



# 企業上雲安全具體實踐與 風險感知回應

Kyle Feng | Security Consultant

YOU DESERVE THE BEST SECURITY

#1 範例  
雲端化 + 雲端安全



#2 範例  
傳統網路移轉至 SASE



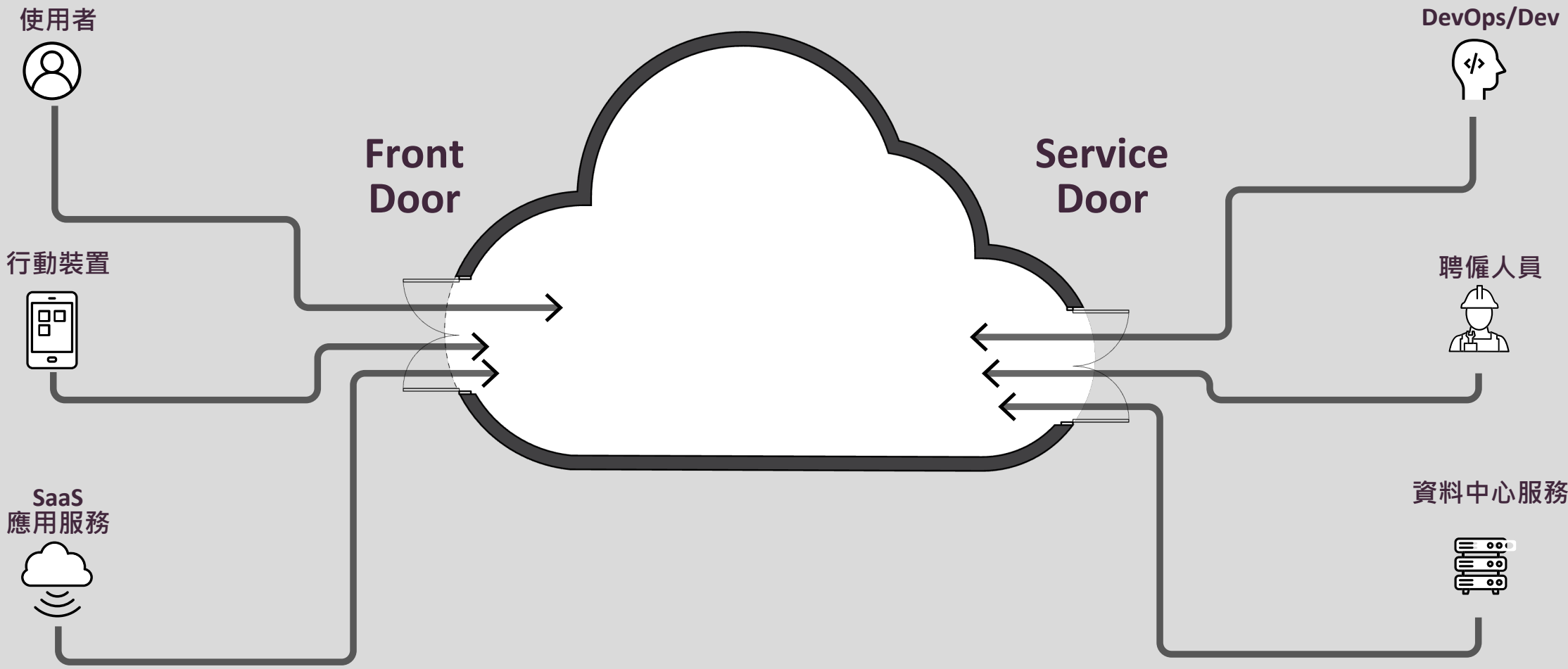
#3 範例  
地端郵件上雲



## 數位轉型雲化應用安全範例

# 數位轉型雲化應用範例 #1

## 雲端化 + 雲端安全



## 對外服務網路

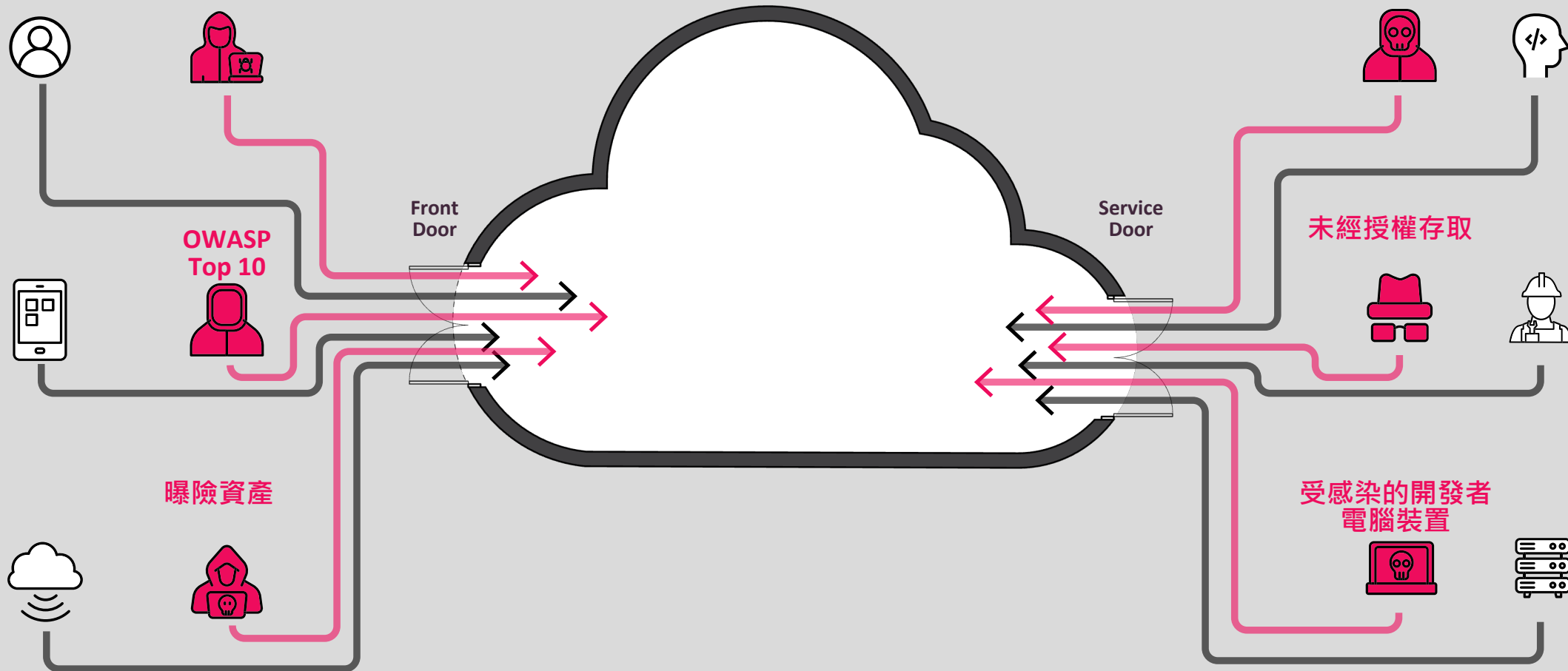
使用者存取  
Web應用程式與API服務

## 企業內部網路

內部團隊和承包商  
維護和更新雲端工作負載

SQL Injection

遺失的帳密憑證



OWASP Top 10

曝險資產

未經授權存取

受感染的開發者  
電腦裝置

攻擊者突破門戶  
(Front Door)

透由內部來源滲透  
(Service Door)



