CATO NETWORKS

使用 Cato SSE 360 構建成熟的零信任架構

Colin Xia

System Engineer–（亞太地區）

安全風險

內部威脅 → 人為因素構成了一大挑戰。

隨時隨地存取 → 擴大的攻擊表面

組織化的網路犯罪 → 更廣、更迅速、更智能

風險無所不在

檢視被阻擋的事件

Action	Block
Application	HTTP(S)
Category	
Destination Country	France
Destination Country Code	FR
Destination IP	162.19.138.120
Destination Port	443
Domain Name	lb.eu-1-id5-sync.com
Event Count	1
Sub-Type	Internet Firewall
Event Type	Security
Event Internal ID	u5jesYQHHL
IP Protocol	TCP
ISP Name	Globe Telecom Inc
OS Type	OS_MAC
OS Version	13.0.1
PoP Name	Manila
Rule	Default Prompt Rule
Source Country	Philippines
Source Country Code	PH
Source IP	
Source is Site or SDP User	
Source ISP IP	
Source Site	
Time	2023/01/11 20:40:25.025
Event Reference ID	7825410

CATO NETWORKS

錯誤的規則.....

允許未經授權存取的規則

允許惡意軟體滲入的規則

允許 停留時間 的規則

過度信任

信任危機
的開端

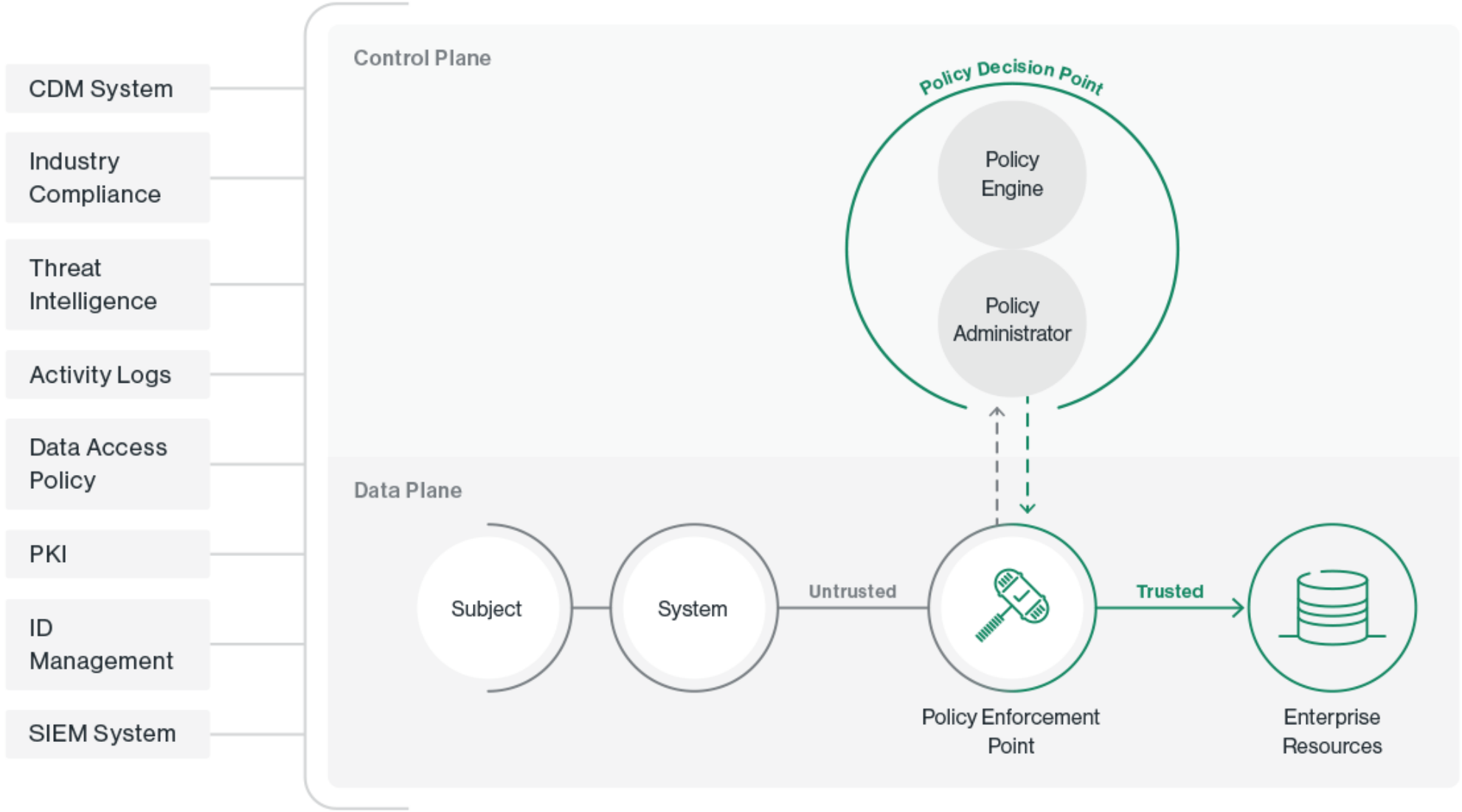
允許未經授權存取的規則

允許惡意軟體滲入的規則

允許 停留時間 的規則

CATO NETWORKS

NIST SP-800-207



零信任架構只是起點

*至2025年，預計將有 **60%** 的組織將以零信任架構作為安全的出發點。*

Gartner®

