



零信任的落地實戰

從使用者、裝置到資料中心的全方位防護

Lance 朱育民
思科台灣

2025





Why are we here today?



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

台灣零信任政府網路基礎架構

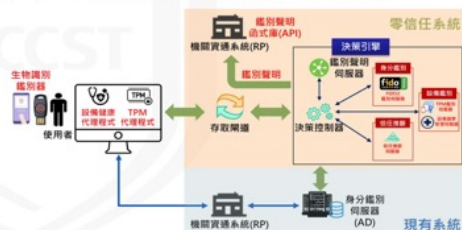
基於 NIST SP 800-207

國家資通安全研究院

政府零信任網路架構



- 參考NIST零信任架構，結合向上集中防護需求，政府零信任網路採存取門戶部署方式，具備身分鑑別、設備鑑別及信任推斷3大核心機制
- 身分鑑別：FIDO2身分鑑別與鑑別聲明
- 設備鑑別：TPM設備鑑別與設備健康管理
- 信任推斷：基於分數與情境之信任推斷機制



金融資安行動方案 2.0



六、鼓勵零信任網路部署，強化連線驗證與授權管控

世界重要國家政府推動規劃



- 零信任已從概念探討階段進入實務部署規劃，世界重要國家之政府紛紛建立國家零信任網路安全戰略



美國
具體規劃2024年前聯邦網路完成初步遷移。



歐盟
2020年建立歐盟網安戰略，提出標準框架，協助成員國轉型。

- 行政院「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任網路資安防護環境，推動政府機關導入零信任網路，完善政府網際服務網防禦深度



台灣零信任政府網路基礎架構

基於 NIST SP 800-207



金融監督管理委員會
Financial Supervisory Commission

金融業導入 零信任架構 參考指引

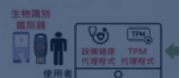
金管會
2024.7.18



國家資通安全研

政府零信任網路

- 參考NIST零信任架構
- 府零信任網路採存取
- 設備鑑別及信任推斷
- 身分鑑別：FIDO2身分
- 設備鑑別：TPM設備鑑
- 信任推斷：基於分數與



，強化連線驗證與授權管控

推動規劃



進入實務部署規劃，世
立國家零信任網路安全

歐盟



2020年建立歐盟網安戰
略，提出標準框架，協助
成員國轉型。

年至113年)之「善用智慧前瞻科技、主動
任網路資安防護環境，推動政府機關導入零
深廣度

113

資通安全責任等級
A級公務機關

信任推斷

依設備健康狀態、
資安威脅情資及使
用者情境等資訊，
動態支援存取決策

權限，並循環監控



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

CISA 零信任成熟度模型 六大高風險場域

零信任導入指引

遠距辦公

- 使用者及設備位於傳統資安防護邊境外

雲端存取

- 雲端資源位於傳統資安防護邊境外

系統維運管理

- 含重要主機設備及系統軟體(作業系統、資料庫等) 系統維運管理 之特權帳號管理

應用系統管理

- 重要應用系統之管理者(如帳號管理員)或高權限使用者帳號(如可接觸大量個資或機敏資料使用者)

服務供應商

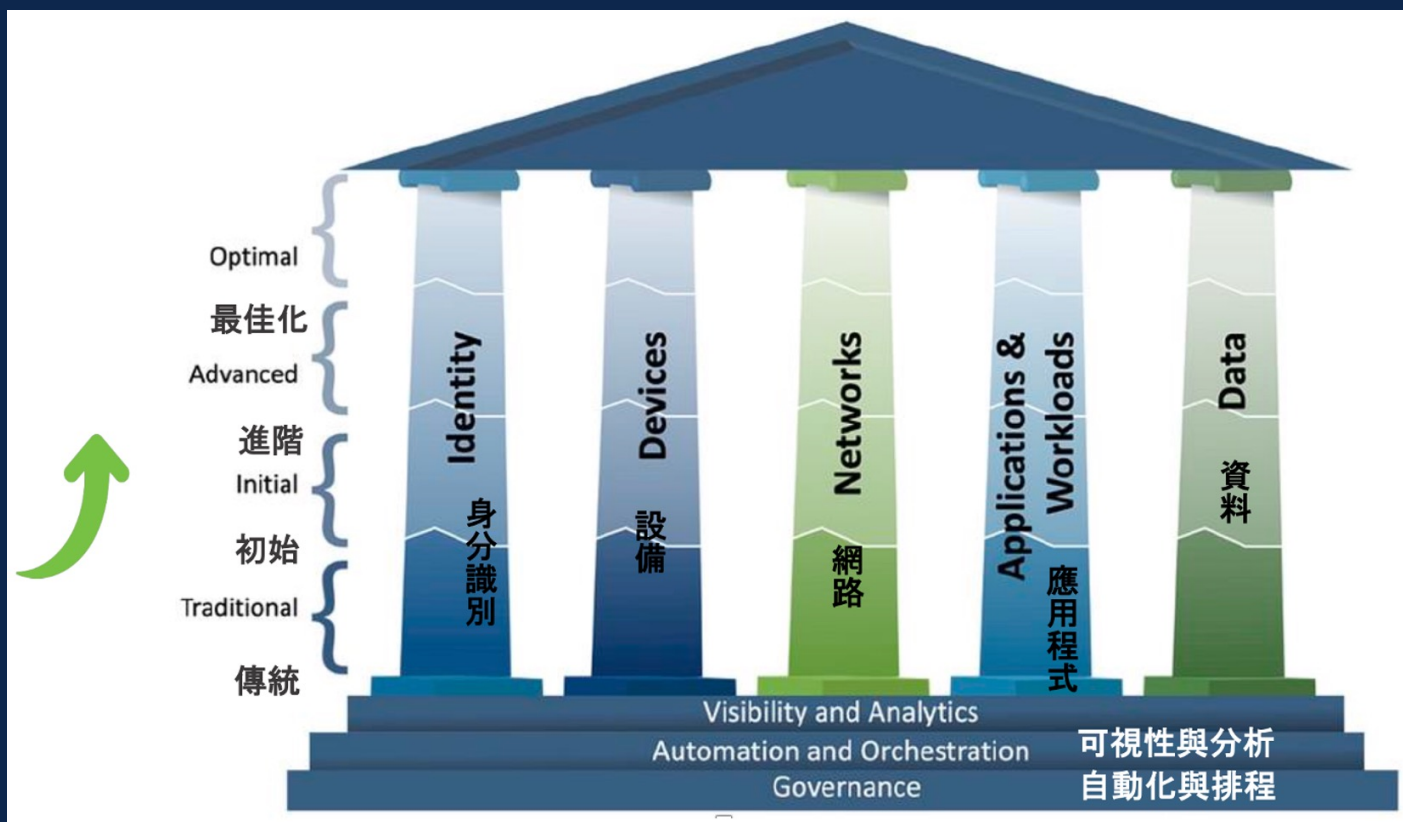
- 如委外廠商之遠端維運管理

跨機構協作

- 如重要應用系統之外部使用者

CISA 零信任成熟度模型 五大支柱

零信任導入指引



CISA 零信任成熟度模型 四大成熟度進程

零信任導入指引

循序漸進->依分級指標分階段導入

I 傳統

靜態指標

- **RBAC 基於角色存取控制**
- 優先盤點既有資安防護機制之完整性, 規劃防禦深度之優化及整合。

II 起始

動態指標

- **ABAC 基於屬性存取控制**
- 將動態屬性(如時間、地點、設備合規性等) 納為授權審核條件, 動態撤銷、限縮存取授權或發出告警。

III 進階

即時指標

- **SIEM/SOC**
- 整合或收容事件日誌, 建立定期審查及異常行為(IOC、Mitre ATT&CK TTP)之偵測、告警及回應機制。
- **UEBA** 使用者和實體行為分析。

IV 最佳

整合指標

- 建立可依資安政策快速調適之一致性且自動化之管理機制, 確保安全性及合規性。
- 點►線►面

永不信任、持續驗證



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

1. 身份

項次	支柱	功能	原則	等級	Cisco 對應解決方案	補充說明
1.1	身分	身分認證	採用多因子驗證機制，降低帳號密碼遭破解、竊聽等風險。	I	Cisco SSE + Duo	符合，Cisco SSE可以整合Cisco Duo或Microsoft AAD等機制來達成多因子認證(MFA)與無密碼認證>Passwordless)
1.2	身分	身分認證	採用包含綁定實體載具(如 FIDO、動態密碼產生器、晶片卡、蜂巢式機具具數字配對 APP 等)、排除簡訊、語音及電子郵件等 OTP 的多因子驗證機制，可抗網路釣魚風險。	II	Cisco SSE + Duo	符合，Cisco SSE可以整合Cisco Duo後可以使用 1. 硬體式FIDO2認證器 2. 手機安裝FIDO2認證App 3. 手機推播MFA驗證 4. 硬體式passcode Token 5. 軟體式passcode Token 6. 電話簡訊 7. 電話語音 8. 一次性bypasscode(用於用戶臨時遺失認證機制使用)
1.3	身分	身分互通	對外部使用者(如服務供應商或跨機構協作)提供或採用不低於內部使用者相同等級之身分驗證機制。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	I	Cisco SSE + Duo	符合，Cisco SSE可以整合Cisco Duo或Microsoft AAD等機制來達成多因子認證(MFA)與無密碼認證>Passwordless)，提供第三方使用者登入，第三方的帳號管理可以獨立與公司帳號管理切開
1.4	身分	身分互通	如具多元身分識別機制且有互通之必要，其信賴等級應具一致性之標準。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	I	Cisco SSE + Duo	符合，Cisco SSE可以整合Cisco Duo或Microsoft AAD等機制來達成多因子認證(MFA)與無密碼認證>Passwordless)，這些不同的身份識別機制都透過Cisco Duo做統一風險識別與登入驗證管理
1.5	身分	權限存取	完成身分驗證後，除依角色屬性存取控制(RBAC)落實最小授權原則外，並具基本屬性存取控制(ABAC)機制，可將每個工作階段(Session)之動態屬性(如時間、地點等)納為授權審核條件，動態撤銷、限縮存取授權或即時合約解除。	II	Cisco SSE + Duo	符合，Cisco SSE可以整合Cisco Duo，根據每次的身份驗證結果賦予對應的單一App存取權限，落實最小授權原則，並可將時間、地點也納為授權審核條件
1.6	身分	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制。如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單或 SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控態勢基準)	III	Cisco SSE + Cisco XDR & Splunk	符合，Cisco SSE可以整合Cisco XDR & Splunk，達成日誌整合(SIEM)與資安監控(SOC)，並對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TPP)進行即時的判斷與應處
1.7	身分	自動化治理	建立可依資安政策快速調適及一致性目動化管理機制，確保於帳號生命週期之安全性及合規性。	IV	N/A	帳號的生命週期管理必須由IDP以及其相關機制來進行，例如 AD+AD Audit解決方案

2. 設備

項次	支柱	功能	原則	等級	Cisco 對應解決方案	補充說明
2.1	設備	設備合規	具有效盤點且可唯一識別(如 TPM 等)網管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應應機制；對未網管設備具有即時偵測及風險控管(如強制隔離)機制。	I	Cisco SSE	符合，Cisco SSE可以在遠端設備連線接入時，對設備進行各種識別檢查，例如是否安裝指定防毒軟體、病毒碼是否更新、作業系統是否更新等，並可檢查跟呈現整個設備資產相關資訊，例如 Hostname、作業系統版本、硬體規格相關資訊等，如果設備違反公司設備檢和安全政策，則拒絕連線進入，亦可試網路架構設計方式，允許連線至隔離區進行作業系統與防毒軟體更新(VPN模式並搭配ISE)
2.2	設備	設備合規	具納管設備合規檢測及弱點修補機制(如未更新或具已知資安漏洞)，可持續監控之設備並及時採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警等)。	II	Cisco SSE	符合，Cisco SSE可以在遠端設備連線接入時，對設備進行各種識別檢查，例如是否安裝指定防毒軟體、病毒碼是否更新、作業系統是否更新等，並可檢查跟呈現整個設備資產相關資訊，例如 Hostname、作業系統版本、硬體規格相關資訊等，如果設備違反公司設備檢和安全政策，則拒絕連線進入，亦可試網路架構設計方式，允許連線至隔離區進行作業系統與防毒軟體更新(VPN模式並搭配ISE)
2.3	設備	供應鏈風險	對外部設備(如 BYOD、服務供應商或跨機構協作等)，應建立不低於內部設備防護基準之管控措施；或限制需經由可控之公用中繼網道(如 VDI 等)存取。	I	Cisco SSE	符合，Cisco SSE可以針對BYOD、服務供應商或跨機構協作等外部單位進行檢查跟限制，包括但不限於限制只能連線VDI、對接入設備進行設備合規檢查等等
2.4	設備	資源存取	可將設備之動態屬性(如是否為網管及合規、設備位址或是否屬外部設備等)納為每個工作階段(Session)之授權審核條件，動態撤銷、限縮存取授權或即時告警；或具備隔離機制，可即時偵測並阻斷未合規設備之連線；或於資源存取路徑限制須經可控之公用中繼網道(如 VDI 等)存取。	II	Cisco SSE	符合，Cisco SSE會獨立檢查每一次的工作連線階段(Session)的設備合規狀態，不合規即阻斷連線，或依政策需要導入VDI等受限制與監控的環境
2.5	設備	威脅防護	對設備活動紀錄具有即時偵測及回應機制(如 EDR)，在偵測到威脅指標(IOC)時，可自動隔離或即時應(如發出事件單即時追蹤處置)。	III	Cisco SSE + EDR	符合，Cisco SSE可以啟動EDR模組，在偵測到威脅指標(IOC)時，可自動隔離或即時應(如發出事件單即時追蹤處置)。
2.6	設備	可視化分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制。如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控態勢基準)	III	Cisco SSE + XDR & Splunk	符合，Cisco SSE可以整合Cisco XDR & Splunk，達成日誌整合(SIEM)與資安監控(SOC)，並對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處
2.7	設備	自動化治理	可依資安政策快速調適及一致性目自動化管理機制，確保於設備生命週期之安全性及合規性。	IV	Cisco SSE + ISE	符合，Cisco SSE可以啟用ISE模組，針對設備進行基於人工智慧的自動化識別(Cisco AI Endpoint Analytics)，來進行資安政策快速調適及自動化管理，確保於設備生命週期之安全性及合規性。

3. 網路

項次	支柱	功能	原則	等級	Cisco 對應解決方案	補充說明
3.1	網路	網路區隔	具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制網段主機間連線及資源存取，防止攻擊者利用滲入侵的主機作為跳板機進行橫向擴散。	I	ISE + Cisco Secure Workload	符合，Cisco Secure Workload可以進行網路微分段級別隔離，採最小需求原則限制存取資源之網路連線，並得限制網段主機間連線及資源存取，防止攻擊者利用滲入侵的主機作為跳板機進行橫向擴散。
3.2	網路	網路區隔	具軟體定義網路(SDN)或網路微分段(Micro-Segmentation)機制，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界，並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表面。	II	ISE + Cisco Secure Workload	符合，Cisco Secure Workload可以進行網路微分段級別隔離，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界，並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表面。
3.3	網路	流量管理	呈現對系統、端點與網路間連線的相依性關係，可配置一設備為單位延伸至到相關系統、端點與網路之狀態，並具備需要異常監控及應處機制。	II	ISE + Cisco Secure Workload	符合，Cisco Secure Workload可以視覺化方式呈現對系統、端點與網路間連線的相依性關係，可配置一設備為單位延伸至到相關系統、端點與網路之狀態，並具備需要異常監控及應處機制。
3.4	網路	流量加密	於資源存取路徑之資料傳輸加密(如採 https 等加密協定)。	I	Cisco SSE	符合，Cisco SSE可以確保所有的資源存取連線方式都被加密傳輸
3.5	網路	網路韌性	對網路連線紀錄具有即時偵測及回應機制(如 NDR)，可因應業務需求，偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離，切換備援接口或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。	III	Cisco Software Defined Access + Cisco Secure Workload	符合，Cisco Secure Workload具有即時偵測及回應機制，可因應業務需求，偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離，切換備援接口或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。
3.6	網路	可視化分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制。如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控態勢基準)	III	Cisco Secure Workload + XDR & Splunk	符合，Cisco Secure Workload可以整合Cisco XDR & Splunk，達成日誌整合(SIEM)與資安監控(SOC)，並對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TPP)進行即時的判斷與應處
3.7	網路	自動化治理	具可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。	IV	Cisco Secure Workload + XDR & Splunk	符合，Cisco Secure Workload可以整合Cisco XDR & Splunk，透過SOAR機制，對於當下發生的資安事件動態且自動化的進行網路存取權限的變更，如隔離異常端點、動態變更ACL存取權限等等

4. 應用程式

項次	支柱	功能	原則	等級	Cisco 對應解決方案	補充說明
4.1	應用程式	存取授權	以作業屬性及風險區隔角色，並依角色風險等級定義授權條件(如身份及密碼驗證引之等級)，採最小授權原則定義授權範圍；並針對特權作業採獨立角色授權(不混用於非特權作業)，減少特權帳號之濫用及風險。	I	Cisco SSE	符合，Cisco SSE可以針對獨立使用者by不同應用服務給予個別的存取驗證條件，並要求每次的存取都必須經過驗證。
4.2	應用程式	存取授權	可將帳號動態屬性(如 MFA 強度、設備合規、連線時間及地點等)納為每個工作階段(Session)之授權審核條件；並針對特權作業採即時存取(Just-in-Time Access)機制，可動態撤銷、限縮存取授權或即時告警。	II	Cisco SSE + Duo	符合，Cisco SSE可以整合Duo後啟用基於風險的驗證檢核(Risk Based Authentication)針對MFA強度、設備合規、連線時間及地點等進行連線授權審核條件；並針對特權作業採即時存取(Just-in-Time Access)機制，可動態撤銷、限縮存取授權或即時告警。
4.3	應用程式	威脅防護	對應用程式活動紀錄具有即時偵測及回應機制，並可根據使用者行為或使用模式等因素評估風險(如離異常特徵圖但不特作業等)，動態撤銷、限縮存取授權或即時告警。	III	Cisco EDR	符合，Cisco SSE可以啟動EDR模組，在偵測到威脅指標(IOC)時，可自動隔離或即時應(如發出事件單即時追蹤處置)。
4.4	應用程式	程式安全	從網際網路及防護邊界內部對應用程式執行資安檢測(如源碼檢測、弱點掃描、滲透測試等)，確保應用程式本身安全性，具直接開放至 Internet 存取之防護能力。	II	Cisco EDR	部分符合，Cisco EDR模組，針對端點上部署的應用服務進行弱點掃描並進行CVE弱點管理
4.5	應用程式	程式部署	為應用程式開發、測試及部署建立持續整合及部署(CI/CD)通道，符合階段採最小授權原則，並評估採自動化機制減少人員介入誤失，或由不同團隊執行分離權責分離。	II	Cisco Panoptica	符合，Cisco Panoptica會在CI/CD過程中進行安全掃描跟評估，設定與操作過程均符合最小授權原則，並支援自動化機制跟權責分離(Separation of Duties)
4.6	應用程式	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控態勢基準)	III	Cisco XDR & Splunk	符合，可以整合Cisco XDR & Splunk，達成日誌整合(SIEM)與資安監控(SOC)，並對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處
4.7	應用程式	自動化治理	可依資安政策快速調適及一致性目動化管理機制，確保於應用程式生命週期之安全性及合規性。	IV	Cisco Panoptica	符合，Cisco Panoptica的自動化管理機制可以在應用程式的資安政策進行快速調適、一致性、自動化管理、符合應用程式生命週期的安全性以及合規性方面的需求

