解決方案的相關注意事項：

建立靈活且具彈性的基礎架構

在當今節奏快速且競爭激烈的商業環境中，敏捷性與創新乃是帶領公司邁向成功的關鍵要點。在技術不斷演進的同時，現代的網路也必須要具備相對的適應性，好利用最新的技術進展來跟上創新的步伐、實現全新應用程式 / 服務的高效部署並提供應對不斷變化之市場需求所需具備的靈活性。

現代化的步伐永不停歇

Gartner 的見解報告指出：相較於 2021 年的 20%，到了 2026 年，至少有 50% 的內部應用程式會迎來現代化，好整合 SaaS 管理平台（SMP）工具。在迎來數位化的同時，網路的動態程度也隨之變得愈加顯著，且會不斷地變化更迭。各式各樣的因素（舉凡遠端工作、多雲端擴展、全新的網路安全需求以及全新技能組合的需求）都加快了當今網路現代化的速度。

傳統關鍵網路服務的缺點

網路基礎結構有包含許多的元件，例如防火牆、路由器、交換器、Wifi 裝置、網域名稱伺服器、DHCP 伺服器等等。企業組織大多已有將重點基礎結構的元件升級為現代的硬 / 軟體。那麼，網域名稱伺服器與 DHCP 伺服器的升級事宜呢？還有，想請問您的核心網路服務採用的仍是傳統的技術與服務嗎？過度仰賴傳統的網路服務（免費軟體、自助式服務或是各種不同的系統）可能會是您數位化旅程中的巨大阻礙。

- **傳統系統間會相互** 脫節：手動管理成本高昂，且停機和服務中斷的風險極高。
- **傳統系統的**運行效率低下：作為數位化或是併購策略計劃的一部份，當今的網路必須要能夠快速地應對全新的想法和技術。
- **傳統系統**漏洞百出：安全差距和缺乏情境意識輔助容易導致威脅修復效率低下或是有所延誤。

DNS 和 DHCP 對所有網路都至關重要，如果您仍在使用原生服務，您的網路可能會遭受大規模的中斷。

現代化的關鍵驅動因素：放眼未來

各家企業組織都有在著手現代化其網路，以應對不斷增長的法規環境、資源限制、演變不斷的威脅以及安全領域技能缺口等等的挑戰。企業組織必須不斷地縮短停機時間、管理開銷並將安全漏洞降到最低，好提供 100% 的正常運作時間、接受全新想法並加強既有的安全堆疊。想要這麼做的話，我們就會需要重新思考應對重點網路作業的方式，舉凡 DNS、DHCP 和 IP 位址管理（統稱為「DDI」）。以下是推動您網路現代化的重點因素。

簡化作業：以專門打造的工具來取代免費軟體

天下沒有白吃的午餐。即便業務初期的資本支出看似較低，但長期下來，使用免費或是低成本 DDI 工具所會產生的營運支出將會逐步蓋過其優點。由於系統本身以及缺乏高階功能（高可用性、發現閒置的虛擬機器、政策制的驗證功能等）的限制，Microsoft 或是其他開源工具所提供的免費軟體解決方案無法因應眼下的成長並適時進行擴展。Microsoft 的基礎結構也容易因為一次又一次的修補更新而中斷或是停機，也或者會迫使您遷移至 Azure AD。手動管理分散式網站會導致整體作業效率低下，並導致開銷成本的增加。

最好的方針是去利用**專門打造的工具**來精簡化重點任務的作業。這些工具是以「全球化」的理念為基礎所打造的，讓您能夠將其流暢地擴展到多樣化的基礎結構與遠端地點，從而減少作業任務。這些工具會透過提供自動化、發現和集中式網路的資訊能見度來精簡管理業務、盡可能提高維護效率並節省大家的時間。您可以藉由這些工具來實現零停機的升級事宜，好透過更高的可用性來縮短停機時長。

加速創新：使用單一一個集中式工具來取代分散式系統

大多數企業使用兩到四個 DNS 解決方案，這使得管理關鍵服務和更快地回應問題變得更加困難。組織和資訊孤島經常導致延遲和錯誤。不同雲端供應商的命名慣例和作業模式導致配置錯誤和停機。網路中的碎片化可見性增加了故障排除和審計所需的時間。

企業組織必須要能找到一個效率高且有效的解決方案，好加速創新並實現多雲端的擴展 / 併購業務計畫。投資**集中式工具**能夠幫助您透過自動化、單一 DNS 命名慣例以及內部部署和雲端網路的情資能見度來實現這些目標。與其混合使用多種不同的系統，您可以考慮改用集中式的工具來快速地對應作業需求並提高工作效率。集中式的工具能夠幫助您取得策略控制機能 / 一致性、實現更高的故障排除效率 / 更優質的協作體驗，消除錯誤配置 / 相關錯誤並降低審計 / 合規性風險以及營運成本。

