白皮書

迎接多雲端網路的挑戰：最佳化雲端工作負載與應用程式體驗

贊助商：思科

Brad Casemore
2020 年 11 月 12 日

IDC 觀點

隨著各組織持續追求數位化轉型，以達更佳的靈活性、效率及競爭優勢，他們積極採用混合型 IT 和多雲端作為實現這些目標的不可或缺手段。因此，先前處於內部部署企業資料中心的集中式應用程式和工作負載皆分散於各雲端。與此同時，勞動力變得愈來愈流動和分散，他們在園區、分支辦公室工作，且愈來愈多人（因為 COVID-19 疫情緣故）在家庭辦公室工作。這些趨勢正重新定義傳統資料中心的參數，並迫使各組織現代化和延伸其網路基礎架構，以因應分散式多雲端工作負載，以及前所未見橫跨多個網路端點和位置的應用程式存取。

> 多雲端網路必須能夠提供以雲端為主的組織所需之靈活性、彈性、延展擴充性、營運效率及安全性。

網路為啟用與支援數位化轉型的中樞神經系統。事實上，在多雲端的背景下，網路在現今顯得極為重要。事實上，將應用程式和工作負載移轉至公用 IaaS 和 SaaS 雲端，明顯已促進對於可擴充與穩固多雲端網路基礎架構（從工作負載延伸至存取）的需求，該網路基礎架構能夠提供以雲端為主的組織所需之靈活性、彈性、延展擴充性、營運效率及安全性。

本白皮書探討對於全面多雲端網路的需求，該網路可滿足 IaaS 和 SaaS 雲端工作負載的需求，以及因應雲端應用程式持續可用、回應快速及安全存取的要求。

附註：由於四捨五入緣故，本文件內的所有數字可能並非精確數字。

情況概覽

即便在 COVID-19 疫情爆發前，全球企業皆已運用多雲端作為達成數位化轉型目標的重要手段。雖然大部分企業目前仍於內部部署環境中執行重要的工作負載，但皆已積極採用適用的 SaaS，且愈來愈多組織開始將全新與現有的工作負載移至 IaaS 和 PaaS 雲端（例如，AWS、Microsoft Azure、Google Cloud 及 IBM Cloud）。

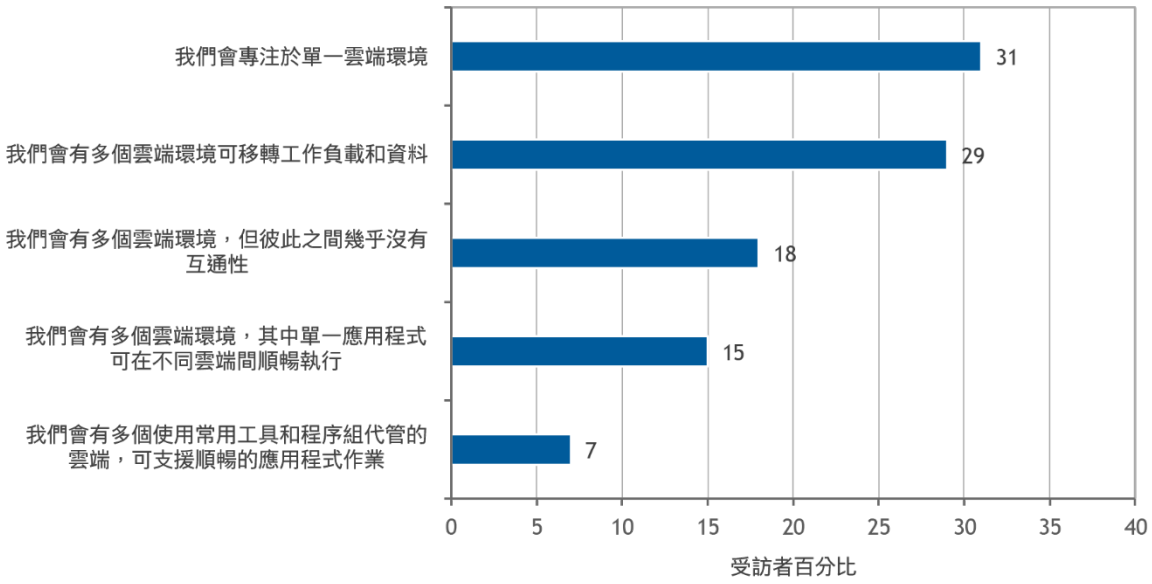
疫情已加快此趨勢的速度，各企業逐漸開始考量雲端的角色，作為促進業務復原能力與持續性的有效策略。

但是，在 COVID-19 疫情發生前，促使積極採用公用雲端的主要原因，為對於支援數位化轉型提升業務靈活性的需求。該目標仍存在，但目前由於希望達成更佳的企業恢復能力，包括業務持續性，以及支援更多額外的數位服務，致使此目標受到深化。根據 IDC 2020 年第 1 季的*雲端趨勢調查* (Cloud Pulse Survey)，69% 的組織開始投資多雲端策略（參見圖 1）。

圖 1

多雲端策略投資

問題： 未來兩年，您會如何描述您的企業在內部和外部環境中部署雲端？



n = 837

資料來源：IDC *雲端振蕩調查* (Cloud Pulse Survey)，2020 年第 1 季

已踏上雲端歷程的組織正不斷加快其發展速度，而仍在考慮朝著該方向前進的組織，也正開始迅速採取行動。隨著企業恢復能力成為長期目標的迫切需求，資料中心網路及延伸至多雲端、分支機構及邊緣位置的廣域網路 (WAN) 皆必須進化。

59% 的企業受訪者表示，「雲端供應商的整合式網路程序」將成為未來兩年內雲端投資的重要領域。

各企業在執行雲端策略時，皆不約而同發現基礎架構現代化（包括網路基礎架構）的迫切需求與高度挑戰性。在 IDC 2019 年的*資料中心營運調查* (Datacenter Operational Survey) 中，企業受訪者認為「確保資料安全性與法規遵循」和「改善網路效能」為混合型 IT 和多雲端環境中的 2 大優先順序與挑戰。同樣地，在 IDC 2019 年第 3 季的*雲端趨勢調查* (Cloud Pulse Survey) 中，59% 企業受訪者表示，「雲端供應商的整合式網路程序」將成為未來兩年內雲端投資的重要領域。

