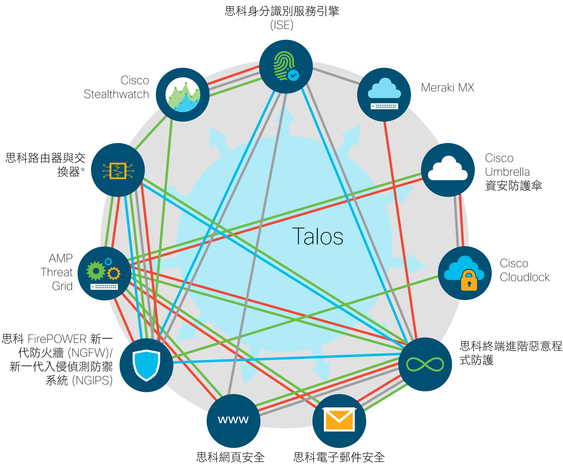
思科資安

思科資安產品以透明、自動化與精簡化的過程與您溝通，並讓安全維護更有成效。

活動　威脅情報　原則　內容



*思科整合/彙整路由器 (ISR/ASR) 與 Catalyst 交換器服務

威脅情報

透過共享**威脅情報**加速偵測的時間。

終端進階惡意程式防護解決方案 (AMP) 在倫敦為思科客戶辨識出惡意檔案。

Talos 人員立即更新有關該檔案的資訊。

Talos 人員分享該資訊給在印度的 AMP for Email 客戶。

AMP for Email 甚至可阻擋以前沒看過的檔案。

原則

透過自動更新**原則**更快地回應。

Cisco Stealthwatch 識別出使用者遭到入侵。

Cisco Stealthwatch 通知思科身分識別服務引擎 (ISE)，變更使用者設定檔為「入侵」。

透過 ISE 的整合，思科網路安全裝置 (WSA) 將自動變更使用者的原則。

內容

透過共享**內容**可防範威脅擴散。

透過 ISE 的整合，新世代防火牆 (NGFW) 與 WSA 原則可控制如使用者、裝置與位置的內容。

活動

共用**事件**以快速識別威脅。

思科認知威脅分析 (CTA) 識別出入侵。

CTA 與終端 AMP 共用警示。

警示與使用者詳細資料可在 AMP 主控台上看到。

只要按一下即可移除所有裝置上的惡意入侵程式。

有效

思科偵測的總時數為 **14 小時**，而業界的平均數為 100 — 200 天。

思科 2017 年度網路安全報告

請造訪 cisco.com/go/security 以瞭解更多>