The bridge to possible

零信任架構的戰略實務

周敬傑 Alex
Cisco 首席安全架構師

Agenda

- 關鍵挑戰
- 客戶成功經驗
- 邁向零信任的五個階段
- Cisco零信任安全評估服務

關鍵挑戰

您也在擔心嗎?

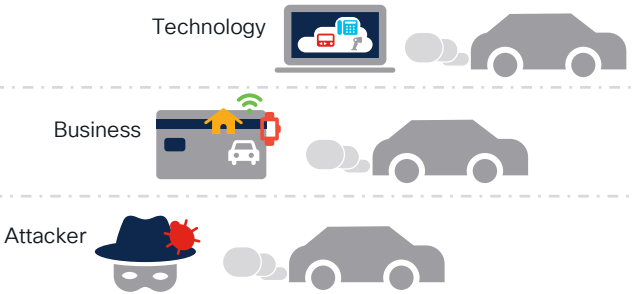
- 降低生產力?

- 破壞營運彈性?

- 減少業務敏捷性?

cisco Engage

為甚麼是現在?



安全始終沒有100%

安全風險持續增高

損失抑制刻不容緩

為甚麼是現在?

USA, Office of Management and Budget，OMB (資料來源)

China, 国家标准化管理委员会 (資料來源)

2022 信息安全技术 零信任参考体系架构

Singapore, 國務資政兼國家安全統籌部 (資料來源)

Taiwan, 行政院國家資通安全會報技術服務中心 (資料來源)

《政府零信任網路身分鑑別機制導入建議》

《政府零信任網路說明》

揭露! 成功的祕訣!

建立安全文化

...不只是CISO的支持

保護既有資產

...不是一蹴而就的投資

制定商業計劃

...跳脫傳統計畫方式

邁向零信任
五個階段

甚麼是零信任?

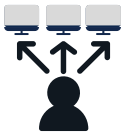
零信任，不是一個產品或技術，是一種安全戰略方法

傳統安全設計邏輯

信任是基於存取請求的網路來源

零信任安全設計邏輯

無論存取請求來自何處
為每次存取請求建立驗證並授予
“Least-Privilege Access” 最小存取權限



攻擊者進入網路後可在網路內
任意橫移以到達目的

確保只有正確的用戶和設備才能存取
正確的應用或數據

第一階段：使用者信任

確保擁有正確的機制與流程，只有授權的用戶才能嘗試存取資源

 指標	 行動	 挑戰	 組件
用戶/權限風險排序	整合身分管理系統(IAM)	使用者擔心生產力	身份資料庫
擴大MFA使用範圍	MFA實施統計		2FA或MFA方案
持續驗證每個使用者	內部效益與分享		

第二階段：設備和行為可視性

需知道每個存取請求來自哪個位置、端點及設備? 包含它的安全狀態

指標	行動	挑戰	組件
設備及應用調查	整合資產盤點	缺乏全面的設備清單	資產盤點系統
應用風險與優先排序	整合應用清單資料庫	缺乏全面的應用清單	應用程式資料庫
持續驗證應用存取	納管/非納管設備		Access Proxy
	納管/非納管應用		單點登入系統(SSO)
	持續的設備檢康檢查		

第三階段：設備信任

無論是否為組織內的設備，都將其註冊並與使用者關聯

指標	行動	挑戰	組件
設備風險與優先排序	持續設備漏洞審查	使用裝置安裝Agent	可信任設備資料庫
建立設備信任的技術	建立違規行為政策	缺乏全面納管的資源	EDR, MDM
持續驗證身份與設備	資產清單與政策同步		

