思科 IT 如何保護其資料中心

思科 IT 方法

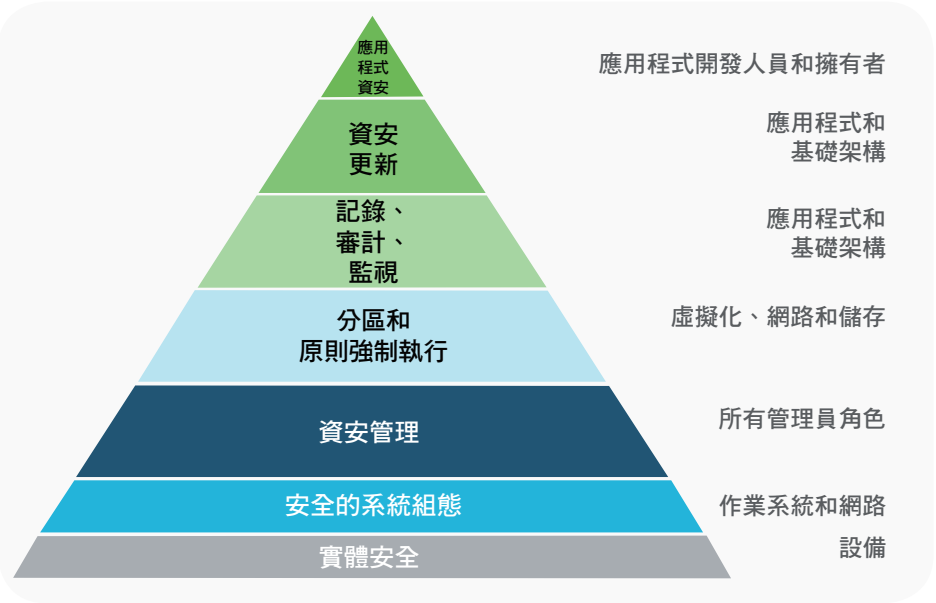
簡介

在保護企業網路安全的方法中，實作健全的資料中心安全功能是相當重要的基礎，以便保護敏感的關鍵任務型應用程式及資料。除了保護實體資料中心外，還必須顧及資料中心和虛擬環境會合的交集，而其中的複雜性構成了相當獨特的情況。在虛擬環境中複製存在於實體資料中心的相同分段，使多租戶成為重要的資安創新。多租戶架構可讓應用程式以虛擬方式為資料和組態分區，讓每個用戶端都能自訂虛擬應用程式。資料中心內的重要資產包括支援身分識別、認證和授權、組態管理及安全性的系統，且均需進行特殊處理。為了保護網路，資料中心資安採用了多項功能，並將其整合至資料中心的多項技術。

部署：資料中心空間中的安全階層

資料中心資安的基礎，是設計為多個層級的一系列程序，以便保護客戶資料和智慧財產等重要資產。思科的資訊安全架構師 Scott Stanton 表示：「思科託管了大量的客戶資料，因此我們採取以資料為主的資安方法。我們把重點放在包含客戶資料的系統，因為這些系統是維護客戶信任的關鍵。」資料中心安全性基礎必須具備五項安全功能：預防和減緩、評估、修復、偵測及遏制。我們實作控制項來預防或減緩已知的風險；評估環境中的資安漏洞；修復並解決所有已知問題；偵側事件在網路、伺服器或應用程式上發生的時間；最後，遏制已遭入侵的系統，以防止受影響的系統進一步執行動作（請參閱圖 1）。

圖 1. 資料中心資安基礎概覽



Stanton 說明：「我們擁有安全的系統組態、安全的管理程序、階層分區和網路安全性原則強制執行、防火牆、入侵偵測系統 [IDS] 或入侵防禦系統 [IPS] 類型的監控與封鎖技術、可更新環境的能力，以及應用程式安全性控制項和安全的軟體開發，可有效保護資料本身。在較低層級的控制項一旦失敗或遭到入侵，則遭到入侵的控制項通常會破壞更高層級的控制項。」前述五項能力皆會套用至資料中心內的技術，包括系統上的應用程式、在硬體上執行的作業系統、虛擬化技術（例如 VMware 或 OpenStack）、儲存系統及網路。應用程式安全性控制項、遏制、防禦及監控能力皆為保護資料安全的必備條件。

