需的存取權限。隨著環境的自動擴展，Zscaler工作負載分段政策會在本地或公共雲中的所有 VM和 Kubernetes容器上自動適應。



為您的多雲、混合雲環境提供集中管理

Zscaler工作負載分段可為所有的環境提供最廣泛的支援，不論它是本地的裸機、虛擬化的私有雲、公共雲還是它們的任意組合。環境可以是靜態的，也可以是高度動態的。Zscaler工作負載分段支援 Linux的10個發行版本（具有800以上補丁級別，可追溯到2.6）、Windows 7及更高版本以及任何 Windows伺服器作業系統。支援的容器環境包括Kubernetes、Docker和 AWS彈性容器服務 (ECS)。

Zscaler的工作負載分段持續自我調整平台和產品由 API驅動。Zscaler工作負載分段可以與現有的安全工具和DevOps流程集成，從而實現一鍵式自動分段。

Linux Windows Windows Server kubernetes docker Amazon ECS

Azure Google Cloud Platform aws vmware

Zscaler工作負載分段用例

用於雲工作負載保護的零信任

從一個中央平台保護所有雲環境上的關鍵業務應用程式。

確保法令遵循的零信任微分段

將應用程式劃分為“安全區域”，以在違規發生之前查看並阻止違規行為。

提高可視性的資料流程映射

視覺化應用程式拓撲，並查看何時發生更改。

容器安全

在不中斷 CI/CD工作流程的情況下，保護短暫生產環境中的應用程式。

事件關聯和安全監控

將應用程式通信日誌傳送到您的 SIEM中，從而啟動修復優先次序。

關於Zscaler

Zscaler（納斯達克股票代碼：ZS）加快了數位化轉型，使客戶可以變得更加敏捷、高效、靈活和安全。Zscaler零信任交換透過安全連接任何位置的用户、設備和應用程式保護成千上萬的客戶免遭網路攻擊和資料丟失。在全球，基於SASE的零信任交換分佈在150多個資料中心中，是世界上最大的內聯雲安全平台。

Zscaler, Inc.
霍爾格路120號
加利福尼亞州95134聖約瑟市
+1 408.533.0288
www.zscaler.com