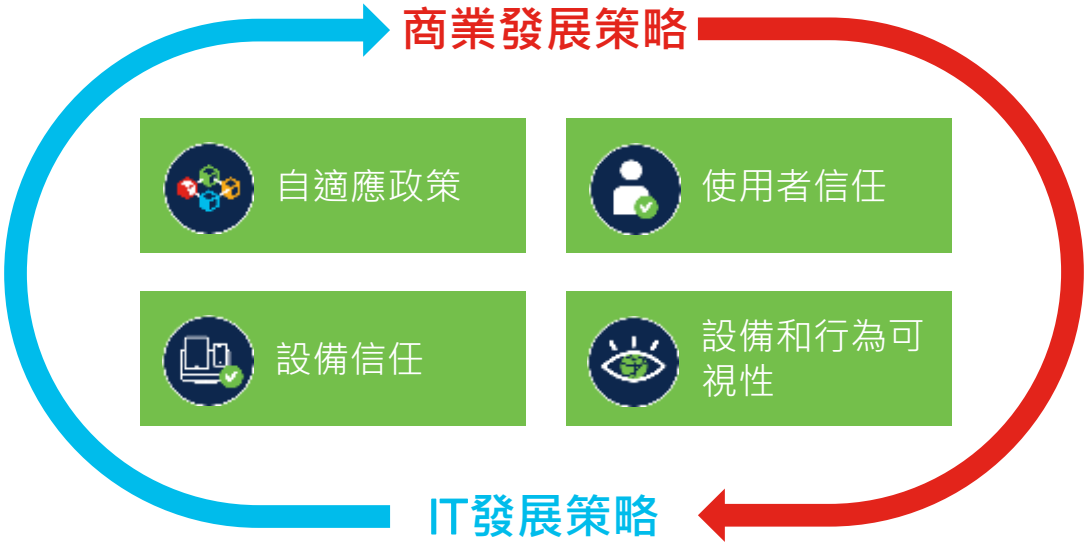
第四階段：自適應政策

根據資源敏感性和已知的安全狀態設置存取政策，管理風險

指標	行動	挑戰	組件
風險承受能力政策	制定驗證異常的流程	各部門政策意見不一	存取控制
整合身份驗證流程	安全通報流程		信任推斷
整合分段(微)技術	組織業務流程		

