CATO NETWORKS

Cato 案例研究

銀行/信用合作社和金融服務

目錄

Guardian Credit Union 借助 Cato 改善網路控制及安全

防火牆即服務 • 成本合宜的 MPLS 替代方案

雲端應用程式需要更大的網路可見性，但不影響安全性或增加複雜性

Guardian Credit Union 是一家區域性企業，面臨著巨大的網路挑戰。該信用合作社需要改善其可見性和應用程式控制，但不會影響安全性，或使網路變得過於複雜而需要找一支專業資安團隊來操作。

如同許多公司，Guardian曾經依賴點對點、第 2 層連線的混合式架構來連接站點。MPLS 和Metro Ethernet network配置hub-and-spoke網路，將請求回傳至 Guardian 的中央資料中心，再從那裡通過一個設有安全防護的入口網站存取應用程式和資料。簡而言之便是那種傳統企業網路的複雜組態。

Guardian的技術副總裁 Scott Rosen 說道：「我擁有複雜環境方面的經驗，所以理解及支援這類網路難不倒我，但我也有其他事要做，我們的團隊也是。」

> **「我擁有複雜環境方面的經驗，所以理解及支援這類網路難不倒我，但我也有其他事要做，我們的團隊也是。」**

Scott Rosen,
技術副總裁

關於 Guardian Credit Union

位於阿拉巴馬州的信用合作社 Guardian Credit Union 擁有一個連接阿拉巴馬州十多個縣、20 個站點的私人網路。第 2 層網路混合MPLS 及都會乙太網路點對點連線，從資料中心連接至分支機構。雲端存取須經過中央資料中心的安全入口網站。應用程式包括語音及越來越多的雲端應用程式，例如 Microsoft 365 和 Zoom 等。

管理一個複雜的網路需要大量培訓，Rosen希望 Guardian 的 IT 運作團隊能免除這項要求。「這需要大量的時間和專業知識。你不可能出去上幾堂課就能了解網路在複雜環境中如何運作。」Rosen說。「所以對我們來說，轉移至 SD-WAN 不一定是爲了降低成本，雖然這確實會發生，但更重要的是提高網路的可見性。我們希望降低網路的複雜性，但能維持其防護能力及韌性。」

提高可見性對 Rosen 和他的團隊格外重要的一個原因，在於語音和雲端運算應用程式在 Guardian 這樣的私人網路中存在的難處。該公司對視訊會議、Microsoft 365 及其他應用程式的需求日益增加，因此在邊緣上提供服務品質 (QoS) 極其重要。

以 SD-WAN 取代 MPLS 需要安全保障

SD-WAN 提供一種簡化網路的方法，但這意味著隨處使用網際網路，其固有的風險顯而易見。「當我們捨棄私人連線之後，在所有地點提供網際網路連線 將使我們面臨暴露自己的危險。這是一個需要權衡的問題。我們如何才能降低此風險？」

這表示，在評估 SD-WAN 時必須將安全性納入考量。傳統網路設計上普遍認為廣域網路上傳輸的流量可信任的觀念必須被顛覆。「如果你信任分支機構與資料中心之間的流量，你的風險就會增加。如果分支機構有一個惡意軟體 (幸好我們從未有過) ，這個惡意軟體可能在網路上傳播。你必須檢查流量。」