來源：Gartner’s 8 Cybersecurity Predictions for 2022 Through to 2026

CATO NETWORKS

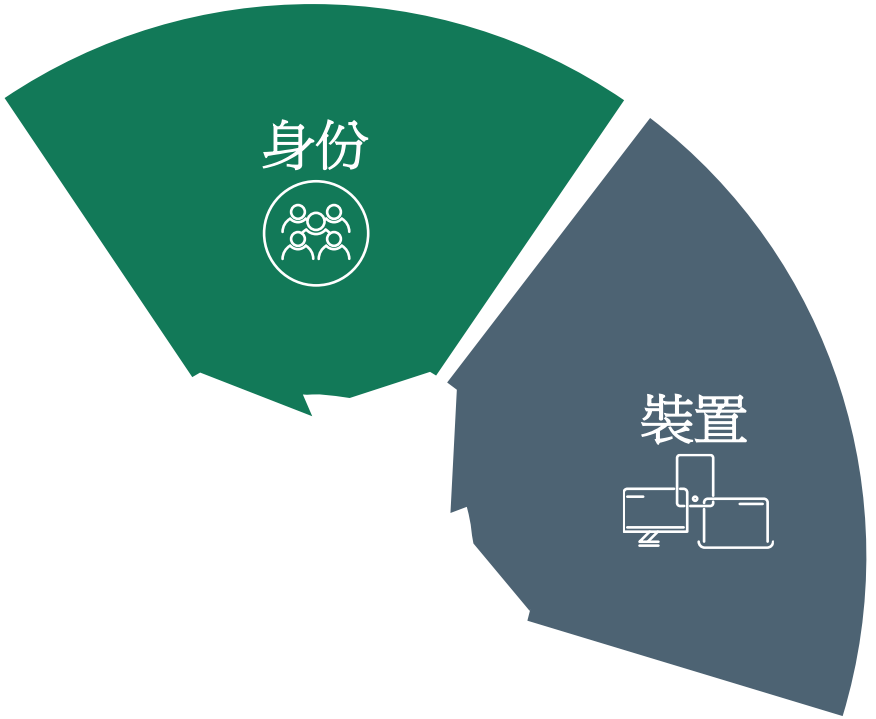
零信任架構原則

- *動態的資源訪問政策*
- *持續監控與評估*
- *網路分段與最小權限原則*
- *情境感知*
- *整體影響*

CISA零信任架構成熟度模型

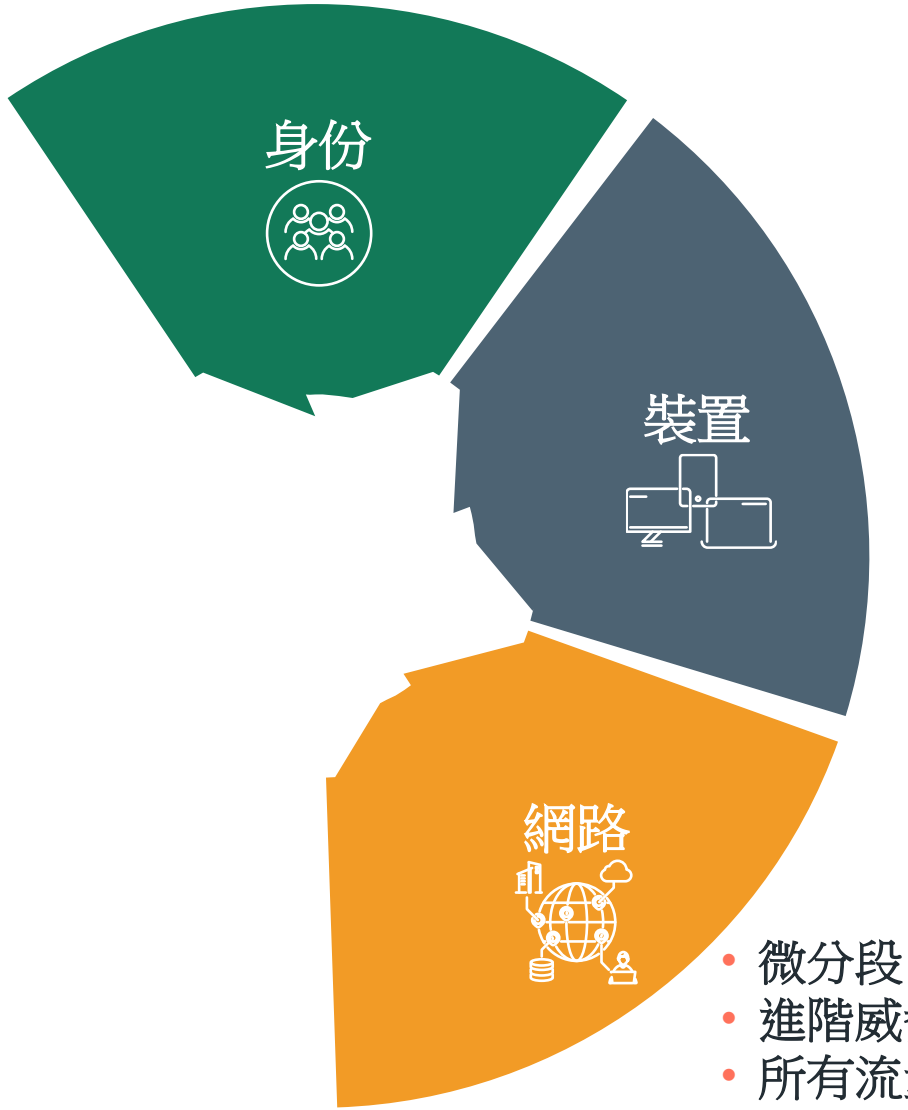
- 持續驗證
- 即時人工智慧/機器學習分析
- 全球意識

CISA零信任架構成熟度



- 持續驗證
- 以風險為基礎的網絡存取
- 全面姿勢追蹤