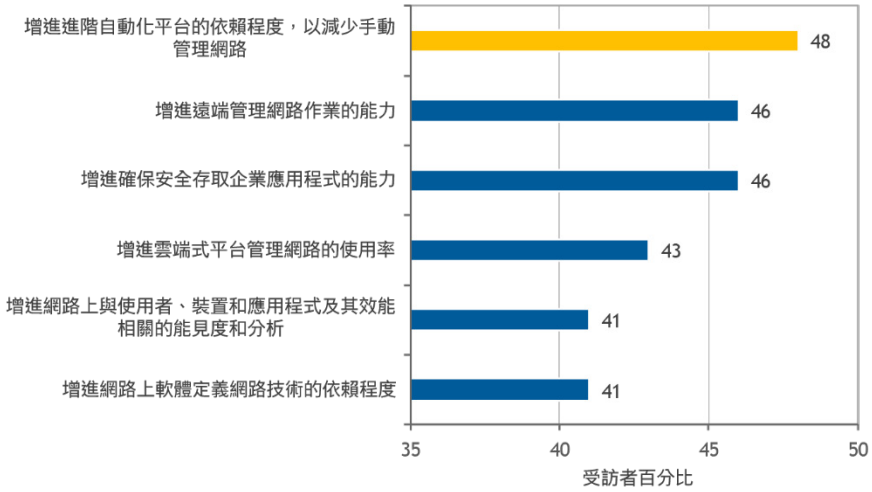
多雲端的網路現代化必須始於基本且無可否認的原則：分散式應用程式為全新的網路重心。在受到不斷提升之智慧與自動化層級支援的多雲端時代中，網路必須比以往更貼近符合應用程式和工作負載的應用程式動態需求。

事實上，網路自動化為 COVID-19 疫情之下促進提升企業興趣與積極採用的領域。在 IDC 2020 年 6 月*前瞻性企業網路調查* (Future Proofing Enterprise Networking Survey) 中，企業受訪者在接受訪問時確認在後 COVID-19 疫情時代環境下提升投資的領域。將近一半 (48%) 的受訪者提出「進階自動化平台的可靠度提升可減少手動管理網路」的想法，而相關領域亦顯著受到提及（參見圖 2）。

圖 2

後 COVID-19 疫情時代環境的網路投資提升領域

問題： 在下列領域中，是否有任何為您組織在 COVID-19 疫情或後 COVID-19 疫情時代環境下，可能會因全新業務營運需求而提升投資的領域？



n = 254

資料來源：IDC *前瞻性企業網路* (Future Proofing Enterprise Networking)，2020 年 6 月

雖然網路在內部部署資料中心內已受到軟體定義，且近期甚至橫跨 WAN（SD-WAN 形式），多雲端的崛起意味著對於控制與靈活性的需求（透過智慧原則型網路自動化提供）將會進一步擴增。隨著 IT 轉向混合型態，支援處於內部部署和公有雲端中的分散式應用程式，您不僅需要橫跨此全新環境的一致且可延伸之網路與安全性原則，亦需要透過雲端中間環節和雲端核心迅速可靠路由傳送流量的全新方式，以便安全輸入和方便移轉至雲端，進而降低延遲、改善可用性及增強應用程式體驗。

完整瞭解多雲端網路可從目前分散式多雲端資料中心（應用程式和工作負載所處位置）延伸至園區、分公司、家庭及其他邊緣位置（其中可徹底提供應用程式體驗）的端點（使用者和裝置）。

隨著應用程式成為所有網路的重心及定向點，各企業必須從核心至邊緣考量以應用程式為主的網路現代化，其中涵蓋從工作負載最佳化至應用程式存取和體驗的完整應用程式歷程。

多雲端網路的現代營運

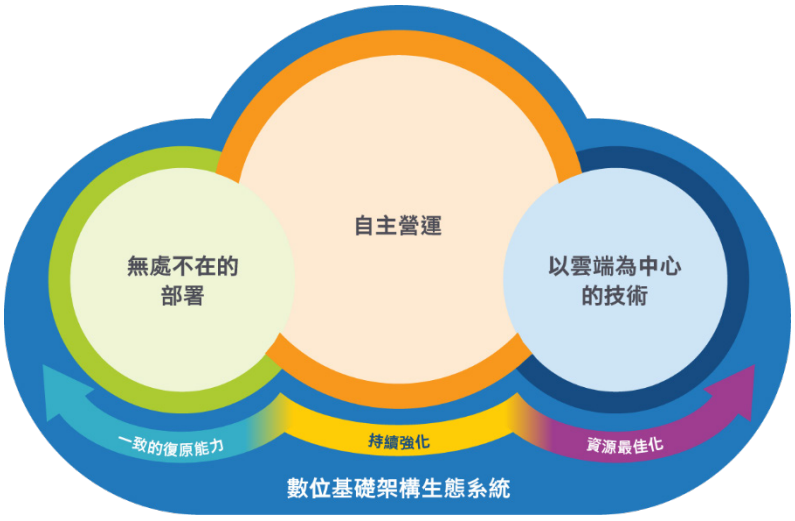
毫無意外地，全新的需求將著重於 IT 營運，其中包括網路架構師和雲端架構師。事實上，IDC 已預測未來幾年主要的營運和組織轉變。IDC 預測，到了 2023 年，55% 的企業會將過時的營運模式更換為以雲端為主的模式，如此可讓 IT 營運和公用雲端營運間更有效的配合，進而推動組織協作，達成更佳的業務成果。

自動化與動態性提升的數位基礎架構未來，大幅仰賴於連線的雲端架構，可讓企業移轉和整合在多個實體位置之不同類型雲端中執行的工作負載和資料（參見圖 3）。

IDC 預測，到了 2023 年，55% 的企業會將過時的營運模式更換為以雲端為主的模式，如此可讓 IT 營運和公用雲端營運間更有效的配合，進而推動組織協作，達成更佳的業務成果。

圖 3

IDC 的數位基礎架構未來



來源：IDC，2020 年

對於網路操作員（其中包括專業人員和雲端架構師）而言，其影響將會相當深遠。多雲端環境的架構與基礎架構必須變得更為靈活、彈性及一致，且操作和管理網路之人員亦必須達到相同要求。