曝露金鑰



過高權限帳號



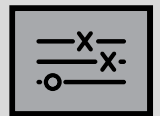
敏感資訊



漏洞

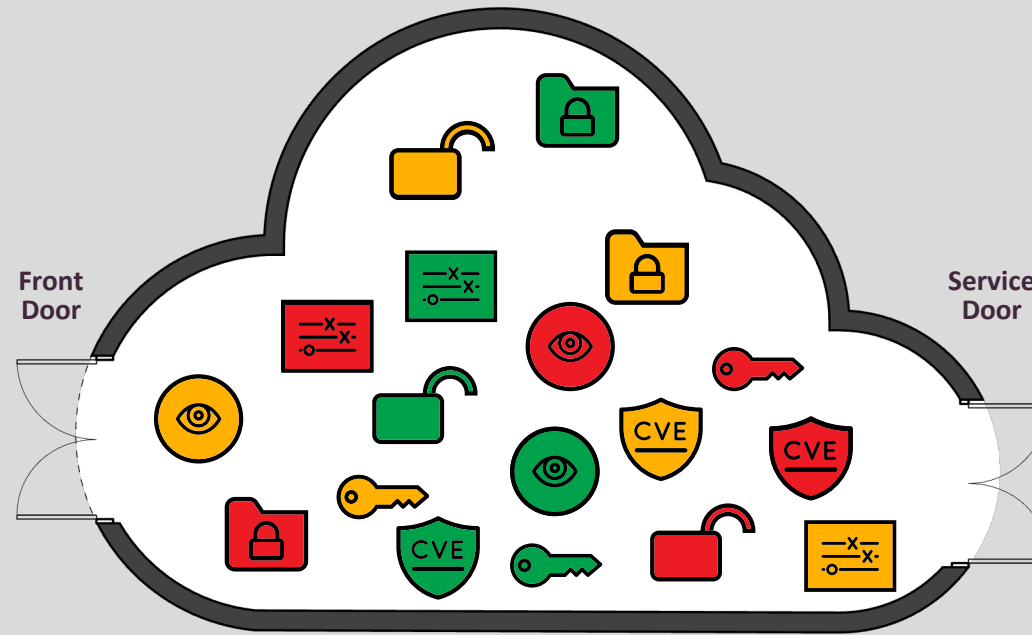


曝險資產

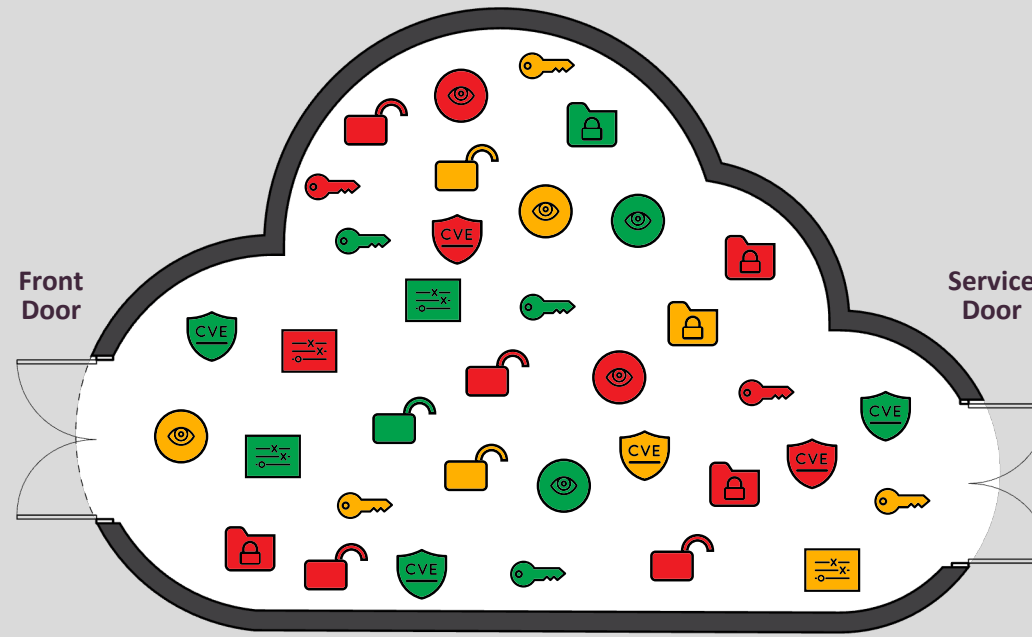


人為不當配置

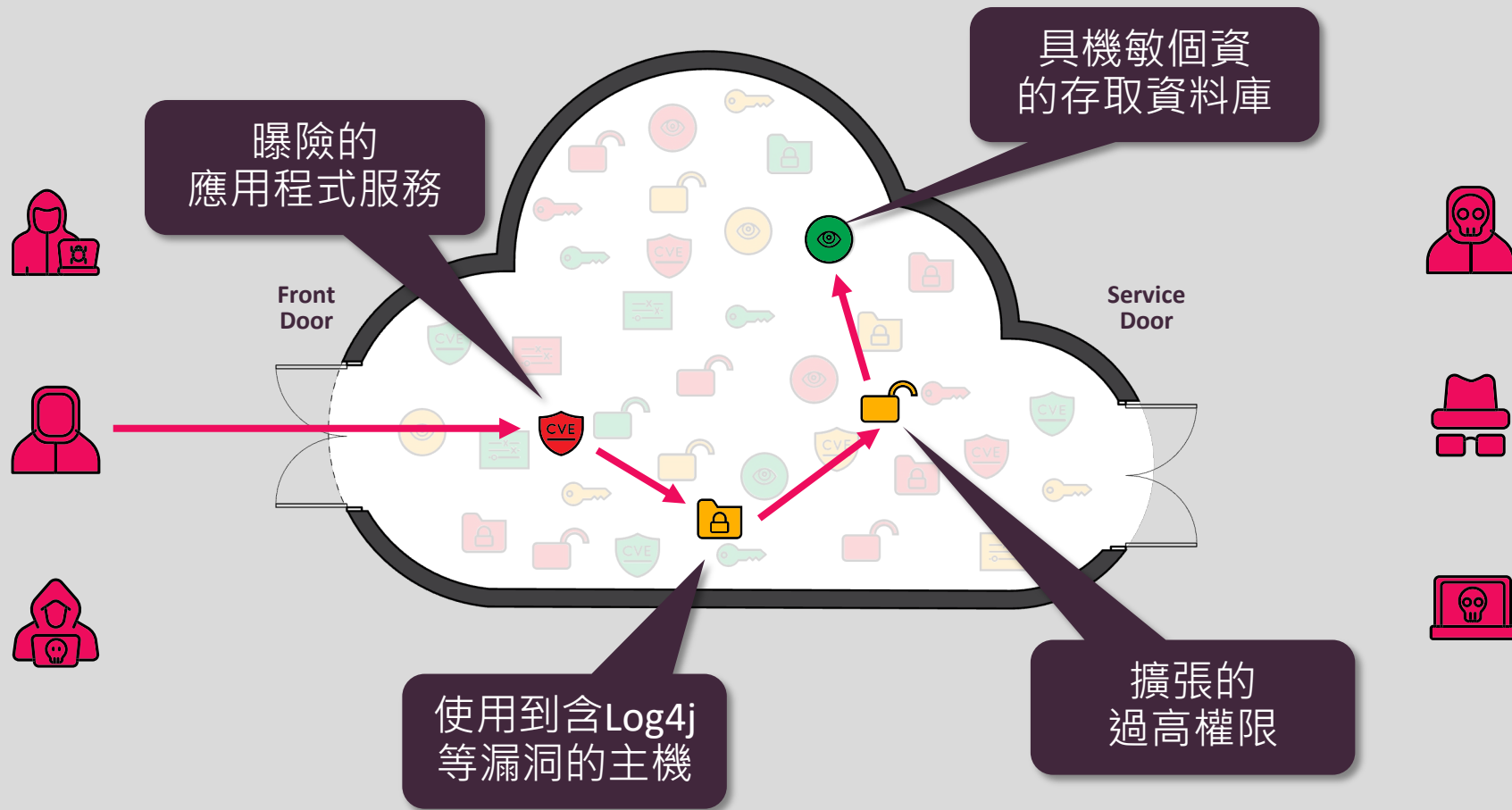
# 雲端服務具備 多重資安風險



您的雲端資產中  
存在數以千計的安全風險



即便您已處理了多數問題  
其他風險仍會與日俱增



## 一旦攻擊者進到雲端服務中 安全風險難料

停止無止境地  
追逐安全風險



具體實踐  
雲端資安  
典範轉移

每天的待處理安全問題

未知(Unknown)的可能重大風險

安全修復的過程過於緩慢

資安人員對於越發敏捷的DevOps失去掌控



強化安全防護 +PREVENTION  
於您的雲端資安!

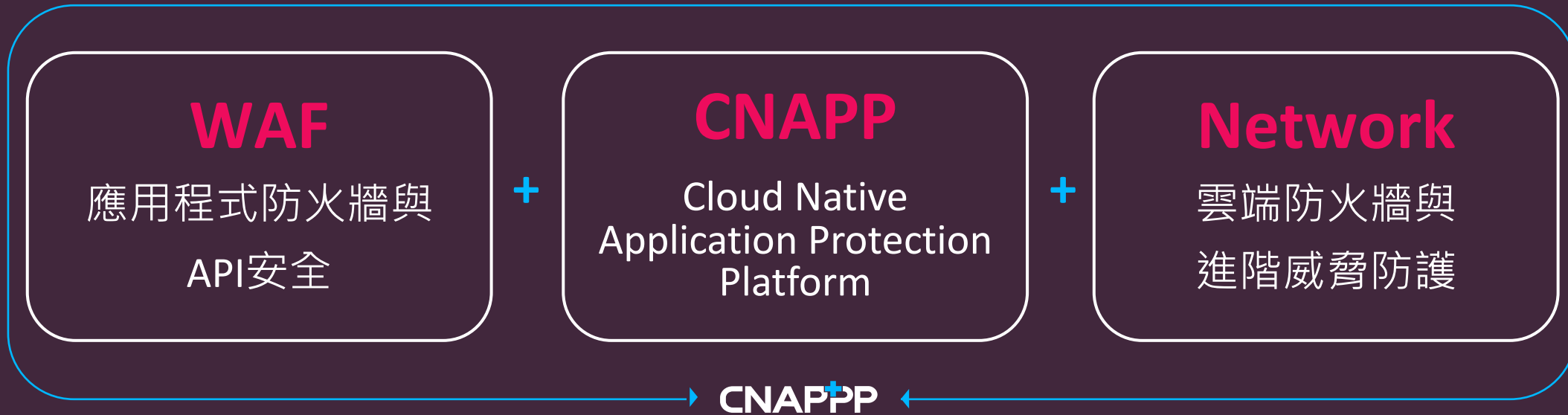


CNAPP+

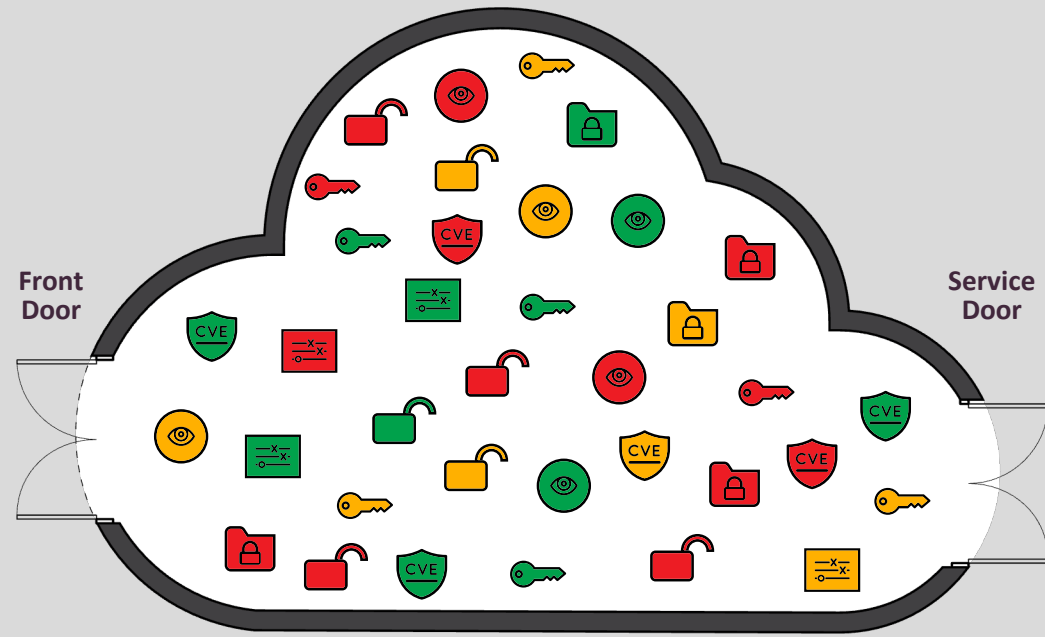
Cloud Native Application Protection & Prevention Platform

# 業界唯一具備Prevention即時防護能力平台

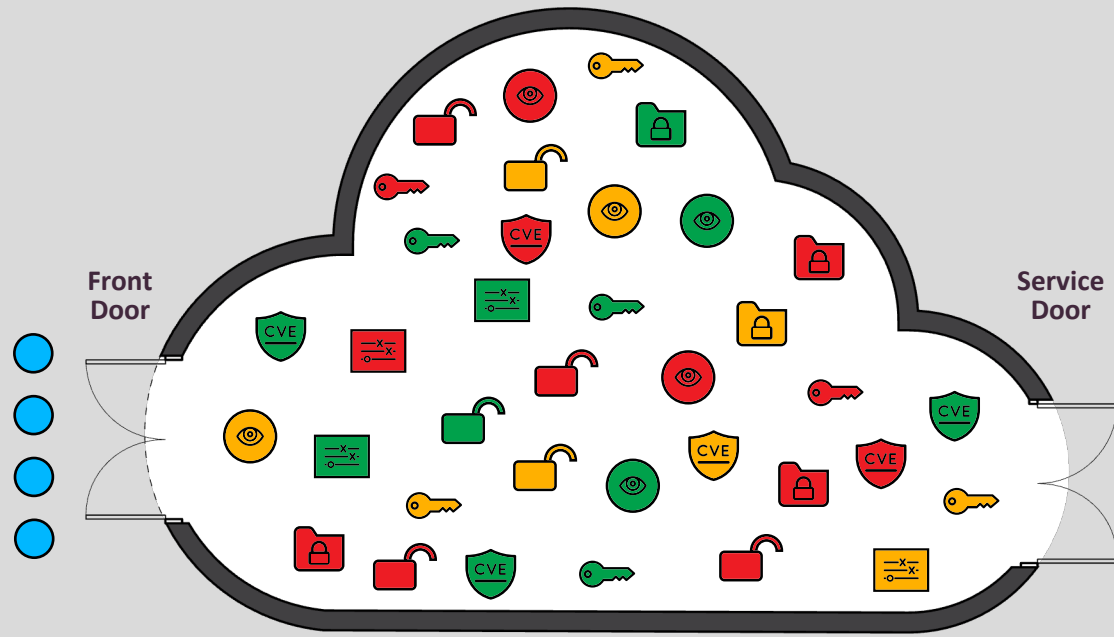
CNAPPP



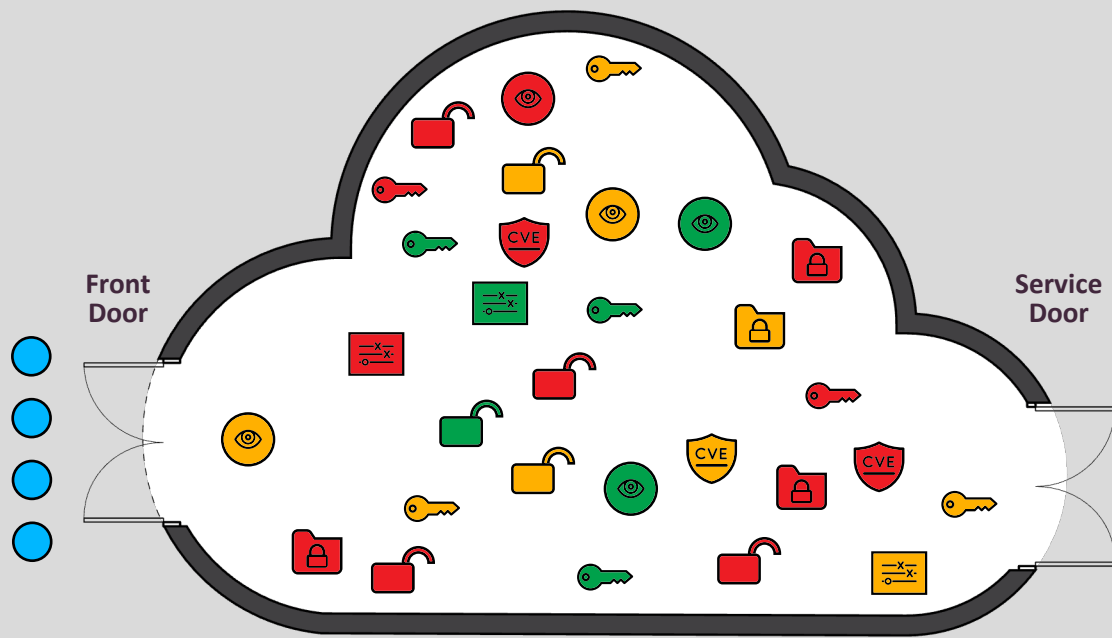
## 全域掌握雲端安全與曝險管理!



回到剛剛強調的安全風險與情境...



