CISCO
SECURE

CISCO The bridge to possible

零信任的資安新思維

華電聯網副總經理 鄭炤仁 / 思科全球安全業務部經理 朱育民

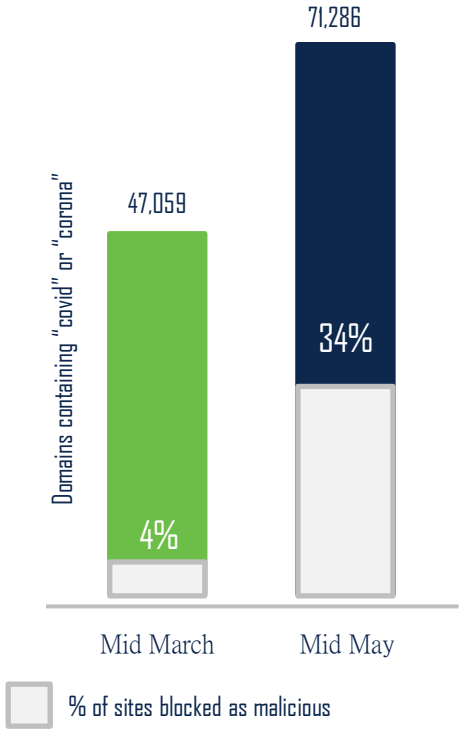
May 5th, 2021

資訊基礎建設正飛快地成長

遠距辦公與駭客的攻擊也同步在改變

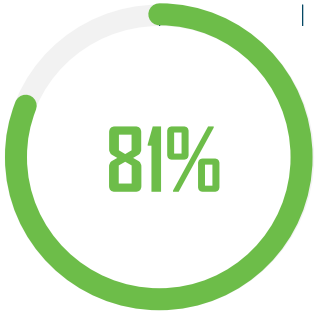
思科調查報告：
自2020/03第一週至最後一週，遠距辦公的人數增加了一倍。

- **在Umbrella公司發布的報告顯示，企業用戶連線至有關“covid”和”corona”的網址數量**
  - 2020/03：47,059個與covid和corona有關的網址，其中僅4%為惡意網址並被阻擋
  - 2020/05：71,286個與covid和corona有關的網址，其中有34%為惡意網址並被阻擋



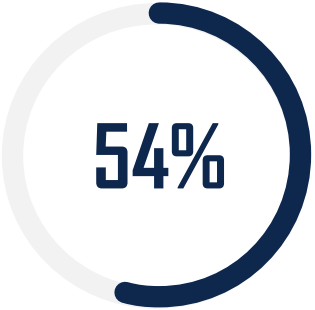
駭客用更簡單的方式，製造更大規模的威脅

我們需要新的安全方法來解決身份，應用和網路威脅。



憑證外洩

81%的攻擊行為涉及憑據外洩



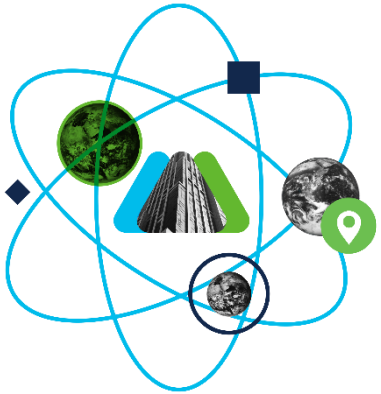
網頁應用程序漏洞

54%的網頁應用程序
存在可被利用的漏洞

萬物聯網的環境改變

針對物聯網設備的攻擊
增加了300%的成長

成長帶來挑戰



Increased complexity
維運複雜度增加

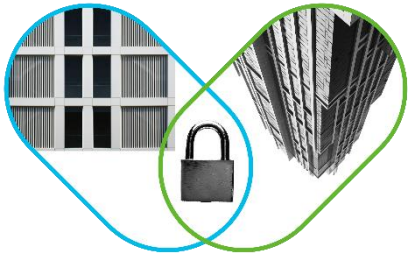
Increased attack surface
攻擊受災面擴大

Gaps in visibility
可視性受限

應用的場景

Secure
remote access
安全遠距存取

Secure
multi-cloud access
安全多雲存取



Threat mitigation/
breach defense
威脅遏止 / 侵入防禦

大哉問：

如何有系統的設計與佈建
資訊基礎架構的安全防禦？

零信任(Zero Trust)與傳統安全防禦設計思維的不同

傳統安全設計邏輯

信任基於訪問請求的網路來源

零信任設計邏輯

無論訪問請求來自何處
都會為每次訪問請求建立信任
“Least-Privilege Access” 最小訪問權限

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訪問正確的應用

針對零信任資安基礎架構提出三個切入的維度

增強的身份治理
(Enhanced Identity Governance)