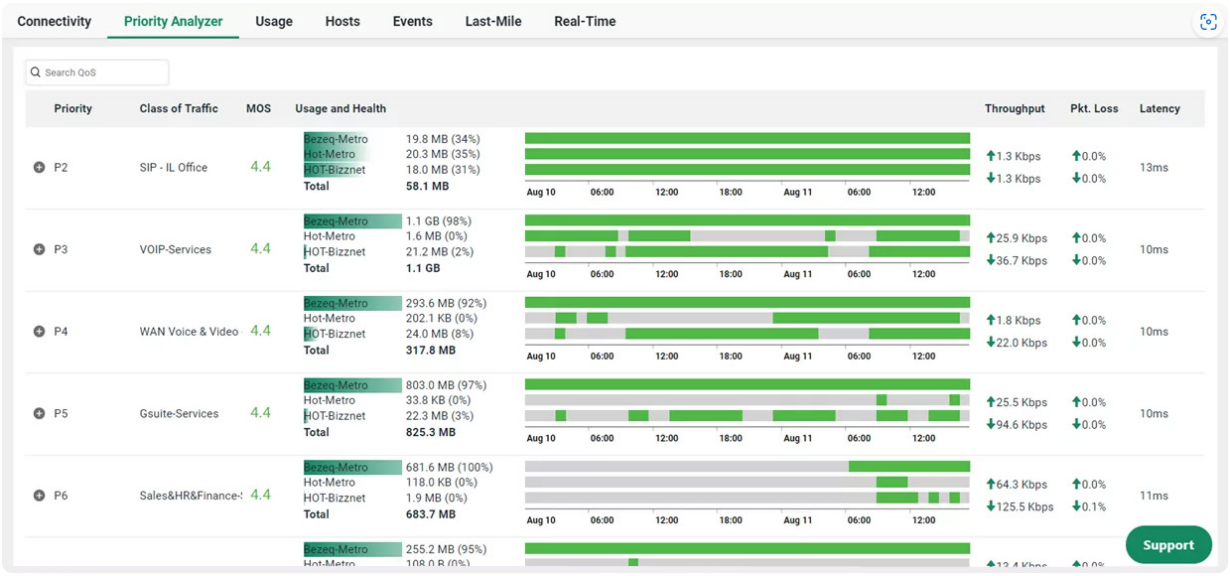
而此檢查必須在網路上進行。「你可以在電腦上使用終端控制，但這不能解決物聯網或那些可能與你控制的裝置使用不同作業系統的裝置。你需要在網路上設置檢查及控制機制。」

Rosen 考慮使用 SD-WAN 解決方案，但發現缺乏安全管理

Rosen 調查過傳統的 SD-WAN 解決方案，但這些替代方案均不是以安全為優先。「我們在評估時以「安全第一」爲優先考量，但傳統SD-WAN解決方案將安全功能作爲附加產品銷售，或需要另外購買安全解決方案。」

> **「我們在評估時以「安全第一」爲優先考量，但傳統SD-WAN解決方案將安全功能作爲附加產品銷售，或需要另外購買安全解決方案。」**

此外, 傳統的 SD-WAN 解決方案需要透過電信服務商或 ISP 為 Guardian 管理解決方案。 該信用合作社早已對電信公司的支援感到不滿, 因此不想讓電信公司承擔更多責任。 「讓他們修復現有提供的服務已經夠難為他們了。」Rosen 說道。「你已經遭遇問題, 而他們現在想要向你推銷整個一站式管理解決方案, 由他們管理你的整個網路。」