為因應此要求，網路工程師和網路操作員皆尋求積極採用控制器型架構，並且在自動化、程式設計能力及雲端（API 和虛擬私人雲端 [VPC]/VNET）等領域獲得知識與熟練度。網路營運 (NetOps) 團隊必須精通自動化佈建與彈性擴充網路基礎架構（以支援數位業務的動態興衰，並在例外情況時維持業務連線和執行），且部署後第 2 天必須能夠提供更快的疑難排解與問題補救，如此可修復網路可用性與效能，並因此影響應用程式體驗。

網路目前作為核心（或中樞）神經系統，具有大腦（控制器形式）、脊髓（網路結構形式）及敏感的神經末梢（遙測形式）。透過此類功能，網路與其操作人員可支援逐漸重要的應用程式和資料，並協助在業務中斷或危機時，維持業務運作。

網路操作員必須利用無所不在的即時遙測和能見度，更快地識別、隔離，以及自動解決網路安全性事件。在此情況下，原則型與事件型偵測和防護變得相當必要，可確保網路與其操作人員扮演重要角色，保護應用程式的完整性和復原能力。其中必須具備企業與公用網路（從資料中心和雲端核心完整延伸至 WAN、網際網路、雲端及邊緣網路，最終至可於園區、分公司及家庭端點存取應用程式的位置）的進階能見度與分析能力。

> 到了 2023 年，超過 70% 的企業會針對多雲端網路的網路營運積極採取主動姿態。

以上許多功能會由人工智慧/機器學習技術啟用作為各項機制，但對於網路操作員與其所屬組織而言，其價值須透過實際的業務成果實現。以 IDC 的角度而言，到了 2023 年，超過 70% 的企業會針對多雲端網路的網路營運積極採取主動姿態，透過緩解集中能見度的需求有效符合業務目標，且必須加快腳步支援數位業務目標，或因應影響業務持續性的中斷和威脅。

分散式工作負載的多雲端網路挑戰

隨著網路上應用程式和微服務的暴增（在資料中心內，作為公用雲端服務、作為網路託管服務，以及位於邊緣環境），資料中心網路不再以地理方式定義及歸類為特定實體位置。然而，此網路與應用程式和資料已成為不斷成長的互連「神經叢集」，將會逐漸應用於能提供最大業務成效與價值的領域。

> 許多企業希望能將現有的原則、管理的租用戶或工作負載延展至橫跨內部部署和雲端環境的網路架構。

事實上，針對這些日益分散的工作負載、應用程式及微服務建立網路為一項複雜的工作。其複雜性通常包括耗時的手動佈建。跨區域和雲端的艱鉅路由挑戰，以及各區域之特定雲端間的差異（例如路由數、分段及可用輸送量），將會促進對於不同雲端特定 API 和雲端特定網路服務間特殊專業知識的需求。應用程式相依性亦會被列入考量。一般而言，企業應用程式具有四到八個應用程式相依性，且此類相依性在未來幾年有望倍數成長。根據 IDC 2019 年第 1 季 *雲端趨勢調查* (Cloud Pulse Survey)，IDC 預測在 2021 年，47% 的應用程式將會使用以容器和微服務為特色之模組化開發架構建置。

在網路中，複雜性往往會表現於成本較高且耗時較長的程序。除先前提及的挑戰外，追求使用多雲端的企業通常會發現，必須過度佈建其防火牆服務，並實作繁瑣的對稱路由，才可容納雲端間的防火牆。其亦努力達成雲端延展自動擴充的承諾，特別是將網路和安全性服務順暢插入堆疊的較高位置方面。

此類問題通常合併大多數企業 IT 部門缺乏跨雲端網路專業知識。公平來說，許多公司並非具備能力可快速掌握不同 IaaS 雲端提供的各種架構、網路 API 及網路和安全性服務，更不用說設計自有方法為管理提供一致性和熟練度。

實際上，企業希望能透過將集中原則佈建和管理套用於此日益重要的網路基礎架構方面，將現有原則、管理的租用戶或工作負載延展至橫跨內部部署和雲端環境的網路架構。

提升著重於整體工作負載保護

分散式應用程式環境亦已產生對於整體工作負載保護的需求。肯定的是，在混合式 IT 和多雲端的背景下（即使許多企業接受未來會包含不斷增長補充的雲端原生應用程式，傳統應用程式仍會保持相關性），工作負載保護是至關重要的。傳統工作負載仍必須受到保護，但多雲端的到來會引發更大的攻擊面，以及漏洞的擴散點。此外，應用程式的提升和主導地位表示工作負載的完整性和安全性（無論其所處位置與其架構方式），皆為所有企業的主要關注點。因此，現代安全性機制和模式必須普及於傳統和雲端原生工作負載（以容器和微服務為特色）。

現代安全性機制和模式必須普及於傳統和雲端原生工作負載（以容器和微服務為特色）。

如今，企業會使用各種單點產品來處理工作負載保護使用案例。舉例來說，他們具有各種工具可解決探索、實施安全性和微分段、法規遵循和稽查、網路鑑識、模擬、網路能見度、容器安全性，以及軟體漏洞和程序行為。可惜的是，此類完全不同的工具（即使其已跟上不斷變化的需求），皆如同分散且不連貫的拼圖，僅可提供部分和零散的工作負載保護元素。單點產品本身亦缺乏能力提供「網路效果」，其中產品或技術會以系統方式用於不斷增長的使用案例數，隨著其解決每個額外使用案例，其優點和價值亦隨之倍數增長。

愈來愈多企業正設法減輕管理多雲端環境的複雜性，尋找各種方式合併其使用的工具，以達到整體工作負載保護。

邊緣安全存取多雲端網路的挑戰

處於邊緣亦為如此，隨著處於 SaaS 或 IaaS 公用雲端（而非傳統內部部署資料中心）之存取和使用的應用程式百分比提升，全新的使用者存取挑戰伴隨出現。

如此導致出現部分常見的 SaaS 和 IaaS 網路挑戰，以及部分各領域獨特的挑戰。如為 SaaS，IT 團隊必須能夠確保應用程式可靠安全地提供給位於分散式（和逐漸擴散式）企業環境之員工和其他利害關係人，無須直接控制多數互連網路。WAN 此處扮演重要角色，且已完成現代化（處於 SD-WAN 形式），可處理 SaaS 應用程式的需求，其中的網路需求包括充足的頻寬、低延遲（特別適用於協作應用程式）、封包遺失和封包重新排序及抖動。

