網路連結+資訊安全化繁歸簡

軟體定義且基於雲端的安全強化企業網路

網路連結+資訊安全
化繁歸簡

內容摘要

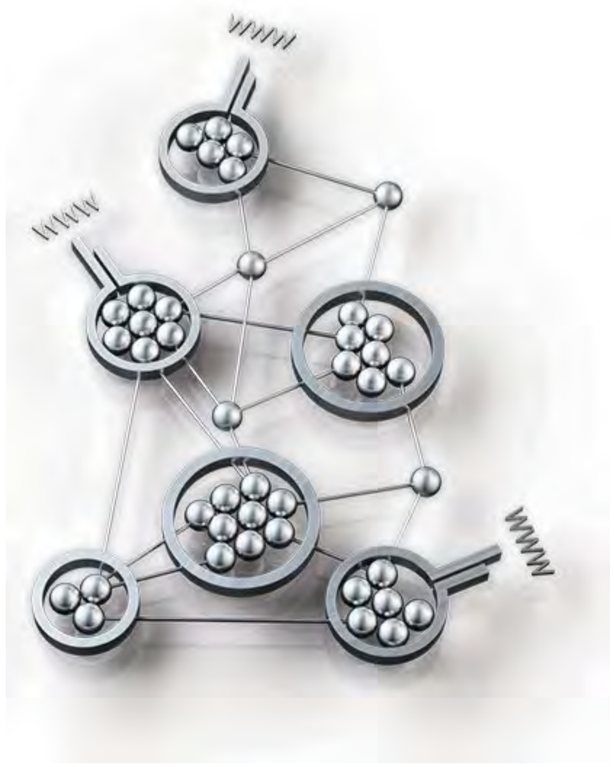
不久之前，管理和保護企業網路是件簡單的事。 我們建置一個單純的網路用來連通外點與企業內部建置的應用程式即可。達到網路安全標準也很簡單，只需在網路邊界部署一個防火牆，還有在端點上安裝防毒軟體即可，

現今實際情況已經改變.

日益分散的企業分點使得建置連通全球的網路成本不斷提高，並由於網路覆蓋了多個位置，因此網路安全部署也變得更加複雜。接下來的問題是雲端，行動化和物聯網。資料和應用程式遷移到雲端。行動存取和BYOD也變成通用模式。網路的簡單架構部署模式正在被破壞，網路的邊界已經崩解。這種轉變已經發生且伴隨著進化和提高複雜程度的網路攻擊。