第五階段：持續工作

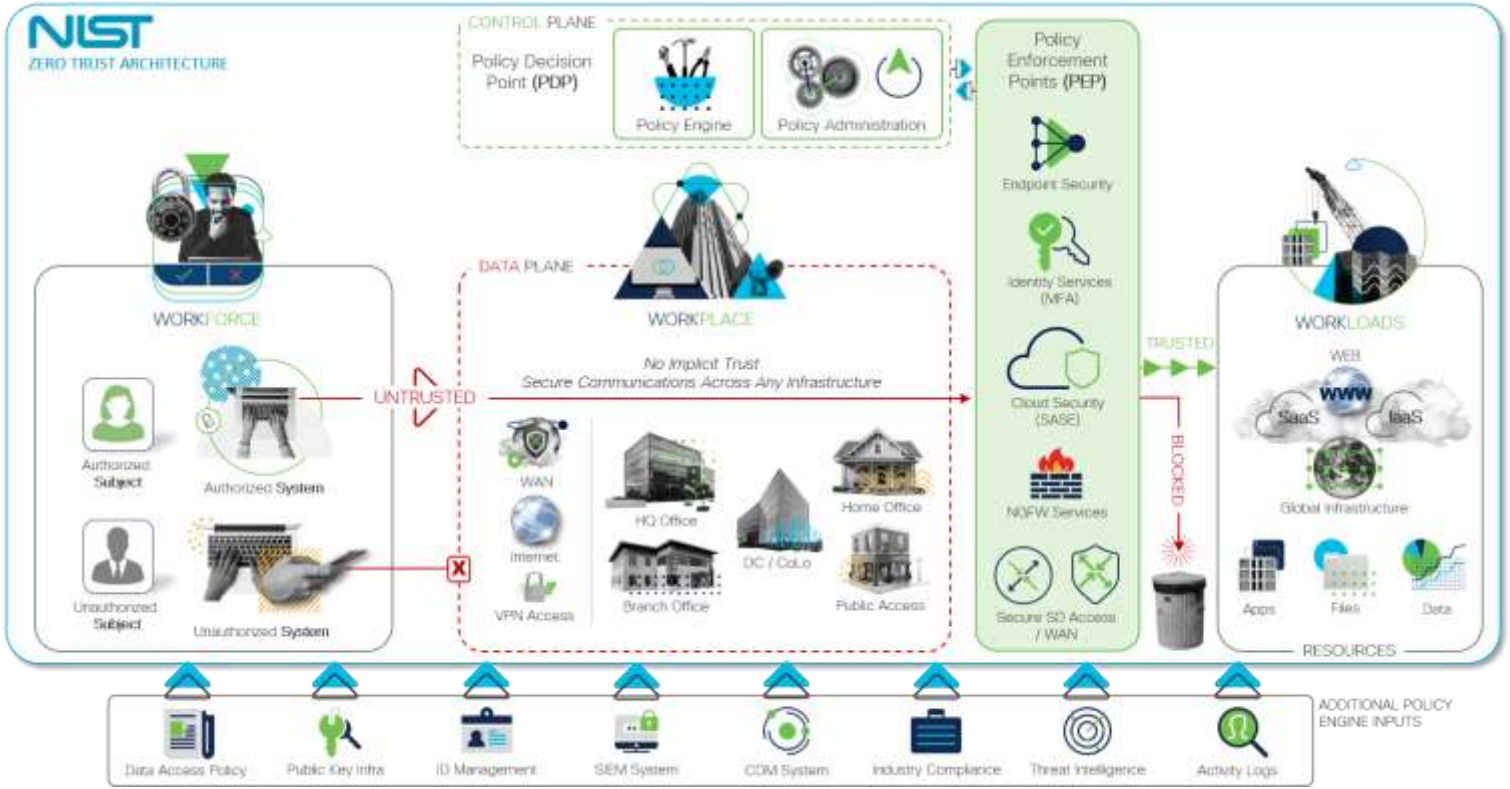
持續驗證與監控，逐步擴大零信任工作流範圍



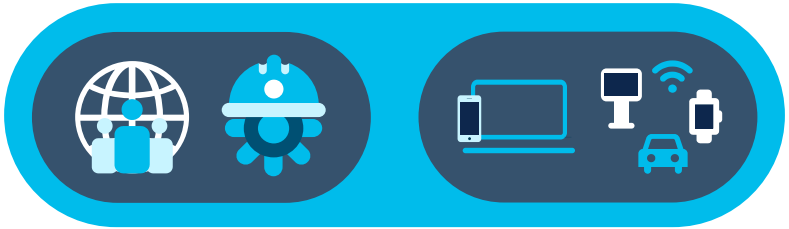
Cisco零信任安全
評估服務

cisco Engage

Cisco解析NIST安全架構



零信任安全評估：三個視角



所有使用者

- ✔ 員工
- ✔ 約聘人員
- ✔ 供應商

任何設備

- ✔ 公司配發設備
- ✔ BYOD
- ✔ 物聯網