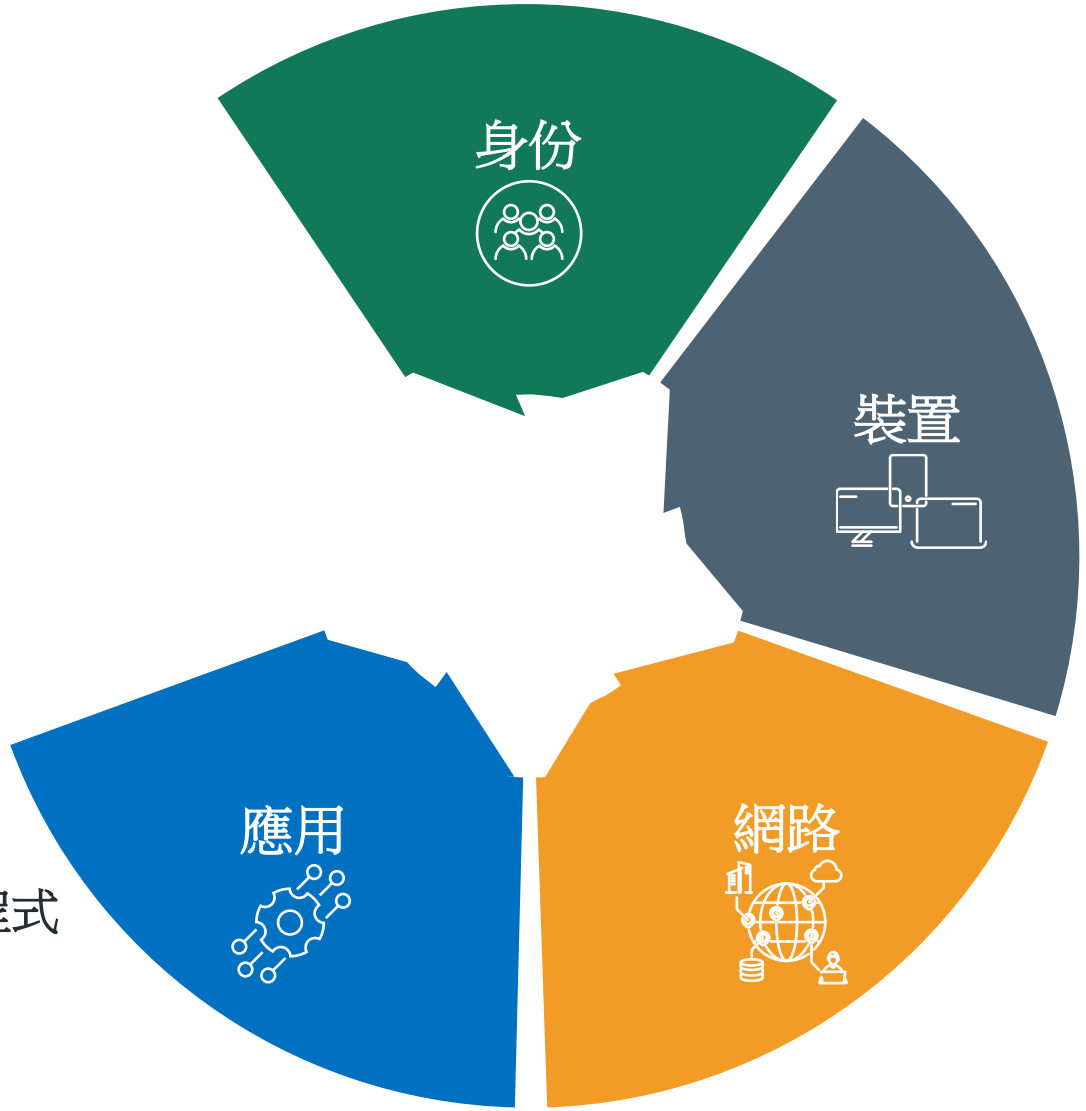
CISA零信任架構成熟度



- 微分段
- 進階威脅防禦
- 所有流量均加密

CATO NETWORKS

CISA零信任架構成熟度



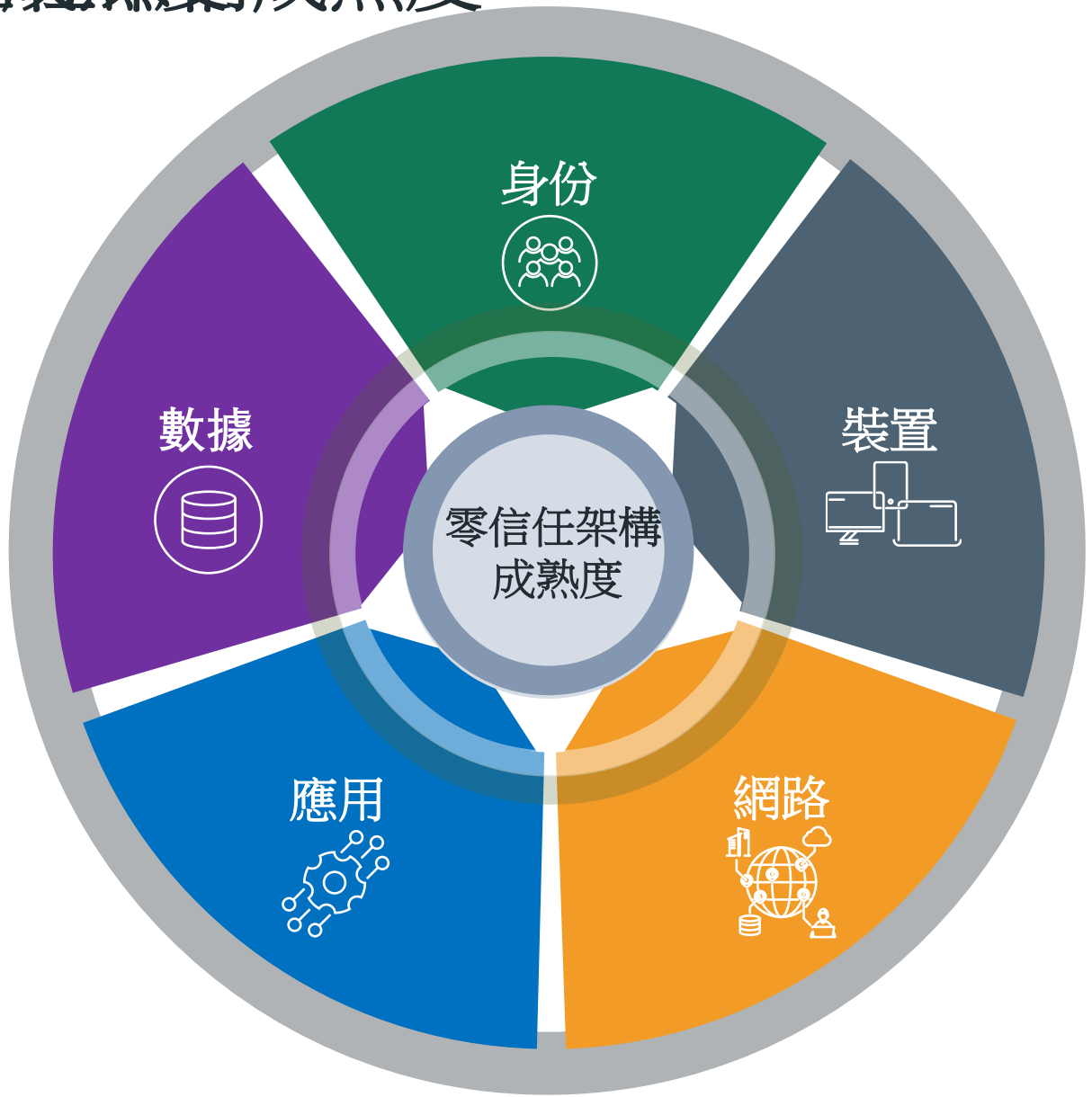
- 以風險為基礎的應用程式存取
- 進階威脅防禦
- 持續授權

CISA零信任架構成熟度

- 動態數據支援
- 數據加密
- 以風險為基礎的數據存取

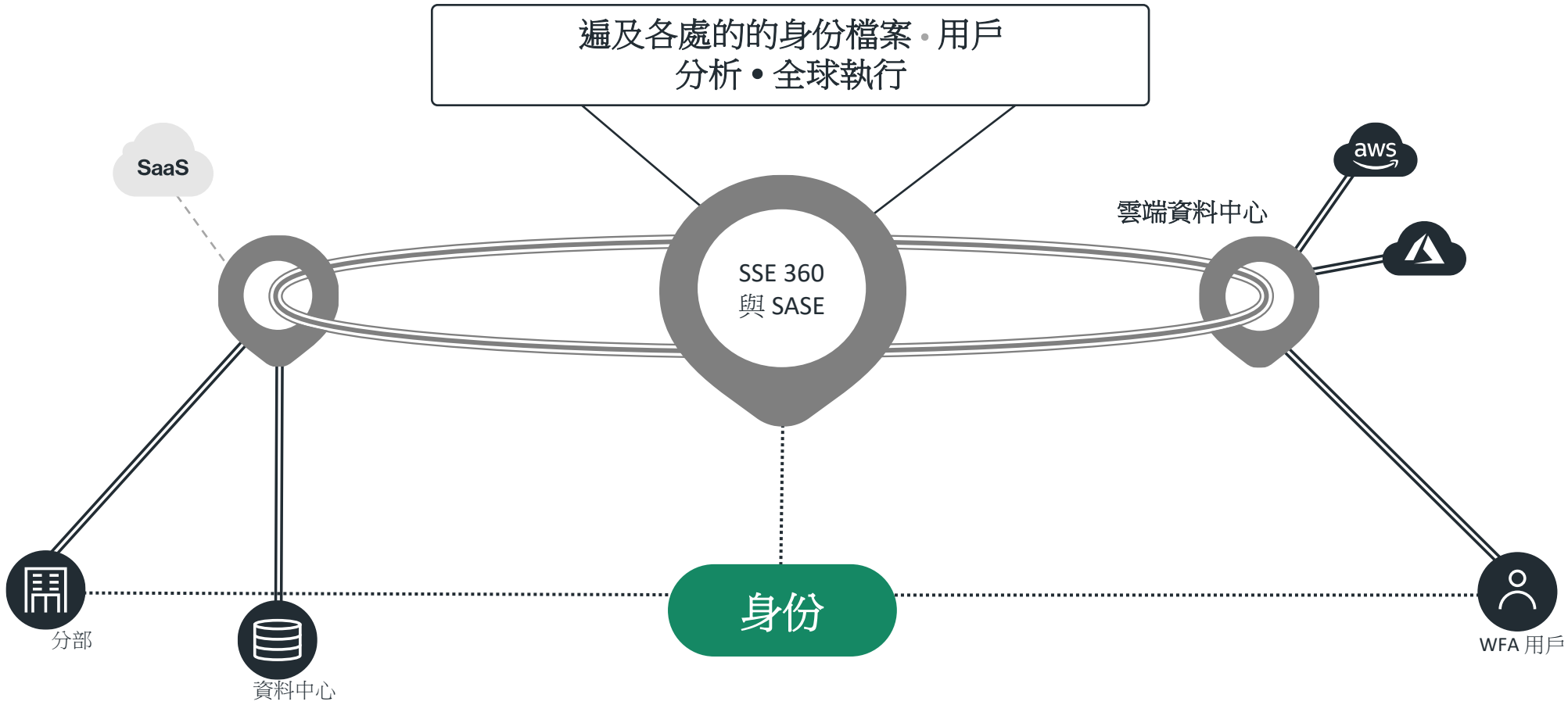
CATO NETWORKS

CISA 零信任架構成熟度

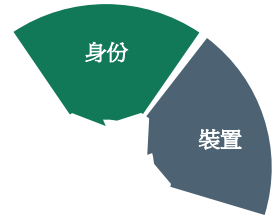