無邊界網路的資訊安全是一件複雜的任務

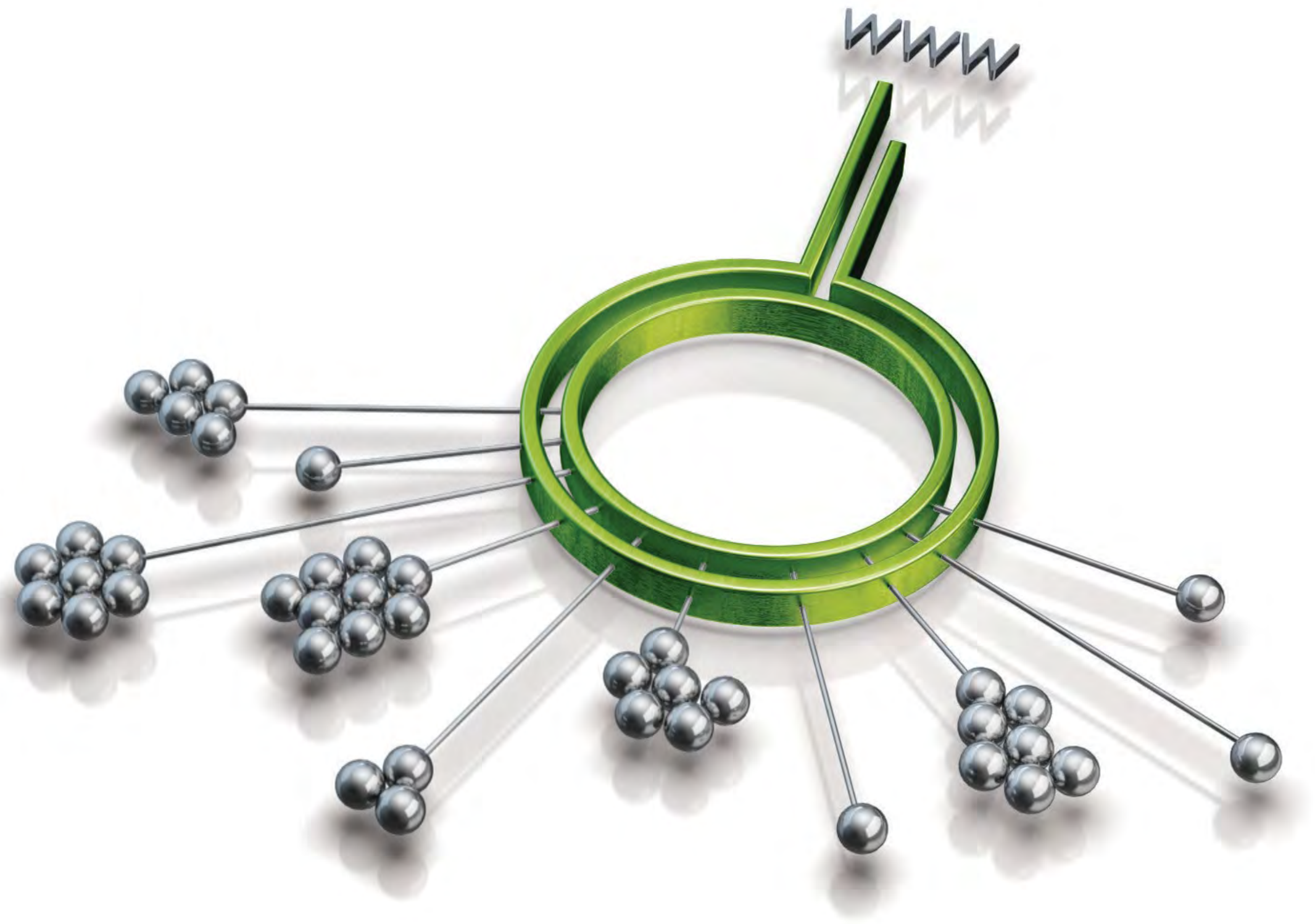
安全設備遍及整個企業， 解決提出新需求的外點新增解決方案不是簡單使用現有解決方案就好。安全防禦團隊受到壓力包含了維護眾多跨產品線的安全策略，管理非常態的網路拓撲，例如複雜的站點到站點mesh架構和流量集中回傳架構，整合與確保新的公有雲基礎架構安全性； 還有管理直接存取互聯網並規避網路安全政策的行動用戶。



數量增加且分散的企業使全球網路連接變得非常昂貴，而且使得網路安全更加複雜

架構底層的全球網路也遭遇了重大挑戰，尤其是在大量耗用頻寬的影片和語音通信成為標準業務需求的時代。無法負擔MPLS網路的組織只能依靠無法控制的internet來存取，這具有無法預測的延遲和用戶體驗。隨著全球分佈的擴大，大型分佈式企業的網路成本爆增。現在，雲端基礎架構和行動用戶已成為業務的關鍵部分，完全脫離了傳統WAN安全性和優化解決方案的範圍。

基於對如此複雜的網路進行管理和安全防護將變得越來越複雜的前提，Cato Networks將網路連結和安全防護放入設計的策略思考方向並將其導入雲中。 Cato首先在雲中重新確立網路邊界，因此網路拓撲變得既簡單又明確，因為只有這樣才能確保其安全性。



所有位置，基於辦公室的用戶和行動用戶，內部部署和雲端數據中心都連接到Cato Cloud Network：Cato Cloud Network：一個經過加密和優化的全球網路，可以最大程度地提高整個企業的最終用戶體驗和生產力。借由快速切換，客戶可以有選擇地啟用Cato的全部企業級安全服務，從而保護廣域網（WAN）和互聯網流量。現在可以在所有網路活動中實施統一策略，而不管源或目標是什麼

使用 Cato, 網路連結+資訊安全就是這麼簡單.