5. 資料

項次	支柱	功能	原則	等級	Cisco 對應解決方案	補充說明
5.1	資料	外洩防護	針對機敏資料部屬防止資料外洩防護機制，如依據資料特徵之 DLP、資料不落地等。	I	Cisco SSE	符合，Cisco SSE支援DLP防護
5.2	資料	外洩防護	具監控資料存取和使用情況機制，可依據資料存取行為或資料處理狀況等因素評估風險(如遠授權範圍但不符作業常規等)；動態撤銷、限縮存取授權或即時告警，偵測及阻止疑似資料外洩之行為。	III	Cisco SSE	符合，Cisco SSE支援DLP防護，可以即時偵測及阻止疑似資料外洩之行為。
5.2	資料	資料分類	建立資料盤點、分類及、標識機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。	I	Cisco SSE	符合，Cisco SSE支援Microsoft Purview進行資產排點、分類及標識機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。
5.3	資料	資料可用性	建立本地端高可用性、異地備份，並確保儲存資料可被有效保護(如離線備份、儲存於隔離環境、防止寫入等)及有效還原。	I	N/A	思科沒有相關解決方案，可以參考如 Cohesity 提供的完整的資料保護和管理解決方案，它適用於本地端高可用性、異地備份、以及強化資料保護的需求。並可以達成高可用性與本地端保護、異地備份與災難復原、強化資料保護：離線備份與隔離環境、防止寫入的保護機制、有效的還原能力
5.4	資料	資料存取	可將資料存取的動態屬性(如 MFA 強度、設備合規、時間、地點等)納為每個工作階段(Session)之授權審核條件，並且啟動重新驗證之機制，可動態撤銷、限縮存取授權或即時告警。	II	Cisco SSE + Duo	符合，Cisco SSE可以整合Cisco Duo，根據每次的資料存取動態屬性(如 MFA 強度、設備合規、時間、地點等)結果賦予對應的每一個工作階段(Session)存取權限，落實最小授權原則，並可動態撤銷、限縮存取授權或即時告警。
5.5	資料	資料加密	依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。	I	N/A	思科沒有相關解決方案，可以參考如 Thales提供的 CipherTrust Manager 來進行加密和金鑰管理方案，它支援多層次的資料分級加密。其產品支援企業級別的加密和金鑰管理需求，符合PCI-DSS、GDPR等合規要求。CipherTrust Manager 也可以與企業現有的資料庫和雲服務整合，並可使用高強度加密技術和HSM保護敏感資料。
5.6	資料	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控態勢基準)	III	Cisco XDR & Splunk	符合，可以整合Cisco XDR & Splunk，達成日誌整合(SIEM)與資安監控(SOC)，並對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處
5.7	資料	自動化治理	可依資安政策快速調適及一致性且自動化管理機制，確保於資料生命週期之安全性及合規性。	IV	Cisco Secure Workload	部分符合，Cisco Secure Workload可以整合能夠監控和保護跨不同工作負載的資料流量，並以細粒度的可視化功能支援動態且自動化的策略管理。透過流量分析、自動化標記與分段策略，確保敏感資料依照資安政策管理，並實現零信任架構要求的最低授權。

Cisco 的零信任戰略

從建立信任到持續驗證：零信任的完整生命週期



建立信任

- 使用者／裝置／服務身分識別
- 裝置狀態 + 情境感知
- 基於風險的驗證機制



強制執行 基於信任的存取

- 統一的存取控制
- 最小權限 + 明確信任
- 微分段 (Micro-segmentation)



持續驗證信任

- 信任的重新評估
- 入侵指標 (IoC)
- 資安元數據的共享
- 行為監控——威脅與非威脅活動
- 弱點管理



回應 信任狀態變化

- 事件優先處理與應變
- 協同自動化修復機制
- 整合式與開放式工作流程

統一的政策生命週期管理

適用於所有使用者、裝置、應用程式、網路與雲端環境

Cisco 的零信任戰略

從建立信任到持續驗證：零信任的完整生命週期



建立信任

- Cisco Duo:
 - 多因子與無密碼驗證
 - 基於風險識別的動態驗證
 - 身份識別管理與分析 (Identity Intelligence)
 - 零信任識別通行證 (Duo Passport)
 - 設備合規檢查



強制執行 基於信任的存取

- Cisco SSE
 - 零信任存取 (ZTNA)
 - 基於身份
給予對應的應用存取權限
- Cisco Secure Workload
 - 雲/地/虛/實/容器
應用微分段



持續驗證信任

- Cisco EDR / NDR / XDR
 - 入侵指標 (IoC)
 - 行為監控——
威脅與非威脅活動
 - 弱點管理
- Cisco ISE
 - pxGrid 資安事件共享機制
 - 信任的重新評估



回應 信任狀態變化

- Cisco Splunk ES / SOAR
 - 事件優先處理與應變
 - 協同自動化修復機制
 - 整合式與開放式工作流程

← 統一的政策生命週期管理
適用於所有使用者、裝置、應用程式、網路與雲端環境 →

從建立信任到持續驗證：零信任的完整生命週期



建立信任

- Cisco Duo:
 - 多因子與無密碼驗證
 - 基於風險識別的動態驗證
 - 身份識別管理與分析 (Identity Intelligence)
 - 零信任識別通行證 (Duo Passport)
 - 設備合規檢查



強制執行 基於信任的存取

- Cisco SSE
 - 零信任存取 (ZTNA)
 - 基於身份
給予對應的應用存取權限
- Cisco Secure Workload
 - 雲/地/虛/實/容器
應用微分段



持續驗證信任

- Cisco EDR / NDR / XDR
 - 入侵指標 (IoC)
 - 行為監控——
威脅與非威脅活動
 - 弱點管理
- Cisco ISE
 - pxGrid資安事件共享機制
 - 信任的重新評估



回應 信任狀態變化

- Cisco Splunk ES / SOAR
 - 事件優先處理與應變
 - 協同自動化修復機制
 - 整合式與開放式工作流程

← 統一的政策生命週期管理 →
適用於所有使用者、裝置、應用程式、網路與雲端環境

Cisco Duo
最多選擇的雙因驗證方式
身份鑑別 | 無密碼驗證



Verified
Push



穿戴式裝置



Soft Token



Hardware
Tokens



簡訊



電話來電

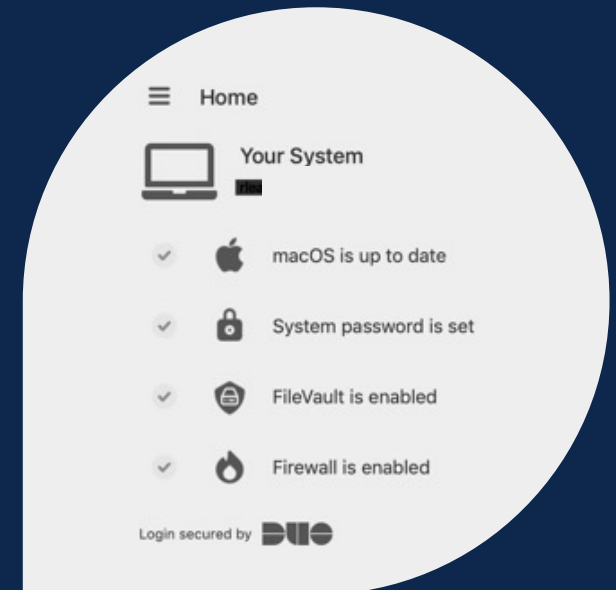
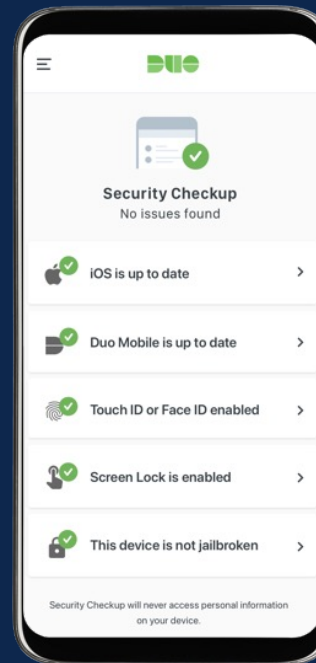


Security
Keys



生物識別

Cisco Duo
最完整的端末合規檢查方式
設備鑑別



Cisco Duo在不同場景下基於風險識別的動態驗證

信任推斷

慣用的連線設備



IP沒有變動
相同的WiFi Fingerprint



基於風險識別的動態驗證

No Re-Auth
Required

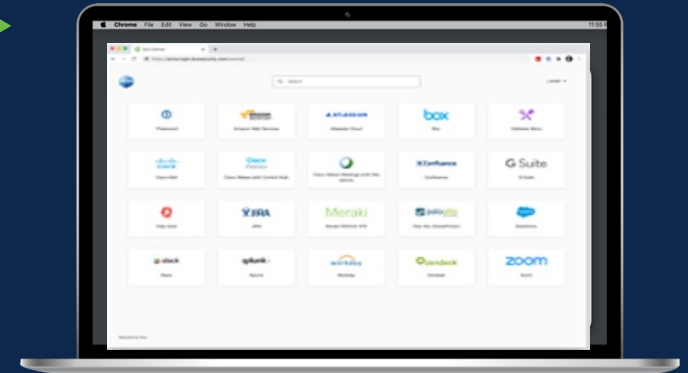
Duo Push
2FA required

Verified
Duo Push
required

FIDO2
Authentication
required

Access Denied

無摩擦的應用服務存取



Cisco Duo在不同場景下基於風險識別的動態驗證

信任推斷

推播釣魚攻擊



帳密外洩的可能性



基於風險識別的動態驗證

No Re-Auth
Required

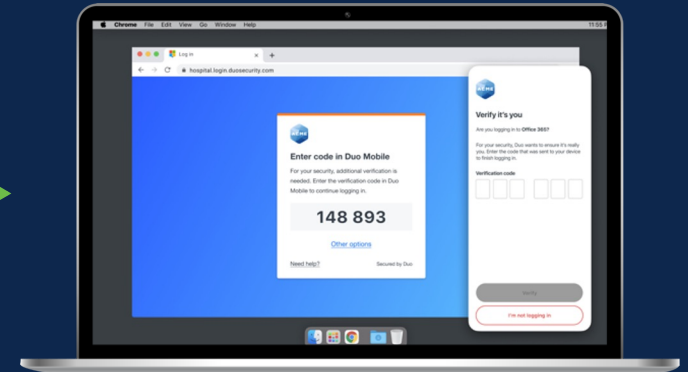
Duo Push
2FA required

Verified
Duo Push
required

FIDO2
Authentication
required

Access Denied

Verified Duo Push



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco Duo在不同場景下基於風險識別的動態驗證

信任推斷

推播釣魚攻擊
已知裝置、常用網段

- 異常地理位置(如突然從俄羅斯登入)
- 裝置未註冊、未加密
- 多次登入失敗後成功登入
- 行為分析:慣用瀏覽器/模式異常

基於風險識別的動態驗證
信任提高(環境熟悉) Verified Duo Push

No Re-Auth
Required

- 信任降低(地理位置異常)

Duo Push
2FA required

- 信任降低(裝置風險高)

Verified
Duo Push
required

- 信任降低(潛在暴力破解風險)

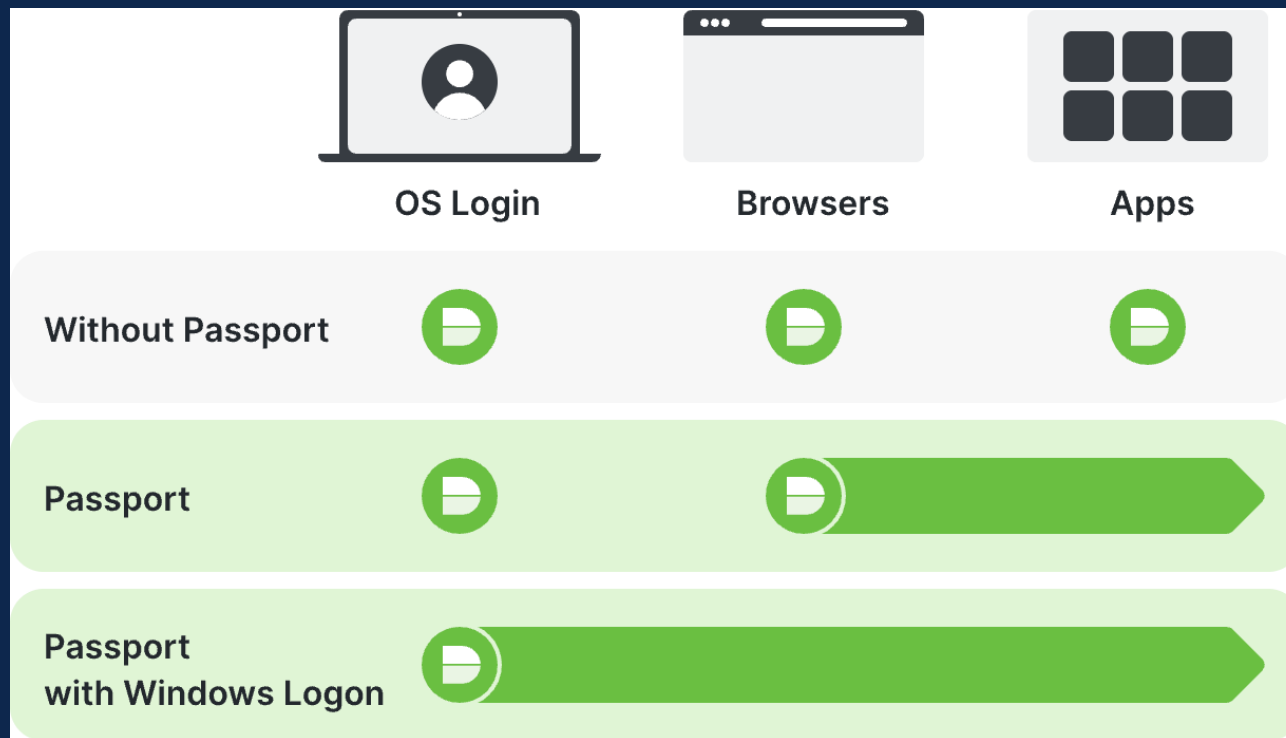
FIDO2
Authentication
required

- 信任降低(使用者行為不一致)

Access Denied

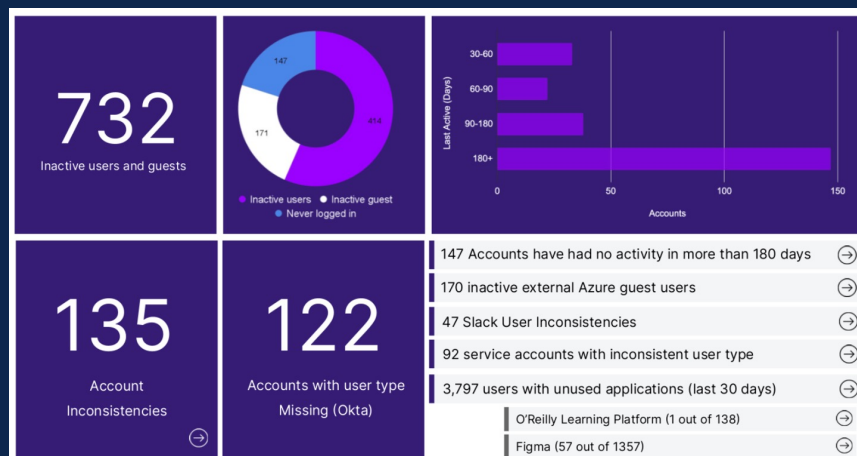
Duo Passport – 更便利的零信任驗證體驗

共享已記憶的裝置會話，簡化存取，減少重複認證

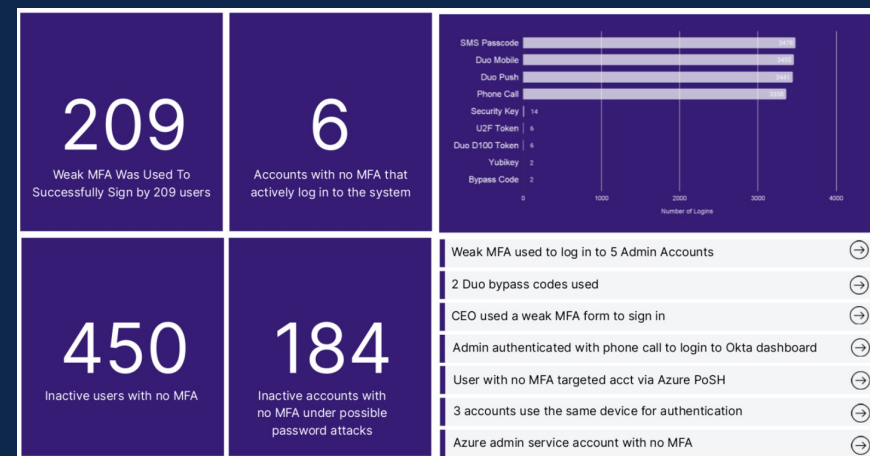


Cisco Duo Identity Intelligence – 將身份驗證行為變成情資

AI 驅動的身份驗證行為分析引擎，提供持續的風險評估與動態存取控制



- 有 147 個帳號 超過 180 天未曾登入使用
- 有 170 個非活躍的外部 Azure 訪客帳號
- 有 47 個 Slack 使用者存在資料不一致
- 有 92 個服務帳號的使用者類型不一致
- 有 3,797 位使用者 在過去 30 天未曾使用其擁有的應用程式
 - O'Reilly 學習平台 (僅 138 位使用者中 1 位使用過)
 - Figma (1357 位使用者中僅 57 位使用過)



- 有 5 個管理帳號 是使用弱 MFA 驗證登入
- 有 2 組 Duo MFA 的繞過碼(bypass codes)被使用
- CEO 使用弱 MFA 進行登入
- 管理員透過語音電話登入控制台
- 某使用者無 MFA 驗證, 透過 Azure PowerShell 登入帳號
- 有 3 個帳號使用相同裝置進行身份驗證
- Azure 管理服務帳號未啟用 MFA 驗證

從建立信任到持續驗證：零信任的完整生命週期



建立信任

- Cisco Duo:
 - 多因子與無密碼驗證
 - 基於風險識別的動態驗證
 - 身份識別管理與分析 (Identity Intelligence)
 - 零信任識別通行證 (Duo Passport)
 - 設備合規檢查



強制執行 基於信任的存取

- Cisco SSE
 - 零信任存取 (ZTNA)
 - 基於身份
給予對應的應用存取權限
- Cisco Secure Workload
 - 雲/地/虛/實/容器
應用微分段



持續驗證信任

- Cisco EDR / NDR / XDR
 - 入侵指標 (IoC)
 - 行為監控——
威脅與非威脅活動
 - 弱點管理
- Cisco ISE
 - pxGrid資安事件共享機制
 - 信任的重新評估