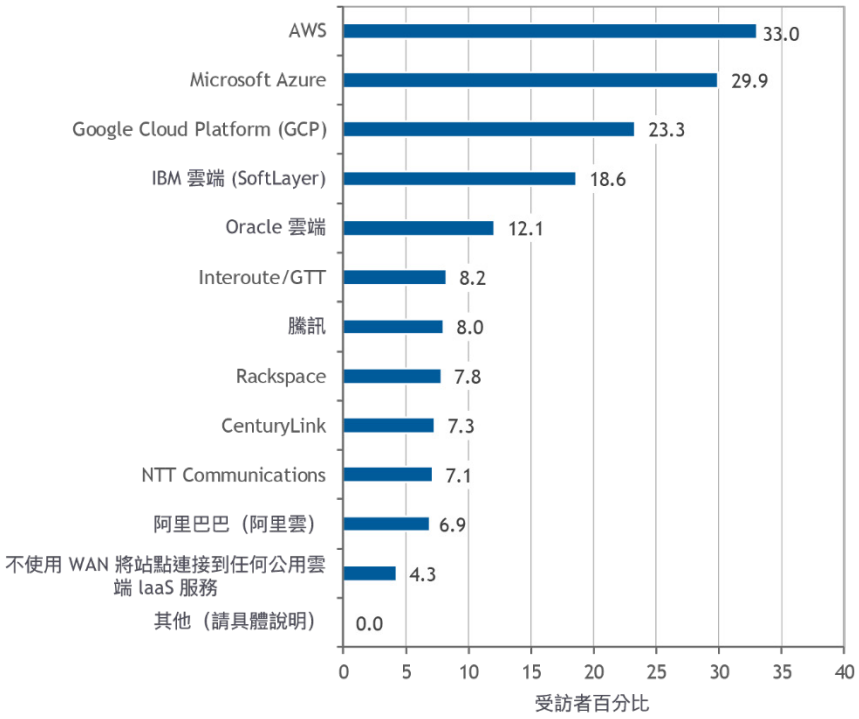
在 IDC 2019 年*軟體定義 WAN (SD-WAN) 調查* (Software-Defined WAN [SD-WAN] Survey) 中，73% 的企業受訪者表示 SaaS 和雲端服務目前對於其 WAN 技術選擇相當重要。

在 IDC 2019 年*軟體定義 WAN (SD-WAN) 調查* (Software-Defined WAN [SD-WAN] Survey) 中，73% 的企業受訪者表示 SaaS 和雲端服務目前對於其 WAN 技術選擇相當重要；而當受訪者遭要求考量未來 12 至 24 個月內情況可能之變化時，其百分比上升超過 78%。此外，僅 4% 的組織報告未與至少一個 IaaS 供應商建立 WAN 連線（參見圖 4）。

圖 4

使用 WAN 連線至 IaaS

Q.　　您的組織目前是否使用 WAN 將站點連線至下列任何公有雲端 IaaS 服務？



n = 1,223

基數 = 所有受訪者

附註：

此調查由 IDC 量化研究小組管理。

資料係依國家/地區 GDP 加權。

解釋小型樣本規模時請小心。

資料來源：IDC *軟體定義 WAN (SD-WAN) 調查* (Software-Defined WAN (SD-WAN) Survey)，2019 年 11 月

隨著混合雲端與多雲端發展，企業將會尋求簡單方式，將站點連線至多雲端，並擁有豐富的遙測和能見度，以取得可付諸實行的深入分析，協助修改以應用程式為基礎的宣告式原則，並促進快速疑難排解、識別及補救多雲端環境的應用程式和網路問題。原因顯而易見。在支援 SaaS 和 IaaS 應用程式方面，傳統 WAN 具有缺陷。這是因為傳統 WAN 係於用戶端/伺服器時代所發展而成，當時應用程式僅處於企業資料中心的防火牆後方。WAN 專門設計和建構用於支援和保護靜態分支對資料中心和分支對分支流量，而非增進支援分支對雲端應用程式流量。此外，傳統 WAN 無法符合與此類雲端應用程式相關聯的安全性要求。

從 SD-WAN 的角度來看，特定要求已成為優先考量。對於以應用程式為中心的宣告式意向型原則，與從 WAN 直到雲端供應商之應用程式背景和效能的完整能見度，以及基礎公用網際網路和雲端網路本身之效能能見度的需求提升。

隨著網際網路和雲端網路在支援工作負載和應用程式體驗方面發揮愈來愈多作用，如此說法尤為貼切。相較於以往，網路操作員需要完整能見度，才可主動偵測和識別出可能影響雲端應用程式效能與體驗的潛在網路效能降低和中斷。

若要存取 IaaS 工作負載和 SaaS 應用程式，具備多雲端功能的 SD-WAN 產品應支援意向型自動化，讓網路操作員能夠控制提供可能適合的應用程式體驗。具備多雲端功能的 SD-WAN 應提供最佳動態路徑選取、雲端服務（中間環節與核心）整合，以及於必要時針對受到延遲和抖動影響之即時雲端應用程式隨時隨地的最佳化。

多雲端存取安全性的重要性

企業必須為多雲端存取提供健全的安全性。保護多雲端存取的有效架構必須結合邊緣環境的網路和安全性，以及雲端型安全性功能，以針對使用者和資料提供一致的保護，無論其所處位置。目前的勞動力變得較 IT 史上任何時期更為分散，但無論員工處於分公司或遠端辦公室或咖啡店，或在家工作，他們始終需要在內部部署、SaaS、或 IaaS 應用程式及工作負載之間，取得安全的網路存取和可能的最佳一致體驗。可惜的是，此方面為傳統安全性架構與雜亂之分散工具的不足之處，這造成使用者易受攻擊，且業務遭受暴露。

> 多雲端存取的安全性功能可透過雲端提供，或整合於 SD-WAN 邊緣路由器，或可結合以上兩者。

網路和安全性團隊逐漸瞭解，他們需要完整但簡單的方法整合網路與安全性功能，以提供安全的多雲端存取。多雲端存取的安全性功能可透過雲端提供，或整合於 SD-WAN 邊緣路由器，或可結合以上兩者。

雲端式安全性提供一致且無所不在的保護，且應全面因應 DNS 安全性、安全 Web 閘道、防火牆即服務、雲端存取安全性代理 (CASB) 及零信任存取等領域。此外，根據分段、進階威脅情報及行為深入分析，安全性應包括針對不明或零時差威脅的保護。