逐漸消失的網路邊界所帶來的挑戰

全球化，雲端計算和行動化化正在改變業務

在過去，連接業務很簡單。我們有一個清晰的網路邊界，將我們的辦公室，用戶和內部應用程式區隔在同一邊。保護網路安全也很簡單：在邊界設置防火牆，將“內部”（企業資源）與“外部”（公網）分開，然後你的網路就算是安全了。

現今這情況已經不再。三大主要力量消滅了網路邊界，造成當前的WAN和安全設備架構過時：全球化，雲端計算和行動化.

全球化使網路拓撲更加複雜。現在，我們需要將各個分點連接到一個單一的全球網路中。 為了保護它，我們必須在每個位置部署許多安全解決方案設備。

雲端計算的使用正在挑戰我們對企業應用程式和數據的控制。公有雲應用程式，本地端應用程式正在遷移到雲端應用程式，例如Office 365，Salesforce.com和Box.com。雲端基礎架構正在使用虛擬伺服器和儲存來替代實體數據中心。現在，我們必須處理分佈在多個位置的數據，有些數據超出了我們的控制範圍。

行動化讓我們的用戶找到了新方法來訪問企業資源，使用“自帶設備”（BYOD）讓個人和工作活動的界線開始混淆。我們控制這些設備的能力及其使用方式的能力卻是有限的。

三大主要力量消滅了網路邊界，使當前的廣域網路設備和安全設備架構過時：全球化，雲端計算和終端流動性。

廣域網路與資安設備在現代企業中的不匹配

網路和安全管理團隊必須使用其供應商提供的套裝工具來面對新的業務問題。這些問題導致了多個挑戰。

網路安全設備挑戰: 每個分佈式位置都必須由完整的安全堆棧覆蓋，其中包括防火牆，URL過濾器和反惡意軟件，以實現安全的Internet訪問。從資本支出和IT資源的角度來看，這是一項代價高昂的提議，許多組織（尤其是中型組織）負擔不起。被吹捧為解決此問題的UTM安全設備正在減少分支機構的佔用空間，但犧牲了容量和安全能力。

流量回傳Traffic backhaul: 為了避免設備氾濫，許多組織選擇將流量回傳到具有完整安全堆棧和安全Internet訪問的中央位置。通過MPLS回傳互聯網流量既昂貴又浪費，但是如果您不想部署分支機構安全設備來實現安全，直接的互聯網訪問，這是必不可少的。

複雜的站點到站點和站點到雲端配置: 為了將所有網路資源連接到企業網路中，IT安全性在辦公室防火牆之間配置了VPN隧道。此外，需要使用單獨的解決方案和流程來將雲資源連接到網路（Amazon AWS或Microsoft Azure網段），並使IT人員能夠對其進行管理。這是一個敏感的配置，應考慮多個訪問路徑和網路冗餘。錯誤可能導致嚴重的網路中斷，使IT部門不願接受更改，並導致過時的規則積累，從而可能造成安全隱患.