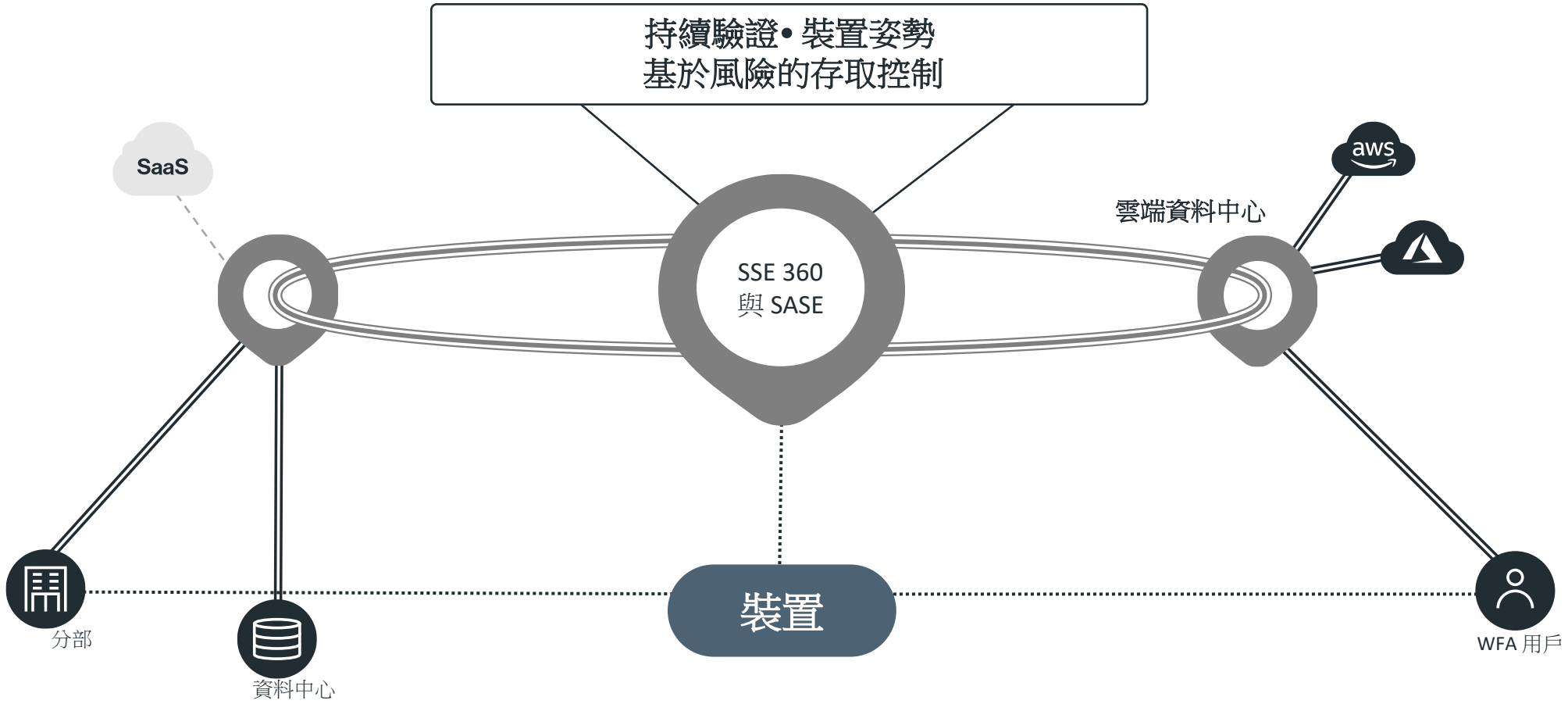
強化可見度及分析機制，建立自動化機制，有效地編排及管理

架構視角 - 使用 Cato SSE 360 實現零信任架構成熟度



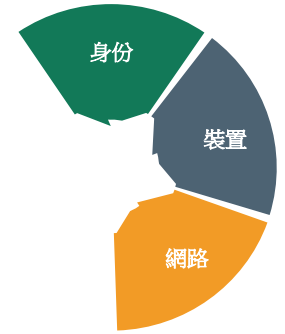
架構視角 - 使用 Cato SSE 360 實現零信任架構成熟度

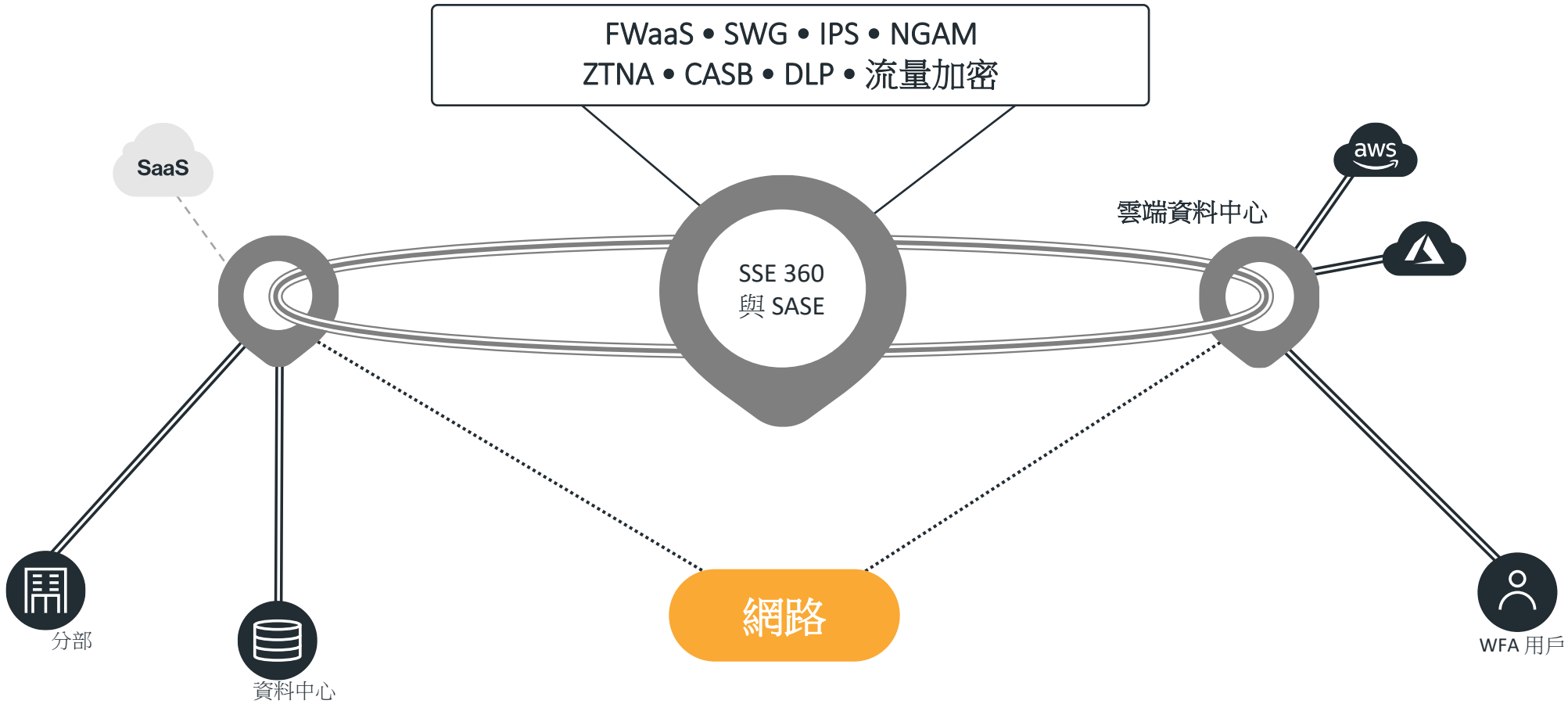




CATO NETWORKS

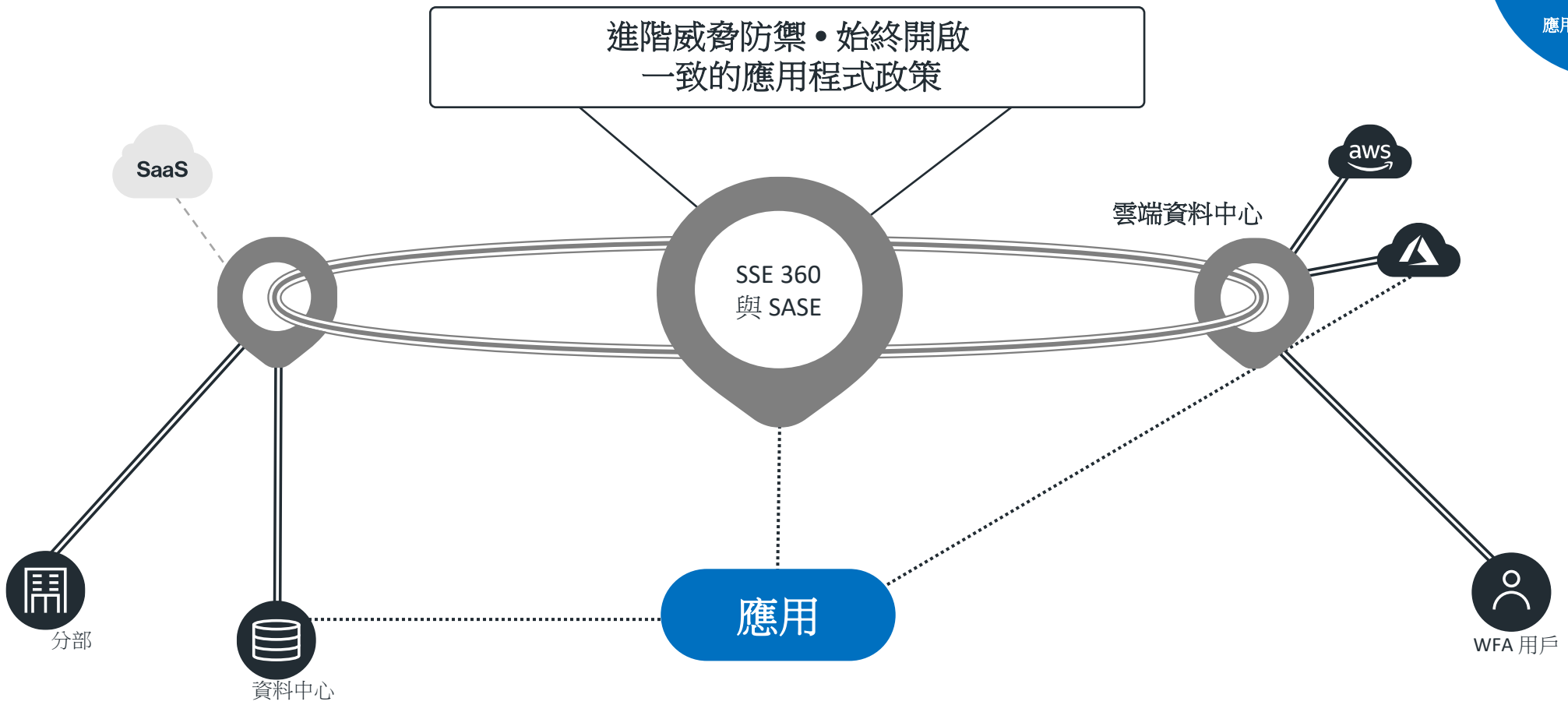
架構視角 - 使用 Cato SSE 360 實現零信任架構成熟度





