概覽

益處

- 開發與業務目標一致的高安全分段策略
- 降低組織資料和資產的風險
- 在多個安全性規則間套用有效的資安和政策控制
- 簡化您的稽核設定檔，以減少稽核時間，達到節省成本的目的
- 抵禦來自內部和外部的網路攻擊，保護資料和智慧財產的安全
- 符合董事會對資安和合規性的要求
- 有效地執行資料分類計畫

思科資安分段服務

以高安全分段策略降低您的風險

網路以及使用者、應用程式和系統之間的互動非常複雜，這讓資安團隊更難以保護資料和系統的機密性、完整性和可用性。傳統的資安方式並未不能滿足以及擴充這種新技術環境，它們缺乏一致性和可擴充性，亦無法提供有效控制和監控所需的恰當詳細資料。

思科®安全細化服務提供一種策略性的基礎架構分段方法。它能讓與您類似的組織降低風險、簡化稽核概況、保護資料及應用程式，以及達到更佳的防禦力，足以滿足現今超連通複雜環境的董事會要求。

超越資料與系統保護的策略性模型

這是新的分段方法，更充分考慮到對企業和應用程式的影響以及縱向設計模式。我們的方法不僅是客戶導向，而且能延伸到網路以外，並融合了可重複使用的設計模式。這種方法給您的效益，便是一個能降低風險、簡化稽核設定檔、保護資料及符合董事會要求的分段框架。

開發您的分段策略時，我們會考慮到您特定的企業目標和技術環境。我們跳脫了典型的網路考量範圍，例如狹隘的把焦點放在孤立上；相反，我們提供的框架會考慮到身份識別與信任、可視性、政策實施、可用性及應用程式相互依存。

思科的資安顧問會與您共同識別在您環境中定義安全性範圍的重要參數。我們會視需要評估和融合不同的基礎架構分段設計模式，包括：

- 垂直產業常見的設計模式
- 根據業務或代理做區分的設計模式
- 旨在保護地域限制的設計模式
- 拓撲為主（例如遠端站台與資料中心）的設計模式
- 根據上述各項發展相互混合的設計模式

這些可重複使用的設計模式有助於確保組織間的問責制度和可視性獲得提升。它們提供一致的控制項，可以隨組織及業務的改變而靈活變化，能簡化合規性以及管理資料存取權限。思科將應用程式、資料、使用者和業務流程納入考量，以超越網路層的角度處理分段。我們的方法直接將分段策略連繫到您的業務目標。

思科資安顧問諮詢服務：經驗豐富的資安專家

思科資安顧問團隊是由一群策略和技術顧問所組成，可協助引導組織識別資安的策略性機遇。我們會協助您保護網路效能、創造競爭優勢，並獲取長遠的永續企業價值。有了優越的資源組合做為後盾（廣泛的研究與威脅情報、成熟的方法，以及跨越資安、雲端、行動能力、協同合作與數據中心作業領域的多學科專家），我們的客戶能更有效管理風險與合規性、發展強而有力的資安狀態、控制成本和達成策略性 IT 與企業目標。

後續步驟

思科資安分段服務是思科資安顧問諮詢服務組合的一部分。我們的資安顧問可協助貴組織針對安全性、合規性和威脅管理制訂穩健的策略。如需深入瞭解資安分段服務如何為您的企業帶來優勢，請聯絡當地客戶代表或授權思科經銷商。如需深入瞭解思科可如何協助您保護組織免受現今不斷變動的威脅侵擾，請造訪 cisco.com/go/services/security。

C45-736578-00 01/16