# #1 強化 WAF 保護 自Front Door存取Web應用程式與APIs



攻擊情境

- 零時差攻擊防護
- 防護特徵碼
- 準確度
- API 保護
- 支援多雲環境



CloudGuard WAF

- ✓ 立即防護
- ✓ AI為主
- ✓ 最高評級 97%
- ✓ Yes
- ✓ Yes



Cloud Native WAF

- ✗ 平均達40以上\*
- ✗ 以靜態特徵為主
- ✗ 87%\*
- ✗ 未提供
- ✗ 單一雲平台

# 基於AI機器學習的新世代WAF防護

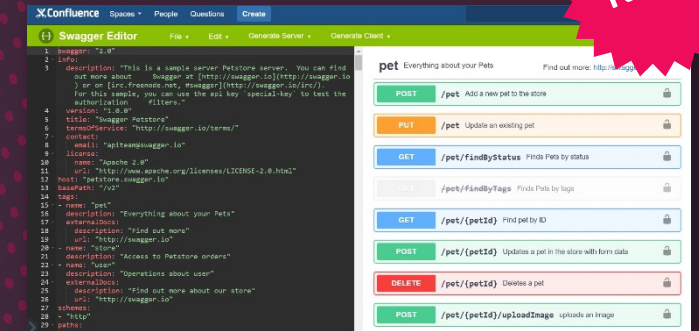
## WAF Plugins



## WAF as a Service

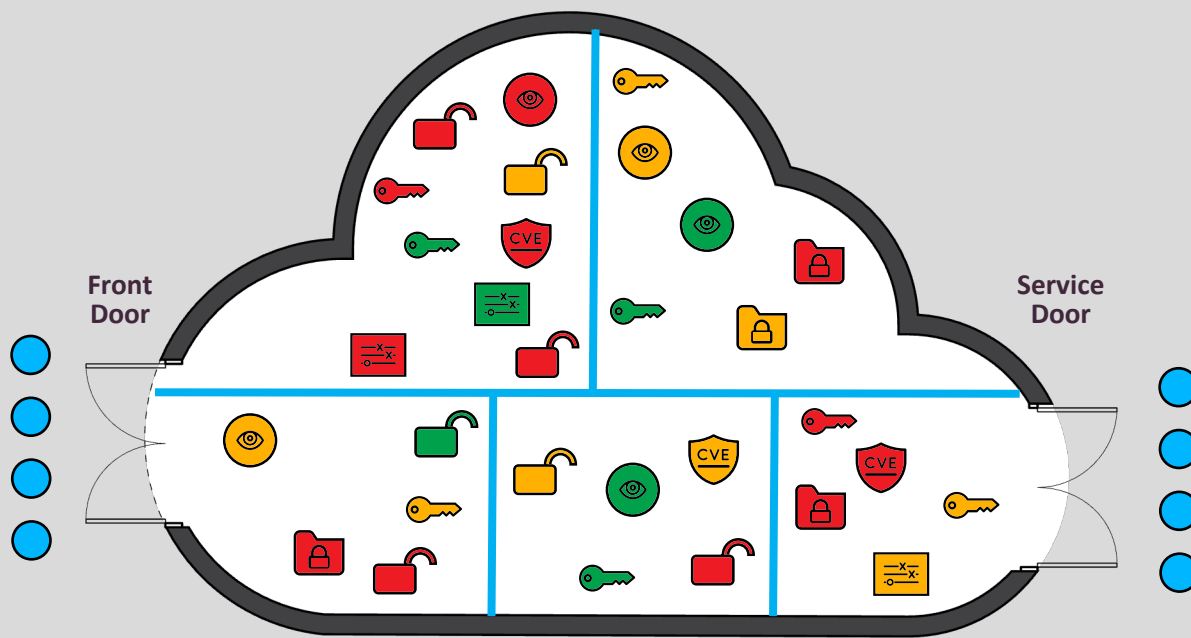


## API Discovery

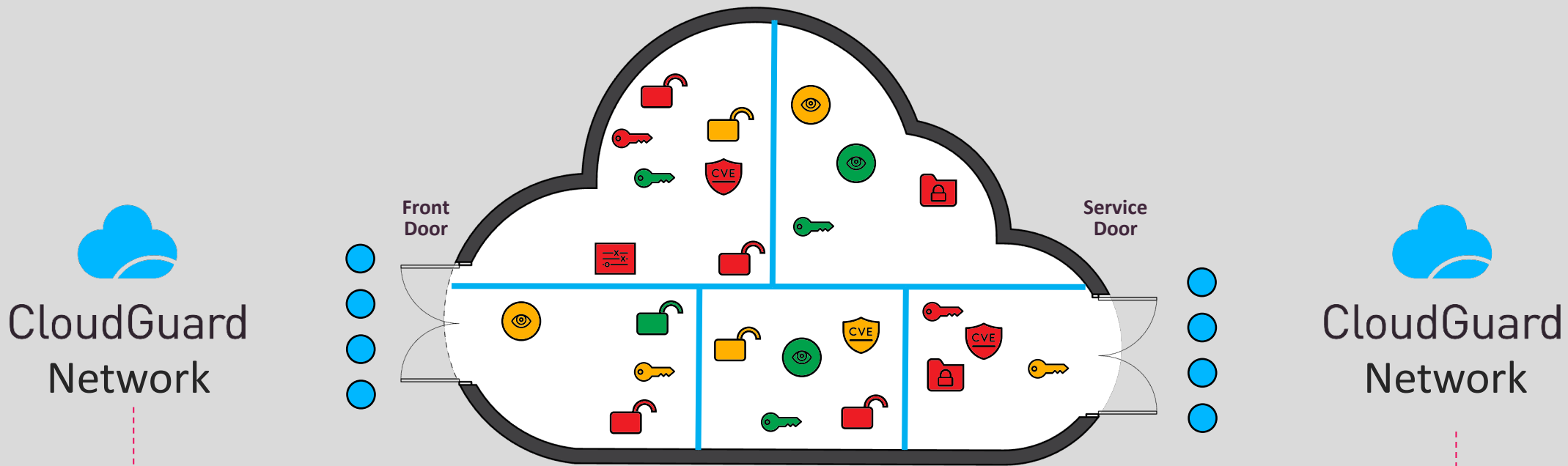


自動模式建置和實施

# CloudGuard WAF: 更具靈活性的部署與支援模式



## #2 強化進階網路安全保障安全存取 雲端Front Door/Service Door 以及雲端微分段服務



使用情境	<b>CloudGuard Network Security</b>	<b>Cloud Native FW</b>
威脅防護	✓ 業界最佳網路防火牆	✗ 僅有IPS為主
混合雲支援	✓ Yes	✗ 無地端支援
多雲支援	✓ Yes	✗ 單一雲平台
ROI	✓ High 169%	✗ Low <40%

# Gartner 評為最佳雲端情境-網路安全防火牆

# CloudGuard Network Security for 雲原生WAN服務



整合於Azure  
Virtual WAN



整合於AWS  
CloudWAN



整合於GCP  
Packet Inspect

**CloudGuard Network: 更貼近雲原生的部署與安全設計**



CloudGuard  
CNAPP



#3 採用 **CNAPP** 整合安全防護  
針對雲端風險進行即時補救與緩解

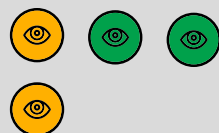
CNAPP+



工作負載保護



偵測與回應



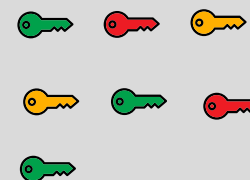
態勢感知



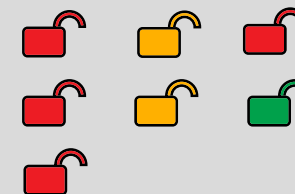
資料感知



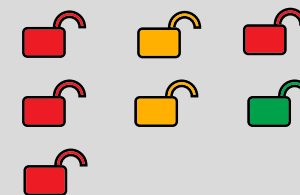
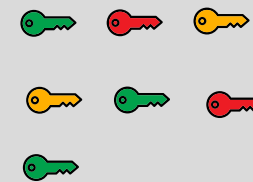
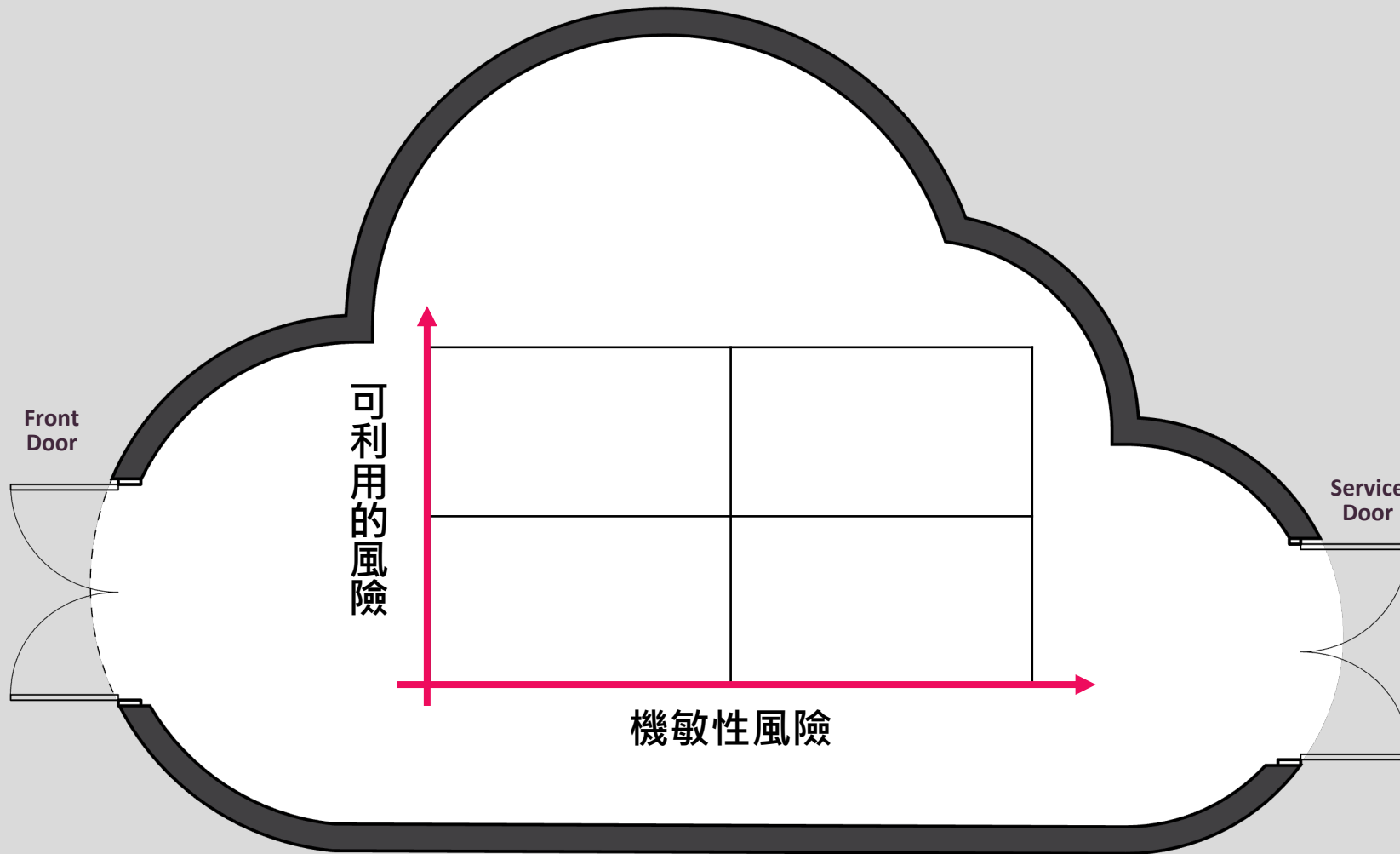
身份管理