擷取並檢查重要的網路流量，讓您可以迅速採取行動。為了密切查看網路和執行異常偵測，思科®資安團隊將重點放在兩個區域：網路本身的封包和從網路平台擷取的 NetFlow 資料。從這些來源取得的資訊會透過遠端切換連接埠分析器 (RSPAN) 或 NetFlow 摘要回饋至網路設備旁邊的安全性裝置，並接收大量有關該資料品質的資訊。來自思科收購之 SourceFire 思科 IPS 技術會搜尋資料中心內的殭屍網路、病毒及主機已被入侵的證據，並同時在核心資料中心閘道層上實際執行監控作業。雖然該層使用了多項技術，不過主要元件仍為可提供負載平衡功能的思科 Catalyst® 6500 系列交換器。

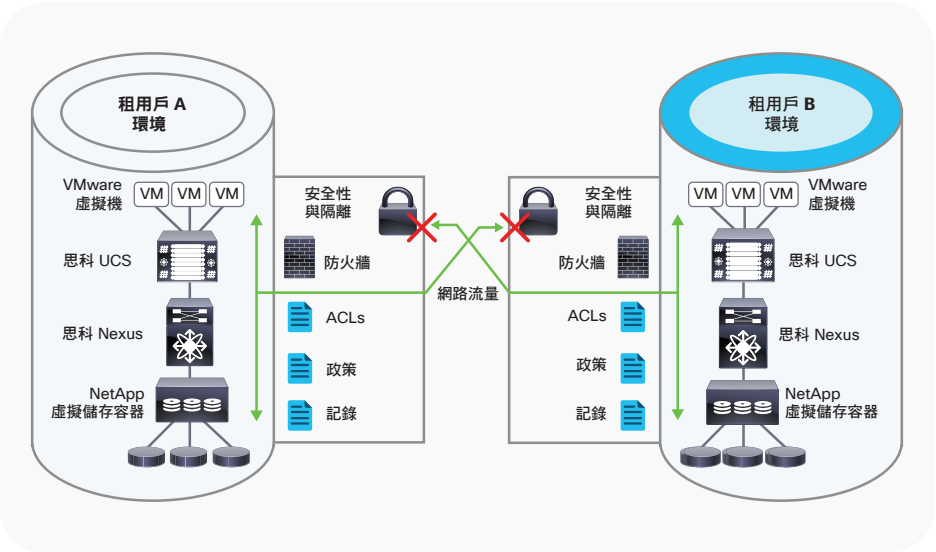
從網路角度來看，思科主要的作用在於預防和減緩、偵測及遏制方面，並以防火牆作為其中一個首要控制項。技術人員 Ben Kelly 表示：「在資料中心網路安全空間中，我們建立了一些容器，並將應用程式或應用程式的階層放到這些容器中。這些通常為子網路式邊界，並透過存取控制清單或 ACL 及防火牆來保護流量。我們在思科 Nexus 平台上託管此項目。」思科擁有許多防火牆，包括公司防火牆和資料中心對資料中心特定的專用防火牆。在內部和非軍事區 (DMZ) 資料中心網路的交會處，流量會進入一個安全控制堵塞點，即為專用防火牆。

資料中心的基礎為可執行分為存取、分佈及核心等三層網路架構的思科 Nexus® 平台。其中思科 Nexus 交換器會用於存取層。在分佈層中，思科 Nexus 可作為第 2 層和第 3 層之間的界限。從網路的角度來看，分佈層也屬於 Pod 之一。Pod 由 思科 Nexus 的分佈切換和分佈層之下的所有項目（包括存取層、伺服器和與該層連接的儲存空間）組成。這些 Pod 上方具有以思科 Nexus 交換器為基礎的高速、高彈性核心。運算則以階層式思科整合運算系統™（思科 UCS®）伺服器為根據。思科 UCS FabricExtender 可從思科 UCS 網域直接上行至思科 Nexus 分佈層（請參閱圖 2）。