進階使用者身份驗證　端點可靠性評估

生產力

Workforce

任何應用

- ✔ 資料中心
- ✔ 多雲
- ✔ SaaS

通訊稽核

工作負載

Workload

任何地方

- ✔ 本地
- ✔ 通過VPN存取
- ✔ 不通過VPN存取

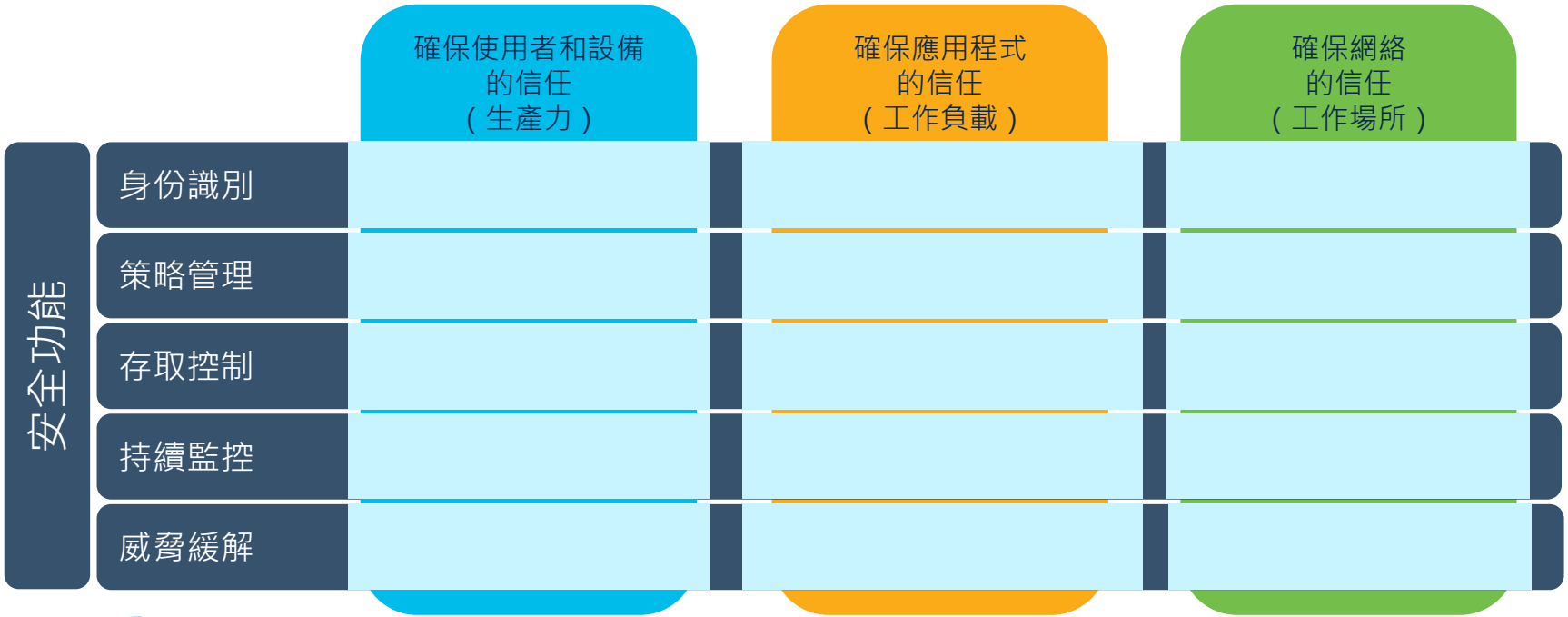
最小許可權

工作場所

Workplace

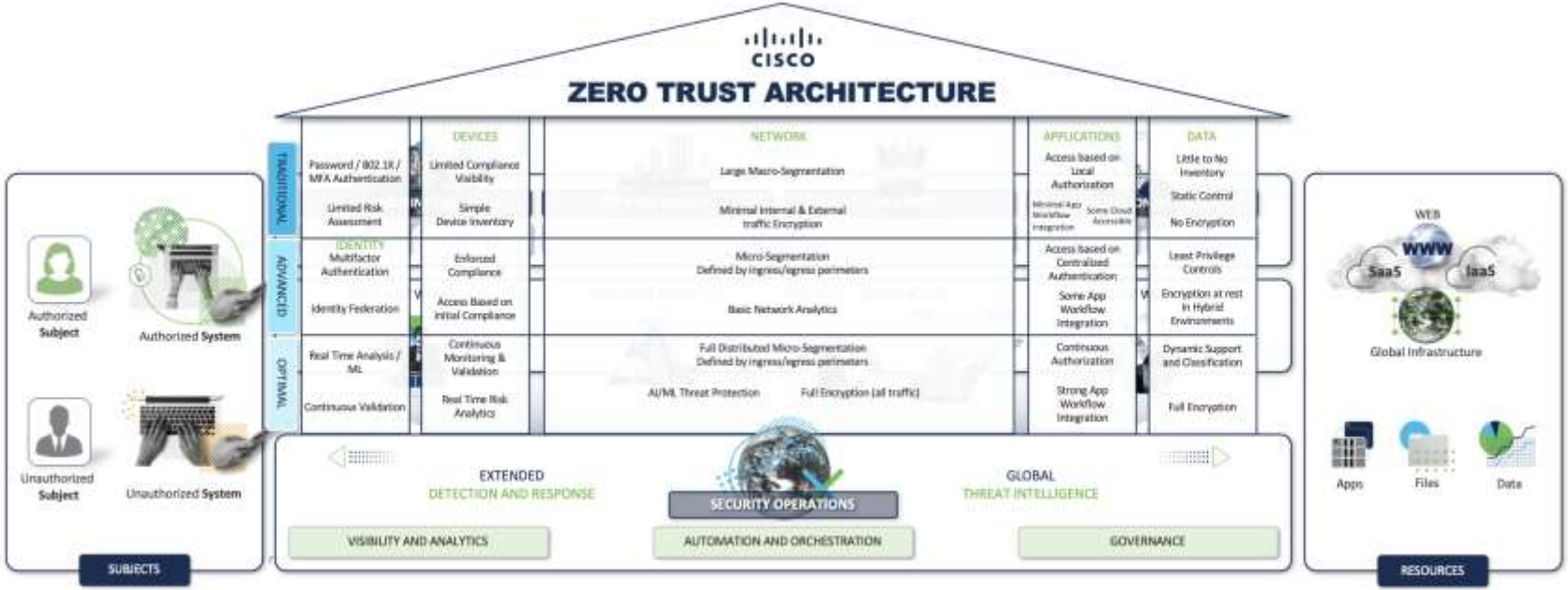
零信任安全評估：30+評估內容