Cato 的 SASE 架構可讓 Guardian 設定流量的優先順序, 確保 VoIP 及其他應用程式獲得所需的頻寬

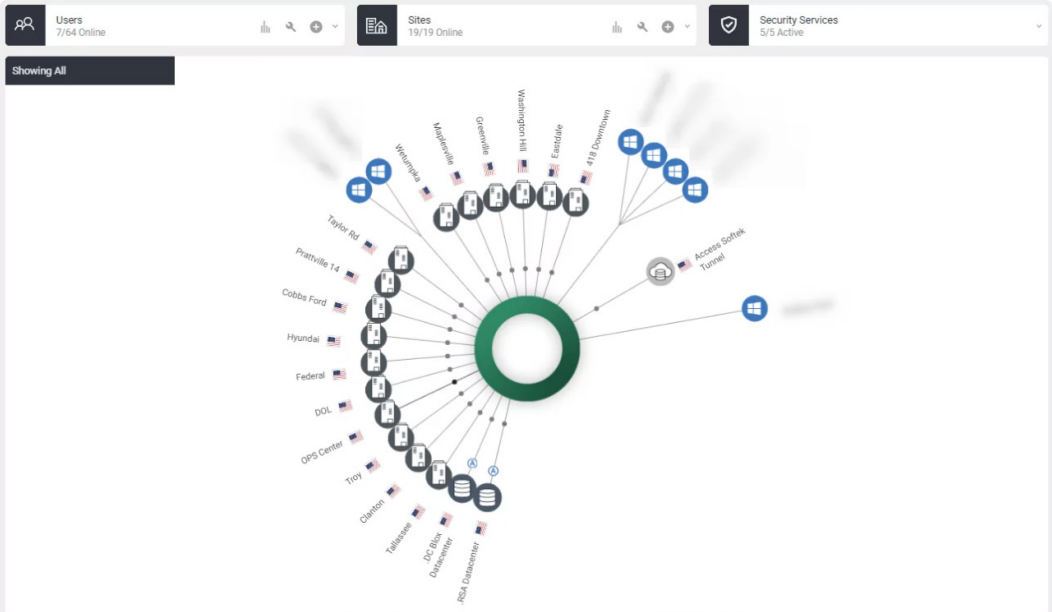
Rosen 為了 SD-WAN以及其他優點改用 Cato 的 SASE 平台

Cato 為 Guardian 提供信用合作社所需的更強大安全性、應用程式控制及操作簡便性。 Cato 可讓 Guardian 實現所需的安全性而無需在防火牆及其他安全服務上分層, 避免增加網路的複雜性。「安全性不僅是 Cato 技術解決方案的一部分。它已深植於 Cato。他們的執行長和創始人就是從那個領域起家。」Rosen 說道。

Cato 也很容易理解, 可提升 Guardian IT 團隊的工作效率。IT 團隊不需要大量網路專業知識, 即可快速排除問題。「現在, 我們團隊中的任何一人都能輕易上手並了解流量流向何處及其運作方式。」Rosen 說道。Cato 也很容易理解, 可提升 Guardian IT 團隊的工作效率。IT 團隊不需要大量網路專業知識, 即可快速排除問題。「現在, 我們團隊中的任何一人都能輕易上手並了解流量流向何處及其運作方式。」Rosen 說道。

> **「 安全性不僅是 Cato 技術解決方案的一部分。它已深植於 Cato。他們的執行長和創始人就是從那個領域起家。」**

轉移至 Cato 也讓 Guardian 爲Covid-19疫情做足準備。「誰會料到我們幾個月前爲改善我們的網路所採取的措施正好為 Covid-19 期間的使用做好準備。」Rosen 說道。「不過轉移向 Cato使我們更有彈性及動力去應對問題，而不僅是轉為遠距工作模式的問題。Cato 不僅可支援我們的遠距員工，我們也不需要將雲端和網路流量帶回我們的資料中心並消耗我們的資源。我們可以將這些流量放在雲端上的所屬位置。」



透過 Cato, Guardian 獲得對其整個網路及安全基礎設施的網路可見性。

Cato 的支援很「靈敏」 且回應快速

整體上，Rosen 對 Cato 客戶服務的盡責態度留下非常深刻的印象。Rosen 說，有一天晚上，他在 9 點之後打電話給 Cato，儘管已經很晚，Cato 仍然提議進行遠端支援。Guardian 當時正在執行 Cato 的概念驗證 (PoC)，不過 Cato 事後才知道。Cato 對支援遠遠超乎預期的盡責態度促使 Guardian 決定將業務交給它。

Cato 對改善的建議也能快速回應。「Cato 很靈敏。當我需要修復或改進產品時，Cato會傾聽我的想法。」Rosen 說道。

> **「 Cato 很敏捷。當我需要修復或改進產品時，Cato會傾聽我的想法。」**

Guardian 和 Cato 擁有相同的企業文化，那就是以客為尊。「老實說，我很想告訴你一切是因為產品，但人員也是一項差異化因素。」

BANK avera

Cato SASE Cloud 保護 Bank Avera 據點及其流動員工的網路連線安全

安全及最佳化的 SD-WAN • 安全的分支機構網路存取 • 雲端加速及控制 • 區域 SASE

行動安全及最佳化 • 遠端存取安全及最佳化 • 成本合宜的 MPLS 替代方案

Avera 這個名字是由意大利文的「avere」(擁有) 和「vera」(真實) 合併而成。這個名字的意思就是「擁有真實的東西」。因此，這家銀行的特色是個人化建議、全方位做法以及為個人量身訂製的金融解決方案。對 Bank Avera 而言，讓據點良好、穩定且安全地連接非常重要。

Ralf Luchsinger, Bank Avera 資訊技術、服務與供應商管理總監

挑戰

Bank Avera 以往依賴外包的 IT 基礎設施。重新掌握控制權並由內部執行 IT 服務是業務策略的一個重要環節。做出此決定的重要因素是橫跨所有網路及站點的靈活性、可見性和安全性。這些系統必須統一且互連。他們已評估及測試不同的網路連接變項。基於系統必須自行運作且無需購買基礎設施，他們選擇了現成的解決方案 SASE (安全存取服務邊緣) 。

從 Bank Avera 的角度來看，其主要訴求是：

- 保護 Bank Avera 的行動裝置使用者在所有裝置上免受威脅
- 在一個平台上根據企業政策統一管理對所有企業資料的存取
- 確保所有銀行據點的延遲率低且頻寬加快
- 確保所有 Bank Avera 分行及居家使用的網路存取安全
- 保護及加快對雲端服務的一般存取