存取雲端資源的複雜保護方式，點解決方案爆炸式增長: 隨著新業務需求的出現，定點解決方案也應運而生。例如，對雲應用程序的越來越多的使用創建了新類別的雲訪問安全代理（CASB）解決方案。自然，它們部署在用戶和雲應用程序之間。但是，由於網路內部和外部都有許多訪問雲端的方法，因此部署變得非常複雜。 IT團隊必須使用代理和API的組合來保護所有不同的數據路徑。

行動用戶規避安全控制: 行動化員工團隊的擴展以及使用個人設備訪問業務數據（BYOD）進一步挑戰了傳統網路的安全性。行動用戶可以直接訪問Internet並規避網路強制的安全策略。迫使行動用戶透過VPN確保安全訪問Internet會造成性能和用戶體驗問題，特別是對於全球移動的使用者。這些問題確實會引起違反安全策略，讓用戶和數據之間的規矩進入“你的視線”，互聯網和雲訪問上實施訪問控制是解決邊界問題的標誌性挑戰

Cato Networks: 軟體定義與基於雲端的安全強化企業網路

Cato Networks由資深網路安全人員創立，旨在為各種規模的企業提供安全的網路，以支持全球性，分佈式，以雲端和行動化為中心的業務。

Cato已經確定了未來安全網路必須解決的三個核心挑戰：:

網路已經凌亂不堪：跨位置，數據中心，雲端環境和移動員工的網路分散性使其更難管理，優化和維護安全性。

網路安全無法跟上：網路安全必須能快速擴充，進化和快速自動調適。對任何正在尋找能抵禦越來越快和越來越複雜的網路攻擊的單位來說，這些條件都是至關重要的。

建置和維護安全網路的成本太高：由於安全預算受到廣泛檢視，因此從資本和資源密集型安全模型中進行根本性轉變是一項業務必需。

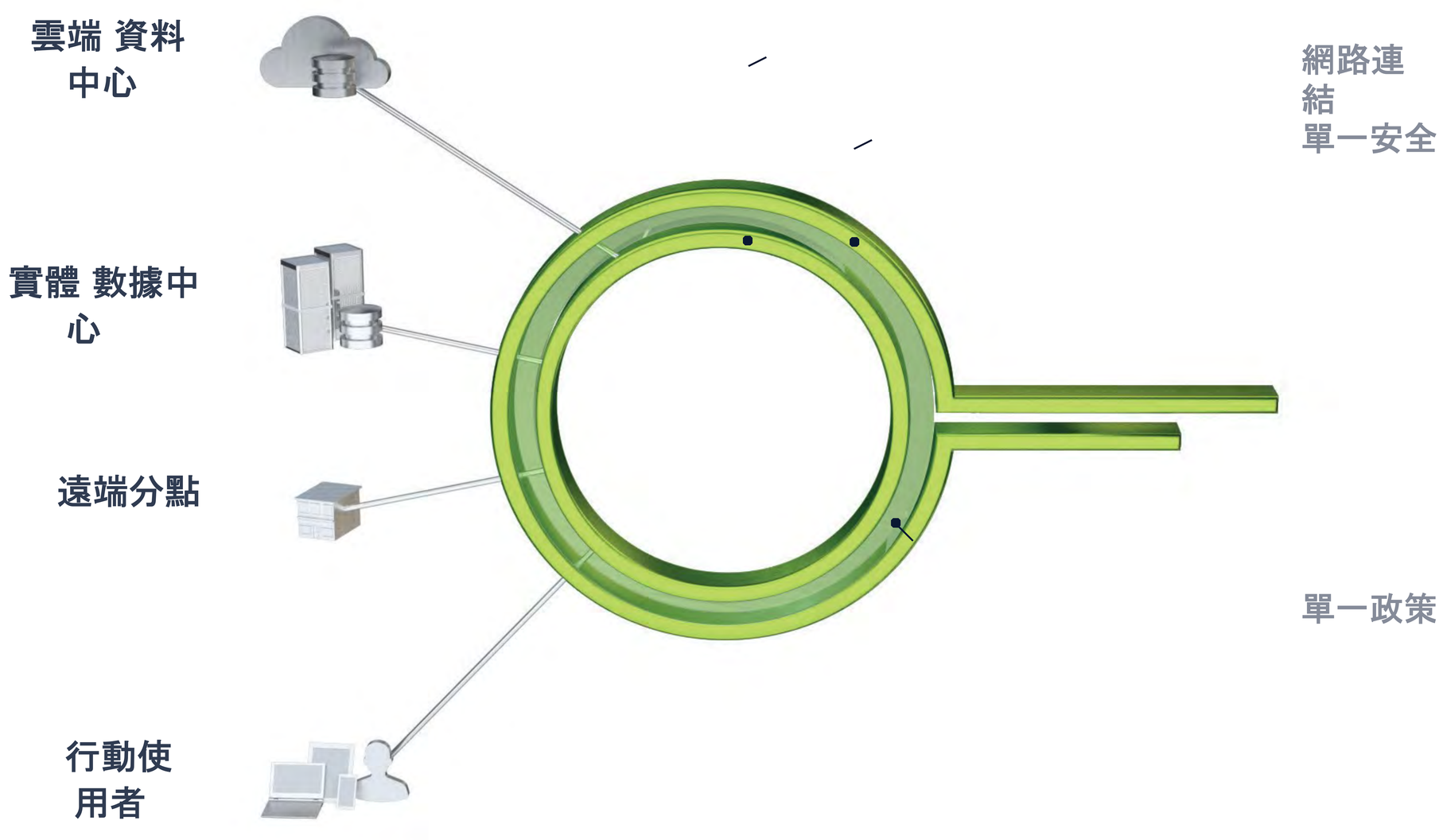
Cato採用三個步驟來提供安全的網路：

簡化網路：Cato首先在雲端中重新建立企業網路邊界，並將所有網路資源連接到雲端。解決了網路過於破碎的問題.

保護網路安全：Cato然後應用一組緊密結合的敏捷和彈性安全服務來保護網路。這滿足了快速發展安全功能同時降低本地安全基礎架構成本的需求□

強制部署統一策略：通過整合網路與安全層，不管來源（用戶，系統，位置）和目的地（內部，雲端或Internet）如何，可以在所有流量上部署公司安全策略。

Cato Networks建立了一個全新的平台，該平台從頭開始建立，以安全地連接現代企業為目標。它由兩個緊密結合的元件組成：Cato Cloud Network和Cato Security Services.



Cato Cloud Network: 全球化，加密和優化的企業網路骨幹

Cato Cloud Network是新企業網路邊界的代名詞，它將所有網路資源（分點，實體和雲端數據中心以及移動用戶）連結在一起。 除了LAN連結外，Cato Cloud Network負責所有WAN和Internet連結．