回應 信任狀態變化

- Cisco Splunk ES / SOAR
 - 事件優先處理與應變
 - 協同自動化修復機制
 - 整合式與開放式工作流程

← 統一的政策生命週期管理 →

適用於所有使用者、裝置、應用程式、網路與雲端環境

VPN（虛擬私人網路）的連線方式

- VPN撥號連線至Datacenter並取得內部IP位址



VPN一但連線，可以存取任何服務
需透過ACL或Segmentation做限制

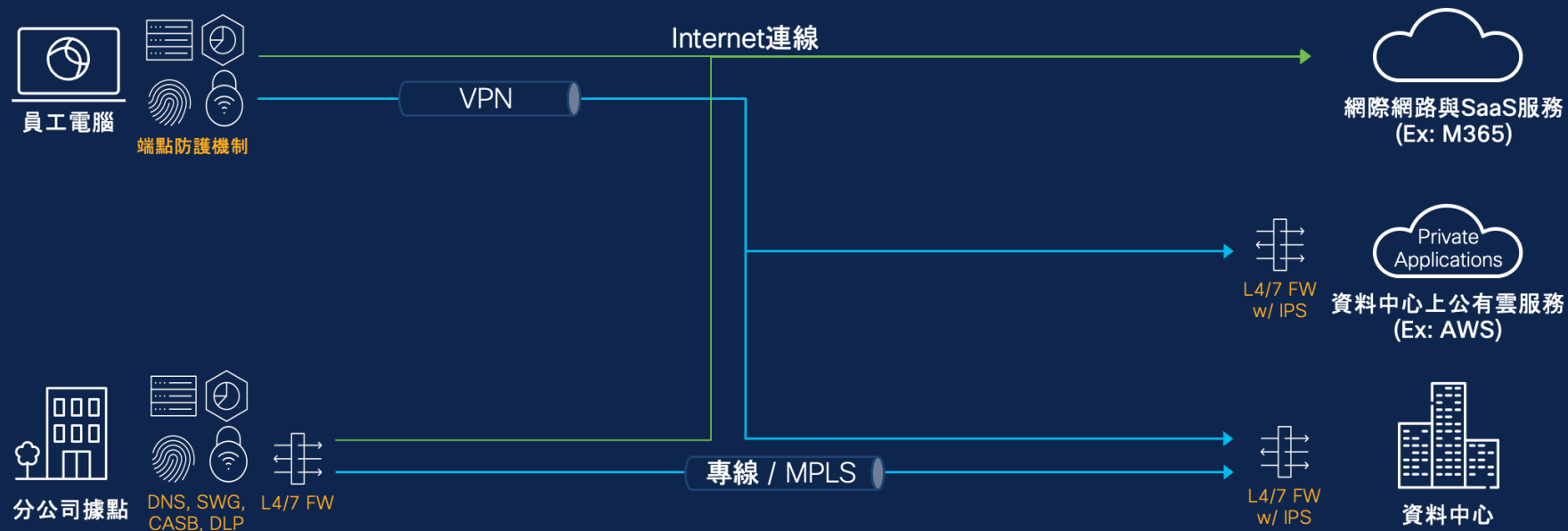
ZTNA（零信任網路存取）的連線方式

- 不需 VPN撥號連線，不會取得Datacenter的內部IP位址



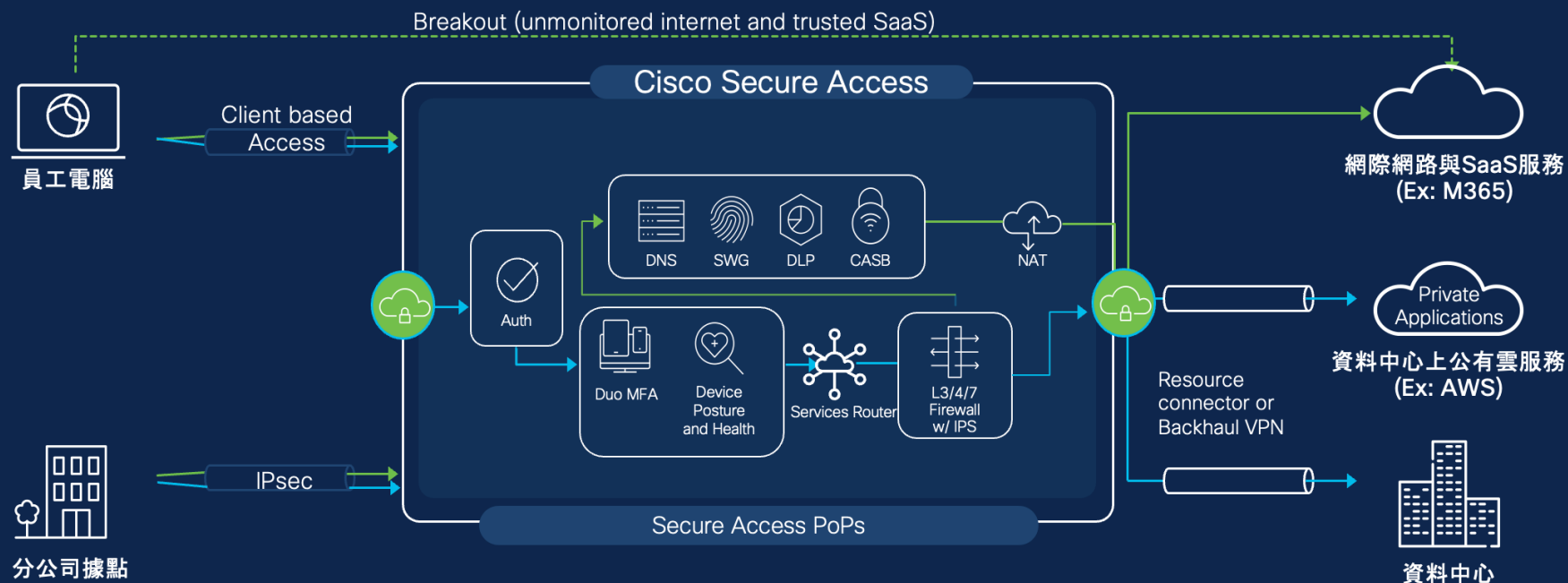
遠端使用者只透過代理取得需要的Datacenter資源
最小授權精神！

從建立信任到持續驗證：零信任的完整生命週期



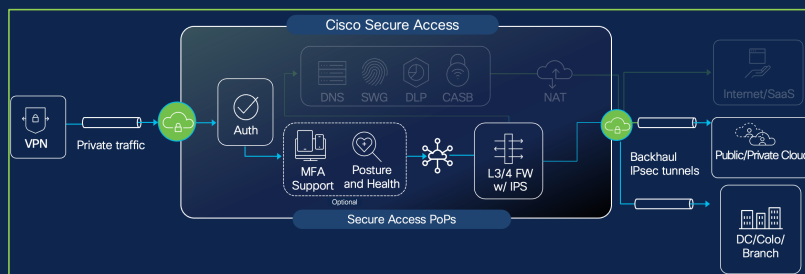
Users ————— How ————— Apps

從建立信任到持續驗證：零信任的完整生命週期



Users ————— How ————— Apps

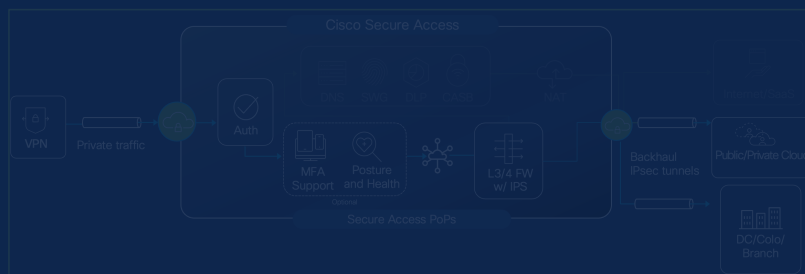
所有你需要的安全可信遠距存取方式，Cisco SSE都幫你準備好了



• IT管理者 | Legacy App 使用者

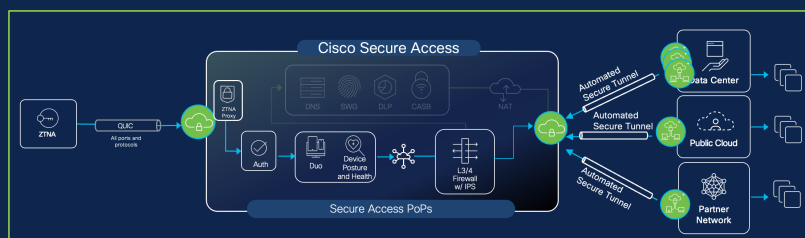
- 透過**VPN**aaS存取資源，需要安裝**VPN代理程式**
- 支援完整 IP 層連線，可存取封閉式內部網段與傳統應用（如 SAP GUI、遠端桌面）
- 透過DUO完成身份與設備可信查核

所有你需要的安全可信遠距存取方式，Cisco SSE都幫你準備好了



• IT管理者 | Legacy App 使用者

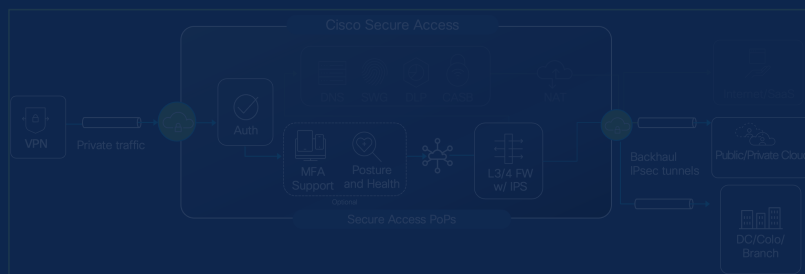
- 透過VPNaaS存取資源，需要安裝VPN代理程式
- 支援完整 IP 層連線，可存取封閉式內部網段與傳統應用（如 SAP GUI、遠端桌面）
- 透過DUO完成身份與設備可信查核



• 一般組織員工 | Modernized App 使用者

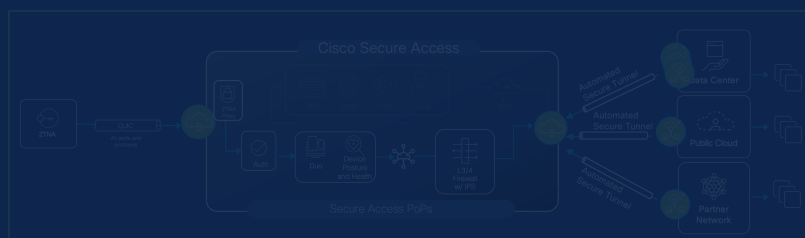
- 透過ZTNA存取資源，需要安裝ZTNA代理程式
- 基於身份與裝置狀態給予App存取權限
- 僅建立應用層(L7)連線，非整個 IP 通道，攻擊受面最小化
- 支援持續驗證與會話風險重新評估，可主動斷線或強化驗證機制（例如與 Duo Adaptive MFA 整合）

所有你需要的安全可信遠距存取方式，Cisco SSE都幫你準備好了



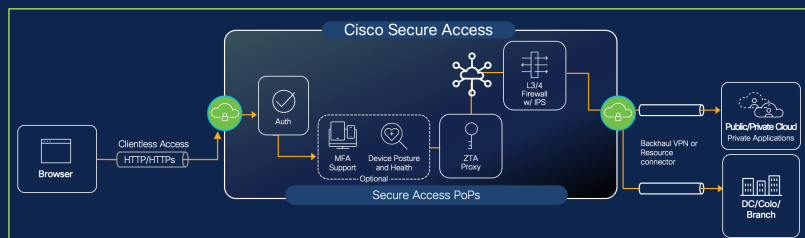
• IT管理者 | Legacy App 使用者

- 透過**VPNaaS**存取資源，需要安裝**VPN代理程式**
- 支援完整 IP 層連線，可存取封閉式內部網段與傳統應用（如 SAP GUI、遠端桌面）
- 透過**DUO**完成身份與設備可信查核



• 一般組織員工 | Modernized App 使用者

- 透過**ZTNA**存取資源，需要安裝**ZTNA代理程式**
- 基於身份與裝置狀態給予App存取權限
- 僅建立應用層(L7)連線，非整個 IP 通道，攻擊受面最小化
- 支援持續驗證與會話風險重新評估，可主動斷線或強化驗證機制（例如與 Duo Adaptive MFA 整合）



• 外部協力廠商 | 合約員工

- 透過**瀏覽器**進行**ZTNA**連線存取資源，無需安裝任何 Agent 或 VPN 客戶端
- 支援單一應用層反向代理，可控可審，可設定用途與時間限制（Just-In-Time Access）



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

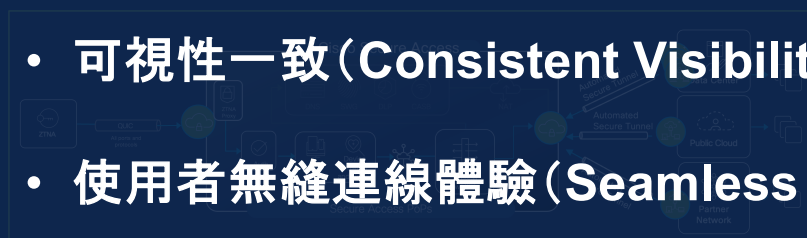
所有你需要的安全可信遠距存取方式，Cisco SSE都幫你準備好了



• 單一政策中樞 (Unified Policy Engine)

• IT 管理者 | Legacy App 使用者

- 透過VPNaaS存取資源，需要安裝VPN代理程式
- 支援完整 IP 層連線，可存取封閉式內部網段與傳統應用（如 SAP GUI、遠端桌面）
- 透過DUO完成身份與設備可信查核



• 可視性一致 (Consistent Visibility Across Access Modes)

• 使用者無縫連線體驗 (Seamless User Experience)

• 一般組織員工 | Modernized App 使用者

- 透過VPNaaS存取資源，需要安裝ZTNA代理程式
- 基於身份與裝置狀態給予App存取權限
- 僅建立應用層 (L7) 連線，非整個 IP 通道，攻擊受面最小化
- 支援持續連線與會話風險重新評估，可主動斷線或強化驗證機制（例如與 Duo Adaptive MFA 整合）



• 降低營運負擔

• 外部協力廠商 | 合約員工

- 透過瀏覽器進行ZTNA連線存取資源，無需安裝任何 Agent 或 VPN 客戶端
- 支援單一應用層反向代理，可控可審，可設定用途與時間限制 (Just-In-Time Access)



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

從建立信任到持續驗證：零信任的完整生命週期



建立信任

- Cisco Duo:
 - 多因子與無密碼驗證
 - 基於風險識別的動態驗證
 - 身份識別管理與分析 (Identity Intelligence)
 - 零信任識別通行證 (Duo Passport)
 - 設備合規檢查



強制執行 基於信任的存取

- Cisco SSE
 - 零信任存取 (ZTNA)
 - 基於身份
給予對應的應用存取權限
- Cisco Secure Workload
 - 雲/地/虛/實/容器
應用微分段



持續驗證信任

- Cisco EDR / NDR / XDR
 - 入侵指標 (IoC)
 - 行為監控——
威脅與非威脅活動
 - 弱點管理
- Cisco ISE
 - pxGrid資安事件共享機制
 - 信任的重新評估



回應 信任狀態變化

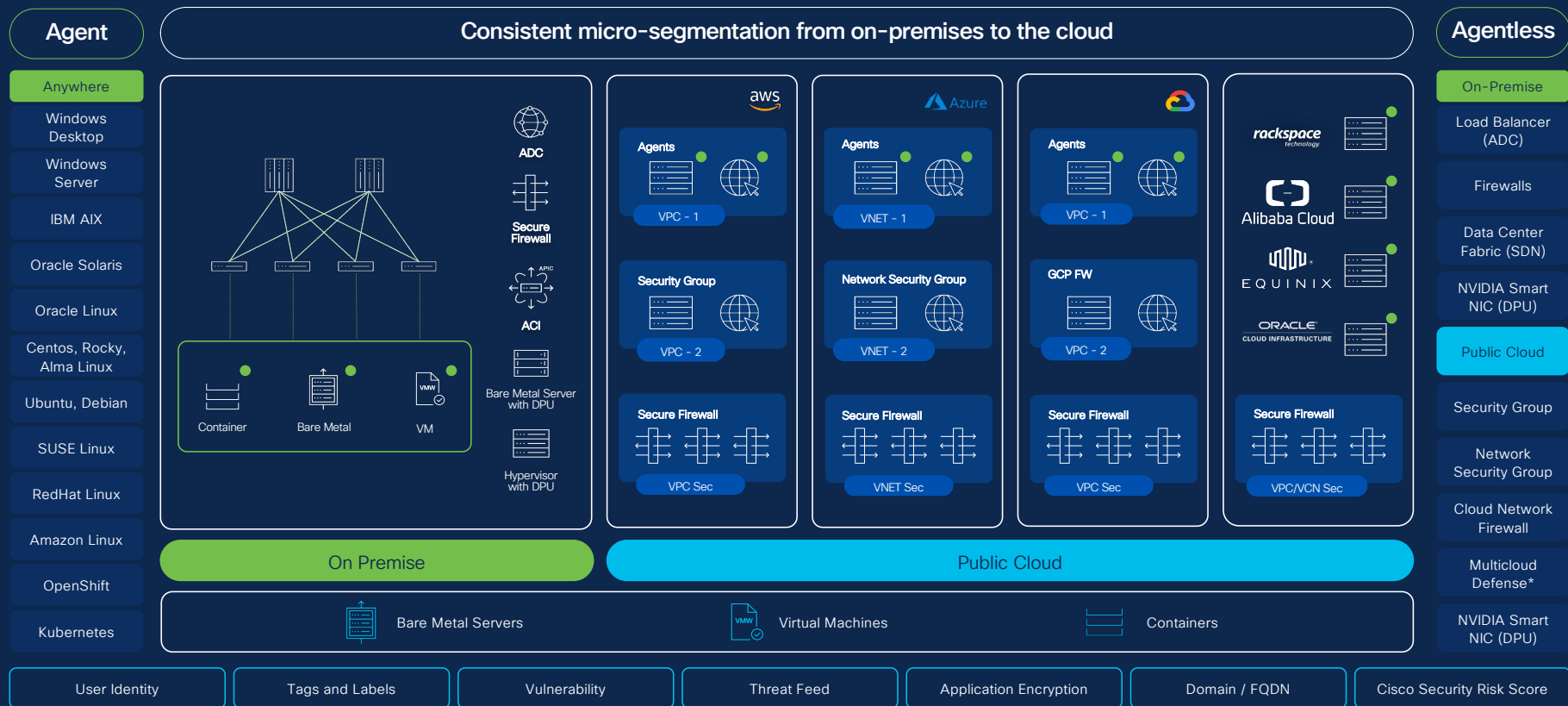
- Cisco Splunk ES / SOAR
 - 事件優先處理與應變
 - 協同自動化修復機制
 - 整合式與開放式工作流程

統一的政策生命週期管理

適用於所有使用者、裝置、應用程式、網路與雲端環境

Cisco Secure Workload 與 Micro-segmentation

統一的微分段策略，橫跨雲、地、虛、實、容器

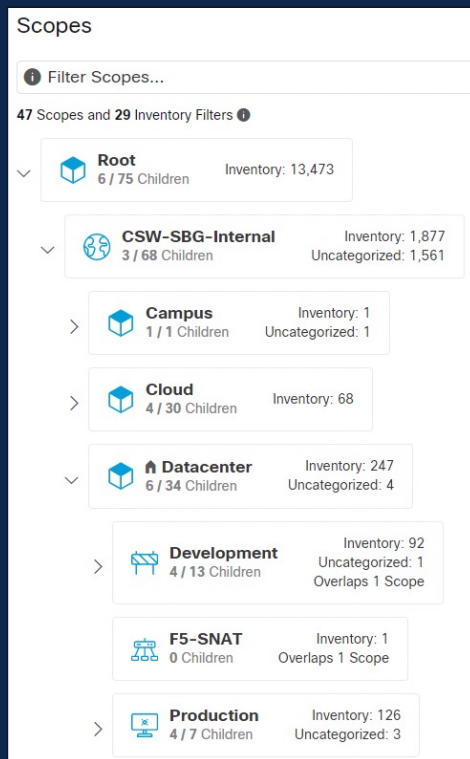


© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco Secure Workload 與 Micro-segmentation