關於 Bank Avera

該州最大的區域性銀行 Bank Avera 自 1828年起紮根於大蘇黎世地區，透過由 12 個據點組成的網路爲大約 45000 名客戶提供滿意的服務。Bank Avera 向 Inseya 提出以一個現代、未來的解決方案將所有銀行據點網絡連接起來的想法。網路及安全的整合應該易於實施及自動化。

解決方案

Cato 的安全存取服務邊緣 (SASE) 解決方案被認為是一個全球雲端原生平台，執行融合式軟體堆疊以提供適應性強大且安全的網路服務。

Cato SASE Cloud 的安全引擎作為雲端服務的一部分供應，Bank Avera無需為滿足要求購買或配置額外的設備。Cato 提供下一代防火牆 (NGFW)、包含 URL 過濾功能的安全網路閘道器 (SWG)、反惡意軟體服務及入侵防禦系統 (IPS) 服務。

重點在於站點之間資料流量 (WAN) 的最佳化及加密，這是網路軟體堆疊的必要組成部分。Cato 解決方案使用 TCP 代理伺服器及服務品質演算法將檔案的傳輸速度最大化。

Cato Socket 是 Cato 的邊緣 SD-WAN 裝置，利用多個網路連線提供可靠、高性能存取全球可用的 Cato SASE Cloud。流量也可透過 IP-sec 隧道遞送至第三方裝置。

結果：為所有 Bank Avera 據點帶來最佳解決方案。

Cato 的解決方案顯著提升 Bank Avera 連網站點的穩定性與安全性，並且減輕系統的負擔。 以往外包的服務現可由內部自動化執行。Cato 取代了現有的 VPN 連線。

整體而言，複雜性降低，正常運作時間增加且流程更為簡化。該解決方案的簡易整合方式使提高可見性成為可能。IT 部門可接管可任意擴展式解決方案的組態配置，輕鬆整合新使用者、增加的頻寬及更多據點。該銀行在很短的時間內整合更新、更好的 WAN 解決方案。總之，IT 管理層對 Cato 的安全解決方案非常滿意，並可為員工提供系統穩定性及安全性的保障。

> **憑藉 Cato Networks 的 Cato SASE Cloud，我們可以安全、輕鬆且快速地連接據點及員工。我們現在可自行管理 IT 解決方案，隨時根據我們的需求以所需的靈活性調整基礎設施。」**

Blender擺脫防火牆硬體束縛

淘汰分支點設備 • 雲端資料中心整合

挑戰

當 Blender 最初從以色列的總部起步時，他們安裝了一個頂級供應商的防火牆設備。技術長 (CTO) Boaz Aviv 發現其管理、升級及修補都很複雜。「擁有這些資安硬體設備的成本很昂貴，它們需要持續管理。即使每個月管理防火牆所需的時間只是 10個小時，那也是 10 小時的損失。」Aviv解釋說。Blender 依賴一家 IT 整合商進行防火牆設備的安裝及支援。在週末發生系統故障時，他們的 IT 整合商無法爲他們提供支援。這導致長時間的停機並影響他們的業務。

> **「自從我們改用 Cato 之後，我們的頻寬比以往增加大約30倍的速度。現在，客戶的 Wi-Fi體驗改善許多。自從部署 Cato 之後，我們就不再收到投訴了」**

當他們擴展至義大利和立陶宛的新辦事處時，Blender 的團隊停下腳步重新評估他們的辦事處網路安全足迹將如何影響未來的成本及容量。如果沒有專門人員支援遠端設備的升級和修補，Blender 就得依賴昂貴的第三方支援，而且支援範圍不可靠。

此外，作爲一家金融技術機構，Blender 一直希望能升級至更佳的安全服務。「雖然我們是一家年輕的公司，但我們從不在安全上妥協。」Aviv 說道。作爲一個以雲端爲核心的企業，Blender 須遵守法規並將大部分資料儲存在 SaaS 應用程式及 IaaS 資料中心內，因此特別需要保障資料存取的安全性。

Boaz Aviv,
技術長

關於 Blender

消除全球貸款人與借款人的邊界是 Blender 點對點借貸平台的核心。在三年前成立的 Blender 爲借款人及貸款人提供一種簡單易行的傳統銀行貸款替代方案，爲雙方提供更具吸引力的利率。