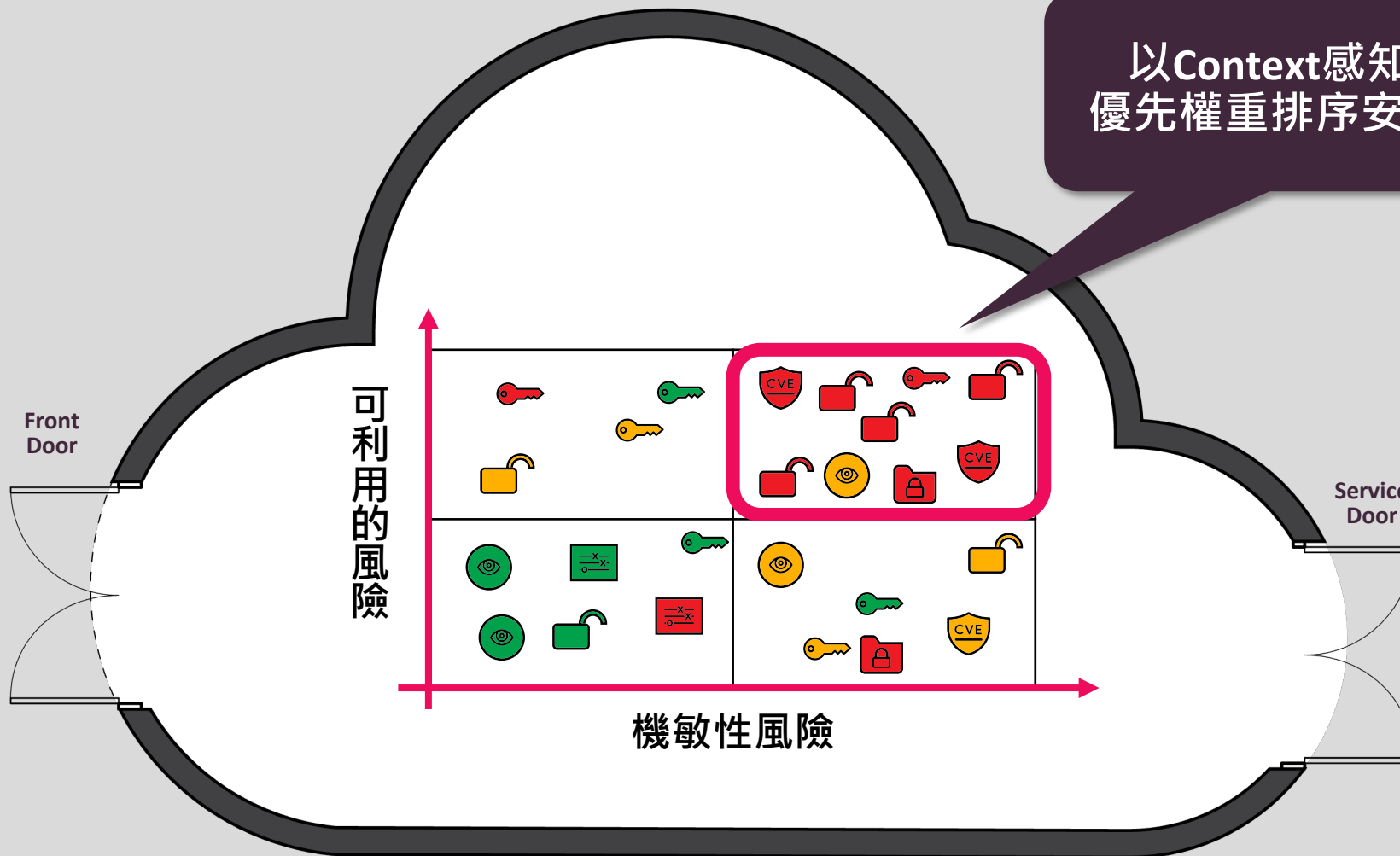
源碼安全

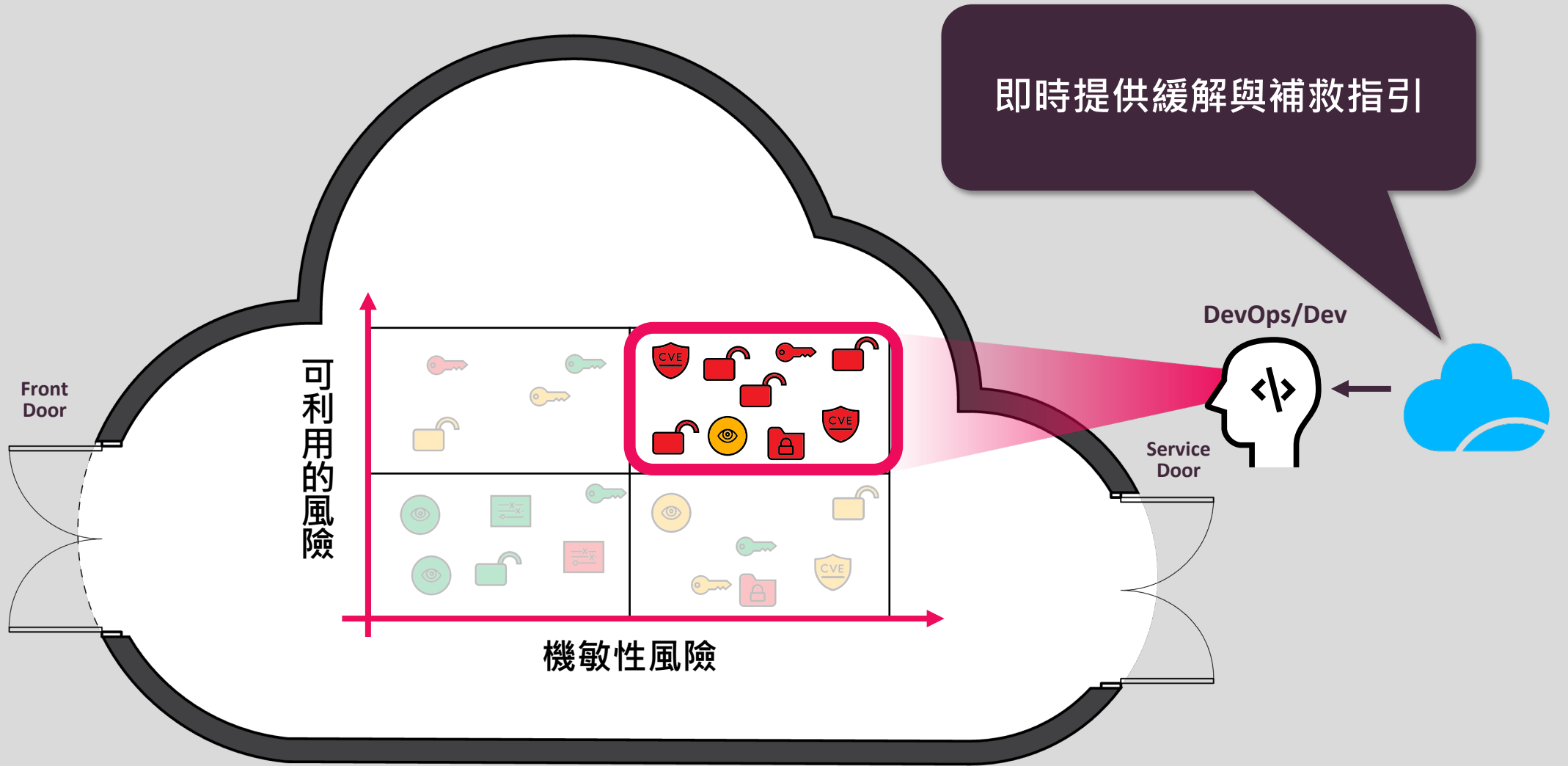


由多重安全模組支援完整的雲端風險分級



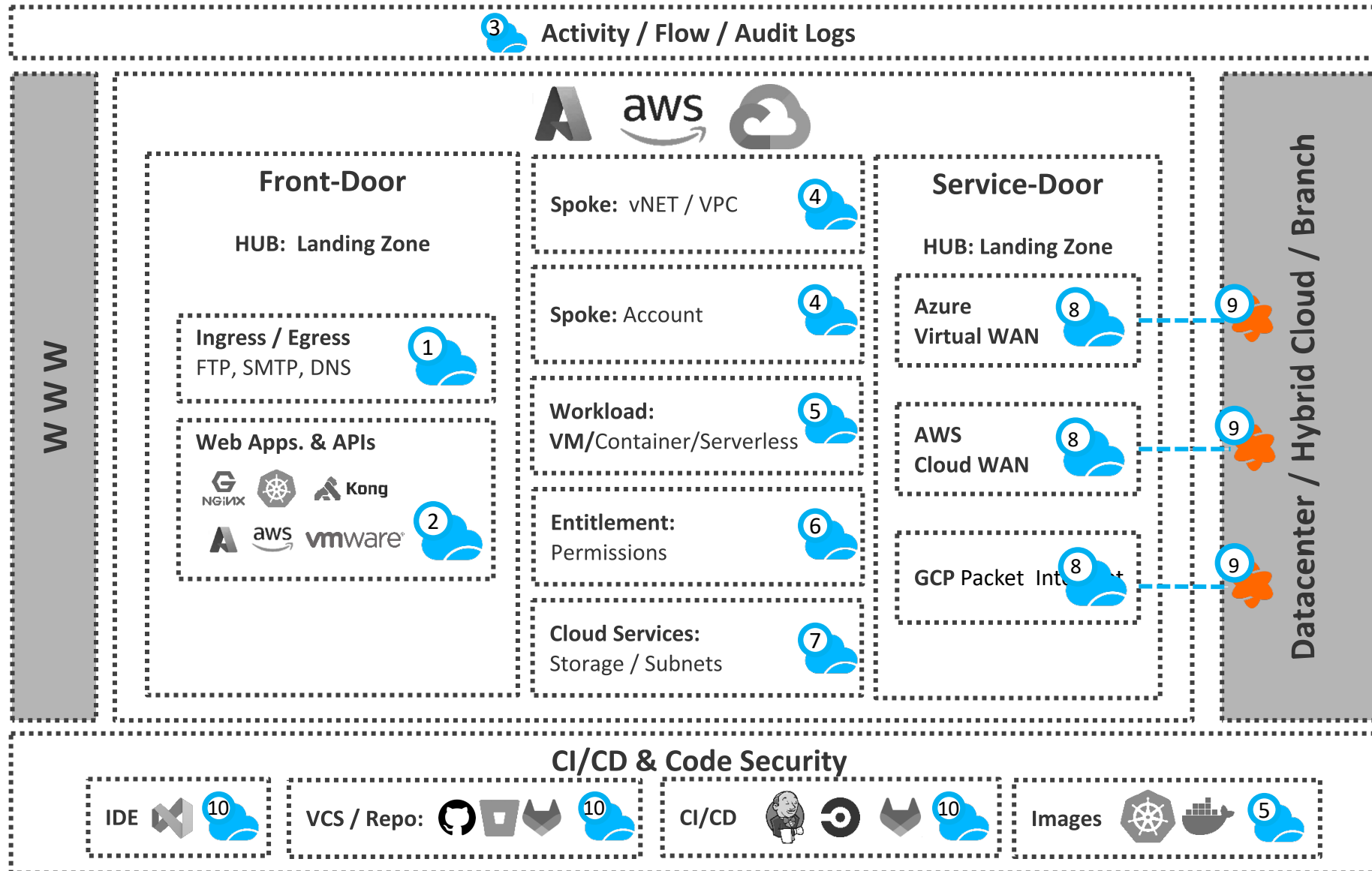
以Context感知分析  
優先權重排序安全問題





## 緊密整合於開發流程 Dev & DevOps

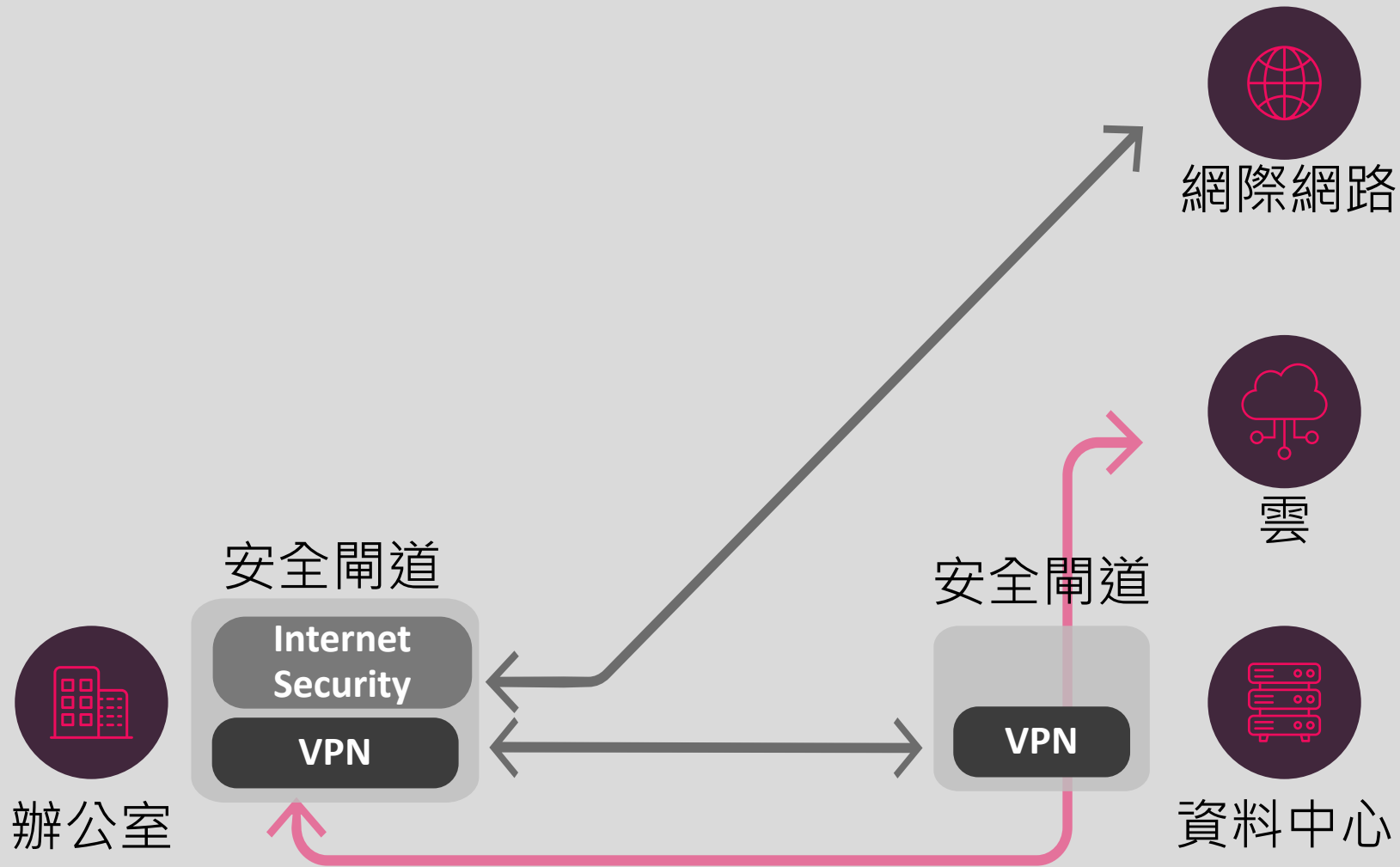
# Check Point CloudGuard 雲安全藍圖



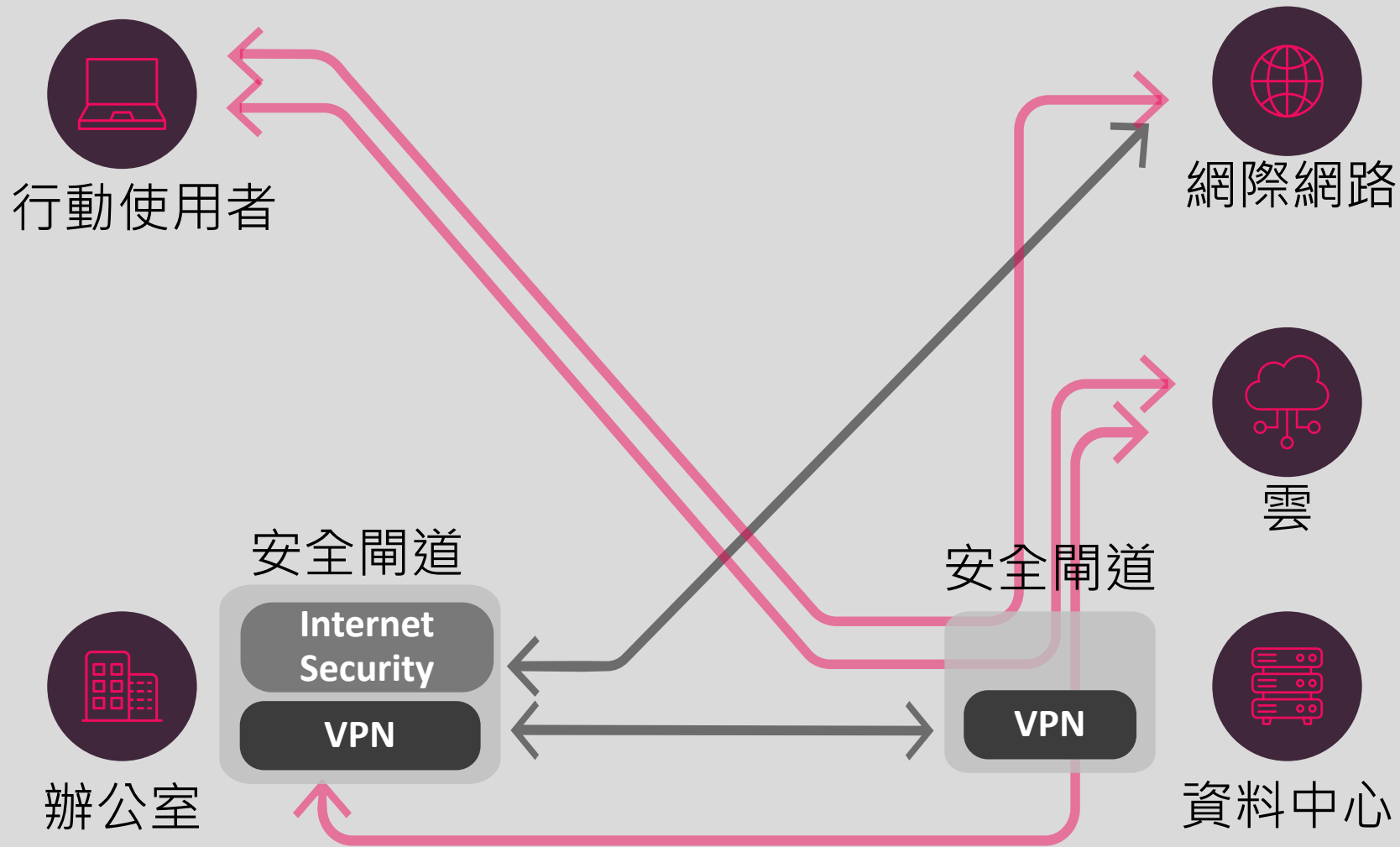
- CloudGuard**
- 1 防火牆、IPS, 防資料外洩
  - 2 WAF & API: Plug-in / SaaS
  - 3 雲端偵測回應 (CDR)
  - 4 Hub & Spoke 區段化隔離
  - 5 工作負載安全
  - 6 Entitlement Security (CIEM)