在 SD-WAN 場景中，IT 團隊不僅希望分支中的直接網際網路存取 (DIA) 成本降低和應用程式性能優勢，而且還希望確保它不會影響安全性。分支的安全雲端連線提供可行的方法，與強大的保護和較低的頻寬使用量、較低的延遲，以及因減少仰賴昂貴私人 WAN 傳輸所達到的成本節省。透過完整的安全性堆疊（新一代防火牆、IPS、AMP 及 URL 篩選）及分析和可付諸實行之深入分析的能見度，許多組織可確保安全性和網路有效結合，以確保和保護企業仰賴之應用程式的完整性。

在部分組織受到高度管制或禁止直接網際網路存取的情況下，可求助於混合方式，透過區域共置或互連設備（可託管和執行完整堆疊安全性架構），以便從多個分支彙總存取網際網路和公用雲端。

如何開始使用多雲端網路

隨著許多組織擬訂多雲端策略作為部分數位化轉型工作，完整的逐步多雲端網路方法對於確保計劃成功，以及提供企業價值和營運效率方面，顯得相當重要。有一種進行方式為訂定網路課程，該課程貼近符合應用程式需求和雲端原則及雲端營運模式，可實現更高靈活性、提升彈性，以及增進營運簡易性的承諾。

此方式可解釋為對於應用程式的重視，其中涵蓋工作負載所處位置，到使用者使用和體驗應用程式的位置。任何不符合工作負載需求的多雲端網路可能無法達到目標。同樣地，任何未考量應用程式體驗和參與度的多雲端網路，可能淪於無法達到預期優勢的風險。

在組織評估其分散式應用程式和目前與未來的雲端目標後，可進行多雲端網路方式，並著重兩個主要考量因素：

- **應用程式：**工作負載（包括微服務和容器組成的現代架構）必須透過靈活、彈性及可延展擴充的網路支援，以提供一致且簡易的佈建、管理及安全性。
- **存取：**必須為各處使用者和裝置提供高度可用與回應性存取應用程式（包括內部部署、IaaS 及 SaaS），以及一致的安全性、可靠性及效能。

開始使用多雲端網路，實現分散式工作負載

1. **延伸網路能見度和分析。**由於應用程式分佈於傳統資料中心之外，因此 IT 團隊必須延伸其遙測、能見度及分析功能，以確保應用程式維持隨時可用與回應快速狀態。由於多雲端網路目前結合資料中心、WAN、寬頻及雲端網路，因此必須能夠掌握所有此類網域狀態。多個網域彙整之資料的進階分析，伴隨作為支援技術之人工智慧/機器學習的使用量提升，將可在日益複雜和分散式環境中，提供更快速的疑難排解和補救。

2. **延伸原則型網路自動化。**在數位化轉型和業務復原能力的背景下，靈活性和彈性理所當然會受到重視。網路自動化應可讓 NetOps 團隊積極採用全新的多雲端程序，並緩解因管理不同雲端環境間之分散式工作負載所提升的複雜性。原則型自動化工具會隨著雲端演進，以利有效率且準確連接多雲端環境內的網路服務/功能。

   自動化工具一般具有介面卡，可使其搭配使用不同雲端服務供應商的各種雲端服務。因此，正確的自動化工具將可促進混合式雲端和多雲端架構的互通性。此外，自動化工具亦會消除雲端和內部部署資料中心間的應用程式和資料可攜性限制。IT 組織可透過利用順暢整合各種雲端服務和雲端服務供應商的自動化工具來限制互通性問題。

開始使用多雲端網路，實現分散式工作負載

1. 延伸網路能見度和分析。
2. 延伸原則型網路自動化。
3. 保護工作負載和資料免於攻擊。
4. 將自動化結合封閉迴路意向型網路 (IBN) 的深入分析工具。

3. **保護工作負載和資料免於攻擊。**工作負載保護為多雲端環境日益增長的業務問題，且許多組織必須掌握威脅狀態，以確保實作可行的防禦。能見度必須兼備普遍性和即時性，可感應橫跨使用者、裝置、應用程式、工作負載及程序（工作流程）的異常情況和威脅，且可促進此類情況的回應速度。

   從網路的角度來看，能見度必須可用於資料中心內（縱向和橫向流動）、資料中心之間，並延伸至園區和分支站點及雲端。能見度亦應向上將堆疊延伸至應用程式元件和行為，提供組織檢視潛在的惡意活動，例如資料外洩和惡意軟體從伺服器水平擴散至伺服器。容器和微服務將更加重視完整堆疊能見度。

   達到能見度後，各組織就能拿取可付諸實行的深入分析完整有效地實作分段，防止攻擊在資料中心內部和資料中心之間橫向傳播，且避免惡意對象取得高價值資料中心資產（包括敏感資料）的存取權。

4. **結合自動化與封閉迴路意向型網路 (IBN) 的深入分析工具。**原則型自動化與封閉迴路 IBN 模式內支援人工智慧功能結合的深入分析，可實現完整網路管理生命週期的自動化，並提供網路基礎架構持續追蹤和遵守業務意圖。IDC 預測，具有強化驗證功能的宣告式管理模式和更佳的封閉迴路程序，將會透過串流遙測和全面性的網路能見度逐漸獲得資訊，使得 2025 年時對於自動化網路基礎架構的信任不斷提高。此信任將從佈建延伸至人工智慧輔助的日常網路營運。此類功能可以共同協助 IT 營運部門從內部部署資料中心至混合雲端與多雲端環境，以達到營運一致性和效率。如果此類營運一致性和效率可在目前員工能力和技能持續短缺的情況下實現，則其價值會變得更大。

開始使用多雲端網路，實現安全存取

1. **部署安全的 SD-WAN。**如前所述，多雲端 IT 環境的複雜性會為 IT 帶來挑戰，因為每個雲端供應商具有不同的管理介面、API 及網路架構和服務。因此，企業 IT 人員必須運用多種複雜且耗時的方法，確保為每個雲端服務（例如，AWS、Microsoft Azure 與 Office 365、Google 及 Salesforce）提供一致且安全的使用者體驗。