該公司目前為超過 10,000 個客戶提供服務，在以色列、義大利和立陶宛設有辦事處，並計劃在 2017 年擴展至兩個新區域。爲了提高競爭力，該公司的網路架構和 IT 員工也必須以特別精實的方式運作。

解決方案

當 Aviv 最初了解到 Cato Networks 及其以雲端為架構的安全網路時，他認為它是 Blender 的完美選擇。「我辦公室裡唯一的金屬就是我們的電話機和防火牆 — 我想要將它們全部清除」Aviv 解釋。「我覺得隨著我們的成長，這些盒子也會越來越多，管理和支援它們的負擔也會隨之加重。」

爲部署 Cato，Blender 只需將總部辦公室裡累贅的防火牆替換成 Cato Socket，這是一種小巧、零接觸的隧道裝置，可將流量從辦公室轉遞至 Cato Cloud。連接他們的分支機構很簡單，而且無需任何技術專業知識。

所有據點現在透過 Cato 使用安全的網路存取。這是一套包含下一代防火牆、應用程式控制及 URL 過濾功能的完整安全堆疊，負責檢查 Blender 的流量，並在分支機構與 Cato Cloud 之間提供完全加密。

在雲端上集中管理網路安全，可為所有使用者、據點及應用程式實行統一政策。在使用 Cato 之前，Aviv 原本計劃購買更多設備來支援公司的災難復原 (DR) 站點。現在安裝 Cato 可讓他省去管理額外設備的大量費用及 IT 資源。而他的團隊正在將 DR 站點安全連接至 Cato Cloud，並從雲端連接至其他業務。

Blender 員工可使用其行動裝置上的 Cato Client 應用程式隨時隨地存取 Office 365、Salesforce 和 Amazon AWS 應用程式。Cato Client 建立一個通往 Cato Cloud 的安全隧道，所有雲端流量都受到 Cato 保護。爲了防止未經授權存取並預防憑證竊盜，Blender 使用一個獨特的 Cato 功能，容許他們將其 SaaS 應用程式設定成只接受來自 Cato Cloud 特定 IP 範圍的流量。由於 Cato Client 只能在裝置完整註冊之後使用，駭客無法使用未經註冊的裝置攻擊雲端應用程式。

未來方向

投入生產一年之後，Blender 正在滿足業界安全稽核的要求，同時隨著業務的成長擴展容量，並且讓使用者使用以雲端為架構的管理應用程式輕鬆存取網路資源。Aviv 對他在整個過程中獲得的支援水準印象深刻。

CIAL Dun & Bradstreet 透過 Cato 改善拉丁美洲的網路連接及安全

成本合宜的 MPLS 替代方案 • 成本合宜的 MPLS 替代方案

挑戰：改善拉丁美洲辦事處的網路基礎設施

CIAL Dun & Bradstreet 面臨著一個再熟悉不過的網路問題: 整合不同的業務。「完成收購之後，我們意識到有些辦事處需要升級網路基礎設施。」CIAL Dun & Bradstreet 技術長 Yoni Cohen 表示。「部分地區的網路速度不夠快，這對業務來說是個真正的障礙。」

Centro de Información América Latin (CIAL)　Dun & Bradstreet 在 CB Alliance 成為 Dun & Bradstreet International 在拉丁美洲的 WWN 合作夥伴時成立。CIAL Dun & Bradstreet 是拉丁美洲商業貿易信貸及供應商風險管理資料與解決方案的主要供應商。辦事處分佈於阿根廷、巴西、墨西哥、秘魯和南佛羅里達，並在整個區域的國家/地區設有其他人員。

CIAL 迫切需要建立一個新網路來統一這家新公司並連接至現有的辦事處，包括薩格勒布、以色列及紐約的團隊。「我們希望一切都在一個統一、但安全的網路上。」Cohen 說道。

Yoni Cohen,
技術長

關於 CIAL Dun & Bradstreet

CIAL Dun & Bradstreet 的總部位於紐約，是一家全球商業資料技術公司，活躍於拉丁美洲以及特拉維夫和薩格勒布。在選擇 Cato 之前，該公司擁有一個連接八國辦事處的 MPLS 網路，部分來自拉丁美洲的一項重要收購。 四個地方網路分別連接至美國的一個企業資料中心，同時每個辦事處都與全球網路相連。MPLS 線路透過美國的一個資料中心傳遞，其他辦事處有各自的配置並透過 VPN 連接至母公司。