CATO NETWORKS

架構視角 - 使用 Cato SSE 360 實現零信任架構成熟度



CATO NETWORKS

架構視角 - 使用 Cato SSE 360 實現零信任架構成熟度

敏感數據保護 • 進階威脅防護
以風險為基礎的數據存取

SaaS

SSE 360
與 SASE

雲端資料中心

aws

分部

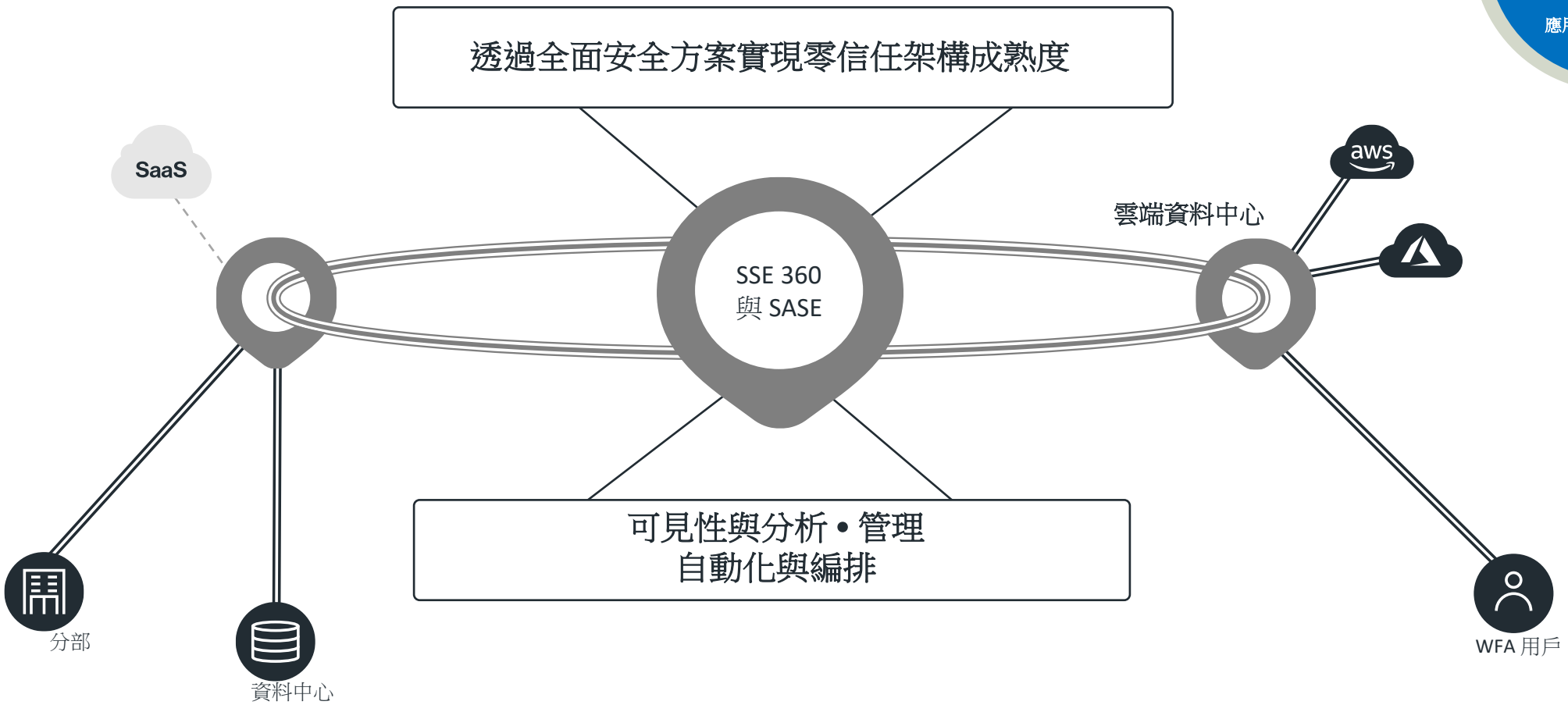
資料中心

數據

WFA 用戶

CATO NETWORKS

架構視角 - 使用 Cato SSE 360 實現零信任架構成熟度

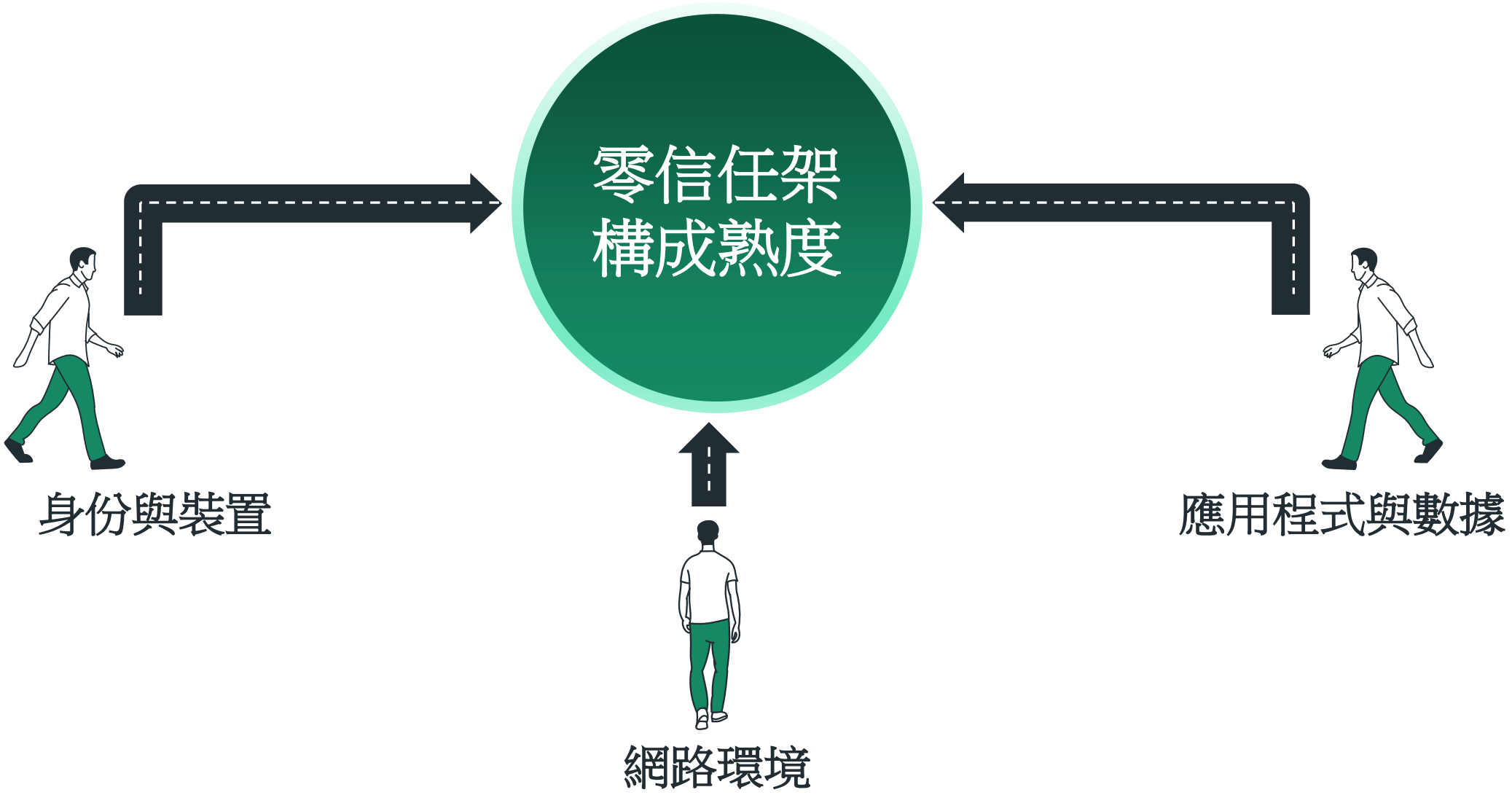


CATO NETWORKS

以風險為基礎的零信任架構成熟度路徑

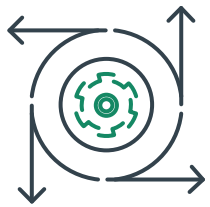
- **識別風險** - 預先評估潛在的風險用戶和設備
- **評估風險** - 確定風險狀況並做出相應定義
- **控制風險** - 全面執行適當的存取政策
- **審查風險** - 持續的風險評估和即時調整

零信任架構是一段旅程



CATO
NETWORKS

總結



持續
驗證

全球覆蓋
與上下文感知

360 度全方位威脅
防護

CATO NETWORKS

CATO NETWORKS

Cato SASE. Ready for Whatever’s Next.