從需要確保信任的三個視角，評估所需五個安全功能實施狀態



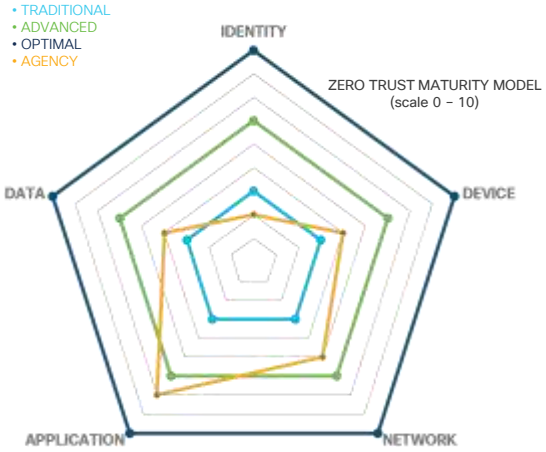
Cisco零信任成熟度評估模型

參考NIST及CISA標準，最完整的評估模型



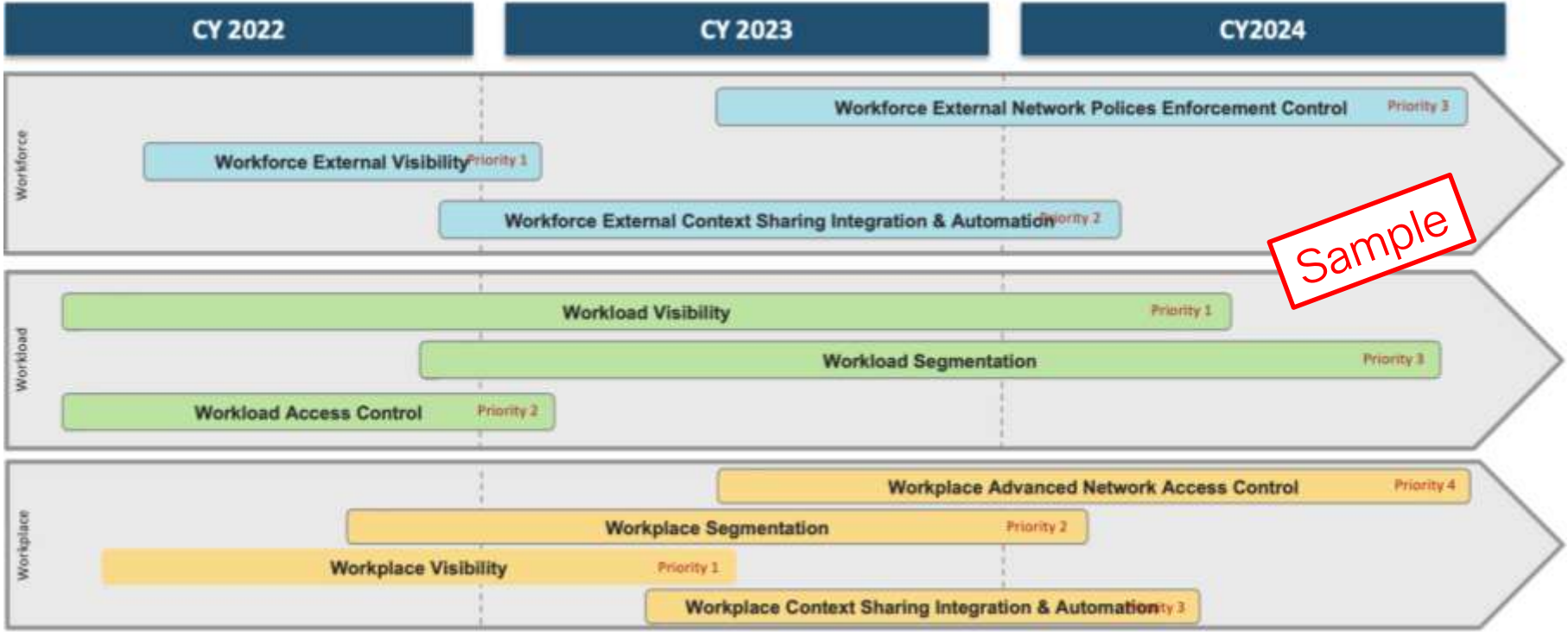
零信任安全評估：評估指標

Pillar	Function	Score
Identity	認證	
	身份存儲	
	風險評估	
	可見性和分析能力	
	自動化和編排能力	
	治理能力	
Device	合規監控	
	資料訪問	
	資產管理	
	可見性和分析能力	
	自動化和編排能力	
	治理能力	



Pillar	Function	Score
Network	網路分段	
	威脅防護	
	加密	
	可見性和分析能力	
	自動化和編排能力	
	治理能力	
Application	訪問授權	
	威脅防護	
	可訪問性	
	應用安全	
	可見性和分析能力	
	自動化和編排能力	
	治理能力	
Data	庫存管理	
	訪問確定	
	加密	
	可見性和分析能力	
	自動化和編排能力	
	治理能力	