保護品牌完整性：利用 DNS 及早偵測威脅

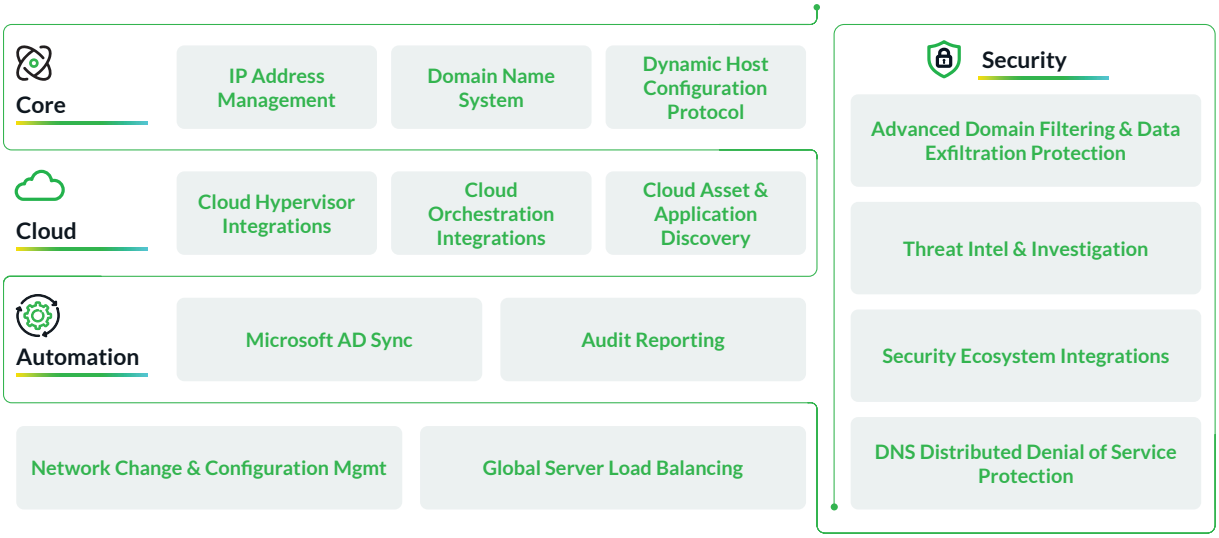
惡意軟體、勒索軟體、仿冒網域、資料外洩和網路釣魚等資安威脅演化不斷，對企業品牌識別和資料保護構成了巨大的風險。市場中現有的解決方案忽略了 DNS 的部份，無法有效預防資安攻擊，進而產生了不容忽視的安全差距。光是在過去一年中，駭客就使用了近 42,000 個仿冒網域名稱來進行大規模的網路釣魚攻擊。此外，由於系統是孤立且分散的、技能短缺、手動管理以及缺乏情境意識等等的原因，SecOps 的作業效率偏低且回應時間容易有所延誤。

及早偵測威脅可以協助降低資安風險並縮小安全差距。運用 **DNS 制的威脅獵捕**功能可以更早一步地偵測並阻斷威脅，這是因為大多數的網路攻擊都會透過 DNS 來發起。使用 DNS 作為第一道防線可以有效攔截資料外洩、網域生成演算法和冒名者的危害，並保護所有 IoT/OT 裝置的安全性。這麼做能夠藉由縮短事件調查時長、實現自動化修復並主動評估弱點風險來提高 SecOps 的作業效率。

適用靈活且具彈性之基礎結構的 INFOBLOX 解決方案

情資能見度、自動化與管控機能

Infoblox 能夠為企業組織提供無與倫比的情資能見度、自動化機能以及掌握與其網路連線之人事物的控制能力。透過消除繁複且效率低下的強制性維護工作並自動化勞力密集的作業任務，Infoblox 能夠幫助您大幅縮短昂貴的停機時長，並減輕網路資產庫存管理相關的工作負擔。Infoblox 解決方案乃是以安全為核心，透過強化情境感知機能來減少誤報的情況並提升工作效率。Infoblox 能夠為您提供：



圖一：Infoblox 解決方案

總結

「現代化」帶動了數位化轉型。選用合適的解決方案能夠幫助您持續推動網路的現代化。過往大家用來管理重點網路服務的傳統方針會阻礙您加快創新、對應更迭不斷的業務需求並保有業界的競爭力。透過善用 Infoblox 所提供的情資能見度、自動化和管控功能，來以合適的速度實現貴公司的網路現代化目標。

企業總部
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

資料版本：20230803v1