   考慮到挑戰，IT 團隊應部署簡易的安全 SD-WAN 架構，簡化和自動化分支連線，為完整服務分公司提供動態連線，以因應行動工作者和增長的 SaaS 和 IaaS 應用程式採用量。此 SD-WAN 會提供一致性，以透過企業 IT 人員熟悉的相同架構來運作任何雲端網路。

   同時，同樣的 SD-WAN 將為日益分散的使用者，提供安全直接網際網路存取和/或透過互連供應商存取雲端應用程式。MPLS 網路固有的低效率（會將分公司連結的網際網路流量傳回公司中心）會增加成本和複雜性，同時影響效能和延遲。許多組織透過於其分支安裝直接網際網路存取連結的次要連結，以卸載前往網際網路的流量。

開始使用多雲端網路，實現安全存取

1. 部署安全的 SD-WAN。
2. 針對 SaaS 和 IaaS 效能和安全性最佳化 SD-WAN。
3. 運用雲端式安全性實現一致的安全存取。
4. 考量共置和 SD 雲端互連。
5. 整合跨 SD-WAN 資料中心雲端網路和園區/分支 LAN 的原則管理。

2. **針對 SaaS 和 IaaS 效能和安全性最佳化 SD-WAN。**雲端應用程式對於各地的業務營運變得愈來愈重要。舉例來說，現今 SaaS 應用程式（例如，Salesforce、Microsoft Office 365 及 Webex）為業務營運和成功不可或缺的一部分。SD-WAN 功能應以自動和動態方式為企業使用者選取通往 SaaS 應用程式最快且最可靠的路徑，並利用即時流量控制功能，以提供最佳使用者體驗。如果網際網路服務問題造成連線品質衰退至可接受程度之下，則 SD-WAN 產品必須能夠自動識別和選取下個最佳路徑，以維持應用程式效能。

   同樣地，SD-WAN 應使連接至 IaaS 環境（例如，AWS 和 Azure）變得簡單、自動化及安全。集中管理主控台可協助網路和營運團隊自動化虛擬私人雲端連線至 IaaS 環境。內建智慧可協助滿足自動化連線要求（遺失、延遲及抖動相關）與尋找前往 IaaS 應用程式的最佳路徑，確保服務傳輸和效能，同時監控託管基礎架構是否有任何異常。

3. **運用雲端式安全性實現一致的安全存取。**隨著工作負載和資料轉移至辦公室之外，且安全性移至雲端，傳統周邊安全性模式是不足的。在此情況下，針對橫跨雲端、資料中心、分支及行動裝置和遠端家庭使用者的完整存取安全性，為完整連線環境之間提供安全存取的需求提升。單一雲端原生平台可融合與合併傳統上由多個單點產品提供的網路與安全性功能。優點是同時享有完整的安全性和降低的營運成本。

4. **考量透過共置和 SD 雲端互通，以彙總和加快雲端連線速度。**SD-WAN 可讓分散式架構使用共置設備作為分支機構的區域中心。共置中心可透過減少雲端輸出點數量來簡化多雲端存取、區域化安全性以縮小攻擊面，並透過實施簡化的一般使用者應用程式原則以促進網路效率。

   此外，由於企業需要保證的底層網路連線至 IaaS 工作負載和 SaaS 應用程式，因此 SD-WAN 應可與互連供應商合作，提供如同 MPLS 的可靠性與具有軟體定義網路特色的靈活性。透過利用雲端互連，IT 團隊可順暢快速將企業 SD-WAN 站點連線至多個不同的雲端，且提供必要的效能和可靠性。

5. **整合橫跨 SD-WAN、資料中心網路及園區/分支 LAN 之間的原則管理。**傳統上，網路操作員已習慣在個別獨特的網域中管理營運。此模式可能會在提供一致服務時造成障礙，減緩組織滿足變更業務需求之能力的速度。在多雲端環境下，網路必須跟上速度。

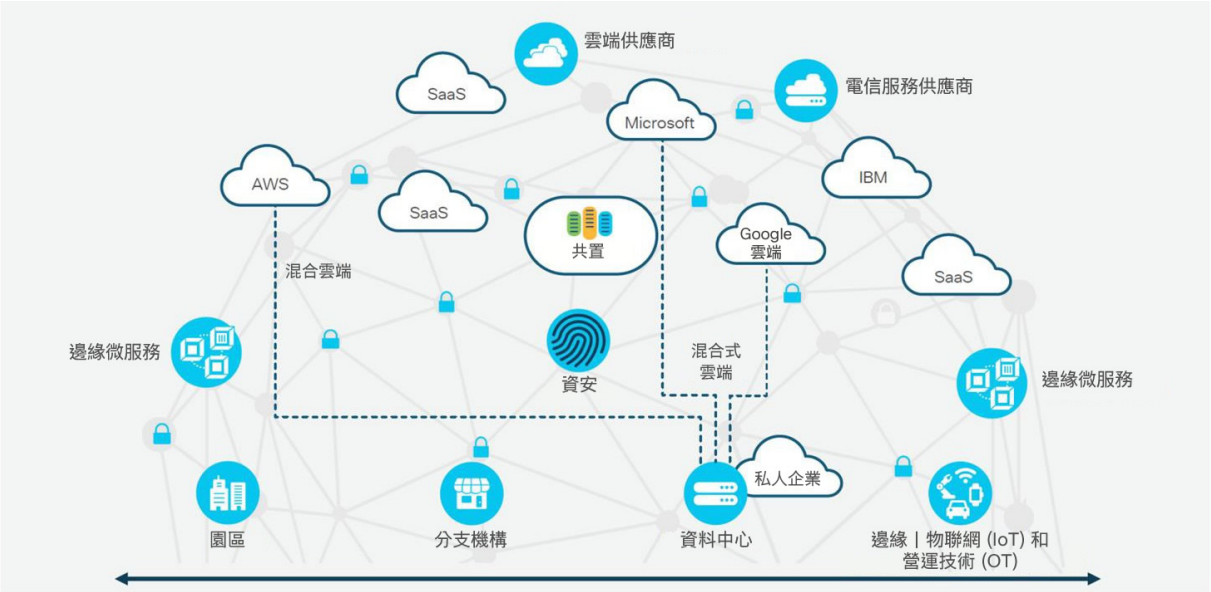
   同樣地，對於橫跨多個網域之間（從使用者到工作負載）之網路營運一致地安全和自動化，以及端對端原則型自動化實現跨網路分段、應用程式服務層級與存取原則的需求日益增加。