SD-WAN 降低網路存取成本並增加對應用程式的跨站點存取

基於幾個理由, Cohen 開始考慮 SD-WAN 做法。「我想要一個靈活的虛擬網路, 因為我知道我們會在不久的將來增加辦事處並進行其他更動。」他說道。「我們沒有被 MPLS 線路的長期合約綁死, 這使我們能夠安裝寬頻線路取而代之, 降低成本。」

拉丁美洲的頻寬成本 – 無論是 MPLS 或寬頻 –都比其他地方高出許多。CIAL 為降低成本所做的任何努力都有所幫助。「在拉丁美洲中部擁有一個主要資料中心似乎不是特別好的做法。這是我們開始考慮採用 SD-WAN 的原因。」

CIAL Alliance 測試 Cato

在 Cohen 開始研究 SD-WAN 解決方案之後不久, 他閱讀了一篇關於 Cato Networks 的文章並開始進一步探查。他對了解到的資訊感到滿意, 於是簽署協議讓 CIAL 成為 Cato Networks 的客戶。

> **「這是一次成功的部署, 我們與 Cato 的網路工程師合作, 他對於我們建立所需連線的能力扮演重要角色。」**

雖然這讓他們成功降低成本, 但降低成本並非 Cato 的唯一優勢:

> **「我們獲得的成果遠超過節省成本。連接我們的據點和雲端、TLS 檢查服務、網路層級的防病毒軟體 – 它的價值非常多。」**

最終, CIAL Dun & Bradstreet 透過 VPN 隧道連接 Dun & Bradstreet 全球資料供應鏈至各種企業資料中心, 隧道連接至 Amazon AWS 中的實例及個別站點。

CIAL Dun & Bradstreet透過 VPN 隧道連接全球資料供應鏈至各種企業資料中心，隧道連接至 Amazon AWS 中的實例及個別站點。

Cato 可設置廣域網路及網際網路流量優先順序的功能特別實用。「由於拉丁美洲的網路連線非常昂貴，提供高速網路連線的成本高得令人卻步。當您有 80 至 100 人共用一個連線時，您必須安排流量的優先順序。」

Cato 也賦予 CIAL Dun & Bradstreet 將流量分段以防止惡意軟體傳播的能力。「我們利用 WAN 規則更仔細地區隔流量。」Cohen 說道。「我們使用 TLS 檢查服務防止任何病毒在我們的網路上傳播。我們增添根據流量類型和傳遞類型運作的安全規則，因此任何惡意軟體將更難從一個站點移動至另一個站點。」

CIAL Dun & Bradstreet 與 Cato 的下一步合作

Cohen 正在尋求方法讓 CIAL Dun & Bradstreet 充分善用 Cato Cloud 以獲取最大效益。「我正在考慮的一件事是在我們所有裝置上安裝 Cato Client，迫使它們通過 Cato Cloud。這可能是我與 Cato 的下一步。」Cohen 表示。

Cato Client 將行動使用者連接至 Cato Cloud，提供對企業 SD-WAN 的安全及最佳化存取。行動使用者可存取所有可從這些位置存取的資源，無論是在實體資料中心或雲端及網路上。經由最近的 Cato PoP 直接連接至這些資源，可實現遠勝於傳統行動 VPN 解決方案的行動使用者效能。這使得他們的團隊能夠快速、有機擴展至新區域。

STANDARD INSURANCE

Standard Insurance 使用 Cato 進行雲端遷移和數位化轉型

保護雲端式 SD-WAN • 雲端資料中心整合 • 淘汰分支設備

許多企業正在經歷數位化轉型，重塑他們的業務經營方式，以便能更創新且更能迅速滿足客戶需求。這通常需要將應用程式遷移至雲端，並透過簡化 IT 基礎設施提高業務營運的靈活性。這兩點無疑都是 Standard Insurance 的目標，其數位化轉型計劃非常成功，還因此獲得領先的全服務企業與 IT架構公司ICMG 於 2018年頒發的「IT 基礎設施最佳架構獎」。

Standard Insurance 是菲律賓的一家全國保險與金融產品供應商，在 2016 年啓動一項爲期數年的數位化轉型計劃。該公司正在轉向線上銷售，並需要改進其老化的後端軟體基礎設施。該系統為保險業務從申請、提案至保單核發、管理、理賠的整個流程提供服務，也就是公司的生命週期。不過，新的自訂開發平台仍在公司資料中心內運作。一次系統故障便可能對公司構成生存威脅，將保險軟體遷移至 AWS 便成了當務之急。