  - 7 雲端態勢管理
  - 8 Cloud WAN with NGFW
  - 9 Hybrid Cloud VPN
  - 10 源碼安全

# 數位轉型雲化應用範例 #2

## 混合式網路存取SASE



## 早期架構: 使用者與應用程式於地端資料中心



## 近年發展: 遠距存取與資料中心

行

## Covid/數位轉型後開始變化...



使用者體驗  
欠佳



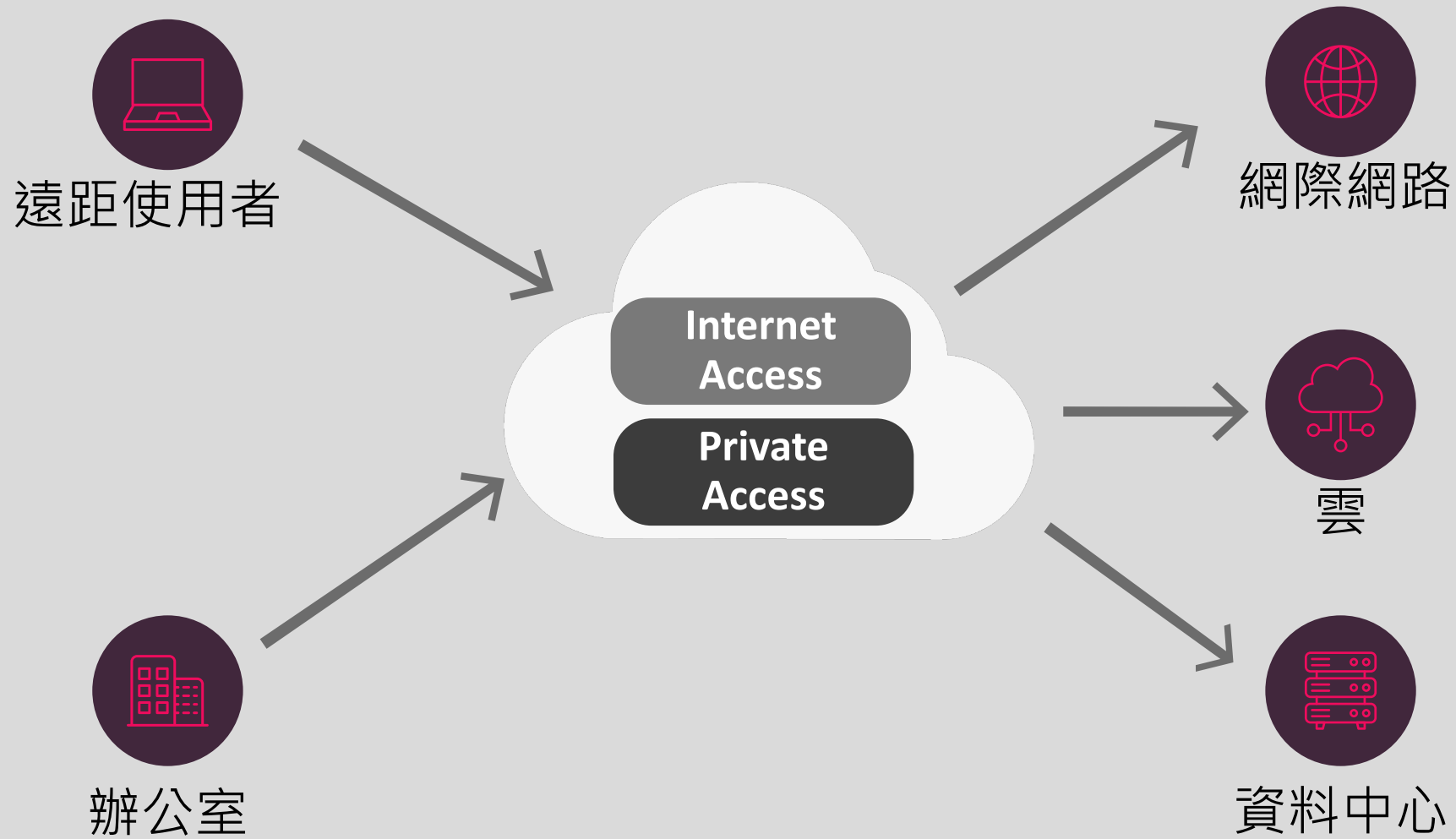
擴充不易



敏捷性差



## 近年發展: 遠距存取與資料中心



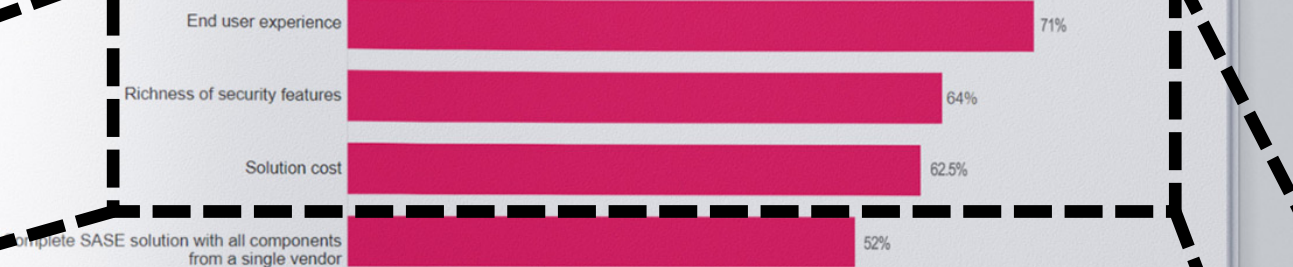
## 現今: IT網路的遷移-Cloud SASE

# 客戶SASE需求:

使用者體驗  
強大安全保護  
成本考量

What are your top considerations when selecting a SASE solution? Choose all that apply.