思科的多雲端網路現代化方法

思科已開發多雲端網路方法，專門設計用於支援管理分散式應用程式，以及安全可靠地存取此類應用程式。在以上兩種情況下，意向型網路為思科的核心方法，專門針對在日益複雜之多雲端環境中提供必要的自動化、深入分析及安全性（參見圖 5）。

圖 5

思科的多雲端網路：各種應用程式服務之間的安全存取與連線



資料來源：思科，2020 年

適用於分散式工作負載的思科多雲端網路

思科的混合式 IT 和多雲端網路方法，可協助雲端和網路架構師開發一致且簡化的作業模式，從內部部署資料中心延伸至公用雲端及邊緣環境。該方法的開發旨在簡化多雲端網路的固有複雜性，其中包括人工智慧輔助的日常網路營運。

適用於工作負載的思科多雲端網路產品組合包括管理、網路、安全性及軟體組件（參見圖 6）。

整合多雲端網路營運

Cisco Nexus Dashboard 平台提供整合的主動式營運，並促進資料中心和多雲端網路之間可付諸實行的深入分析。該平台可透過提供統一的資料中心站點及思科和第三方營運服務入門體驗，協助降低營運複雜性。支援的服務包括：

- **Cisco Multi-Site Orchestrator (MSO)** 為一種混合雲端工具，專門設計用於協調內部部署、雲端及邊緣之間的 Cisco ACI 網路原則和自動化。
- **Cisco Nexus Insights** 提供即時監控和分析，以識別異常狀況、提供根本原因分析、協助容量規劃及加快疑難排解速度。
- **Cisco Network Assurance Engine (NAE)** 可提供持續分析，並確認網路狀態是否與所需意向保持一致。

圖 6

適用於分散式工作負載的思科多雲端網路產品組合

*藍圖

資料來源：思科，2020 年

適用於多雲端工作負載的網路自動化

Cisco ACI 為意向型、軟體定義資料中心網路解決方案，專門設計用於支援應用程式靈活性和多雲端自動化。Cisco ACI 元件包括：

- **Cisco Application Policy Infrastructure Controller (APIC)** 為 ACI 控制器，可進行網路自動化、可程式化和集中管理。
- **Cisco Cloud ACI** 可將 ACI 原則轉譯為雲端服務供應商（例如，AWS 和 Microsoft Azure）提供之雲端原生建構和服務。

Cisco Data Center Network Manager (DCNM) 為管理平台，適用於所有 Cisco NX-OS 支援的部署，其橫跨內部部署和雲端環境之間的全新光纖架構和儲存網路。

保護多雲端資料中心

Cisco Secure Data Center 包含結合 Cisco ACI、Cisco Firepower 新世代防火牆、Cisco Stealthwatch 及 Cisco Tetration，可協助保護現代資料中心和雲端環境。其結合的功能包括：

- 能見度橫跨資料中心和多雲端環境，其中包括使用者、裝置、網路、應用程式、工作負載及程序
- 透過從網路到個人應用程式的精細控制，分段可縮小攻擊面並防範攻擊者橫向移動。
- 在駭客竊取資料或中斷作業以前，威脅保護可阻止外洩，以及快速偵測、封鎖並回應攻擊

適用於存取的多雲端網路

將企業網路延伸至 SaaS 和 IaaS 環境

Cisco SD-WAN OnRamp 專門設計透過互連供應商或甚至透過共置環境，從分支至網際網路，直接為一或多個雲端（IaaS 和 SaaS）提供進階的一致連線。SD-WAN 為使用者在雲端中提供同等的安全性和應用程式效能，如同內部部署環境。此外：

- **適用於 IaaS 的 Cisco SD-WAN Cloud OnRamp** 可將企業 WAN 延伸至公用雲端，並將公用雲端基礎架構整合至 SD-WAN 網狀架構。適用於 AWS 和 Azure 之 IaaS 的 Cloud OnRamp 支援雲端原生建構（例如 AWS Transit Gateway 和 Azure 虛擬 WAN），可透過 Cisco vManage 單一管理介面簡化分支連線至公用雲端中託管的應用程式。
- **適用於 SaaS 的 Cisco SD-WAN Cloud OnRamp** 使用即時分析引導使用者採用最佳執行路徑，以獲得最佳應用程式效能；此分析支援常用 SaaS 應用程式，以及從區域資料中心的分支站點和閘道的直接網際網路存取。

- **適用於共置的 Cisco SD-WAN Cloud OnRamp** 可在重要的區域共置中彙總分支，並讓 IT 操作員能夠在網路邊緣安全地部署多雲端連線網路服務（例如，防火牆和負載平衡器），以獲得強化的服務品質、簡化的管理及提升的安全性。
- Cisco SD-WAN（透過互連供應商）協助建立從分支至雲端的虛擬專用互連，以強化連線至多個雲端供應商的可用性和可靠性。

保護多雲端存取

思科結合網路和安全性功能，可在 SD-WAN 平台和雲端中提供完整堆疊的多層次安全性。整合的 SD-WAN 安全性方法可為 IT 部門配備威脅防禦，以因應隨時隨地需求（針對連線至多個 SaaS 或 IaaS 雲端、至資料中心或在網際網路上連線的分支）。具備 Cisco Umbrella 的 Cisco SD-WAN 可提供完整支援雲端功能的 Secure Access Service Edge (SASE) 架構。

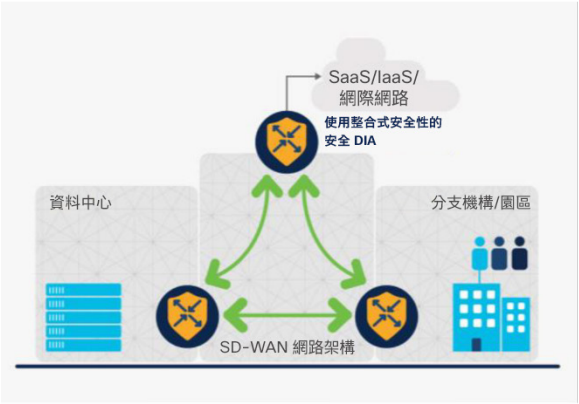
SD-WAN 安全性

Cisco SD-WAN 提供威脅防護和能見度以抵禦 Web 攻擊。透過 Cisco Umbrella 雲端或路由內建功能來提供，企業可取得 SaaS 和網際網路應用程式的能見度，並加以控管（參見圖 7）。此外：