資料中心內的東西向可視性與存取限制，防止駭客入侵成功後的橫移行為，零信任的最小授權精神！



- 透過CMDB輸入建立範圍
- 使用屬性標籤描述組織結構
- 提供Workload可視化
- 基於角色的存取控制(RBAC) 來管理範圍和政策



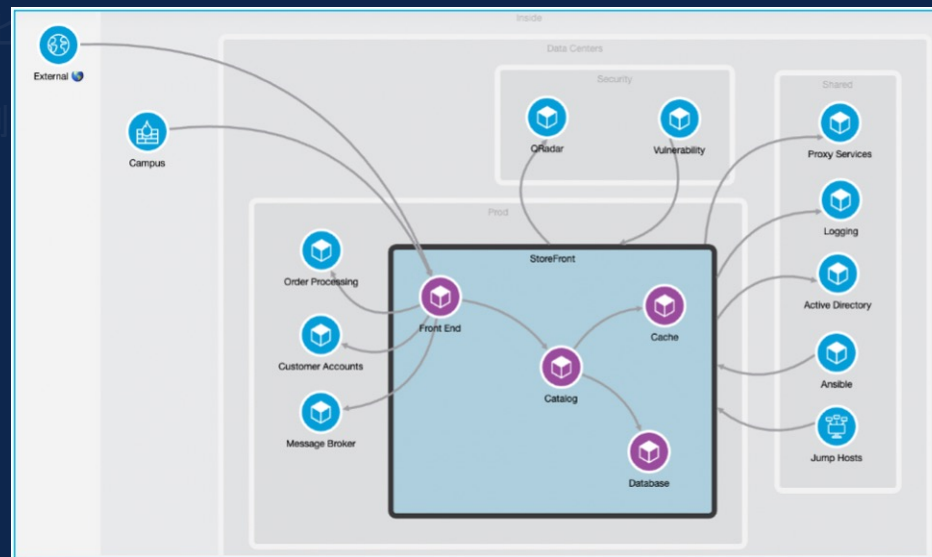
Cisco Secure Workload 與 Micro-segmentation

資料中心內的東西向可視性與存取限制，防止駭客入侵成功後的橫移行為，零信任的最小授權精神！



- 透過持續的學習觀察，確認Workload彼此間的ACL存取關係
- 利用Workload依賴關係映射圖產生藍圖，進一步自動化產生微分割政策
- 藉由AI/機器學習，使Policy Analysis可以輕鬆識別和修正政策

- 提供UX精靈建立範圍
- 使用屬性(標籤)描述組織結構
- 提供workload可視化



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

從建立信任到持續驗證：零信任的完整生命週期



建立信任

- Cisco Duo:
 - 多因子與無密碼驗證
 - 基於風險識別的動態驗證
 - 身份識別管理與分析 (Identity Intelligence)
 - 零信任識別通行證 (Duo Passport)
 - 設備合規檢查



強制執行 基於信任的存取

- Cisco Secure Access
 - 零信任存取 (ZTNA)
 - 基於身份
給予對應的應用存取權限
- Cisco Secure Workload
 - 雲/地/虛/實/容器
應用微分段



持續驗證信任

- Cisco EDR / NDR / XDR
 - 入侵指標 (IoC)
 - 行為監控——
威脅與非威脅活動
 - 弱點管理
- Cisco ISE
 - pxGrid 資安事件共享機制
 - 信任的重新評估



回應 信任狀態變化

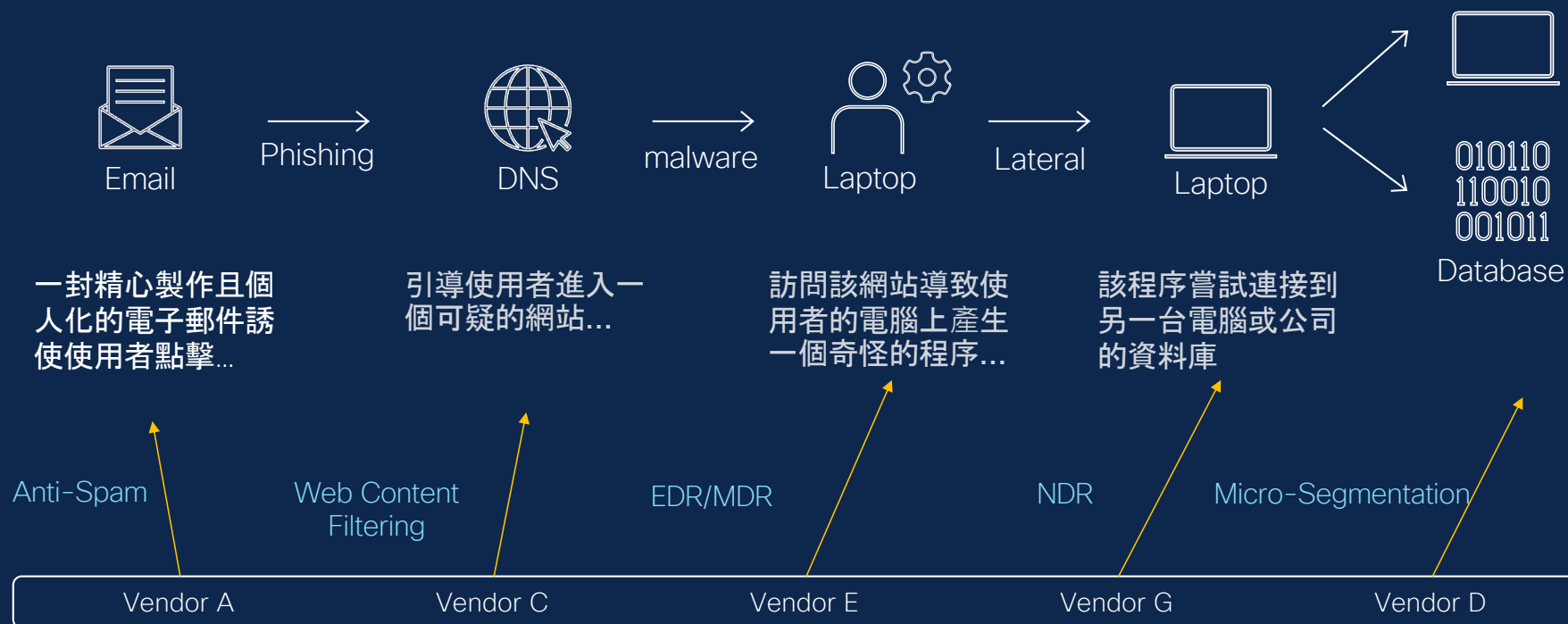
- Cisco Splunk ES / SOAR
 - 事件優先處理與應變
 - 協同自動化修復機制
 - 整合式與開放式工作流程

統一的政策生命週期管理

適用於所有使用者、裝置、應用程式、網路與雲端環境

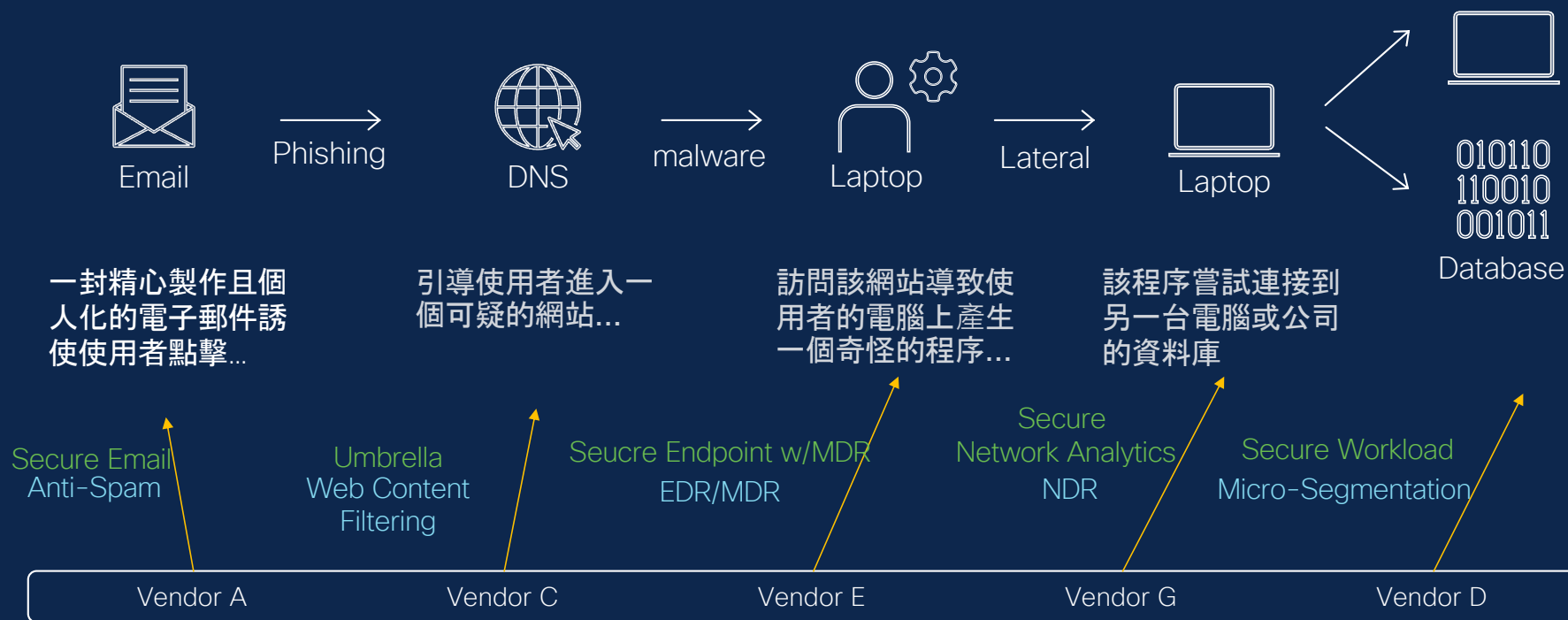
阻止像勒索軟體這樣的進階威脅

大多數駭客攻擊都有這樣的過程...



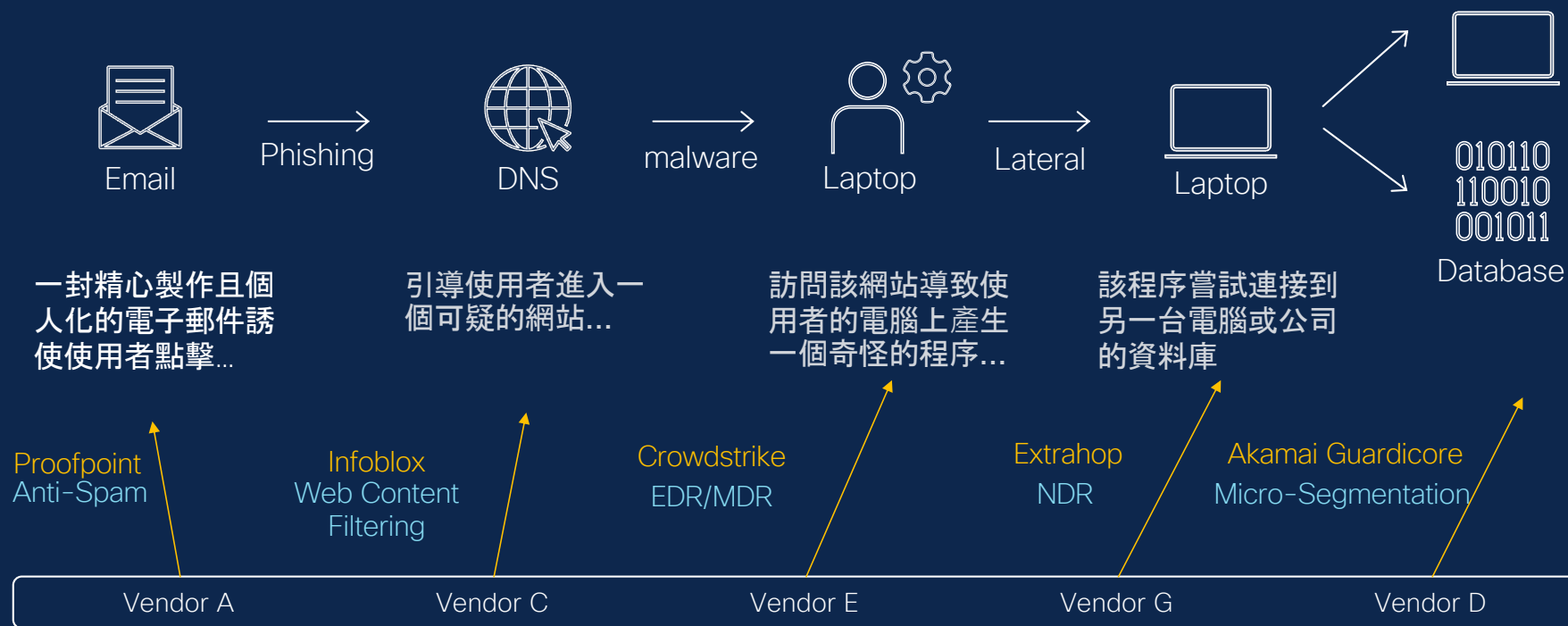
阻止像勒索軟體這樣的進階威脅

大多數駭客攻擊都有這樣的過程...



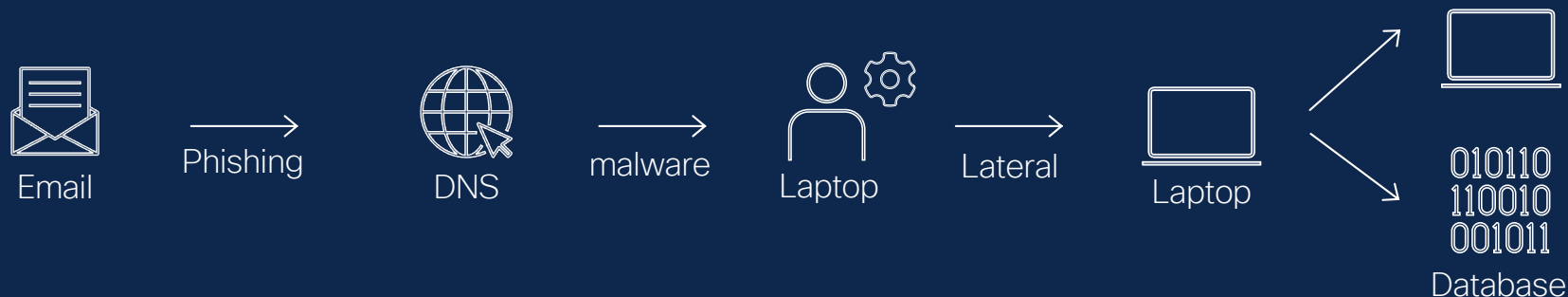
阻止像勒索軟體這樣的進階威脅

大多數駭客攻擊都有這樣的過程...



阻止像勒索軟體這樣的進階威脅

大多數駭客攻擊都有這樣的過程...



需要一種能夠深入看見整個攻擊鏈的解決方案
同時整合各類防護機制的可視性跟威脅遏止能力



Cisco XDR

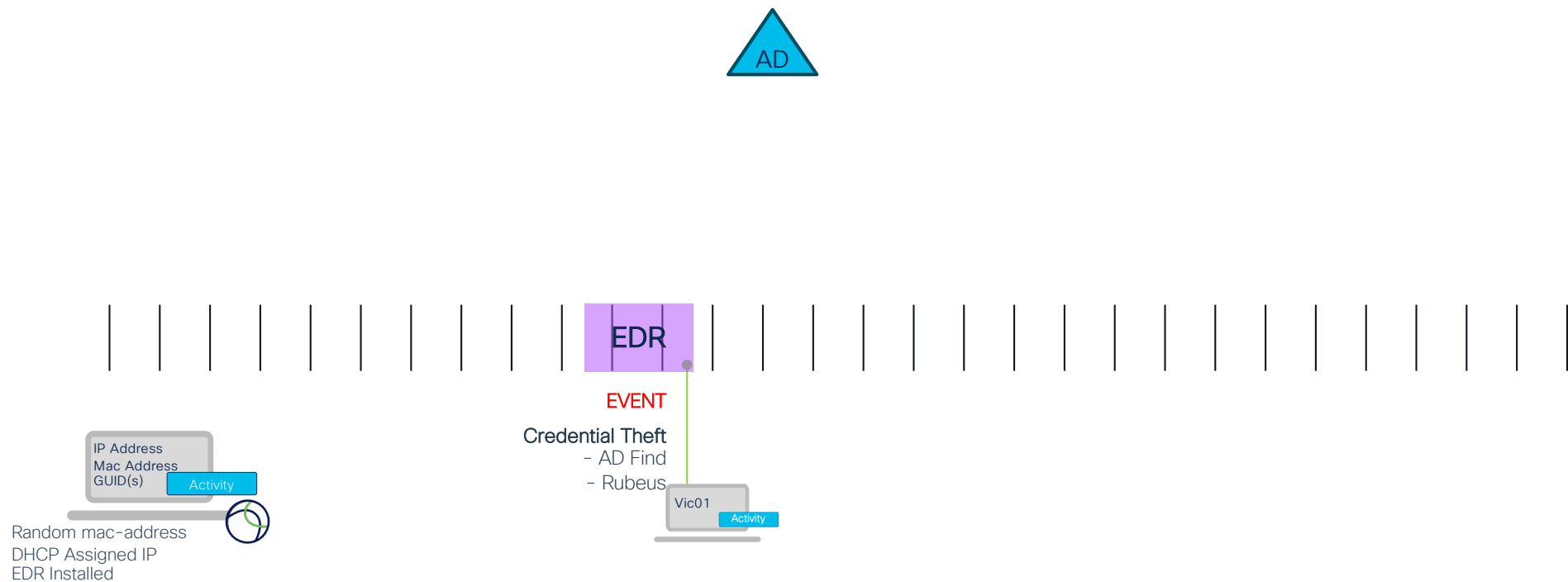


Built on the Cisco Security Cloud platform

即便佈下天羅地網，我們又該如何檢測和應對這一切？

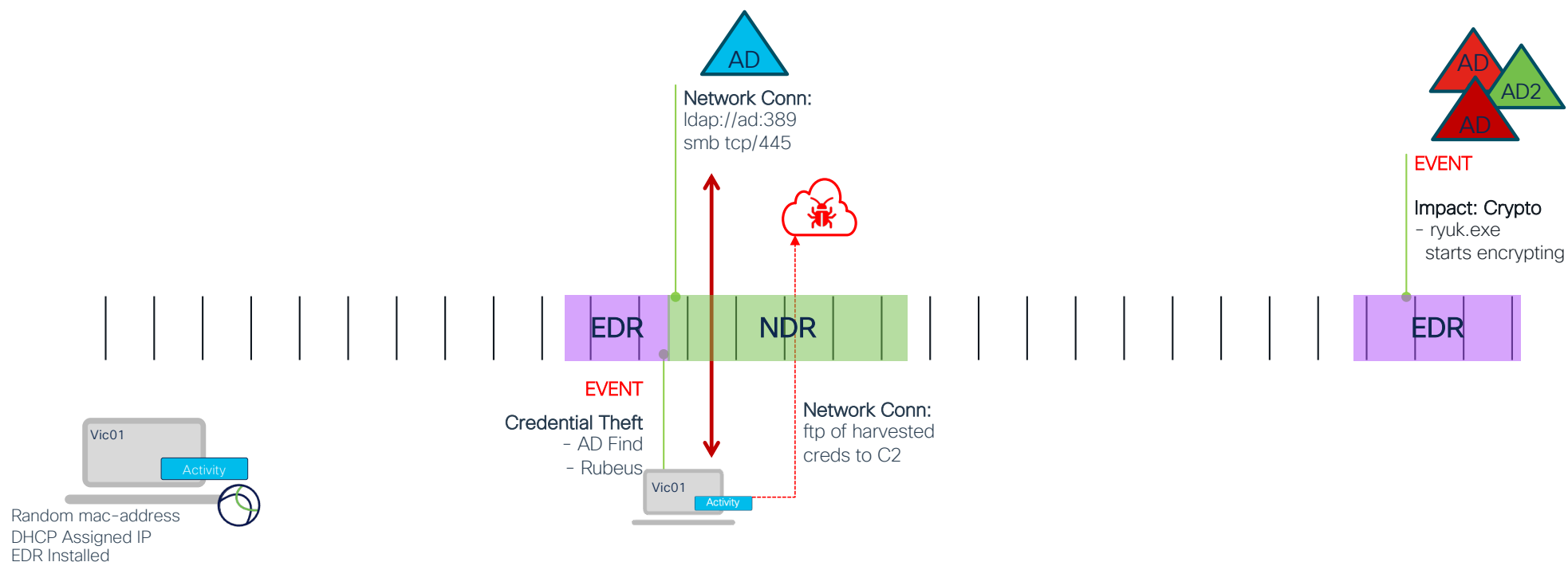
[illegible]