641 Responses



# Introducing



# Harmony SASE

## HYBRID-SASE

最佳使用者體驗  
最理想的網路安全





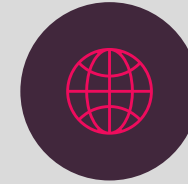
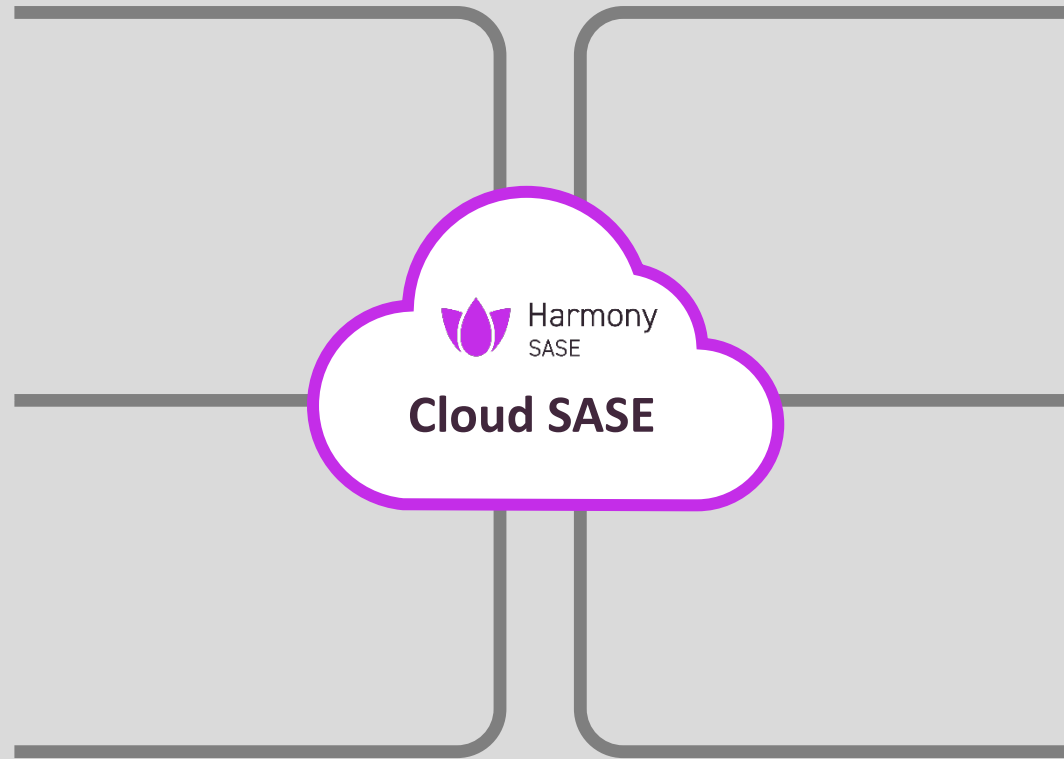
公發裝置



BYOD



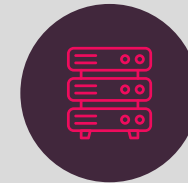
辦公室



Web

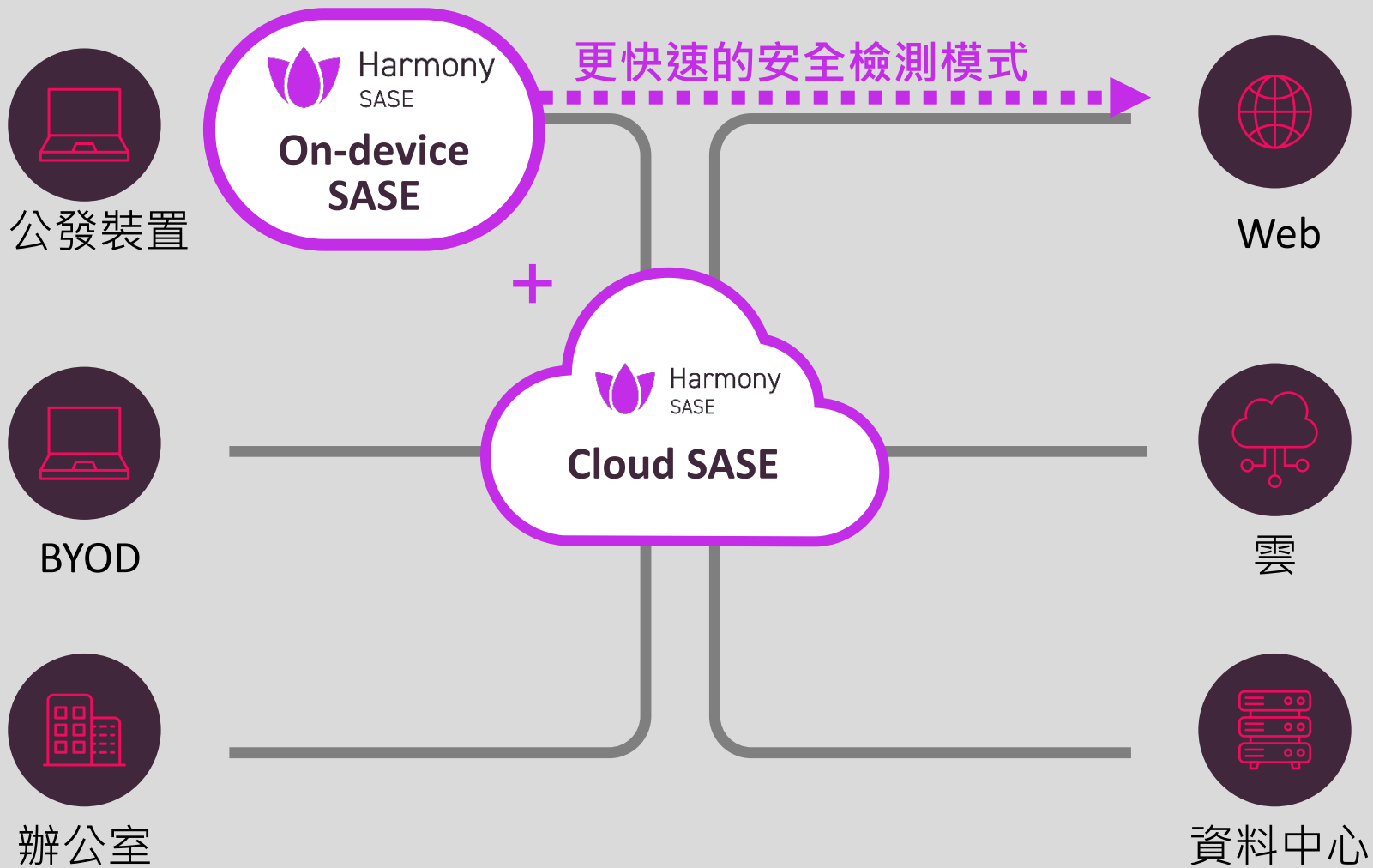


雲

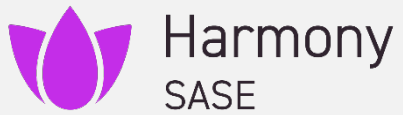


資料中心

# 基於雲服務的SASE



## 最佳典範轉移: Hybrid SASE



# The Power of Hybrid SASE



其他供應商

傳輸效能

220 Mbps

125 Mbps

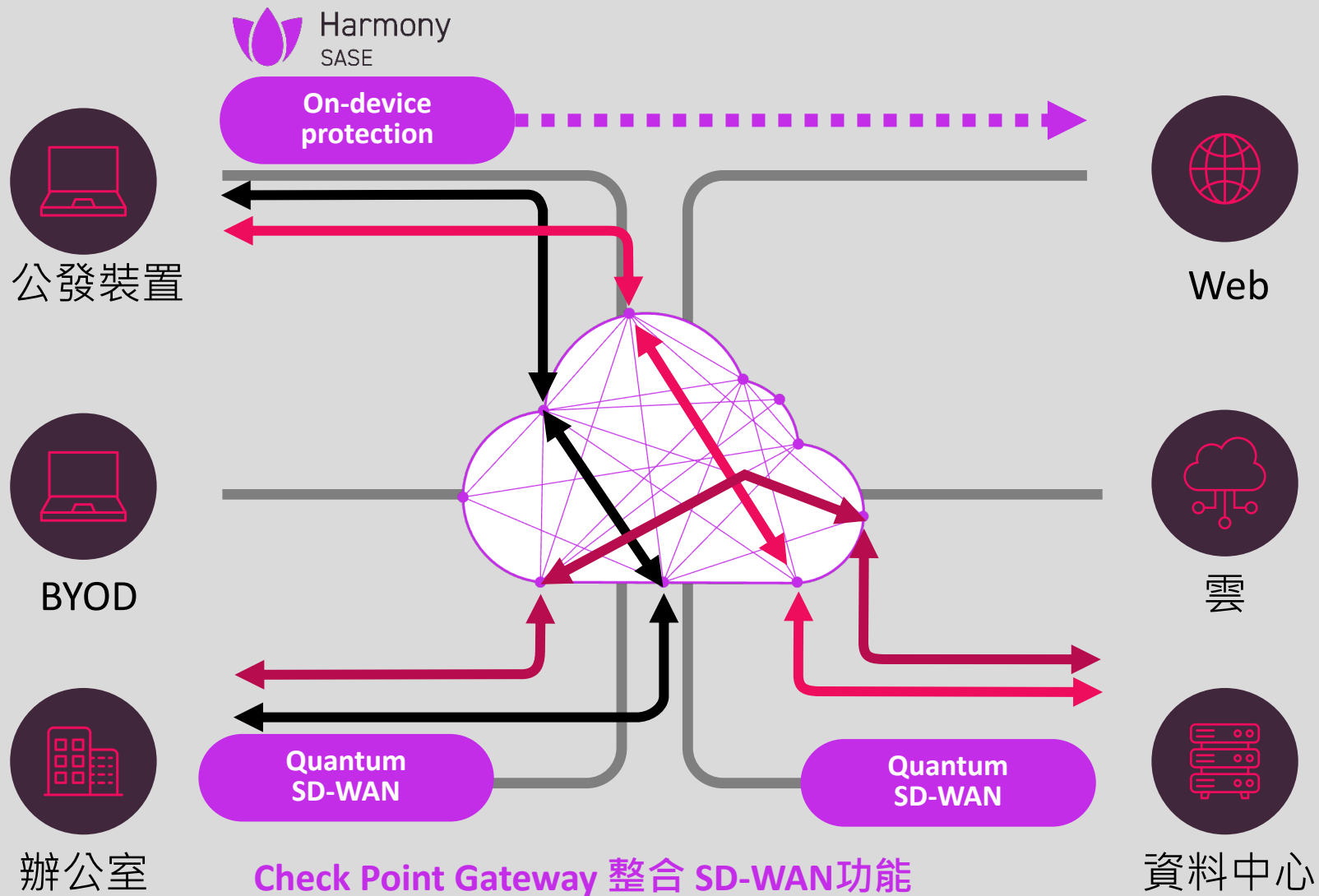
網路延遲

123 ms

165 ms

Hybrid SASE

傳統  
cloud-only SASE



# Hybrid SASE結合 Full Mesh & SD-WAN優化連線能力



## Internet Access: On-device & Cloud



Harmony  
SASE (Internet Access)

URL Filtering

DNS Filtering

Malware Protection

SSL Inspection

Threat extraction

Anti-bot

Zero Phishing

Browser security



## Private Access:



Harmony  
SASE (Private Access)