零信任安全評估：Roadmap規劃建議

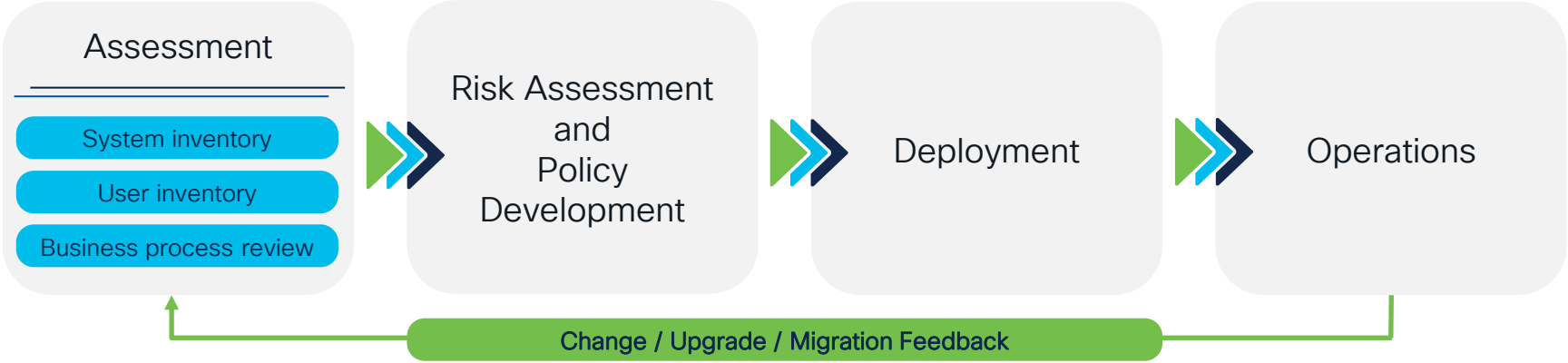


Cisco一站式提供資安解決方案

Network Security	Secure Firewall Formerly NGFW	次世代防火牆 次世代入侵偵測防禦系統
	Secure Network Analytics Formerly Stealthwatch	網路流量行為分析
	Secure Identity Services Engine Formerly ISE	帳號管理 設備識別與認證 (IT/OT/IoT) 網路存取控制
Cloud Edge	Secure Umbrella Formerly Umbrella	雲服務安全 DNS保護與安全存取
User and Endpoint Protection	Secure Endpoint Formerly AMP for Endpoint	次世代防毒 端點事件反應調查
	Secure Email Formerly Email Security	電子郵件安全防護
	Secure Access by Duo Formerly Duo Security	雙因認證 端點合規管理
Application Security	Secure Workload Formerly Tetration	應用程序安全 應用程序級微分割 (Micro-Segmentation)

零信任之旅

一起開始吧!



從低風險服務、雲應用或遠端工作開始

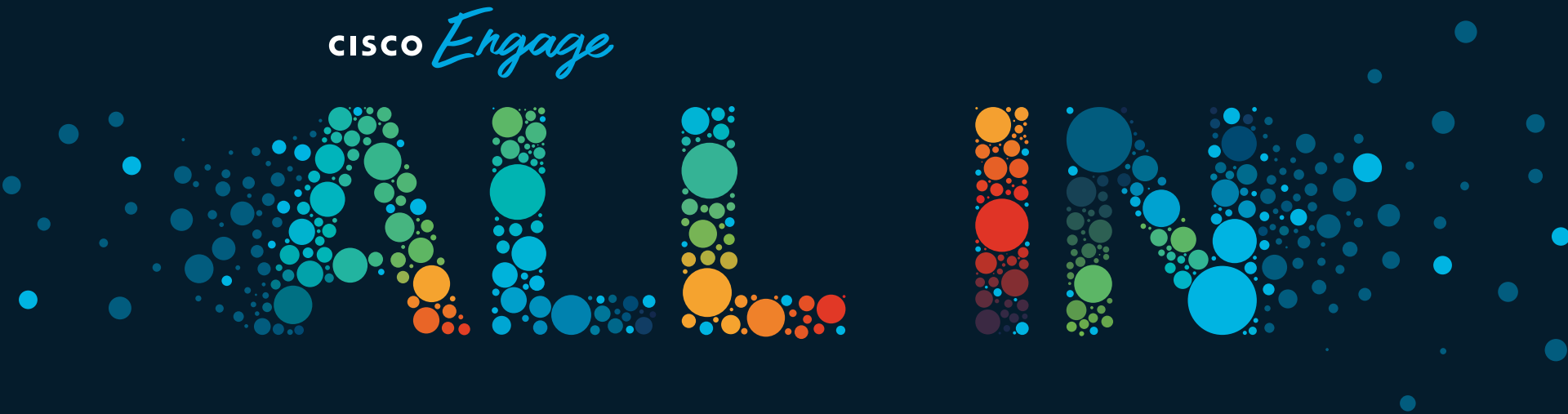
...首先調查您的資產、核心業務、資料流程和工作流程!

The bridge to possible

Thank you

cisco Engage

#CiscoEngage



#CiscoEngage