事件反應調查應該具備構建出事件時間線的能力



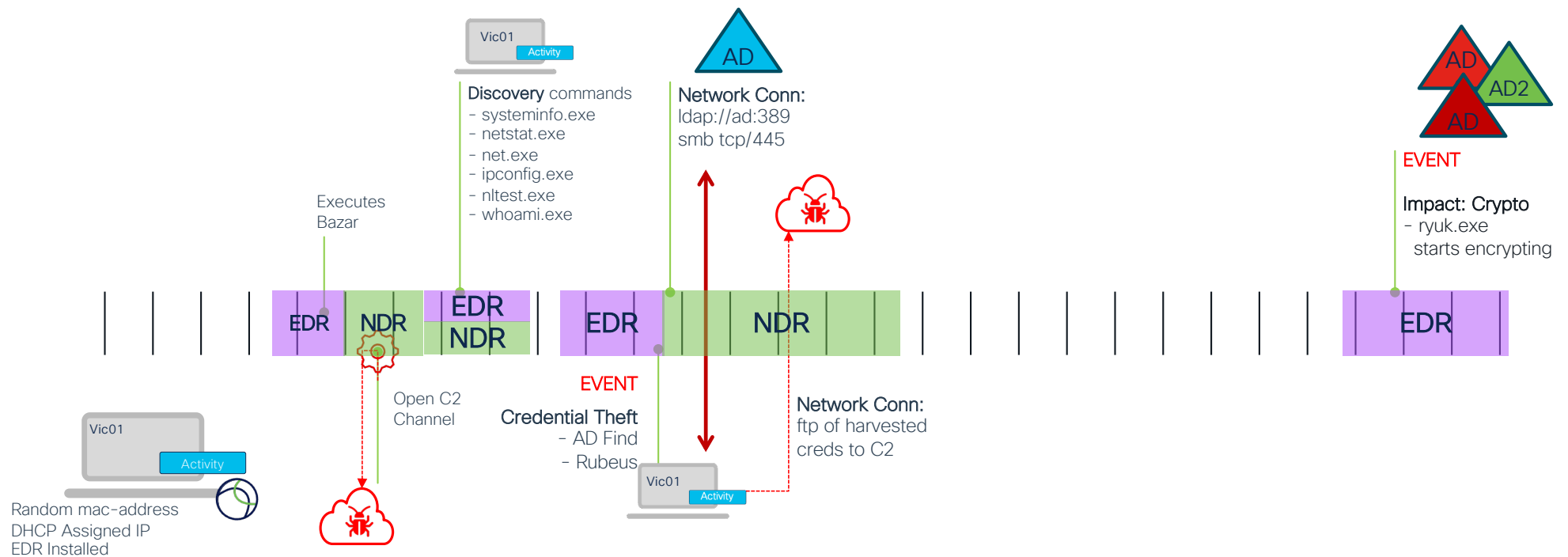
1. EDR 事件，檢測到 Kerberoast 攻擊以獲取憑證。這些資訊足夠行動嗎？

事件反應調查應該具備構建出事件時間線的能力



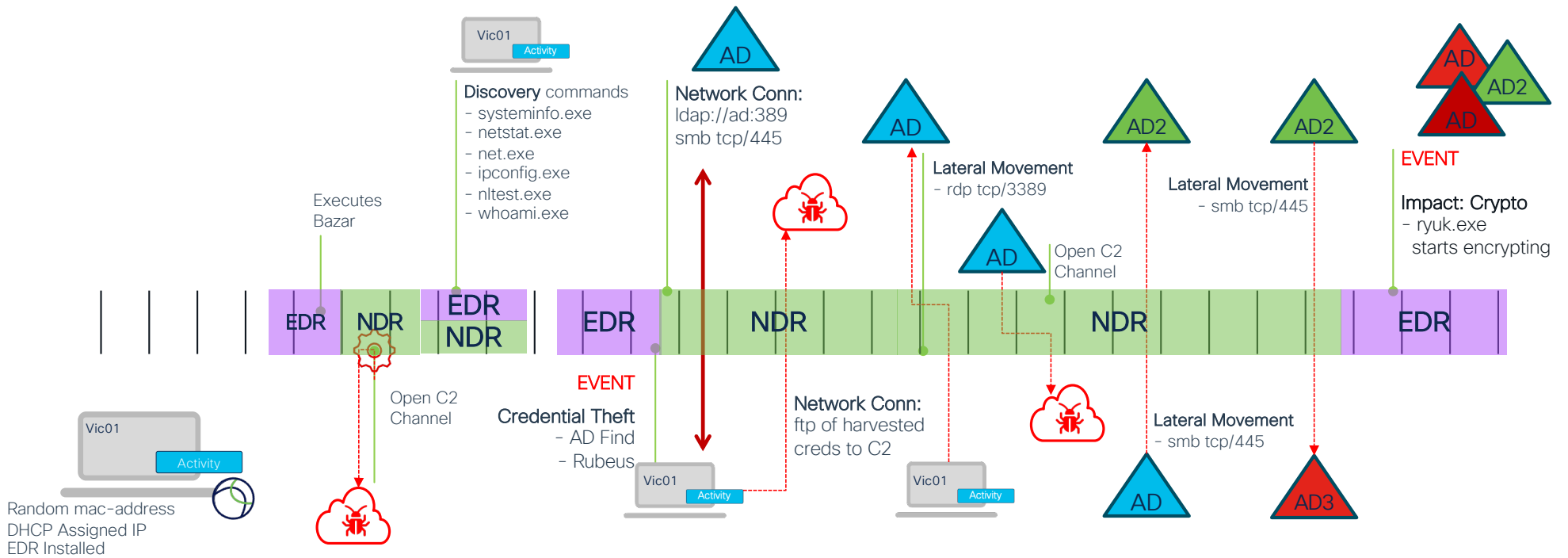
2. NDR：端點 Vic01 通過 LDAP 和 SMB 連接到 AD 伺服器，使 Kerberoast 攻擊成功。
3. NDR：端點 Vic01 將獲取的憑證發送到 C2 伺服器。
4. EDR：第一個系統 (AD) 被勒索！這是如何發生的？

事件反應調查應該具備構建出事件時間線的能力



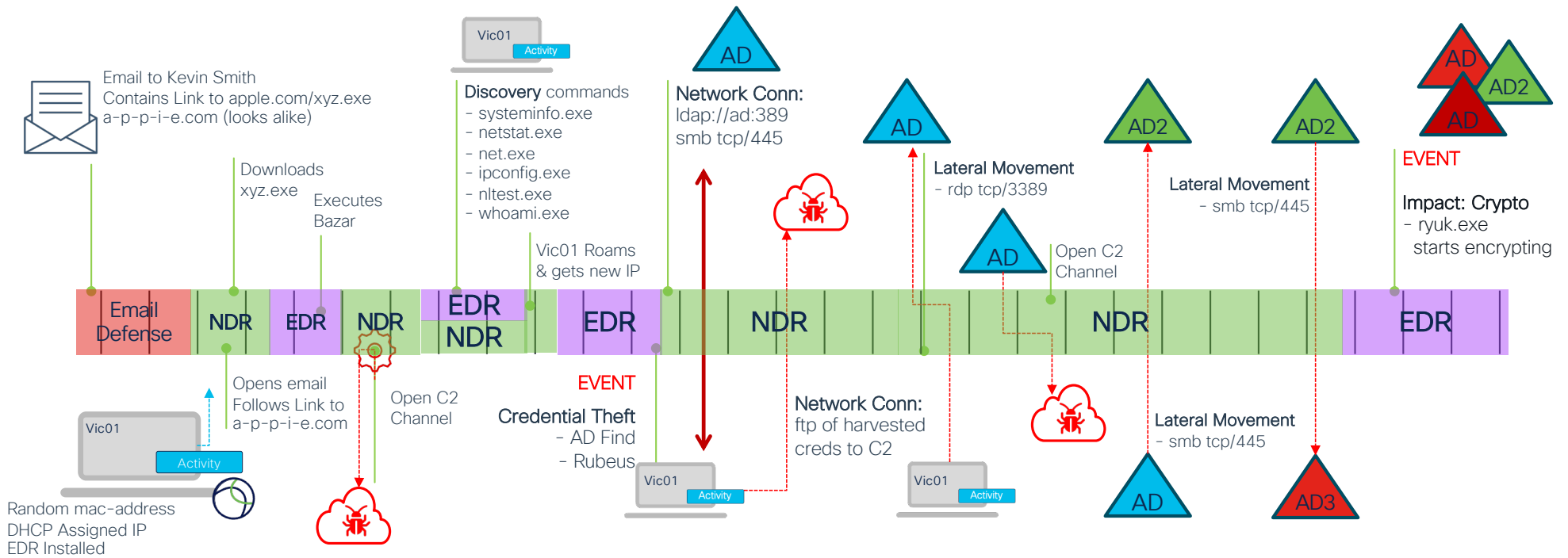
5. EDR：端點 Vic01 之前發送了探索命令，還看到了 Vic01 的什麼行為？
6. EDR：端點 Vic01 在運行這些命令之前執行了一個未知的二進制檔。
7. NDR / DNS / 代理：Vic01 上的 XYZ 正在與一個潛在風險站點進行加密 TLS 通信，這是在命令運行之前。

事件反應調查應該具備構建出事件時間線的能力



8. NDR : Vic01 第一次通過 RDP 橫向移動到 AD。
9. NDR : AD 建立 C2 通道。
10. NDR : AD 通過 SMB 橫向移動到其他 AD 伺服器。

事件反應調查應該具備構建出事件時間線的能力



11. Vic01 進行了漫遊並獲得了一個新的 IP 地址。
12. Kevin Smith 下載了 Bazar 執行檔 XYZ。
K13evin Smith 收到了一封包含仿冒域名的電子郵件，他點擊了該鏈接下載了那個執行檔。

什麼是XDR(eXtended Detection and Response)



從多個資安解決方案收集遙測資料



對收集到的資安機制資料進行應用分析，
以檢測潛伏的惡意行為

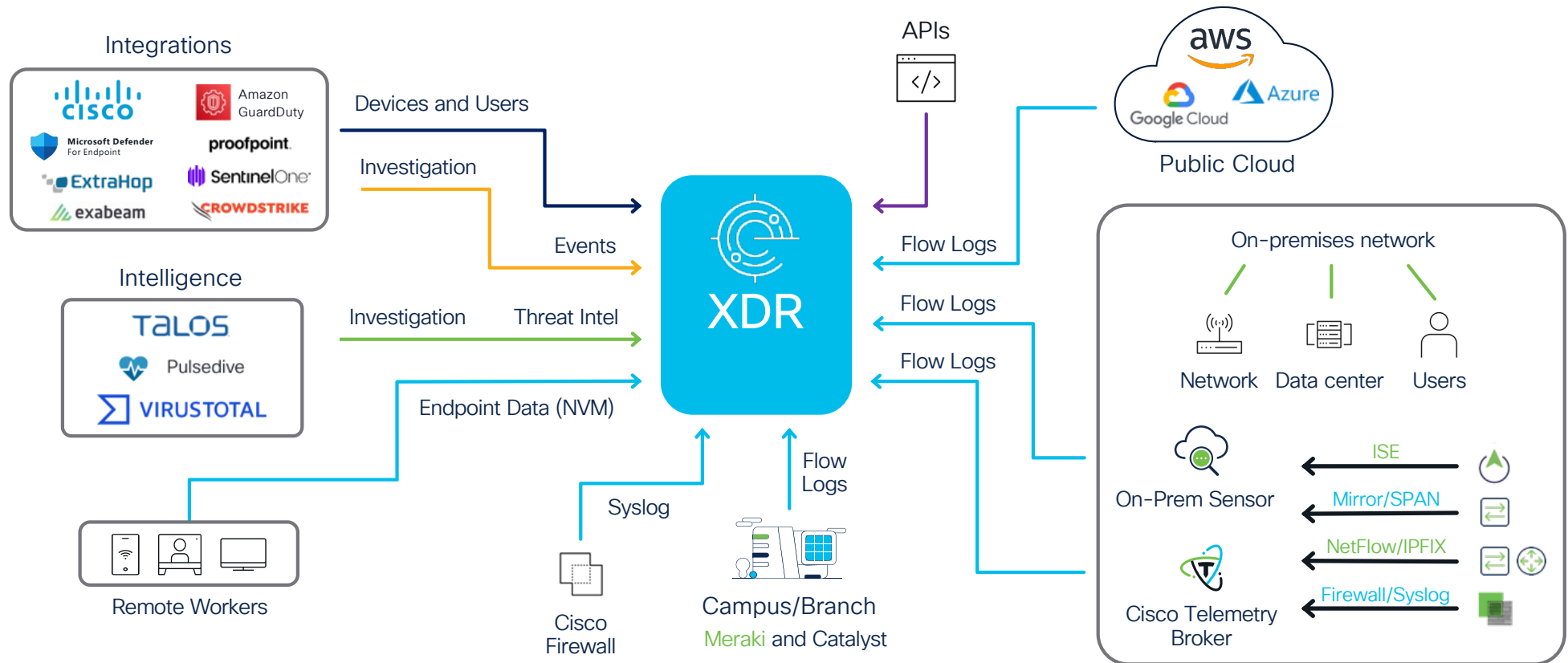


對該惡意行為進行響應和修復



XDR 的資料遙測來源

- 快速整合現有基礎設施



Cisco Splunk & XDR 橫跨時間、洞察全局

透過所有防禦機制的事件關聯，勾勒出潛伏在環境內的駭客足跡與時間軸

The screenshot displays the Cisco XDR interface for an incident titled "Wizard Spider (Ron Weasley has Arachnophobia) Slate-WIN11.explorcorp.com". The interface includes a sidebar with navigation options such as Control Center, Incidents, Investigate, Intelligence, Automate, Assets, Client Management, and Administration. The main content area shows incident details, including a timeline and a network diagram. Three red callout boxes highlight specific sections:

- 事件相關的資產** (Assets related to the event): This box points to the "7 Assets" section, which lists "Slate-WIN11.explorcorp.com" as the top active asset with 36 events.
- 事件相關的可觀察性資訊** (Observable information related to the event): This box points to the "62 Observables" section, which lists "Unknown IP Address" and "108.62.141.250" as top active observables with 55 events.
- 事件相關的攻擊指標** (Indicators of attack related to the event): This box points to the "7 Indicators" section, which lists "Rubeus Toolset Attack" as the top active indicator with 7 events.

Cisco Splunk & XDR 橫跨時間、洞察全局

清楚的MITRE ATT&CK TTP與風險分數，讓調查人員能更快定位事件根因(Root Cause)

逐步披露

查看事件是一個逐步的過程，在需要時揭示相關數據，不會讓 SOC 分析師感到不堪重負。

Priority	Name
1000	Malicious Process and Suspicious SMB/RDP Activity Detected
1000	Unusual External Server for This is localhost

豐富的事件詳情

事件通過從多個來源(包括資產、指標、可觀測對象等)收集的數據進行增強。詳細描述了相關的MITRE ATT&CK 策略和技術，並附有風險評分。

事件摘要與風險分數等級

Priority **1000** Status **New**

Malicious Process and Suspicious SMB/RDP...

Reported by **Cisco Secure Cloud Analytics (rsa)**
15 hours ago
Assigned **BM** **JF**
MITRE **TA0002: Execution**

Priority score breakdown

736 **92** **8**
Detection Risk Asset Value at Risk

Short description

This feature is currently under active development

Long description

Alert Chain
fb56eea65af173cd7286d510722e4f8f7e5c8613

Description

[View Incident Detail](#)

直接顯示 MITRE ATT&CK TTP

MITRE ATT&CK View all Tactics

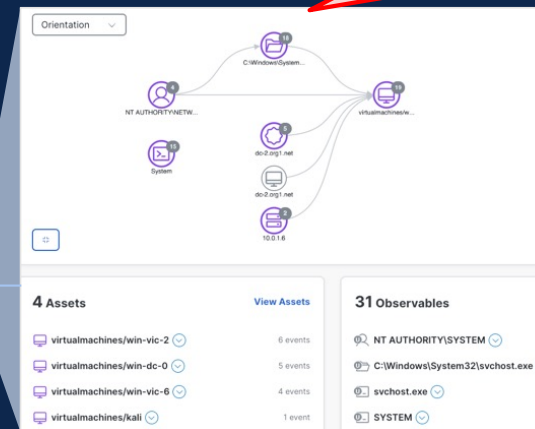
Tactics

TA0002: Execution **100**

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

TA0008: Lateral Movement **66**

事件視覺化呈現



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

從建立信任到持續驗證：零信任的完整生命週期



建立信任

- Cisco Duo:
 - 多因子與無密碼驗證
 - 基於風險識別的動態驗證
 - 身份識別管理與分析 (Identity Intelligence)
 - 零信任識別通行證 (Duo Passport)
 - 設備合規檢查



強制執行 基於信任的存取

- Cisco Secure Access
 - 零信任存取 (ZTNA)
 - 基於身份
給予對應的應用存取權限
- Cisco Secure Workload
 - 雲/地/虛/實/容器
應用微分段



持續驗證信任

- Cisco EDR / NDR / XDR
 - 入侵指標 (IoC)
 - 行為監控——
威脅與非威脅活動
 - 弱點管理
- Cisco ISE
 - pxGrid資安事件共享機制
 - 信任的重新評估