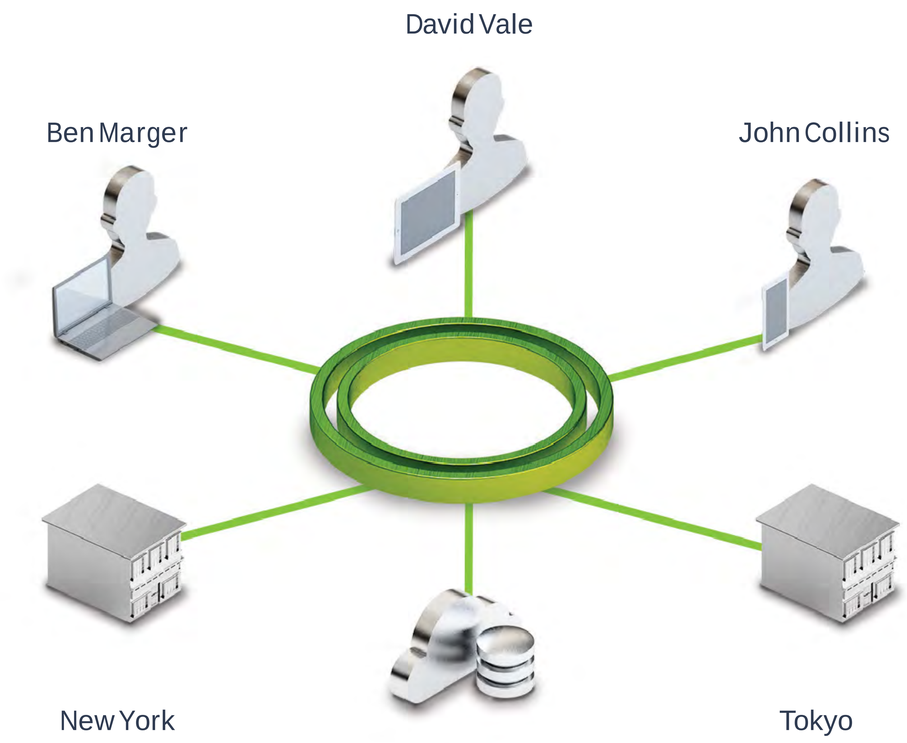
Cato PoPs 組成的全球網路骨幹網

Cato Cloud Network是一個由許多實體PoP組成的全球網路，由具有多個Gbps頻寬線路連接到Tire-1網際網路服務供應商所組成的主幹網。骨幹網中的流量是經過加密的，並且Cato還確保最佳的路由選擇和最小的延遲，這優於不受管理的Internet連接。 PoP旨在實現冗餘和高可用性，並無縫擴充以隨著容量增長調整。 客戶使用安全隧道將其網路資源連接到Cato Cloud網路。每個辦公室，資料中心，雲端資源或移動用戶都動態地連接到最近的PoP，並優化在Cato Cloud網路上享有對本地，互聯網和雲端資源的存取。

Cato Cloud Network是多個物理網路連接點（ PoP ）組成的全球網路，使用多個gigabit頻寬的線路連結到1級互聯網服務商組成的主幹網。

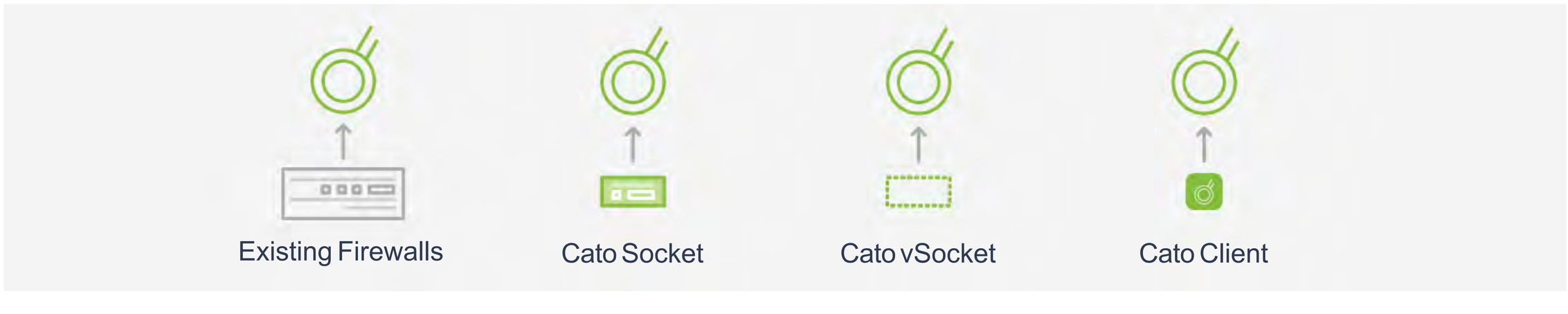
合而為一的邏輯企業網路

不論實體PoP還是網路資源如何連接。Cato建立了單一個邏輯企業網路。資源之間的連接規則在Cato Cloud中進行管理，而無需維護軸輻式系統配置。這種方法非常容易將新資源（新辦公室，新用戶或新雲端資源）接入網路並立即啟用對它的安全存取。