Kelly 表示：「那就是傳統網路。但是，透過 FabricPath 與思科以應用程式為中心的基礎架構（或稱思科 ACI）解決方案等技術，我們看到了廣泛稱為『資料中心光纖』的發展趨勢。」從網路架構拓撲來看，網路會逐漸趨於平坦，而且網路只有兩個階層：連接至端點的分葉和與所有分葉互連的主幹，而非存取層、分佈層及核心層。此特殊的拓撲會呈橫向而非縱向擴展，符合資料中心流量模式的趨勢。」

「過去我們看到較多從北向南的流量，也就是從伺服器到存取層、分佈層和核心層，以及在資料中心範圍之外的流量。而今日我們看到的是更大量的東西向流量，或資料中心內伺服器到伺服器的流量。」網路光纖的靈活度高，具備高輸送量和低延遲的特性，並且可在資料中心任意兩個端點之間提供一致的延遲。

圖 2. 多租戶資料中心安全性架構概覽



為資料中心網路分段

在高階層中，資料中心網路和運算 Pod 會分成生產、非生產及 DMZ 環境，這樣可讓內部區域的分支隔離敏感系統，而不需要重新分段。思科網路區分為兩個主要安全性區域：標記為 DMZ 的網際網路對向系統，以及無法從網際網路直接連線的內部系統。內部網路具有稱為受保護網路的其他安全網路類型，可使用 ACL 來強制執行安全性政策。這些受保護的網路可用於敏感的主機，也可作為 DMZ 和內部網路之間的緩衝。思科資料中心在思科 Nexus 平台上具有數千種 ACL 規則，可保護不同應用程式元件之間的介面。

近年來，網路最佳化、彈性及靈活度的趨勢啟發了虛擬路由轉送 (VRF) 的使用。VRF 為第 3 層網路的分段，但允許使用共用的網路基礎架構。基本上，Pod 可為 DMZ 環境和內部環境，但仍會保有兩個網路之間所需的邏輯隔離。

Stanton 表示：「我們觀察到該趨勢會在未來持續發展，而對此我們可提供各種結構型解決方案，例如思科 ACI™ 以及動態結構自動化，或者稱為 DFA。這個可擴充、具高效能的自動化基礎架構是雲端運算中一項重要的功能。

支援多租戶的資料中心必須能夠在不同業務部門或客戶之間分隔伺服器、網路及儲存服務。而此作業主要是透過虛擬化執行，而非進行實體隔離。除了可提供透明的虛擬環境之外，對每個基礎架構元件的邏輯控制還可強制執行租用戶之間的分段，並提供存取控制、佈建、監控及資源消耗評估等功能。

思科以應用程式為中心的基礎架構原則與資料中心的安全性

思科 ACI 改變了網路管理和資安政策在資料中心中的運作方式。在目前的 VLAN 或子網路容器原則模式中，使用 VRF 對運算工作負載的原始類型進行邏輯隔離相當繁瑣。ACL 通常會分佈在整個資料中心，並且需大量的人力手動進行查找與修改作業。此模式會影響營運費用 (OpEx) 和靈活性。而以應用程式為中心的網路檢視則表示網路的基礎組態將一律以應用程式的網路設定檔為基礎，且對網路技術、拓撲及組態不需要有詳細的認知，即可理解網路相依性。在定義應用程式需求方面，思科 ACI 提供了可讓所有團隊共用的通用營運模式。思科 ACI 利用預先定義的應用程式需求和政策設定檔，自動化網路的佈建、網路應用程式服務、資安政策，以及工作負載配置。思科 ACI 可讓思科資安組織更輕鬆地管理資安政策和資料中心網路中的控制項。

思科 ACI 的顯著優點是它使用可根據關係來定義應用程式的政策式模式。例如，如果應用程式具有 Web 伺服器、應用程式伺服器及資料庫伺服器，這些伺服器會定義為可與其他應用程式共用的政策物件。應用程式工程師可以為 Cisco Application Policy Infrastructure Controller (APIC) 中的系統建立對應，讓 APIC 再接著建立基礎網路，啟用這接關聯。雖然基礎網路定義了網路、子網路及 VLAN，但這些拓撲概念不會用於強制執行原則。政策強制執行是分開的，如此可讓思科 ACI 結構有效轉發流量，同時非常精準地控制哪些系統可進行溝通。思科 ACI 遵循「允許清單」模式並具備預設的安全性，可直接繫結至資安團隊的預防與減緩功能，以及防止不必要的存取。除非已明確設為允許該流量，否則該架構將會封鎖兩個系統之間的流量。在思科 ACI 環境中，資安政策是以結構端點為基礎（即連接埠或 VXLAN），並且與 IP 定址脫鉤。因此，端點移動性對資安政策強制執行的影響很小。資安管理已簡化，並透過自動化集中式管理的合規性與稽核減輕風險。