回應 信任狀態變化

- Cisco Splunk ES / SOAR
 - 事件優先處理與應變
 - 協同自動化修復機制
 - 整合式與開放式工作流程

← 統一的政策生命週期管理 →
適用於所有使用者、裝置、應用程式、網路與雲端環境

混合網格防火牆

邁向雲地一致的資安政策與網路防護架構

Lance 朱育民

思科台灣資安事業部



企業安全挑戰日益嚴峻

應用架構高度分散

任何東西都不能預設信任

漏洞增加, 攻擊加快

← AI 的加入, 讓問題變得更加難困 →

防火牆技術必須進化，才能因應當今的挑戰



Gartner : Hybrid Mesh Firewall⁽²⁰²⁴⁾

混合網格防火牆能因應混合環境與多變應用情境，具備更完整的功能與可視性

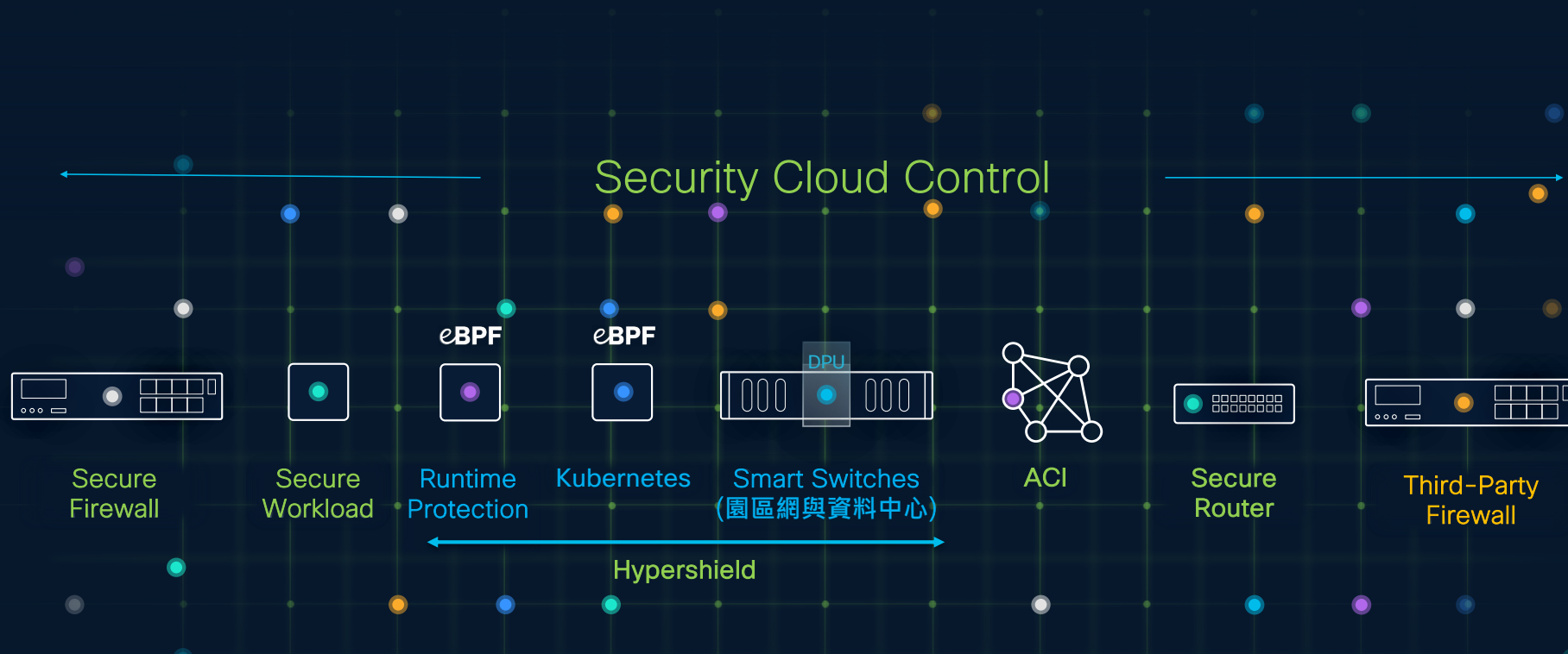
- **標準能力**

- 至少兩種以上部署選項(硬體、虛擬、雲原生、SSE w/ FWaaS、容器防火牆)
- 雲端集中管理平台，具備自動調校與政策推薦功能
- 原生支援 CI/CD 流程整合
- 應用程式發現與連線映射
- IoT 與 DNS 進階威脅防護

- **額外附加能力**

- 安全遠端存取(如 SSL VPN、IPsec VPN、ZTNA)
- 統一端點代理
- 微分段(Agent 或 Agentless)
- 整合 XDR、NDR、EDR、SSE、Identity 等能力

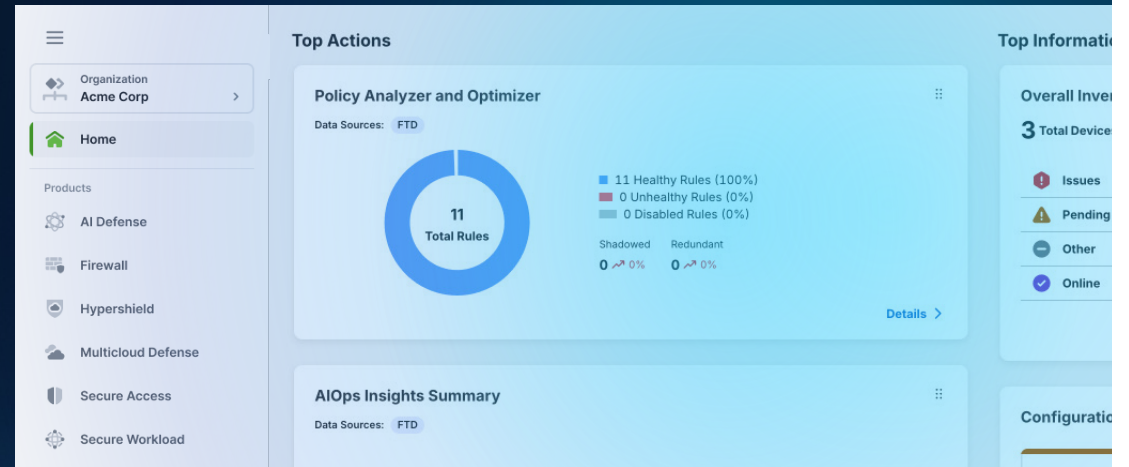
思科混合網格防火牆 (Cisco Hybrid Mesh Firewall)



存取政策一次定義完成，全環境統一佈署

Security Cloud Control

政策管理簡化最多可達 70%



透過AI分析協助政策最佳化

主動式 AI 維運 (AI Ops)

幫助理解目前政策意圖



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

無需汰換現有設備



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

南北向與宏分段

Intent-Based Policy & Mesh Policy Engine

Security Cloud Control

業界首創的多廠牌意圖導向防火牆政策管理平台

支援在 Cisco 與**第三方防火牆**上推行**意圖導向(Intent-based)**的安全政策



理解並最佳化
現有防火牆規則

套用新的控制節點
而非重新設定政策

不需要汰換重建
(No rip and replace)

AVAILABLE AUG 2025*

Cisco Security Cloud Control

支援在 Cisco 與**第三方防火牆**上推行**意圖導向 (Intent-based)**的安全政策

Mesh Policy Engine in Security Cloud Control

在 SCC 中一次定義政策意圖

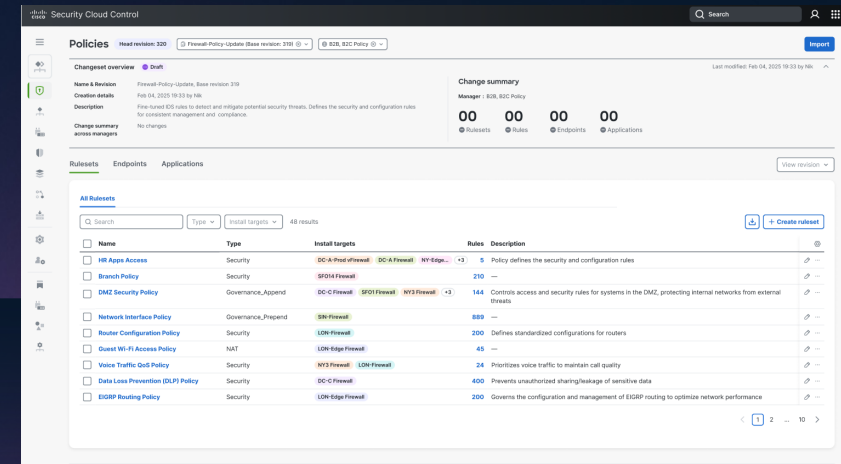
並可佈署至 Cisco 及第三方防火牆

數分鐘內將政策套用至整體網路拓撲

不再需要花費數週逐台設備更新政策

自動最佳化規則與物件

在 Mesh Policy Engine 進行政策變更時自動完成最佳化處理



傳統管理方式現在是如何處理防火牆政策變更的？

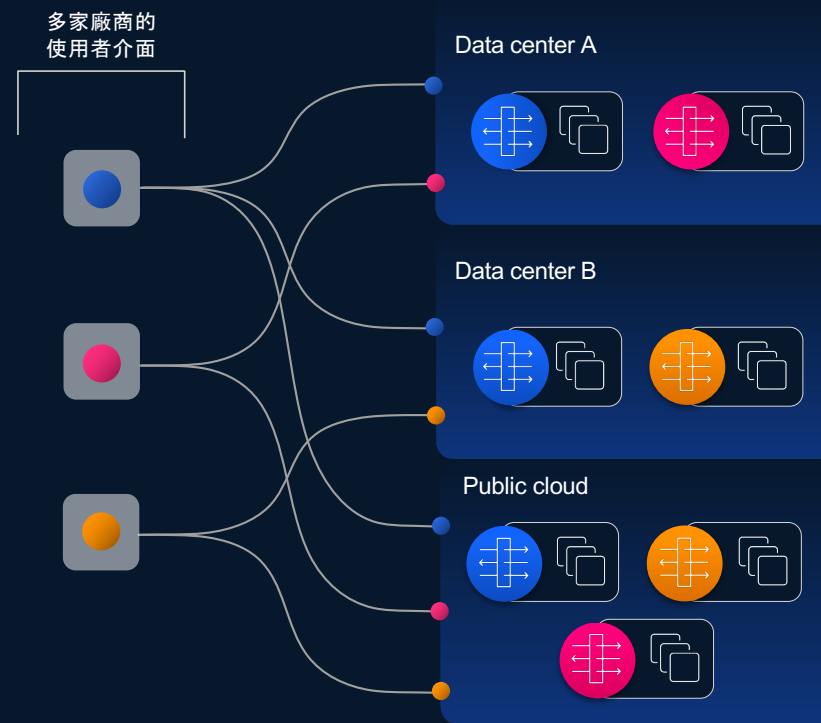


今日用戶的防火牆政策管理是破碎化的

傳統的政策管理方式

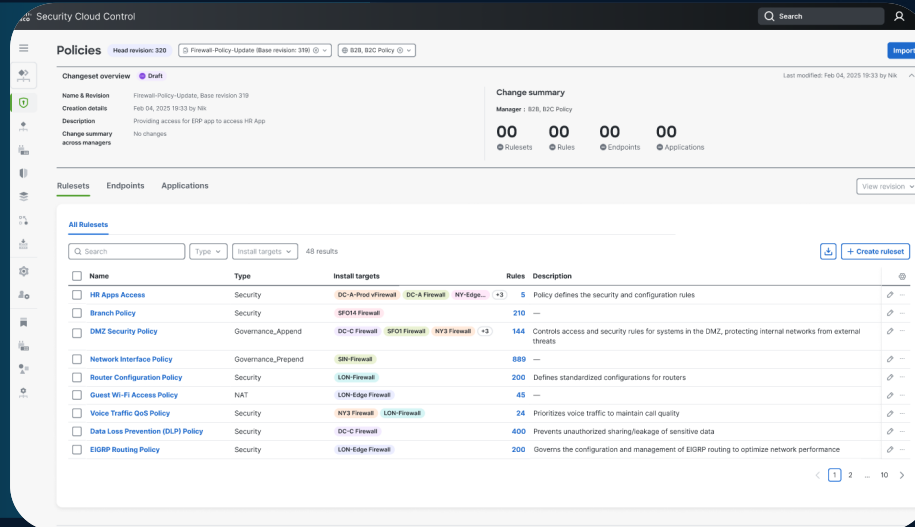
- 每台設備都需單獨設定政策
- 一個「使用意圖」需轉換成多套跨品牌政策，耗時又容易出錯
- 隨著防火牆設備數量增加，管理複雜度呈指數成長

要解決這些問題，就必須採取不同的架構做法



Cisco 是唯一能將防火牆政策延伸至非 Cisco 企業級防火牆的廠商

- 一個政策管理器
(而非僅是設備管理器或政策轉換器)
- 保留政策的「內容(what)」與「適用範圍(when)」, 以及其背後的原因(why)
- 變更強制執行點, 而不是變更政策本身
- 支援 Cisco 及其他企業級防火牆廠商的整合管理



Data center A



Data center B



Public cloud



目的(Why) : A 連到 B, 用什麼Port, 用什麼Protocol

做了什麼(What) 跟 在哪裡做 (Where) : 由Mesh Policy Engine幫你記住跟控制

一次設定，全網執行

Security Cloud Control

← Policies

Create rule Draft Firewall-Policy-Update (Base revision: 319) B2B, B2C Policy HR Apps Access

Ticket ID: [Link ticket](#)

☒ Rule is enabled Logging: ON Time range

Name ^{*} ERP-to-HR app Order ^{*} 01 Description (optional) Controls traffic flowing from ERP to HR Application

☒ Specify Access
Specify which users and endpoints can access which resources. [Help](#)

2 Review Deployment and impact
Review rule impact and reachability across different segments of the network.

+ Add install targets Topology List

Delete Revert changes Back Save

Mesh Policy Engine

能理解您的網路拓撲，將最有效的策略套用到對應的防火牆上。

描述規則名稱與目的

定義使用者與端點的存取權限

部署至整體網路拓撲

一次設定，全網執行

Security Cloud Control

← Policies

Create rule Draft Firewall-Policy-Update (Base revision: 319) B2B, B2C Policy HR Apps Access

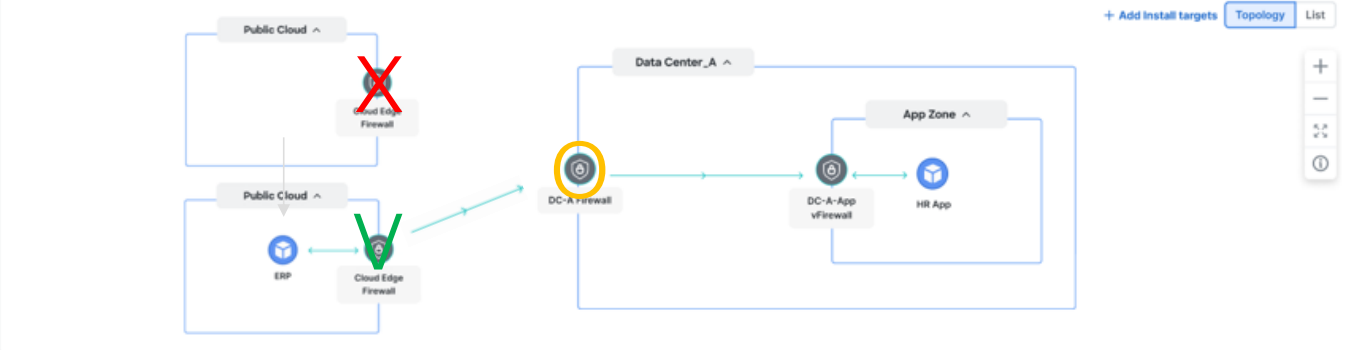
Ticket ID: [Link ticket](#)

☒ Rule is enabled Logging: ON Time range

Name ^{*} ERP-to-HR app Order ^{*} 01 Description (optional) Controls traffic flowing from ERP to HR Application

☒ Specify Access
 Specify which users and endpoints can access which resources. [Help](#)

2 Review Deployment and impact
 Review rule impact and reachability across different segments of the network.



[Delete](#) Revert changes Back Save

Mesh Policy Engine

能理解您的網路拓撲，將最有效的策略套用到對應的防火牆上。

描述規則名稱與目的

定義使用者與端點的存取權限

部署至整體網路拓撲

修改執行政策的執行點，而非存取政策本身

Change enforcement points, not policy

Intent-based policy 範例

- ✓ 讓 HR 應用可存取打卡系統
- ✓ 允許 ERP 系統透過雲端存取 HR 應用
- ✓ 允許 HR 應用存取 HR 資料系統
- ✓ 阻擋非正式環境存取正式區域

政策的 Why(為什麼)
會始終保留在 Mesh Policy Engine 中,
並會隨著環境動態更新, 在不同設備間保持一致。

The screenshot displays the Cisco Hybrid Mesh Firewall management interface. It features a table of GatewaySet Ids and their associated devices. The table has columns for GatewaySet Id, Type, and Status. The devices are listed in a separate pane on the right, showing details for Security_Node_device.

GatewaySet Id	Type	Status
DC-B Firewall	ASA	Active
DC-C Firewall	ASA	Active
DC-D Firewall	ASA	Active
NY-Edge Firewall	FTD	Active
DC-A Firewall	FTD	Active
DC-A-App vFirewall	FTDv	Active
DC-B-Prod vFirewall	FTDv	Active
DC-B-Prod vFirewall	FTDv	Active
DC-B-NonProd vFirewall	FTDv	Active
Cloud Edge Firewall	Multicloud Defense	Active
LON-Edge Firewall	Non Cisco	Active
LON-Branch Firewall	Non Cisco	Active
NY3-Branch Firewall	Non Cisco	Active
NY4-Branch Firewall	Non Cisco	Active

The right pane shows details for Security_Node_device, including its Type (ASA), Status (Active), and Description (Distributed security mode for policy enforcement. Enforce regulatory policies on a compliance firewall.). It also lists Gateways with columns for Name, Hostname, and Management port.

無需汰換現有設備(No rip-and-replace)

Cisco 讓您能輕鬆將 Hybrid Mesh Firewall 整合進現有網路中。

無論使用哪家廠商的設備 都能實現一致的分段政策 (**Segmentation**)



透過單一介面
執行意圖導向的政策管理



幾分鐘內就能佈署政策
大幅縮減過往冗長設定時間



自動最佳化規則與物件

“我們現在處理一筆新的存取請求不再需要兩週，也不用花四小時比對哪幾台防火牆政策需要更新。現在，我們幾分鐘內就能完成整個流程。”

– 防火牆政策管理部門

東西向與微分割

Hypershield & Autonomous Segmentation

將安全性注入網路架構中



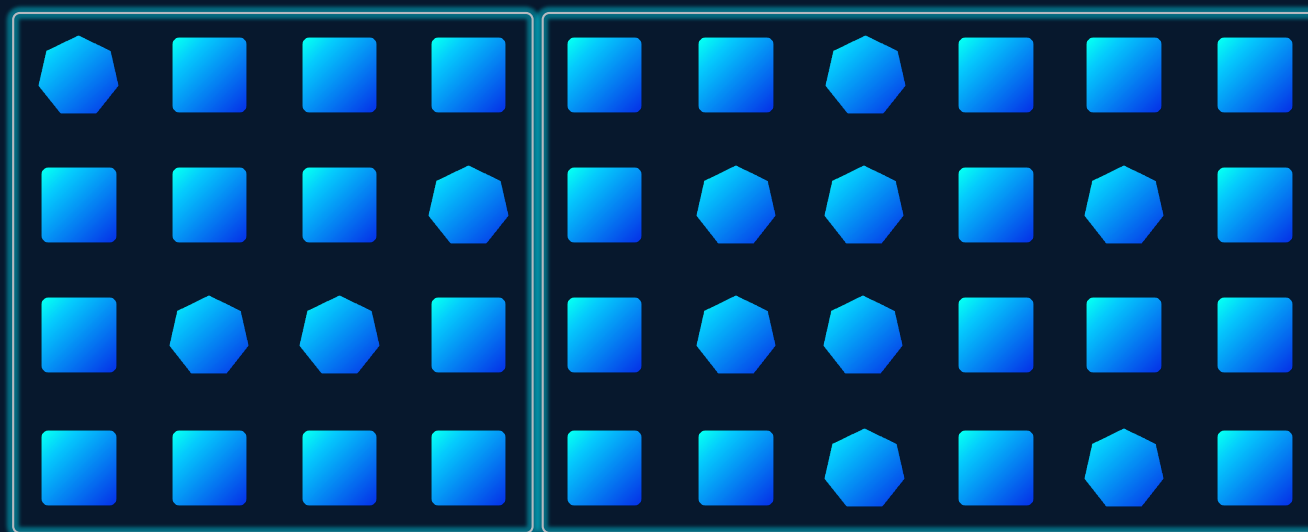
雲端邊界
(Cloud Edge)

區域型網路分段
(Zone-based Segmentation)

資料中心互連
(Data Center Interconnect, DCI)