- **具備 Umbrella Cloud Security 的 Cisco SD-WAN** 提供各種雲端提供的安全性服務（例如，DNS 安全性、安全 Web 閘道、防火牆即服務、雲端存取安全性代理 [CASB] 及零信任存取）。如此可針對惡意的 Web 流量和進階攻擊提供保護，以及從 Cisco SD-WAN 提供自動化設定。
- **Cisco SD-WAN On-Premises Security** 具備內嵌 SSL 加密、企業防火牆、入侵防護、URL 篩選及惡意軟體沙箱，可提供安全 WAN 存取並滿足現場法規遵循需求。

圖 7

Cisco SD-WAN 和 SASE 提供安全的多雲端存取選擇



整合式內部部署安全性

雲端安全性和 SASE

資料來源：思科，2020 年

思科雲端安全和 SASE 架構

思科在 SASE 架構內結合 SD-WAN 網路、雲端式安全性及零信任的元素。

- **Cisco Umbrella** 是一種雲端安全性服務，可將多個安全性功能整合為單一服務，協助各種規模的企業採用直接網際網路存取 (DIA)、安全雲端應用程式，以及將保護延伸至漫遊使用者和分公司。
- **Cisco Duo** 是一種以使用者為主的零信任資安平台，適用於所有使用者、裝置及應用程式。Duo 的多重因素驗證 (MFA) 可讓組織驗證各地任何使用者的身分，再授與內部部署或雲端應用程式的存取權。

挑戰/商機

現代化和轉型企業多重雲端網路的商機，可為客戶和廠商同樣提供巨大的希望。透過現代化核心對邊緣網路，以因應現代應用程式、混合式 IT 及多雲端，許多組織可在橫跨分散式應用程式環境之間，提供所需的靈活性、彈性、延伸擴充性、可靠性及安全性。優點包括產品和服務上市時間加快、企業恢復能力改善、整體 IT 效率提升，與佈建、疑難排解和補救速度加快，以及提供使用者更佳且回應速度更快的應用程式，進而改善數位體驗。

對於尋求現代化多雲端網路的組織，主要的挑戰為瞭解目前和未來應用程式環境，其中包括在公用雲端（IaaS 和 SaaS）部署應用程式的計劃。此外，組織將必須確保其 IT 營運（包括其網路團隊）與業務類別 (LOB) 和開發人員密切配合，以確保基礎架構適切符合策略意圖和業務目標以及開發人員和應用程序要求。

對於尋求現代化多雲端網路的組織，主要的挑戰包括瞭解目前和未來的應用程式環境，以及 IT 和業務類別 (LOB) 與開發人員的配合狀況。

對於思科而言，主要的挑戰為確保其多雲端網路產品組合，透過橫跨多個公用雲端之間豐富的遙測和能見度與廣泛功能等領域之產品功能深度，持續充分地符合、支援及適應變化的混合式雲端和多雲端要求。

思科的網路產品和技術必須持續創新，以及提供位於內部部署和公用雲端環境的工作負載和應用程式之間的連線支援，同時緩解在多個雲端供應商之間建立和維持一致網路和安全性原則的複雜性。此外，SD-WAN 的邊緣產品組合必須持續發展，以滿足網路營運團隊的需求與雲端、應用程式及安全性要求。

最終，思科必須確保滿足客戶需求，超越傳統和非傳統競爭廠商，其中包括其他資料中心網路 SDN 和 IBN 廠商，以及 IaaS 公用雲端服務的多雲端網路新創廠商和供應商。

結論

數位化轉型的必要性和多雲端採用數增加，正重新劃定資料中心的範圍，並重新定義資料中心網路的需求，以及邊緣（存取和徹底體驗應用程式的位置）網路要求。原因在於應用程式和工作負載（現代組織的數位命脈）目前為分散式，不僅處於內部部署資料中心，亦位於多個公用雲端。如此不僅會變更工作負載配置，亦會改變分支機構、園區，甚至在家工作 (WFH) 環境的流量和存取要求。

雖然管理和完整利用多雲端為複雜和艱鉅的任務，但建立用於容納和提供分散式工作負載的現代化多雲端網路，可大幅降低複雜性，並對於成功執行多雲端策略和數位轉型計劃具有重大貢獻。

意向型網路（涉及使用宣告式意向型程序和封閉迴路網路程序）可為此多雲端網路環境帶來簡易性，使網路操作員和雲端架構師能夠主動管理網路，並維持可用性和可靠性，同時在橫跨所有多雲端網路的所有位置之間定義和實施零信任網路安全性。

如果網路和雲端架構師根據應用程式和多雲端策略來發展和執行網路基礎架構的策略藍圖，則將可提供所需的靈活性、彈性、可擴充性及安全性，以支援和提供分散式工作負載，為其組織帶來前所為有的企業價值。

贊助者的話

思科的意向型網路解決方案可協助組織實現多雲端目標，例如管理橫跨多雲端之間的分散式應用程式，以及最佳化使用者體驗。

思科多雲端網路解決方案正協助 IT 團隊在多雲端之間提供連線、安全性及一致原則，以達到輕鬆管理與簡易性。透過彈性的使用模式、廣泛多樣的生態系統及創新來簡化營運和降低風險，IT 人員可將資料中心延伸至資料所在的任何位置，並在使用者隨時隨地需要時提供安全存取。

若要深入瞭解思科產品組合，請造訪 http://www.cisco.com/go/multicloudnetworking

關於 IDC

國際數據資訊 (IDC) 是市場情報、諮詢服務及資訊科技、電信與消費者技術市場相關活動的優質全球供應商。IDC 協助 IT 專業人員、企業主管及投資社群依實際狀況做出與技術採購和企業策略相關的決策。超過 1,100 名 IDC 分析人員在全球 110 多個國家/地區，針對有關技術與產業機會提供全球、區域性和在地專業知識與趨勢。50 年來，IDC 不斷提供策略深入見解，以協助我們的客戶達成其重要的業務目標。IDC 為全球主要技術媒體、研究及活動公司 IDG 的子公司。

全球總部

5 Speen Street
Framingham，MA 01701
美國
508.872.8200
Twitter：@IDC
idc community.com
www.idc.com