思科 ACI 與資料中心中的多租戶

租用戶隔離、資源區隔及身分識別型資源授權為雲端多租戶的三大支柱。多租戶環境必須使租用戶保持獨立並互相隔離，以確保租用戶之間的安全性。多租戶環境中的共用資源也必須根據授權或訂閱來佈建，且必須強制執行資源保證，以便高使用量或使用率不會對其他租用戶造成負面影響。

從運算虛擬化的角度來看，必須在 Hypervisor 中強制執行多租用戶建構。虛擬 CPU 與 RAM 的佈建必須保證提供適當的授權和區隔以及管理上的隔離。在網路與儲存層級中，邏輯分段是執行租用戶隔離與資源分離的主要方法。在這個環境中，程序、自動化和協調流程可確保資源權利並將網路和儲存校準運算和虛擬化平台。在執行網路租用戶隔離時，思科 IT 先前會使用虛擬安全閘道 (VSG)，與思科 Nexus 1000V 虛擬切換進行整合。由於 VSG 在虛擬交換器連接埠進行安全性原則強制執行（第 2 層），因此可在多個租用戶中配置大型 IP 子網路，進而以極具效率且高度彈性的方式使用 IP 地址空間。在此單一子網路中，除非 VSG 安全性原則允許，否則不同租用戶之間無法互相存取。

思科 ACI 會將租用戶建構以原生方式轉譯為基礎網路建構（例如 VRF），以便在網路層級執行邏輯隔離。思科 ACI 原則模型可支援每個租用戶，且租用戶組態會存在於 APIC 介面中。思科 ACI 會透過其本身在原則模型中的建構，以原生方式支援多租戶架構。思科 ACI 原則物件在網路層級中可具有不同的範圍層級（應用程式、租用戶或全域），以及多個租用戶資料粒度層級（端點群組、應用程式網路設定檔、橋接網域及 VRF）。IT 團隊和業務單位可以微調多個租用戶的運算環境，並在一個小時內讓應用程式上線，大幅縮短傳統 IT 佈建流程的時間。

多租戶架構亦需使用整合式身分識別。IT 部門需要知道哪些人具有特定環境的存取權限。授權與權限管理可讓特定使用者管理其在多租戶環境中的資源，並且僅需對其消費的資源付費。

管理、服務及支援

資料中心網路安全性目前包含兩個主要管理類別。第一個類別以防火牆和思科 Nexus ACL 為中心。第二個類別則著重於 IPS/IDS 監控和事件回應功能的管理。思科網路團隊管理會在全域基礎架構服務 (GIS) 中管理防火牆和 ACL 的組態和裝置。GIS 可控制與管理防火牆和 ACL 的變更。使用 GIS 打開報修單後，在網路團隊執行要求的變更之前，資安團隊與 GIS 之間會進行多次的反覆查看。例如，如果員工需要使用特定伺服器與某個連接埠上的其他伺服器進行通訊，則在將請求路由至 GIS 以便進行實作之前，資安團隊會先調查其是否為有效的請求。

IPS/IDS 的管理和監控皆由思科電腦資安事件應變小組 (CSIRT) 負責。CSIRT 會在網路流量和裝置周圍使用可產生資料的感應器。出現異常時，系統會將異常標示為封包或階段作業相關事件，並傳送給第一層級的分析師進行審查。如果分析師發現任何與該事件相關且值得進一步調查的內容，第一層會將警示升級交付給調查人員，以便進行更深入的調查和回應。如果調查人員無法追蹤到有問題之系統的擁有者，網路中的工具得以「黑洞方式」破壞該個發生問題的系統，直到可採取長期動作為止。