Zero Trust Security

Full-mesh connectivity

Device Posture Check

Firewall as a Service

Dedicated static IPs

# Harmony SASE

## 全方位安全保護



Harmony  
SASE

# Harmony SASE – 改變IT生態的Hybrid SASE



其他供應商

Internet Access ✓ 2倍快速存取的網路安全

✗ 仰賴雲端的多節點存取延遲

Private Access ✓ Full mesh-任何方向性連結

✗ 使用者端的單向連結

部署與管理

- ✓ 單一SASE與SD-WAN整合方案
- ✓ 單一控管介面- Infinity portal\*
- ✓ 1-hour 快速部署

- ✗ 多重供應商 SASE方案
- ✗ 多重管理介面
- ✗ 數週以上的部署時間

實際效益

- ✓ 更具效率與網路效能

✗ 更高昂的網路存取成本

安全防護

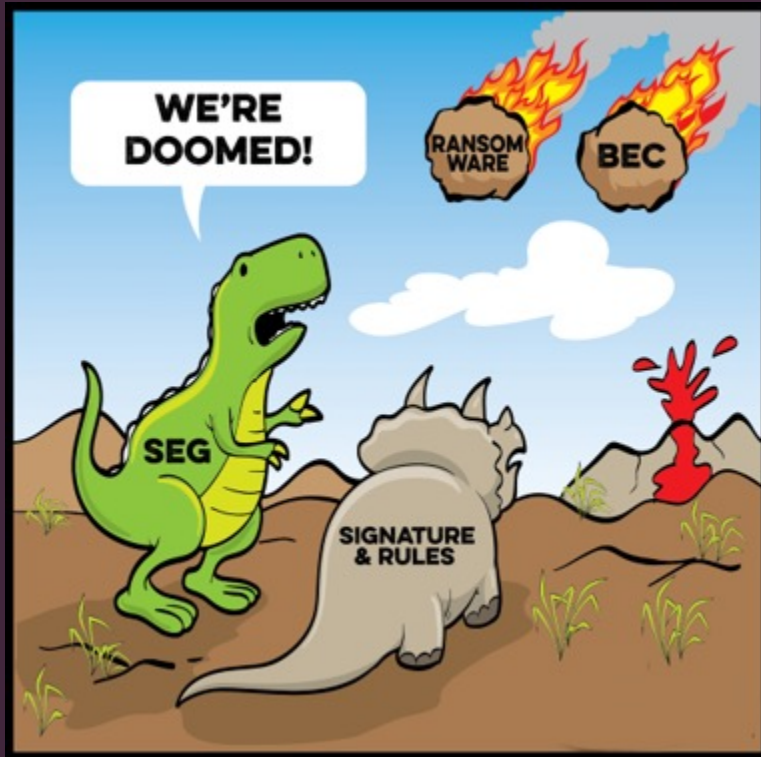
- ✓ 99.8% Threat Prevention

✗ 仰賴第三方安全措施整合

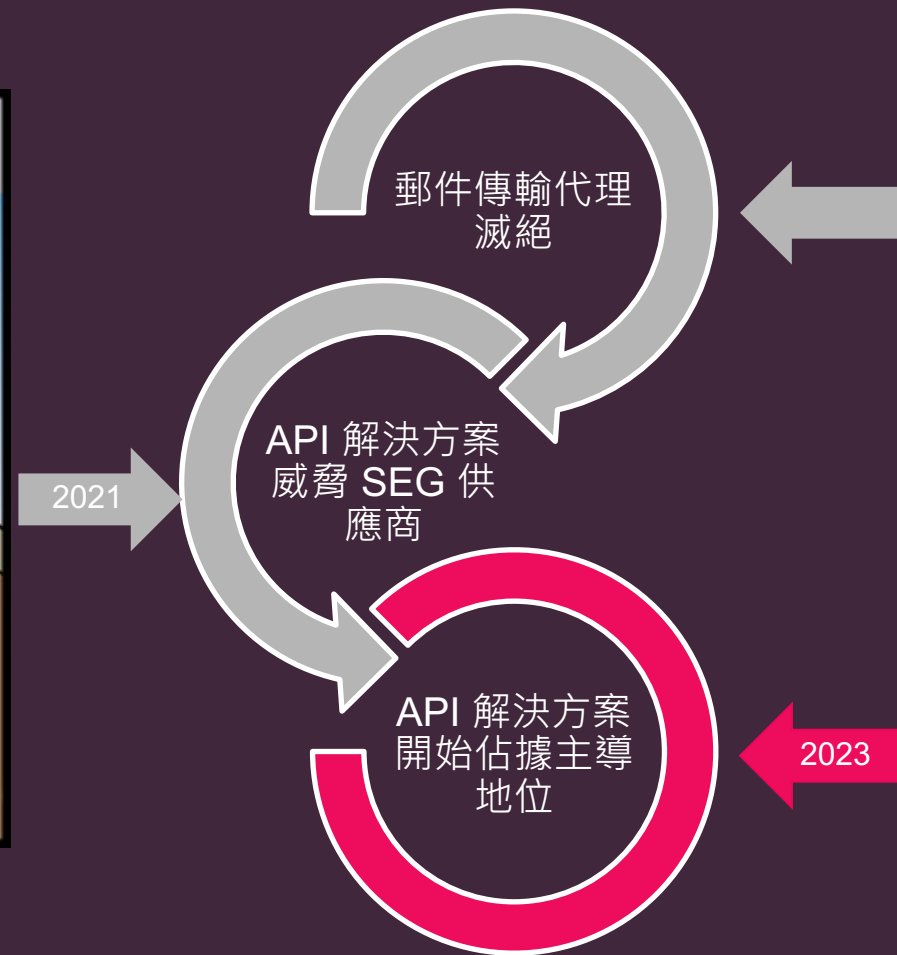
# 數位轉型雲化應用範例 #3

## 雲端郵件與協作應用防護

# 電子郵件安全革命



“Forrester 對電子郵件安全市場的 2021 年 Wave 評估顯示，安全電子郵件網關（SEG）正在慢慢變成恐龍.....”



- Microsoft 不鼓勵客戶在 365 面前使用 MTA
- RFI/RFP 特別指出 – “沒有 MX 記錄更改”。

API 解決方案佔據主導地位

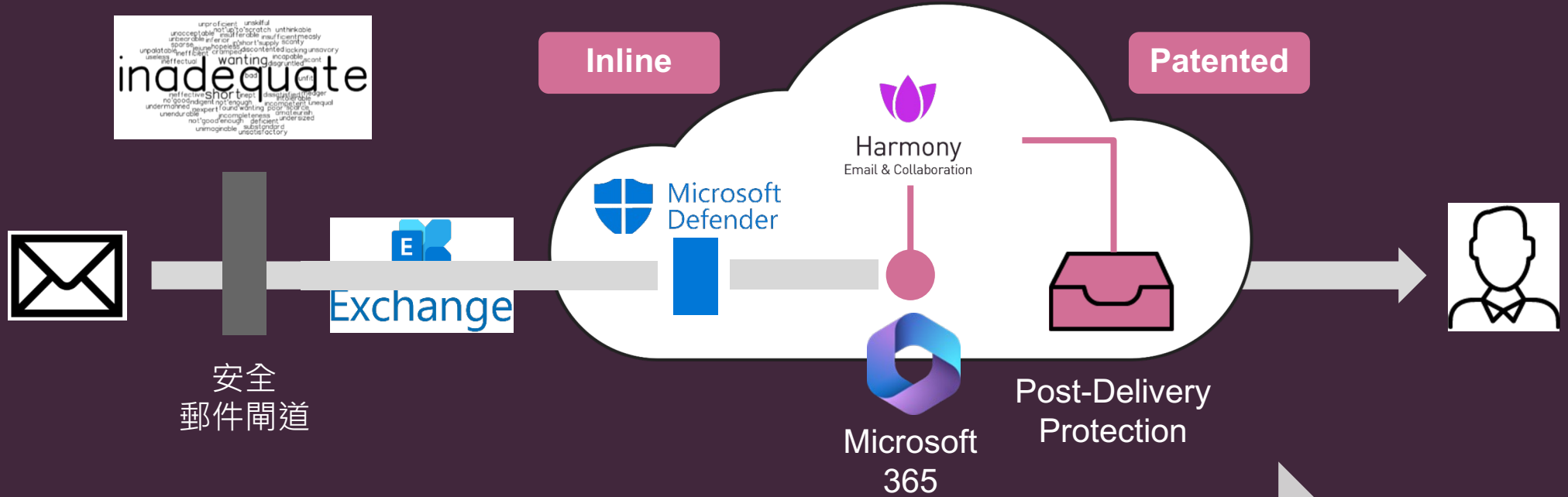
- Check Point 在所有通信方式中防止詐騙
- SaaS、行動裝置、瀏覽器



Harmony  
Email & Collaboration

# How Harmony Email and Collaboration Works

# The Revolution of Email Security

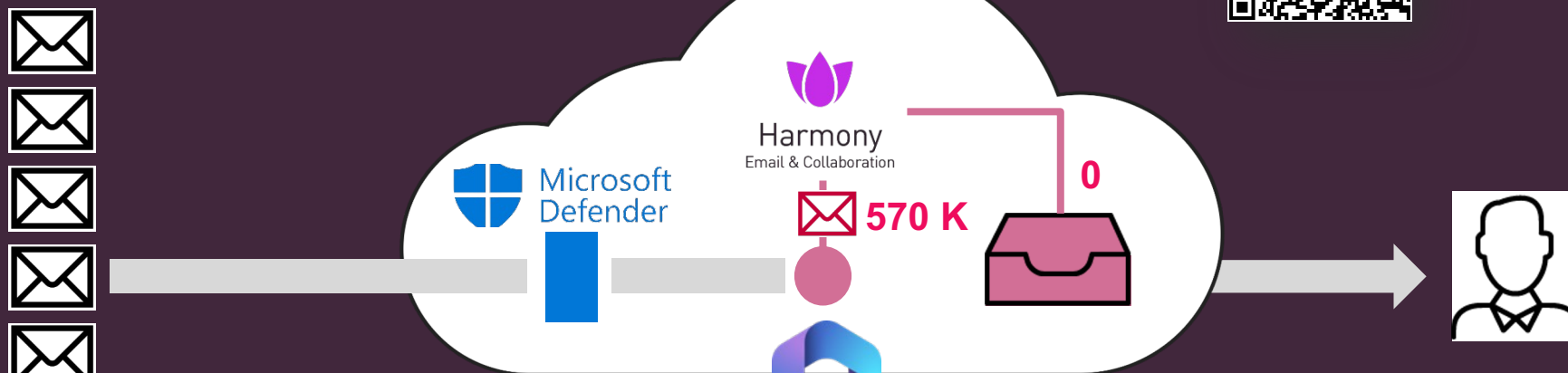


- 電子郵件遷移到雲端
- SEG 不敷使用
- API 解決方案湧現
- HEC首創Inline prevention

# HEC in Action



[Download the Full Report](#)



~19%

Defender 遺漏的惡意  
電子郵件

100%

HEC捕獲遺漏的惡意  
電子郵件

**3M**  
電子郵件  
分析

Customers with >10K Seats  
Using Defender and HEC

# BEC 商務電子郵件詐騙

## 利用人工智慧和進階安全性

寄件者姓名包含  
品牌相關文字

網路釣魚常用的主題語  
言

傳送給  
VIP收件人

低流量網站

內文語言、簽章和風格

+300 多個電子郵件  
AI分析指標

從： 喬許·克萊爾 [mailto:josh365.clair@chu-miens365.fr]  
到： 羅伯特霍夫米爾  
抄送：  
主題： 電子郵件安全團隊！

寄件者姓名包含  
品牌相關文字

傳送給  
VIP收件人

Your Microsoft Outlook Web Account has recently been subjected to security modification as of 2020年12月18日。  
The action requested is as follows: This automated email contains a link to reset and maintain your Outlook Web App password as your current password has expired.

Please [Click Here](#) to go to the Reset Password page. Follow the instructions below to create a new password.

The link above expires after 24 Hours. If you don't change your password before then, your Outlook Web App account locked for security reasons.

Thank you,  
Maintenance and Operations.

Source: Email Security Team.

可疑的文字敘述

# 自動阻止受損帳戶



## 使用者操作

從辦公室登入 (工作時間)

在家登入 (非工作時間)

發送電子郵件 (工作時間)

國外登入 (出差)

偶爾重置密碼

從新國家/地區登入 (公司範圍內)

在非常規時間登入

高郵件發送率

可疑郵箱規則

不可能的旅行

多次密碼重置

首次  
瀏覽器/裝置/VPN

結論：  
**受感染**

THREATCLOUD AI

行為基準 (每個使用者)