確保只有正確的用戶和安全的設備才能訪問應用程序

應用服務間的微分割
(Micro-Segmentation)

保護您應用程序中的所有連接

軟體定義網路基礎架構
(Network Infrastructure and Software Defined Perimeters)

保護網路(包括IoT)上的所有用戶和設備連接

單一而全面的設計思維，確保橫跨網絡，應用程序乃至於多雲環境的所有訪問。

針對零信任資安基礎架構提出三個切入的維度

	 用戶與端點 Workforce	 應用與服務 Workload	 軟體定義網路 Workplace
Who or What 對象	People & their Devices (Laptop, Mobile, Tablet) 人員、設備(電腦、行動裝置)	Apps, Services, Microservices 應用程式、服務、微服務	IT Endpoints & Servers, Internet of Things (IoT) Devices, Industrial Control Systems(ICS) 伺服器、端點、IoT、OT設備
Trust Verification 信任驗證	Accessing Applications 應用存取	Communicating with Other Systems 系統間溝通	Accessing the Network 網路存取
From	Anywhere 任何來源與目的	On-Premises, Hybrid Cloud, Public Cloud 橫跨地端與多雲	On-Premises, Hybrid Cloud, Public Cloud 橫跨地端與多雲
NIST SP 800-207	Enhanced Identity Governance 增強的身份治理	Micro-Segmentation 應用服務間的微分割	Network Infrastructure and Software Defined Perimeters 軟體定義網路基礎架構

零信任是一個不斷循環的旅程

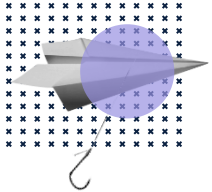
Establish trust
建立信任

Enforce trust-based access
執行基於信任的存取

Continuously verify trust
持續驗證

建立安全的存取

避免風險

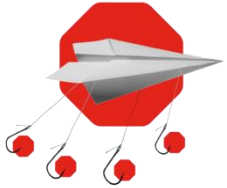


在侵入發生前
降低風險

建立存取行為的可視性

識別違反信任的
風險和指標

降低攻擊受面



遏制侵入並阻止
攻擊者橫向移動

The Zero Trust Approach

啟用基於策略的控制
限制公司環境中的每個訪問請求

查看那些人員與設備
在訪問應用程序，工作負載和網絡

基於策略來分割(Segment)
網路和工作負載

採取零信任方法來確保整個IT環境的訪問安全

如何將零信任設計
落實在客戶環境實現保護

從哪裡開始

Workforce
User and device access

Secure Access

如何確認存取人員身分正確？

他們存取的是對的應用嗎？

他們使用的存取設備是否已受信任？

他們使用的存取設備安全嗎？

Workload
Application and workload access

Secure Workload

在企業系統中使用哪些應用？

應用與資料流是如何溝通的？

這些溝通是否安全與可信任？

Workplace
Network access

Secure Network

用戶和設備是否通過身份驗證？

他們被授予什麼訪問權限？

網路內設備是否安全？

是否基於信任存取原則來設計網路分段(segmentation)？

訪問無處不在 - 如何獲得可見性並確保安全、受信任的訪問？

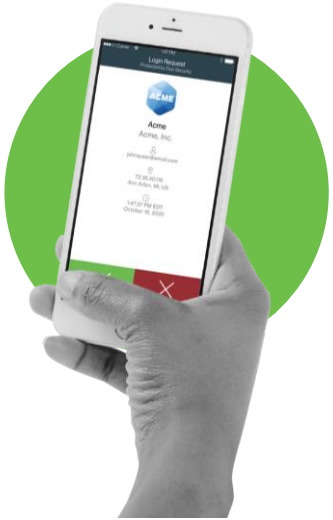
Zero Trust for Workforce

主要應用場景:

Secure Remote Access / 安全遠距存取

為訪問應用程序和資源的用戶及其設備建立信任

Zero Trust for the Workforce



確保只有正確的用戶和安全的設備才能訪問應用程序。

- Phishing / **釣魚攻擊**
- Malware / **惡意軟體**
- Credential Theft / **憑證盜取**
- Remote Access / **遠距存取安全**
- Device Security / **端末設備安全**

Workforce
How to verify trust

確認用戶的身份

取得端末設備的資訊可視
並建立信任

對每一個應用建立存取政策

雙因認證(MFA)

端末設備健康度與狀態管理

基於用戶身份的存取政策

Zero Trust for Workload

主要應用場景:

Secure Multi-Cloud Access / 安全多雲存取

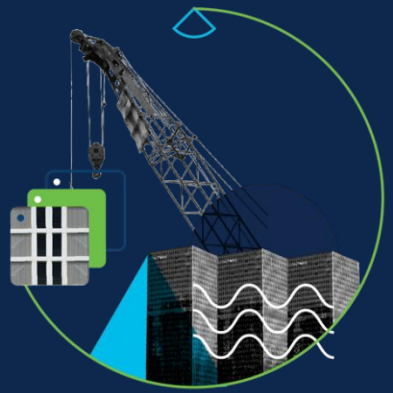
根據風險、上下文策略
和經過驗證的業務需求,
限制對應用程序的訪問。

Zero Trust for the Workloads

保護您應用程序中的所有連接。

- Complete Application Visibility / 完整的應用程序可視性
- Comprehensive Policy Enforcement / 全面的政策執行
- Contain Breaches / 遏止違規侵入存取行為
- Prevent Lateral Movement / 防止橫移行為

Workloads
How to verify trust



了解哪些應用正在運行以及包含哪些重要程序

遏止侵入行為並阻止橫移擴散

違反政策時發出警報或阻止通信

識別工作負載並執行策略

應用程序微分段
(Micro-Segmentation)

持續監控和反應威脅指標(IoC)

Zero Trust for Workplace

主要應用場景:
網路可視性與分段(Segmentation)

為所有用戶和設備(包括IoT)的網路訪問建立最低特權訪問(least privilege access)控制

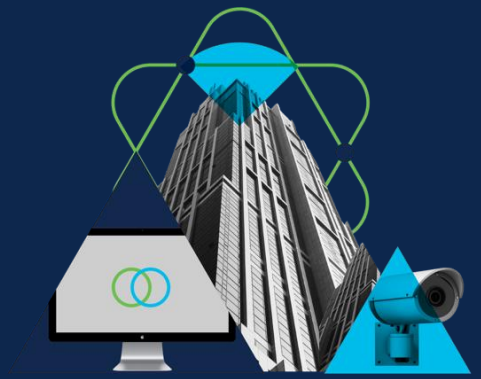
Zero Trust in the Workplace

- 獲得完整的網路可視性
- 防止未經授權的網路存取
- 防止惡意侵入行為

保護整個網路(包括IoT)上的所有用戶和設備連。

cisco SECURE

Workplace
How to verify trust



授予用戶和設備適當級別的網路訪問權限

對網路上的用戶、設備和應用
進行分類與分段

對受入侵的端點
撤消網路訪問權限並隔離

網路身份驗證和授權
(Authentication and Authorization)

網路分段
(Network Segmentation)

持續監控和威脅響應

Why Cisco Secure

持續的資安研究能量 – Talos與他愉快的夥伴們

>500M

每個月執行超過5億次身份與設備驗證

>100M

保護超過1億名IT用戶

100%

財星 100大客戶全數採用
Cisco Secure解決方案

>1B

保護超過10億個端末設備

>20B

每日偵測與阻擋200億個惡意攻擊

歷久彌新的Cisco Secure – 千年傳統、全新感受

資安基礎建設的起點

開始獲取新技術並快速創新

網路與安全的整合

最全面的網路安全整合平台誕生

2007 | 2009 | 2011 | 2013 | 2015 | 2017 | 2019 | 2021

- 2007: Network Segmentation; Email Security; Web Security Gateway
- 2009: Cloud Web Security Gateway
- 2011: Network Access Control
- 2013: Unified Threat Management; Malware Analysis; Endpoint Detection and Response; NGIPS; DC Networking
- 2015: Enterprise Firewall; Security Services VPN; Cloud Security; Traffic Analytics; Workload Protection
- 2017: CASB; Network Security Policy; SD-WAN; SD-Access; Application Performance Management; Cloud Analytics
- 2019: Access Manager; Threat Response
- 2021: SECURE X; Cloud Email Security Supplements