MACROSEGMENTATION

MICROSEGMENTATION



Dev

Prod

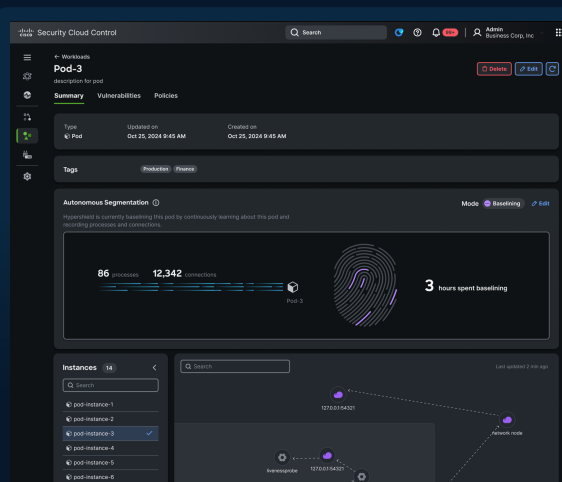
Flow-based rule



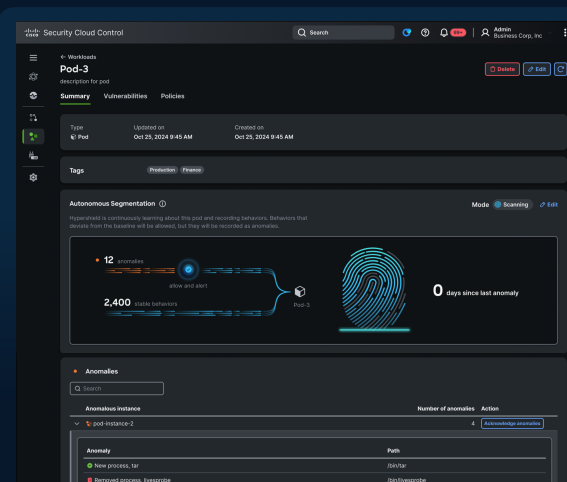
Process-based rule



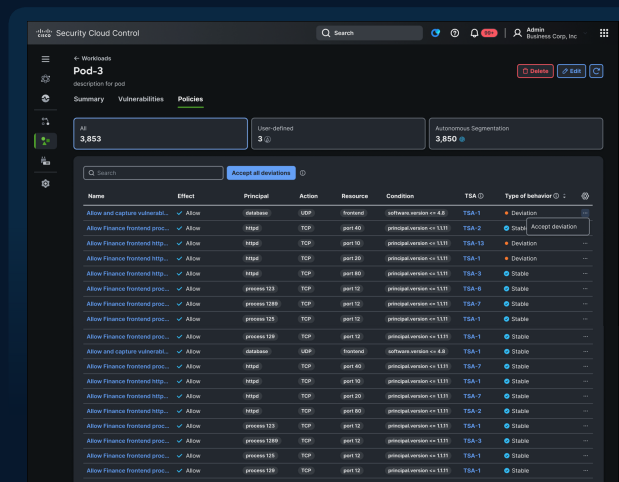
Hypershield – 動態微分段



- 工作負載基線建構
- 觀察控制

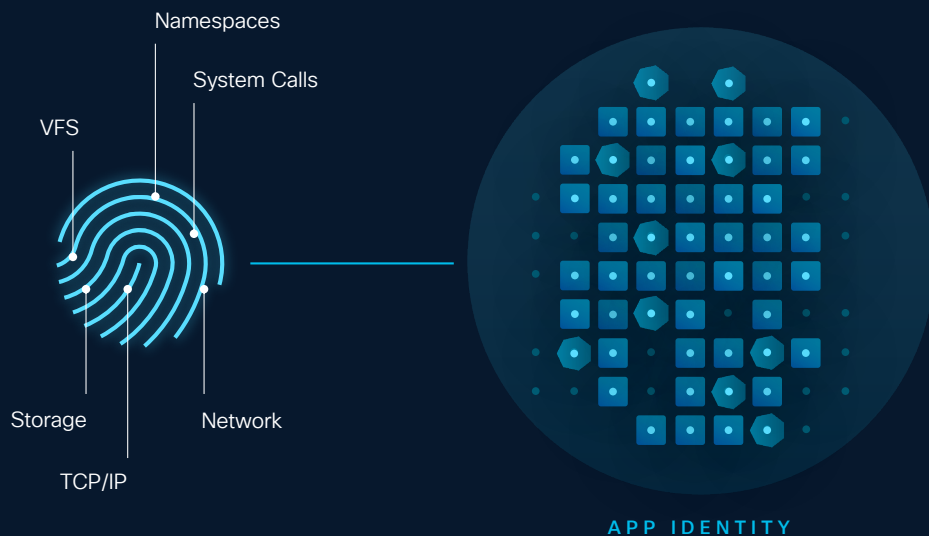


- 惡意行為偵測
- 持續性監控



- 以工作負載行為作為政策依據
- 已允許的行為將作為新的基線參考

學習Application的所有特徵



VALIDATED



SUSPICIOUS

CWE-78

OS command injection

CWE-200

Unauthorized access to sensitive information

MALICIOUS



應用程式行為分析 | 常見弱點編號 (CWE) 與行為解析

Hypershield 會從建立工作負載行為的基線開始

工作負載基線建構 (Workload baselining)

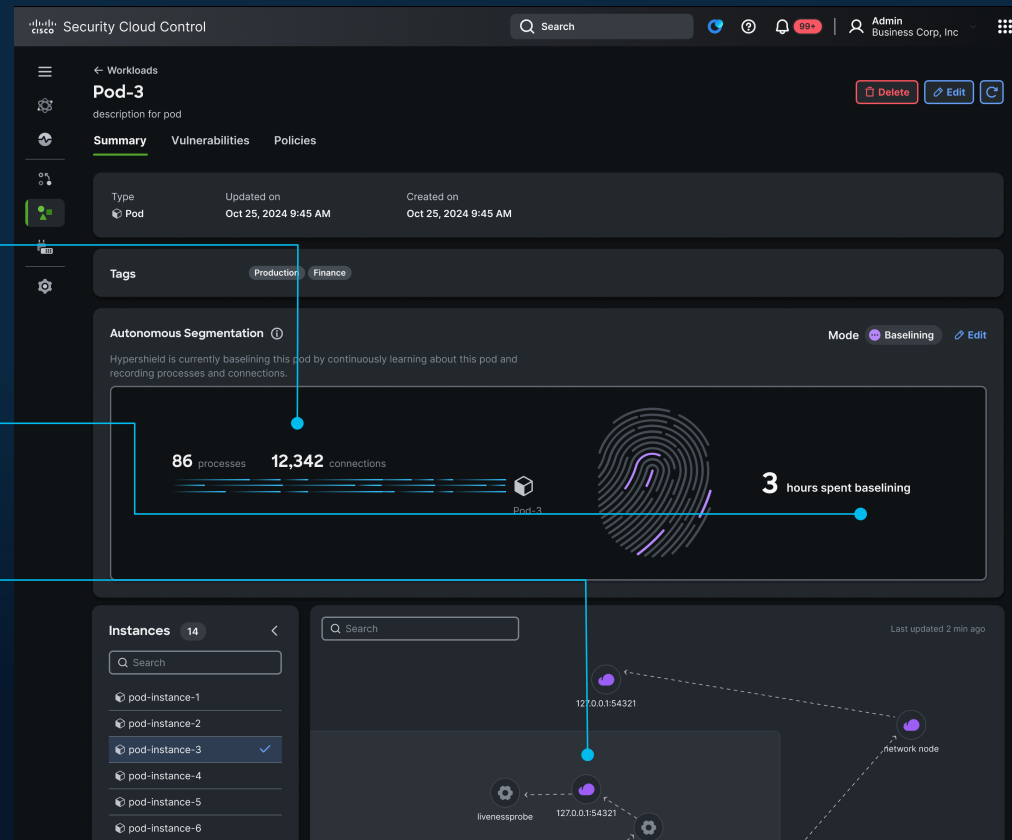
Hypershield 透過觀察程序、檔案操作、網路流量及其他通過其強制執行器(enforcers)的資料，來判斷工作負載的行為模式

彈性控管 (Flexible controls)

管理者可以自訂 Hypershield 觀察工作負載的頻率與範圍

清晰可視化 (Clear-cut visualizations)

Hypershield 所收集的觀察結果，會透過全球圖形引擎進行展示與視覺化



Hypershield 會分析工作負載行為的變化以識別異常

持續掃描

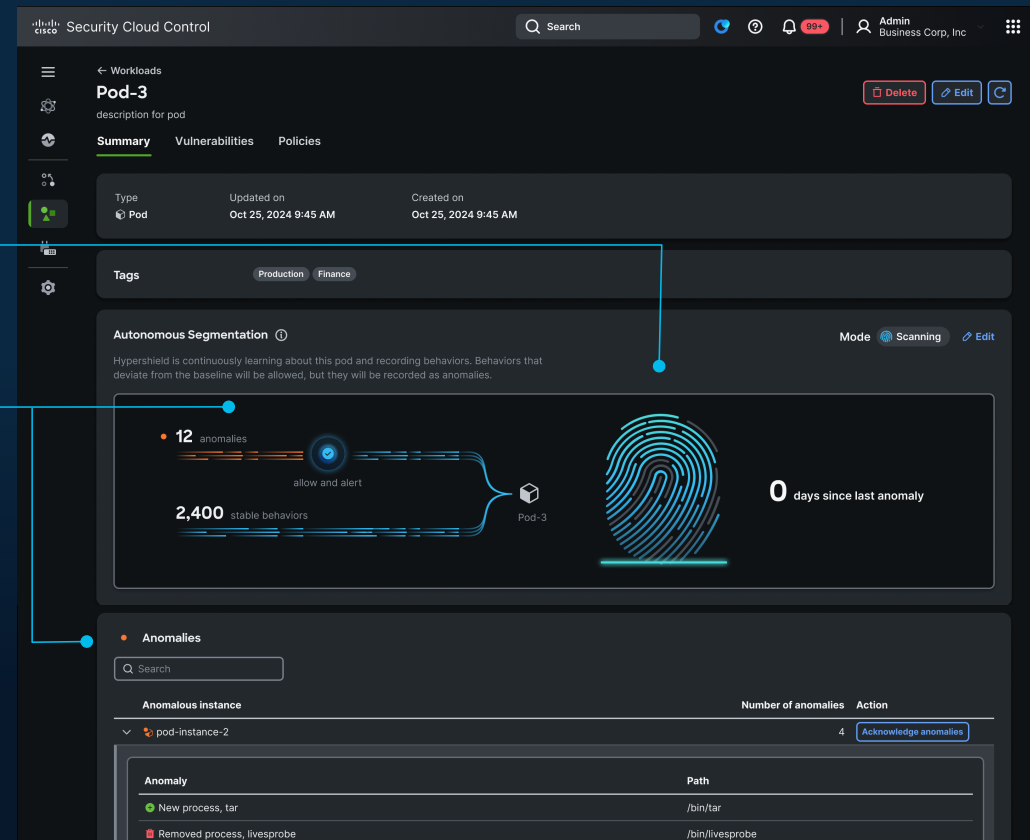
(Continuous scanning)

Hypershield 持續掃描工作負載，以偵測其行為變化

異常偵測

(Anomaly detection)

Hypershield 會記錄過往行為，分析新的行為，並將偏離基準的部分標示為異常



管理者審查工作負載行為變化，以建立新的基線

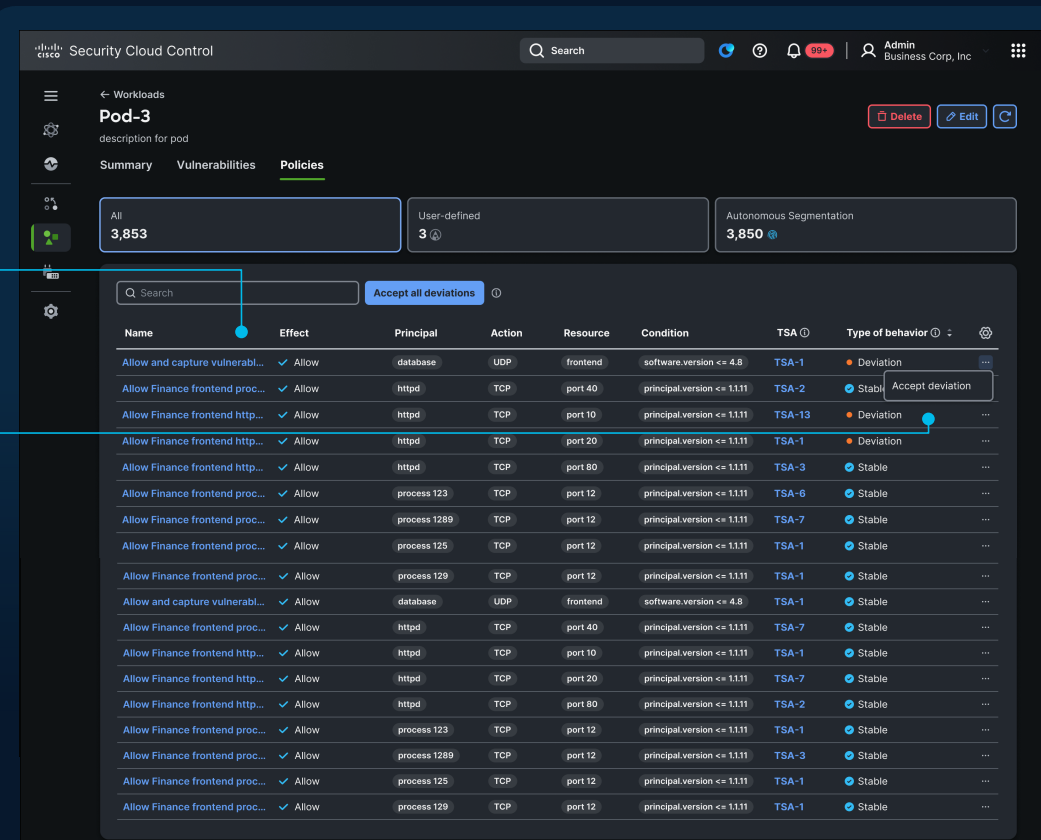
以工作負載行為作為政策 (Workload behavior as policy)

Hypershield 會建立一份已知工作負載行為的允許清單，並透過 PARC 模型將這些行為描述為政策

行為確認 (Behavior acknowledgement)

管理者需審查行為以進行核可：

- 被確認的異常行為將用來更新新的工作負載基準
- 未被確認的異常行為則仍保留在清單中，並標示為偏離行為 (deviations)



Autonomous Segmentation

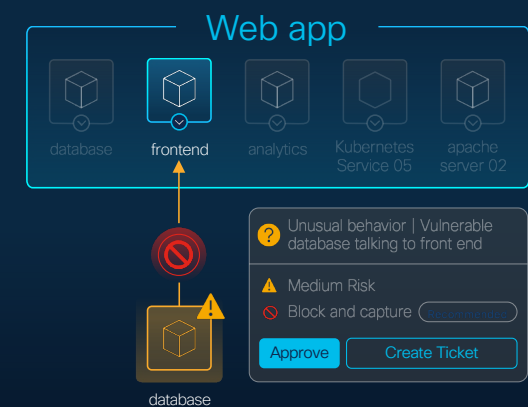


完整掌握應用程式行為變化，從網路層、工作負載層到預 production 環境

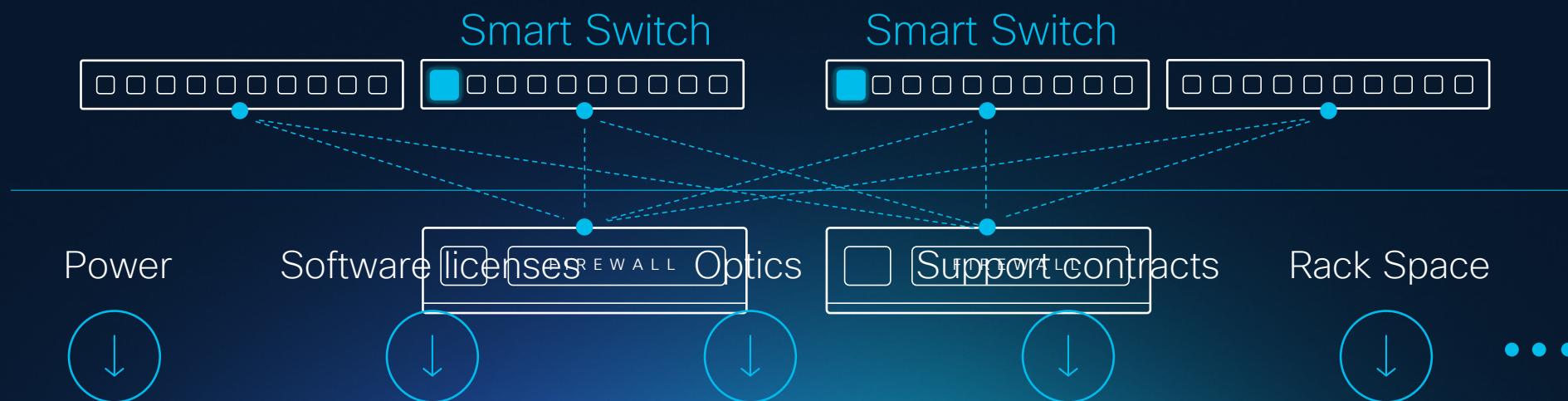
Recommendations

- ✓ 允許 Web 應用前端存取資料庫
- ✓ 允許 Web 應用前端存取分析系統
- ✓ 允許 Web 應用分析模組存取資料庫
- ✓ 預設為「觀察後自動允許」Web 應用政策群組...

彈性的分段規則，避免過度的分割規則造成應用存取失敗產生錯誤



因應可疑事件更新更嚴格的政策規則



Introducing Cisco Smart Switch



- 網路 + 安全 → 交換器



- Silicon One 負責網路流量
DPU負責安全可視性跟管控



- 最高可節省 84% 的 TCO
(總擁有成本)



利用整合 Cisco Hypershield 的 Cisco 智慧型交換器 達成網路與安全的連動整合

Datcenter Networking



N9324C-SE1U
24-port 100G

- Cloud Edge, Zone-Based segmentation, **DCI**, Top-of-Rack
- **2.4T** switch throughput, 800G services throughput
- Silicon One E100 ASIC + AMD DPUs
- Shipping now, **Hypershield** Target Initial Product Readiness: end of July'25



N9348Y2C6D-SE1U
48-port 25G, 6-port 400G, 2-port 100G

- **DC** Top-of-Rack
- **3.8T** switch throughput, 800G services throughput
- Silicon One E100 + AMD DPUs
- Target Limited Orderability: July '25*

Campus Networking



Cisco C9350
48/24 ports 10G/mGig, network-modules, 90W UPoE

- **Campus**
- **1.3T** (800G stacking, 500G for switch) throughput
- Silicon One E100 + Security co-processor
- Target Orderability: June '25*

分散式漏洞防護

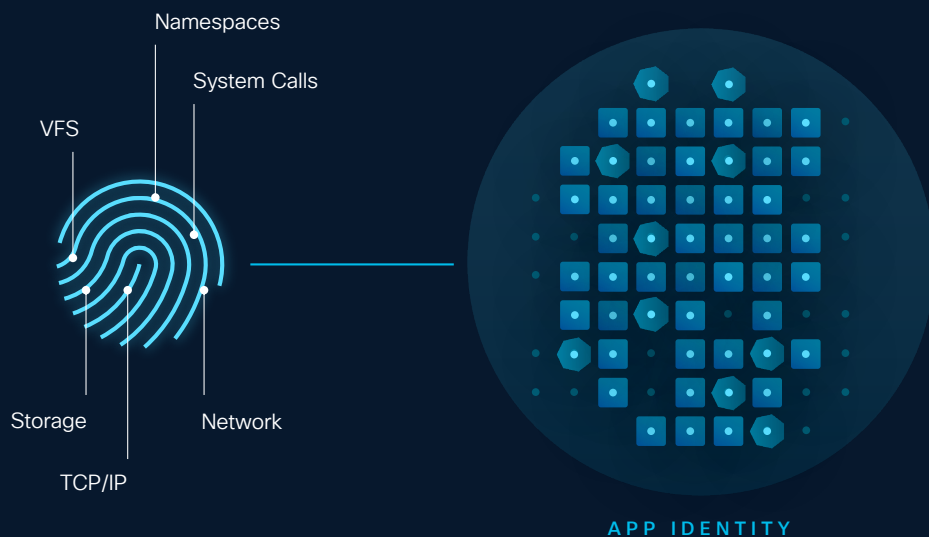
Hypershield & Distributed exploit protection