連接至Cato Cloud Network

透過現有互聯網連接，用戶有幾種方法可以建立連結到Cato雲端網路的安全隧道。客戶可以使用：



- 既有的防火牆：可建立VPN隧道到Cato Cloud
- **Cato Socket：**用於實體位置的隧道設備，可確保不中斷的存取距離最近且運作中的PoP，並支持多個Internet連接以實現最大冗餘。只需將電源插入插座，將網路線插上具有互聯網連結的網路，然後使用雲端控制台將其激活即可。
- Cato vSocket：Cato Socket的虛擬實例，可以連接Amazon AWS或Microsoft Azure中基於雲的虛擬服務器段。另外，Cato可以啟動到本地雲防火牆的IPSEC隧道，以實現零足跡整合。.
- Cato Client：用於筆記型電腦，平板電腦和移動設備的軟體。管理員發出電子郵件邀請後，這些邀請將移動用戶引導到自助服務設定過程中，以他們的設備註冊Cato Client。註冊後，將對公司資源的存取使用Cato Cloud進行隧道安全傳輸，並受公司安全策略管理。.

總的來說，Cato 雲端網路簡化了企業的網路拓撲。它解決了連結所有網路資源（實體，雲端和使用者）到一個有效率且安全的簡單統一網路的挑戰。
Cato創造了邏輯上是視為單一的企業網路。

Cato Security Service : 企業級彈性和敏捷網路安全

一旦將所有WAN和Internet流量合併到Cato Cloud網路中，網路安全就變得更加簡單，因為網路資源的分配不再使安全部署變得複雜。 Cato應用了一組緊密整合的Cato安全服務來保護所有網路流量。

針對雲端服務構建的敏捷且緊密整合的網路和安全性堆棧

Cato從頭開始構建了網路和安全性堆棧。每個Cato PoP都在運行整個堆棧，因此所有流量都經過加密，優化和保護。對PoP進行集中管理，並使用新功能無縫地更新Cato安全服務

Cato利用其無與倫比的可視化功能來監控多個網路的流量，以檢測新興威脅和主動威脅，並透過Cato Security Services透明，快速地制定和部署對策

每個Cato PoP都運行著完整的網路功能和安全性，因此所有流量都是經過加密，優化與安全的。

企業級安全服務

Cato Security Services 包含以下功能

次世代防火牆/VPN

- **從任何地方進行安全的Internet存取**: 可以從任何位置直接存取互聯網，消除了流量回傳
- **簡化Mesh連結**: 使用簡單的規則連接any-to-any位置
- **高效能和彈性**: 無需容量升級即可以數gigabit的速度保護流量
- **應用程式感知**: 識別網路對本地和雲端應用程序的存取，而不是考慮是哪個端口，網路協議，SSL 使用者感知: 識別用戶，群組和位置，而不是哪個IP位址
- **統一且細緻化的安全政策**: 控制對應用程式，伺服器和網路資源的存取

安全網站閘道

- **動態網站分類**: 包括一個URL資料庫，對網站進行了廣泛分類，包括網路釣魚，惡意軟體派送，殭屍網路和其他惡意網站
- **Web存取策略**: 強制執行與網路使用相關的公司政策
- **阻止，提示或跟踪用戶訪問**: 減少因存取風險網頁而導致的法律或安全風險

進階威脅防護

- **Anti-malware:** 掃描HTTP和HTTPS中的惡意文件並阻止端點感染傳播

安全雲端存取與行動存取

- **實施存取控制策略** - 移動訪問內部和雲端資源
- 將安全策略無縫**擴展到雲端基礎架構**

網路鑑識

- **詳細報告和監控**實時和歷史網路
- 收集和轉送完整的網路和安全事件日誌以進行外部分析

Cato 管理應用程式

Cato使Cato NOC / SOC團隊，託管服務提供商和客戶的IT人員能夠使用基於雲端的管理應用程式來：

- 根據位置，應用程式群組或用戶來深入了解與分析整個網路活動
- 根據業務需求部署網路使用政策
- 在整個企業中部署安全政策和資源存取控制
- 監視安全事件和網路使用情況告警