可能的可疑活動

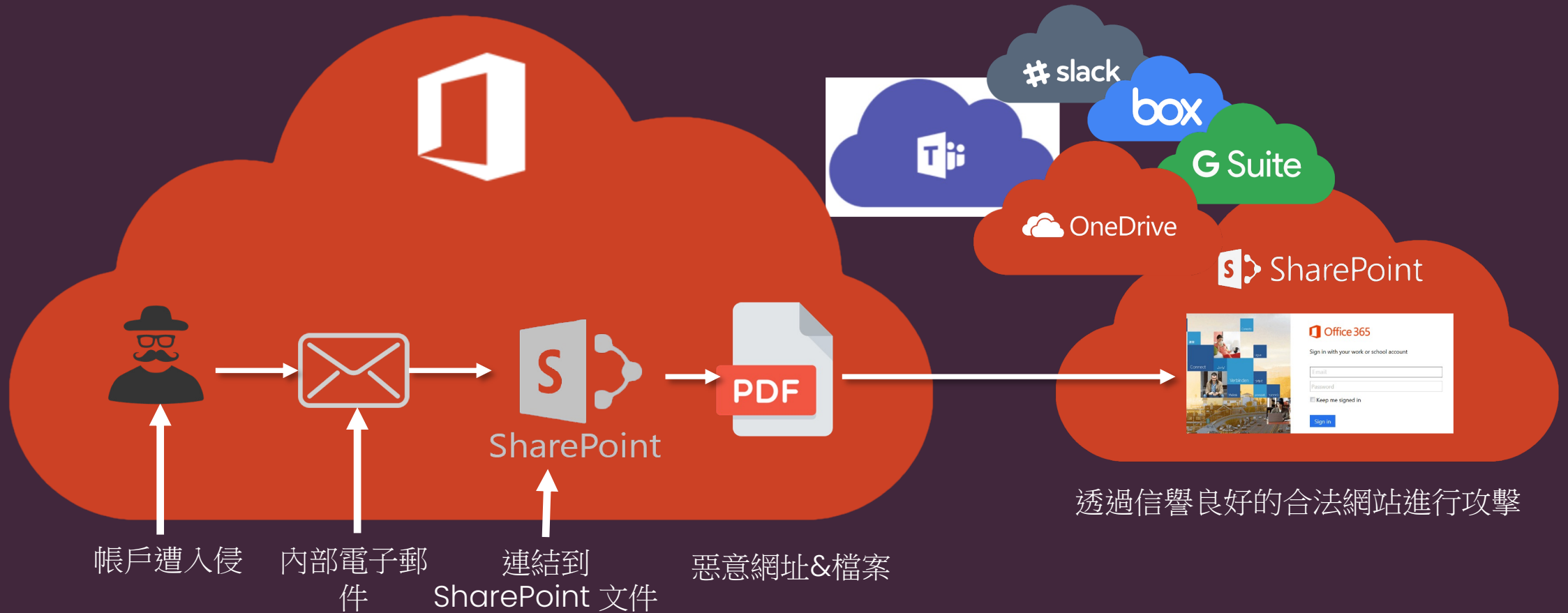
# 合作夥伴風險評估

了解您的供應商並透過機器學習檢測受影響範圍

Risk Score	Partner Domain	Communication Volume	Internal Contacts	Partner Contacts	Risk Indicators	Last Risk Date
	Partner1 partner01name.com	High	Jeff Bloom, Chief Buyer Rony Rodrigue, CFO +5 more	vendorname@domain.com RonyRodrigue@domain.com +5 more	You received phishing email from this partner	12:22 AM 2019-08-14
	Partner2 partner01verylongname.com	Medium	Jeff Bloomshtein-Ron, Chief Buyer Rony Rodrigue, CFO +5 more	Jeff Bloomshtein-Ron@domain.com Rony Rodrigue@domain.com +5 more	1 Partner users sending phishing emails 4 Attempts to impersonate partners	12:22 AM 2019-08-14
	Partner3 partner01name.com	Low	Jeff Bloom, Head of Cloud Security Arch... Alexander Rodrigue, CFO	Jeff Bloom@domain.com Alexander_rodrigue@domain.com	2 Attempts to impersonate partners	12:22 AM 2019-08-14
	Partner4 partner01companyname.com	Low	John McFadden, Chief Buyer Rony Rodrigue, Head of Sales	Jeff Bloom@domain.com Rony Rodrigue@domain.com	1 Attempt to impersonate partners	12:22 AM 2019-08-14
	Partner5 partner1name.com	Low	Jeff Bloom, Chief Buyer Vyacheslav (Slava) Timokhin, CFO	Jeff Bloom@domain.com Alexander_rodrigue@domain.com	10 Attempts to impersonate partners	12:22 AM
	Partner6 partner801name.com	Medium	Jeff Bloom, Chief Buyer Rony Rodrigue, CFO	Jeff Bloom@domain.com Rony Rodrigue@domain.com		Not a partner Latest emails Block-List

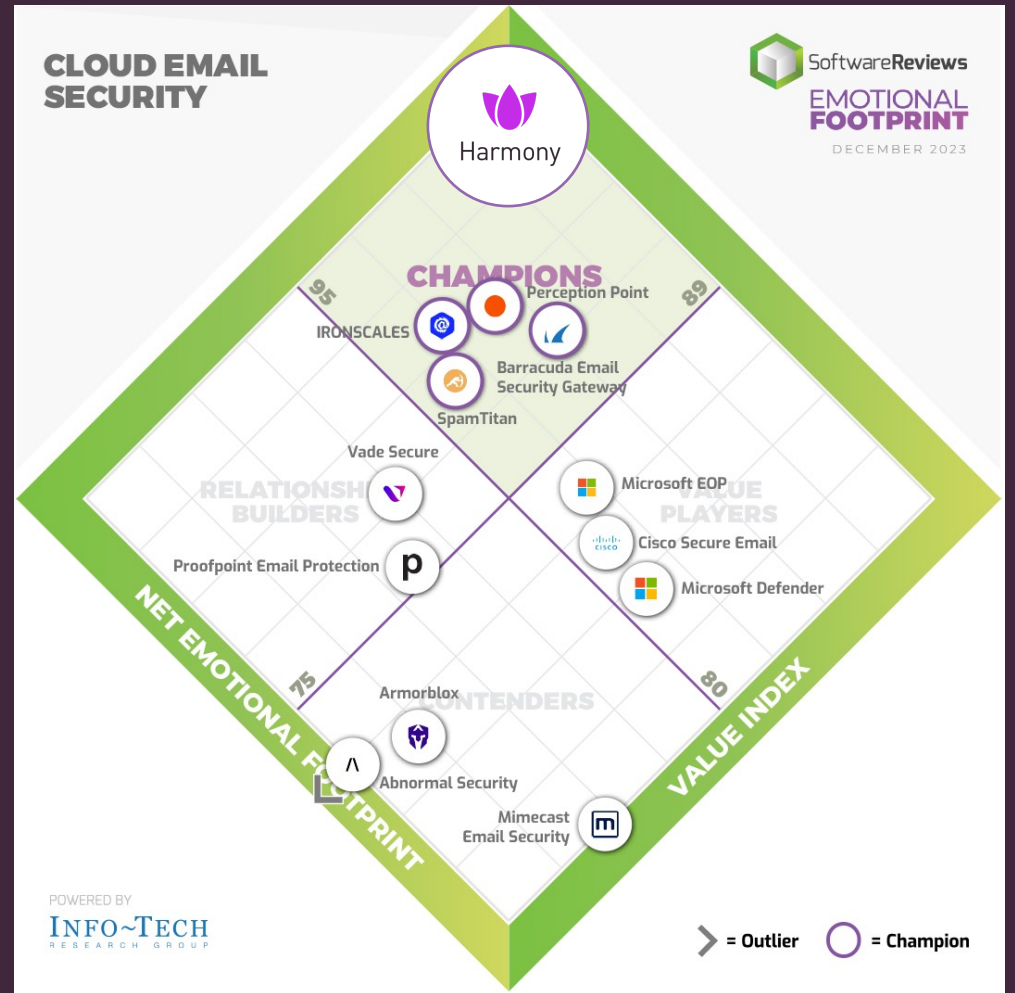
# 完整郵件與協作應用安全性：PhishPoint 攻擊

駭客可能透過非電子郵件管道進行傳播



# Check Point Harmony 電子郵件和協作安全

- 首創 API 的電子郵件安全解決方案 ( 2016 年 )
- 累計至今 23,000 客戶
- 成長最快的電子郵件安全供應商
- 被所有主要分析師評為領導者
- 評測網站排名領先群雄：Gartner Peer Insights、G2、Info-Tech 等



# What Next? 郵件資安健檢服務(POC)

7個按鈕佈署，兩週展現效益！

These graphs provides an overview of the malware detected files and how they were handled by the policy.

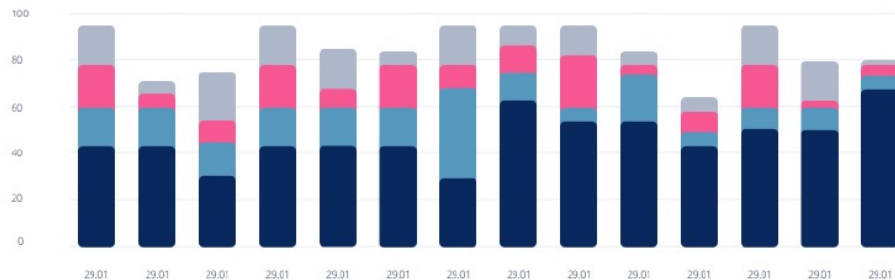
Malware Events by Action



ZERO-day Malware



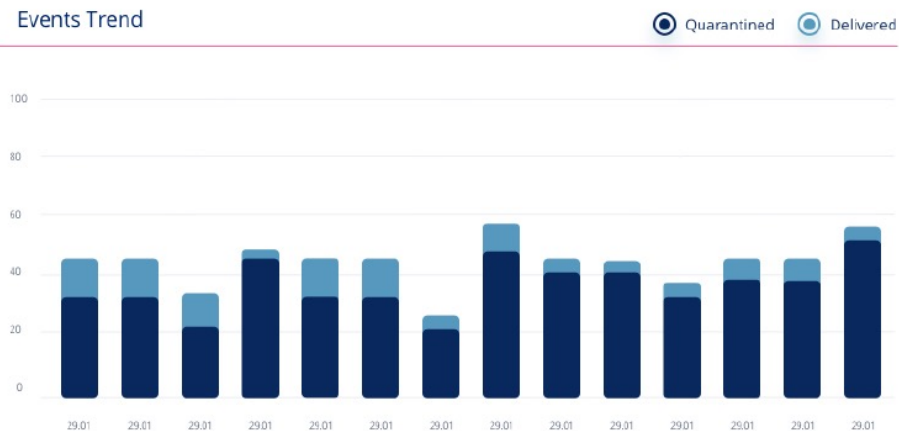
Top Malware Detection Reasons



Top Attacked Users

VIP	User Name	User Email	User Title	Department	Impersonation
	David Angel Williamson	user5@apple.com	Developer	Developer	High
👑	David Angel Williamson	user5@apple.com	Developer	Support	High
	David Angel Williamson	user987654321@apple.com	Developer	Sales	High
👑	David Angel Williamson	user987654321@apple.com	Developer	Support	High
	David Angel Williamson	user987654321@apple.com	Developer	HR	High

Events Trend

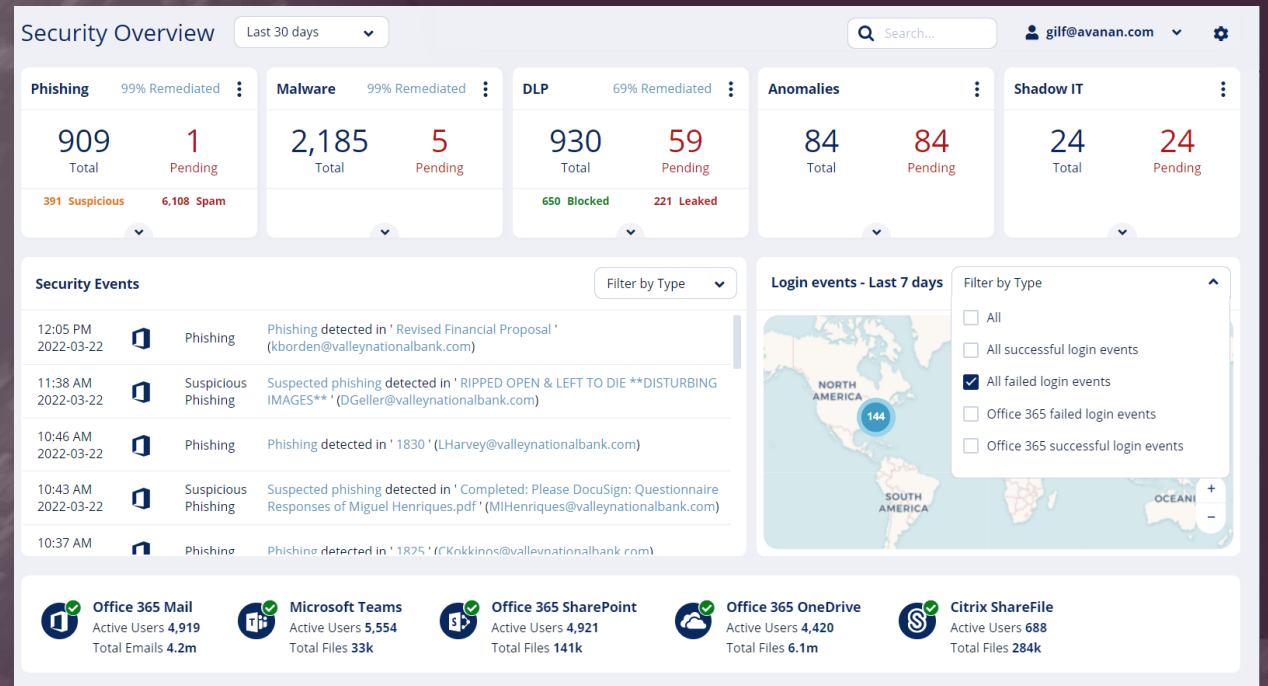


Top File Types

.jpg	200
.txt	200
.pdf	190
.png	100
.exe	100
.zip	100

# Why Check Point Email Security

- 業界最高攔截率
- 完整郵件與協作應用安全性
- 30秒上線 輕鬆維護
- **Prevention First!**





**Thank You!**

YOU DESERVE THE BEST SECURITY