漏洞修補是極受時間壓力挑戰的一項工作



主動防禦未知漏洞

Proactive defense with unknown vulnerability protection



VALIDATED



SUSPICIOUS

CWE-78

OS command injection

CWE-200

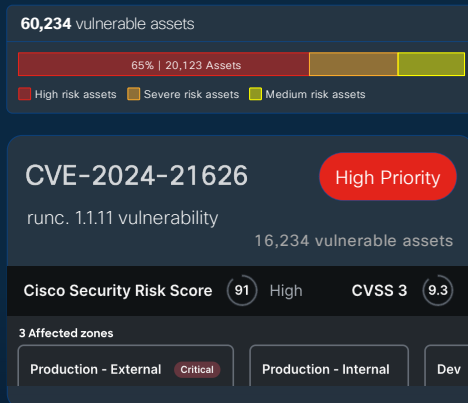
Unauthorized access to sensitive information

MALICIOUS



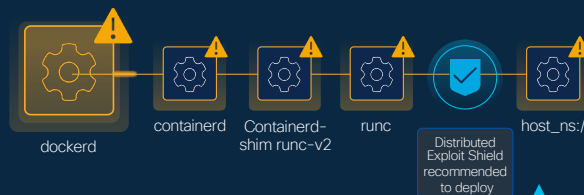
應用程式行為分析 | 常見弱點編號 (CWE) 與行為解析

自動化流程，彌補漏洞防護的空窗期



數據驅動的漏洞優先順序判斷

- 來自 19 個威脅與漏洞情報來源
- 管理超過 127 億筆漏洞資料
- 每月處理超過 10 億筆安全事件



分散式漏洞防護 (Distributed Exploit Shield) 在適合處插入防護：

- ✓ 圖中示範 runc 漏洞防護部署點
 - 阻擋以 root (/) 為執行目錄的新容器行為
- 防護行為：阻擋並警示 (Block and alert)

精準下刀的防護控制，確保應用不中斷



✓ 分散式防護已於實際環境中通過驗證

實際環境下測試，建立信任

Cisco Hybrid Mesh Firewall

其他新支援能力宣布

AVAILABLE OCT 2025

將 Hybrid Mesh Firewall 政策延伸至 Cisco ACI

Cisco Secure Workload integration with ACI

自動化分段政策探索

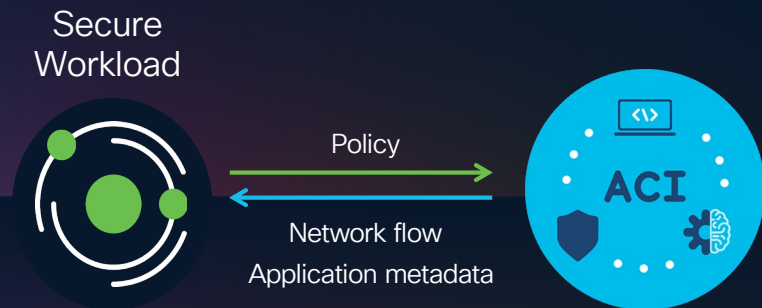
透過 AI 驅動的應用行為與依賴關係可視化，自動找出可執行的分段策略

最佳化的政策套用

Secure Workload 能將網路流量與應用中繼資料，無縫轉換為 ACI 可用的防火牆政策

零阻力部署

無代理 (agentless) 架構，無需更改現有應用程式即可實現可視化與防護



AVAILABLE OCT 2025

將 Hybrid Mesh Firewall 政策延伸至 Cisco ISE

Cisco Secure Firewall / Workload integration with ISE

使用 ISE 標籤即時套用以使用者為基礎的政策

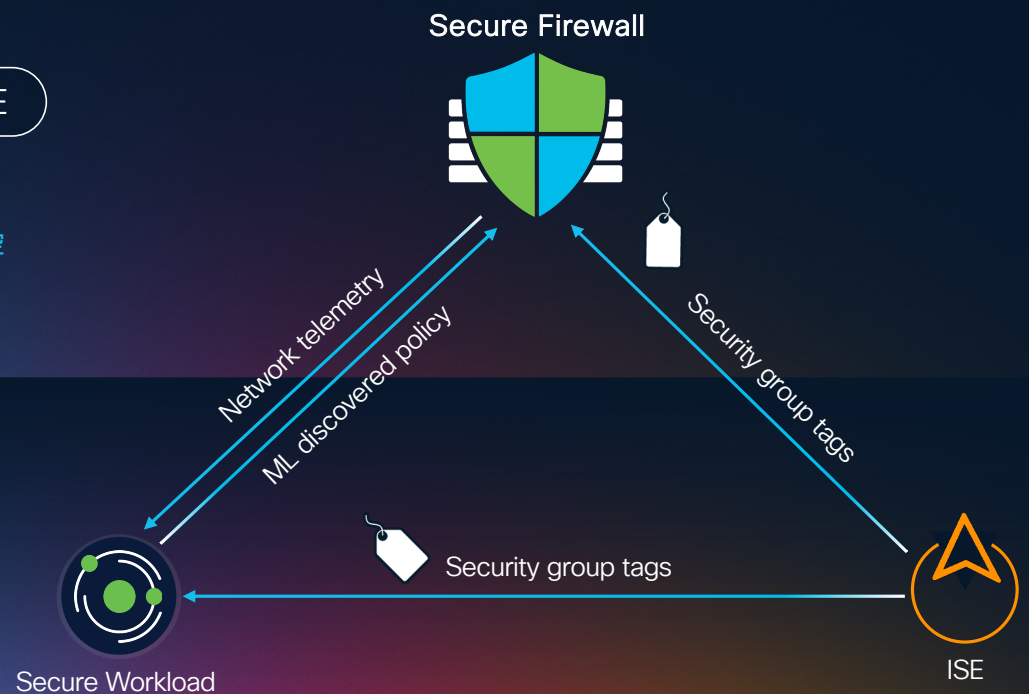
結合 ISE 的身份識別與標籤資訊，實現針對使用者角色與行為的即時安全管控

透過機器學習 (ML) 進行政策自動發掘

AI 能持續學習網路與應用的實際行為，自動建議合適的分段與存取策略

隨著使用者與應用變化，政策自動調整與演進

系統持續觀察環境變化，動態更新安全政策，避免人工維護負擔與遺漏風險。



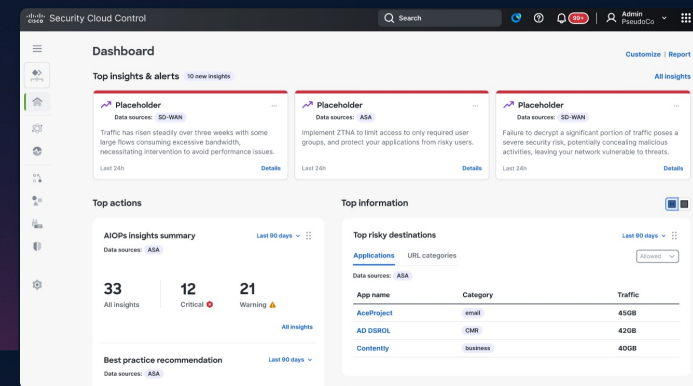
AVAILABLE AUG 2025

將Secure Router的政策管理納入 Security Cloud Control

Cisco Secure Routers

Security Cloud Control 現可支援以下功能：

- 建立物件與安全政策(Create objects and security policies)
- 同步與管理既有的 Secure Router 設定項(Sync and manage existing secure router objects)
- 建立新的安全政策(Create new security policies)
- 在 SAL 中視覺化安全路由器事件(Visualize secure router events in SAL)
- 將 SD-WAN Manager 與 Security Cloud Control 的 RBAC 權限模型進行同步(Sync RBAC model)



支援型號

Cisco 1000 Series Integrated Services Routers
Cisco 8000 Series Secure Routers



AVAILABLE JUL 2025

將 Firewall Threat Defense 升級簡化 導入 AIOps 智慧化升級流程

AIOps 在 Security Cloud Control 中的應用

省下大量升級前規劃時間

AI 根據實際環境提供專屬見解，免除繁複規劃作業

輕鬆識別並處理潛在風險

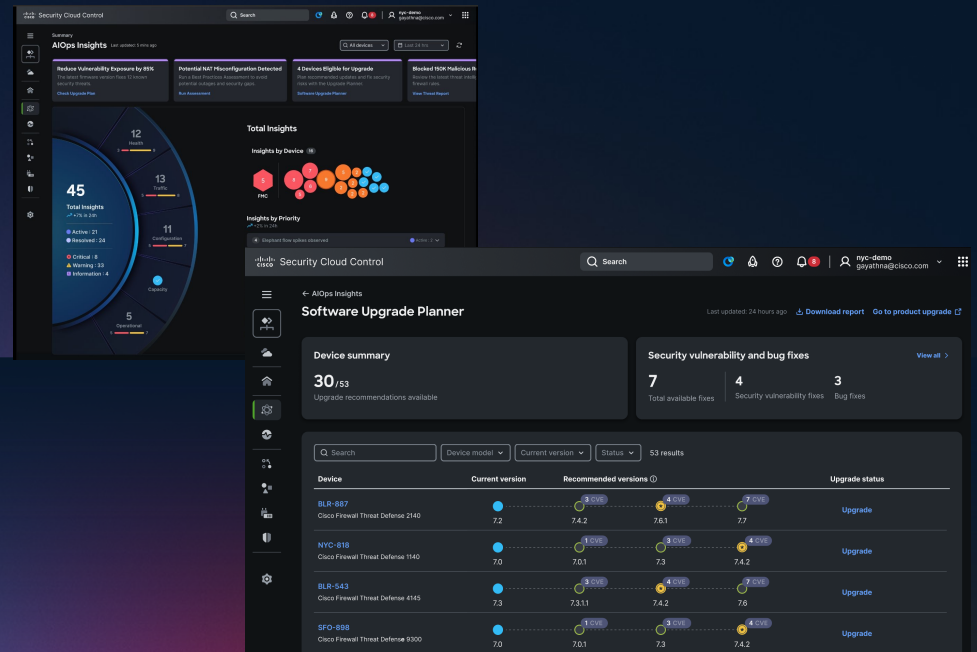
透過 PSIRT 安全公告與當前版本錯誤的客製化分析，及早掌握可能問題

取得個人化升級建議

升級建議與組織的穩定性與創新目標對齊，確保最佳部署策略

降低 90% 人工作業負擔

導引式流程協助您無縫完成升級，避免人工失誤與操作延誤



SCC內建人工智慧助手（ AI Assistant ） – 提升管理人員維運效率

Assist

+ 政策設定

Augment

+ 問題排查

Automate

+ 政策生命週期管理

Cisco AI Assistant

You

Allow Lee access to Facebook but only from office source zone

AI Assistant

11:05 am PST

Here is your rule recommendation, This rule will be added in policy 'Test_1' in the category, 'Geo.Controls'.

Rule Name	Action	Source zone	Destination zone
Rule_Test_1	Allow	Office	guest_zone

>

AI Assistant

11:05 am

'Rule_Test_1' is successfully created in policy 'Test_1'.

Congratulations, your rule named, 'Rule_Test_1' is successfully created in policy 'Test_1'. The rule is created in a **disabled state** as of now. You can enable it from your 'Test_1' policy detail page.

[Go to policy detail page](#)

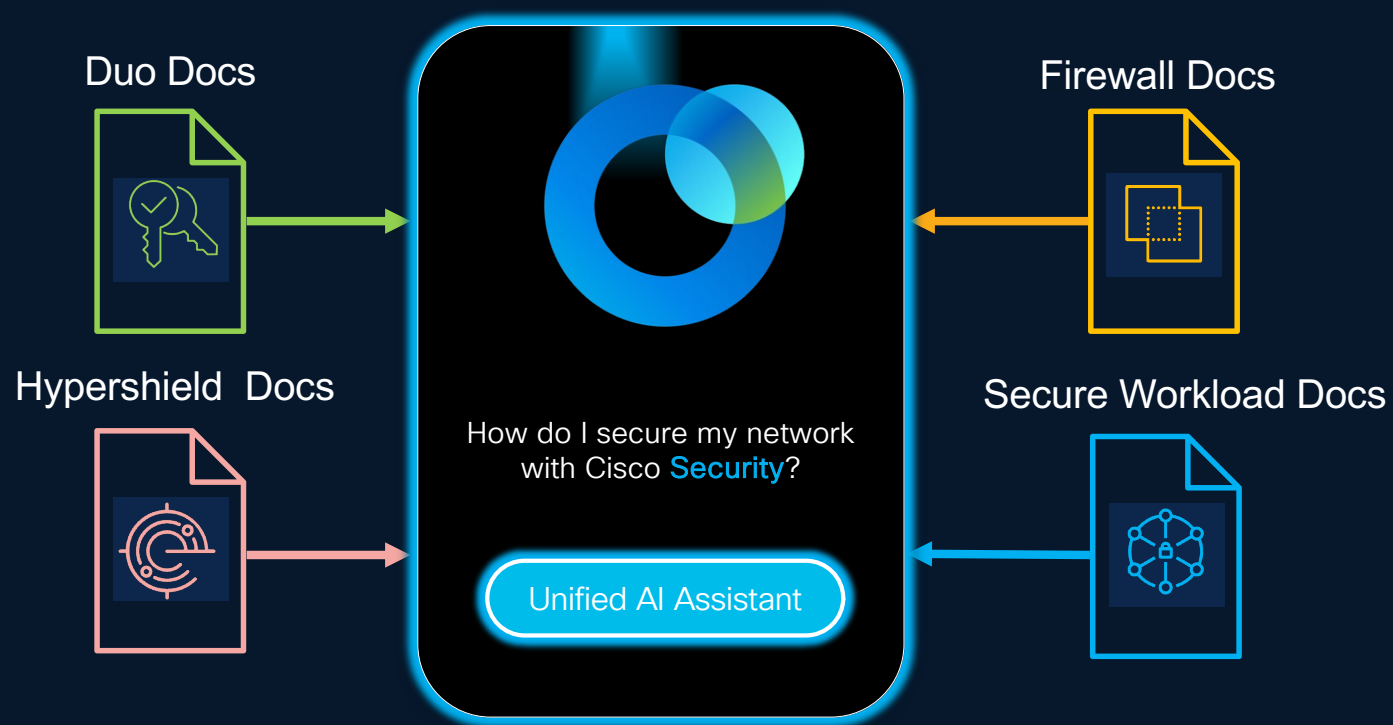
>

Ask the AI Assistant a question

>

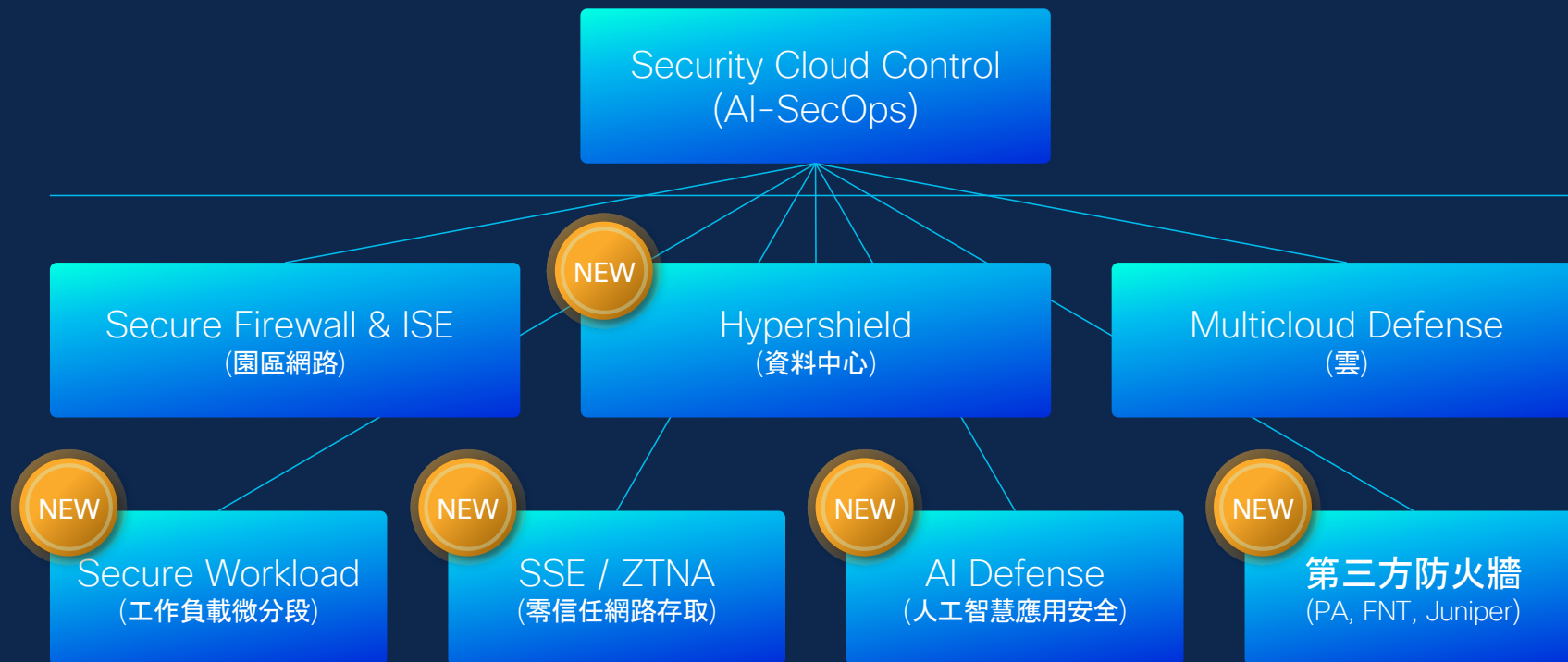
The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

SCC內建人工智慧助手 (AI Assistant) – 思科解決方案知識庫



Cisco Hybrid Mesh Firewall (混合網格防火牆)

只需定義一次微分段政策即可在全域範圍統一執行



Security Insight, on Us

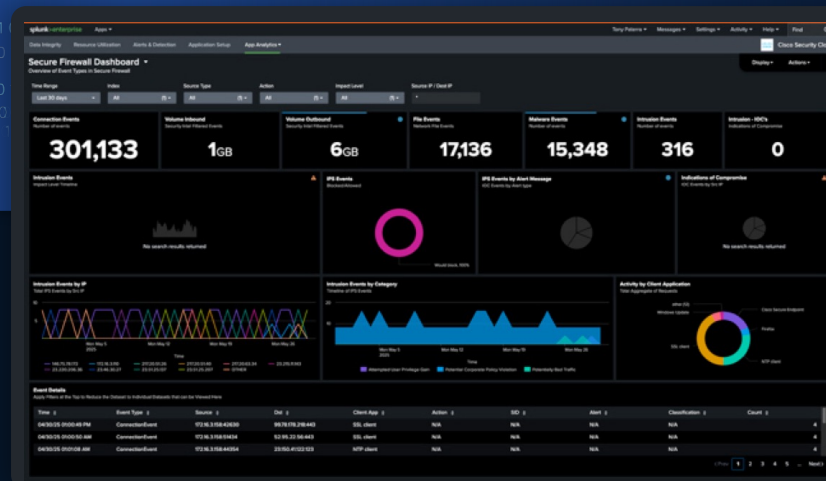
Firewall logs free in Splunk

Free log management*

AVAILABLE AUG 2025



- 需為銷售中的 Cisco Firepower 防火牆型號客戶
- 正在訂閱Firepower資安授權期間(IPS, AMP等功能)
- 每台Firepower可獲得5GB/Day Splunk Core 使用權
- 必須有相同容量的已採購授權
(Ex: 已購買5GB, 透過一台Firepower獲得贈送的5GB)
- 額外贈送上限最高1TB/Day
- 必須連線到 Splunk Cloud
- 申請制, 8月開始受理



New detections | Automated response