Over $6B in M&A
over the past 6 years

Over 400
threat researchers

Unparalleled
platform breadth

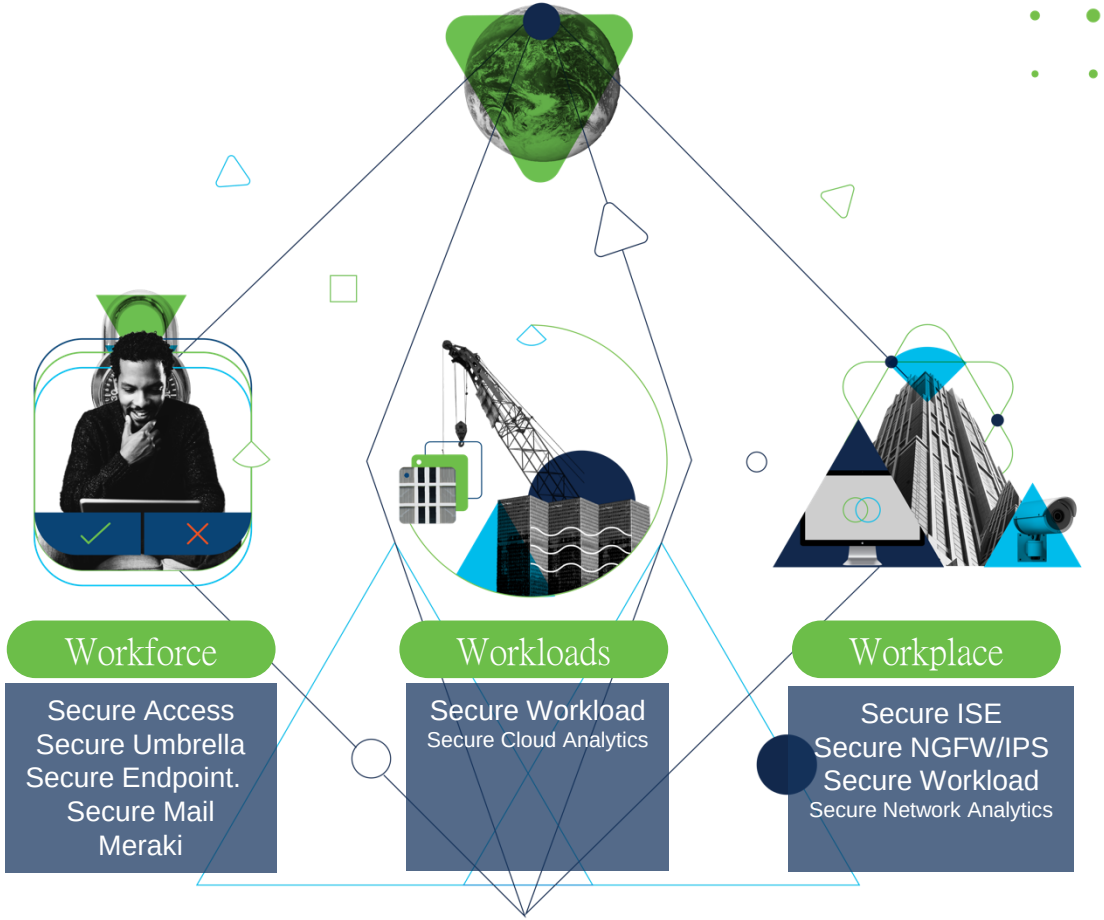
改變資安維運生態：Cisco SecureX

- 無額外使用授權
- 整合思科安全所有方案
- 跨平台可視性
- 全面自動化
- 強化零信任佈建的維運

思科的零信任之旅

A comprehensive approach to securing all access across your networks, applications, and environment.

“一種全面的方法，可確保跨網絡，應用程序和不同平台環境的所有訪問”



THANK YOU

CISCO SECURE