60個分支機構的保險代理人及員工透過 VPN 進入馬卡蒂總部存取公司的保險應用程式。這些站點由分支機構的防火牆設備保護，並使用電信公司提供的 VPN 服務連接。但是由於電信覆蓋範圍不足，Standard Insurance 的第一副總裁兼 IT 基礎設施與網路安全總監 Alf Dela Cruz 和他的團隊必須管理多個供應商關係，以實現全面的分支機構連接。這是個相當棘手的問題。

安全也是一個問題。本地防火牆設備需要升級，這是一項持續性的開支，而且不足以保護企業安全。在發生兩起勒索軟體事件之後，執行長要求大幅改善安全態勢。

防火牆設備的複雜性也使站點部署變得複雜。「如果使用硬體防火牆，我們必須將資訊複製至每個站點並確保持續更新，我們在總部所做的任何更動都需要散佈至每個分支機構。」Dela Cruz 說道。

Alf Dela Cruz,
第一副總裁 / IT 基礎設施與網路安全總監

關於 Standard Insurance

Standard Insurance Co. Inc. 是菲律賓的一家非壽險公司。該公司的總部設於菲律賓馬卡蒂，在全國擁有 60 家分支機構，700 多名保險經紀/代理人以及 1500 個合作夥伴。在使用 Cato 之前，Standard Insurance 使用本地防火牆以及電信公司提供的低頻寬 IPVPN 服務連接分支機構和公司總部。在完全遷移至AWS 之前，應用程式最初是在公司內部及AWS內托管。具體的應用程式包括核心的保險核發應用程式、CRM、會計系統及其他辦公生產工具。

在一次詳盡評估中，Cato 將安全成本降低一半

IT 團隊原本打算將防火牆設備替換成公司內部設置的下一代硬體設備，但在等待新硬體交付時，Dela Cruz 聽到了有關 Cato 的訊息。

> **「當我們瞭解 Cato 的解決方案之後，我們喜歡這個簡單、集中式管理的概念。我們再也不必擔心本地防火牆修補管理流程過於耗時的問題。」**

Cato 將所有企業資源 (據點、雲端資源及行動使用者) 連接至一個通用且最佳化的全球骨幹網路，目前該骨幹由全球超過 42 個 PoP 建構而成。針對 Cato 骨幹上的所有流量，Cato 採用一個通用安全政策來保護所有資源。下一代防火牆 (NGFW)、安全網站閘道器 (SWG)、URL 過濾、惡意軟體防禦皆內建於 Cato 服務中。Cato MDR 是一項托管式威脅偵測與回應 (MDR) 服務，它可將資源密集且依賴技術的終端威脅偵測流程卸載到 Cato SOC 上。