Stanton 表示：「如果我們網路上的受感染系統嘗試散佈到其他系統中，我們能夠在我們的核心網路中，透過稱為『即時黑名單』或 RBL 的程序，在網路階層中以黑洞方式進行破壞」。「有問題的封包將永遠不會到達他們的目的地。」

CSIRT 可能會在不知道主機網路連接位置的情況下，將主機從網路中移開，並從本質上移除主機的網際網路連線。視主機與網路核心的距離而定，這些黑洞路由器之中的一個也可能會將這些主機從思科內部網路中移開。主機新增至 RBL 或黑洞之後，來自該主機的封包會進入黑洞且不會出現。

程序和管理

前述為以網路為中心管理控制項的兩個主要類型。我們的應用程式與資料安全性大多仰賴於金字塔的頂端（請參閱圖 1），並且把焦點放在程序上。從軟體角度來看，資安團隊對我們環境中的應用程式具有安全性需求。此外，Web 應用程式防火牆 (WAF) 通常會在 Web 伺服器上保護 Web 應用程式免受惡意要求的攻擊。WAF 與網路入侵偵測系統監視異常網路活動的方式極為類似，可分析特定 Web 伺服器或 Web 伺服器組前面的網路流量是否有異常的 Web 要求，例如跨網站指令碼、SQL 資料隱碼攻擊、參數篡改、暴力攻擊、邏輯迴避，以及其他等級的 Web 應用程式攻擊。WAF 可在應用程式安全性階層中提供監控與防護功能。而與測試 Web 應用程式是否有資安漏洞相關的程序和管理則由資安團隊 Web 應用程式安全性程式負責管理。這些程式包括基本的應用程式弱點評估 (BAVA) 和深入的應用程式弱點評估 (DAVA)。第一個為自助服務程式，可讓每個開發人員使用以 IBM Appscan 企業為評估基準的 BAVA。開發人員可在建立 Web 應用程式時使用此工具進行掃描。如果他們遵循此程序，即可在建立應用程式時主動測試、開發及掃描程式碼以便找出弱點。開發人員將所有程式碼元件拼接在一起，並得到一個可運作的應用程式後，如果其為關鍵業務應用程式，則會進行 DAVA 檢測。DAVA 為思科的紅隊/老虎小組。這些團隊可藉由駭入應用程式來偵測並找出漏洞，以便開發人員進行修復。此作業主要為人工程序，因此需要由開發人員與資安團隊共同合作執行。此為思科應用程式安全性程式在資料中心中的關鍵元件。

資安團隊實現了 IT 和其他組織的夥伴關係價值，並設立了一個管理計畫，可將安全責任擴展到這些組織中。資安團隊為每個 IT 服務區域中的指揮，可代理許多安全質數來負責執行安全性程式，並提供 IT 服務中的資安能見度與感知功能。

Stanton 表示：「其超越了公司 IT，並包括工程和服務 IT，使我們的管理擴大至資安團隊可獨立完成的工作範圍之外。此外，整合安全指標程式能夠評估這些質數和 IT 服務擁有者的安全性法規遵循，或者應用程式是否已進行 BAVA 或 DAVA 檢測，以確保我們的人員正當行事。」

安全性不斷演進，而 IT 團隊同樣必須持續進化，並調整其資料中心的安全性。思科 ACI 可以高度安全性和完整的應用程式能見度，迅速且大規模地提供部署應用程式的網路基礎架構。思科 ACI 將整合至安全的雲端環境，以為實體和虛擬工作負載提供一致的資安政策，並讓資安團隊能夠更有效地保護資料中心的安全。

附註

本出版品說明了思科如何透過部署自家產品獲益。許多因素對於前述的結果和優勢可能都有所貢獻。思科不保證其他地方的比較性結果。

思科僅以現狀提供本出版品，其中不含任何明示或暗示的保證，包括適銷性及針對特定目之適用性的暗示性擔保。

部分司法管轄地區不允許明示或默示擔保的免責聲明，因此上述限制可能不適用於您。

更多資訊

要閱讀其他的思科 IT 案例研究，瞭解多種業務解決方案，請造訪 Cisco on Cisco: Inside Cisco IT，網址為 www.cisco.com/go/ciscoit。

C36-740863-00 06/18