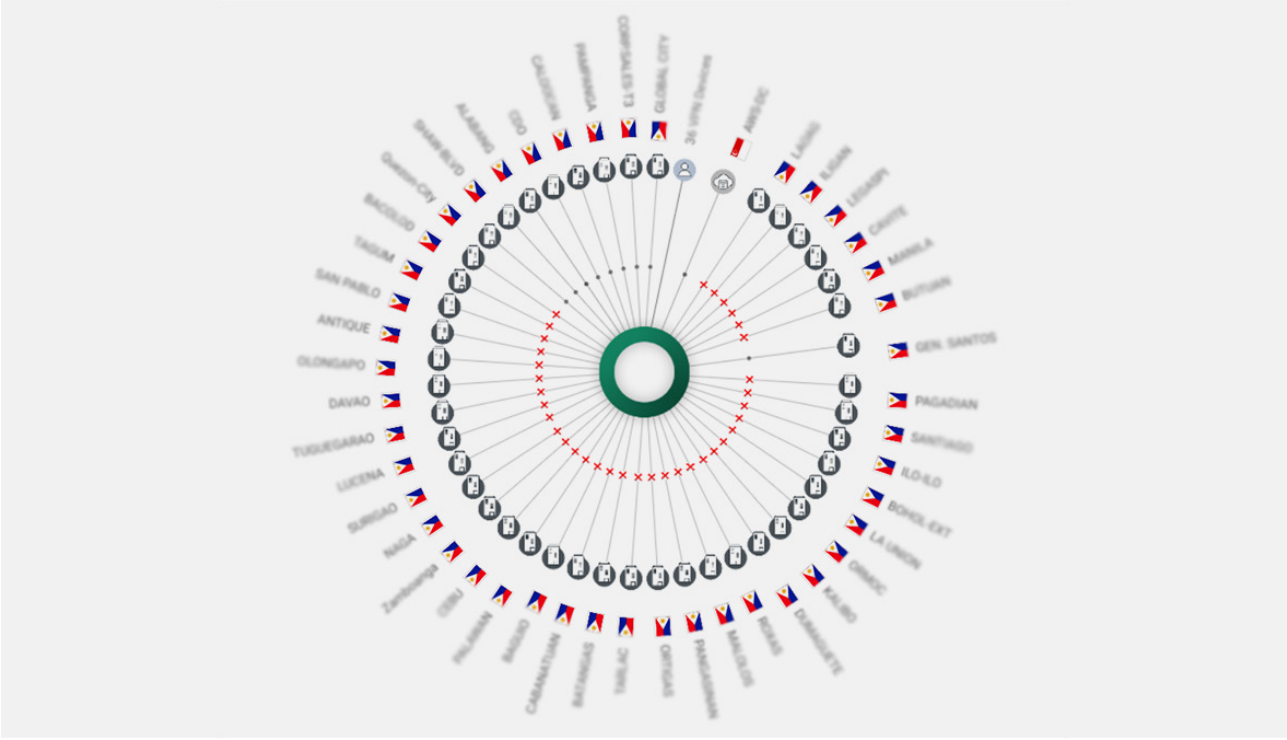
Standard Insurance 擱置它的硬體購置計劃並對 Cato 進行詳盡評估。「我們差點花費比 Cato多一倍的成本。」他說道。

> **「Cato提供我們的整個解決方案 – 包括集中管理、雲端監控及報告 – 的成本就與單單防火牆設備的成本不相上下。然後，我們還得加上設備管理和進階安全防護以及其他防火牆組件的費用」。**

Cato 簡化網路和安全基礎設施

如果說 Cato 以其低成本吸引 Standard Insurance 團隊的注意，那麼贏得他們青睞的是 Cato 的 AWS 連接能力。Cato 的接入點 (PoP) 與亞馬遜 AWS、微軟 Azure 及其他雲端資料中心服務的 IXP 共用同一個實體資料中心，提供跨越雲端供應商及全球區域的雲端資源快速存取。「一旦我們將關鍵應用程式遷移至 AWS 雲端上，我們將更倚重 Cato，因爲他們與雲端網路的相容性，可讓我們的分支機構通過 Cato 網路輕鬆連接至 AWS 雲端。」Dela Cruz 說道。

使用 Cato 也讓 Standard Insurance 縮短部署時間。Dela Cruz 和他的團隊可淘汰所有分支機構的防火牆及網際網路 VPN，同時發送一個小巧的 Cato SD-WAN 裝置 Cato Socket至各個分支機構，非技術人員只需插入即可使用。一旦 Socket 連上網路之後，Cato 網路即可識別並將 Socket 加入SD-WAN。該 Socket 將繼承Dela Cruz及其團隊爲網路設定的全球安全政策。「有了 Cato，我們可在幾分鐘內設置好一個分支機構。」Dela Cruz 說道。



借助 Cato，Standard Insurance 將所有使用者、站點及雲端資源連接至一個骨幹網路。

在雲端上爲所有使用者和資源實行一套安全規則，可讓安全更易於管理及更新。政策也可從 Cato 管理控制台自訂，以滿足個別據點、使用者等的需要。「Cato 管理控制台非常容易理解。」Dela Cruz 說道。在使用者方面，Standard Insurance 的員工享有更完美的使用者體驗。IPVPN 頻寬以往受限於 1 Mbits/s。

> **憑藉 Cato，我們的網路頻寬足足增加了 10倍，在成本未增加的情況下顯著提升性能。」**

Standard Insurance 與 Cato 的下一步合作

Standard Insurance 將繼續其大規模轉型行動。計劃包括為其所有應用程式實施單一登入 (SSO) 及多項應用程式變更。在基礎設施方面，Standard Insurance 期望推出更多行動客戶端，讓更多保險經紀及代理人加入網路。

> **我們向我們的業務合作夥伴推薦 Cato。我們喜歡這個解決方案以雲端為基礎、易於管理，而且比其他選項成本更低。」**