IBM Security™ with TSMC
Benchmark of IBM Cybersecurity Offfering

蔡睿誠 Mark Tsai, CISSP
臺灣 IBM 資訊安全顧問

目錄 (連結可點)

IBM Security 全球有 12 座 SOC 提供資訊安全服務與研究中心

X-Force Command Centers

- Global SOC
- Regional Centers
- Cyber Range / C-TOC
- Security Research Center

威脅情資與安全研究中心

Threat Prevention, Detection & Investigation
Threat Response and Recovery
Security Technology Management & Monitoring

由 X-Force Global Operations 提供 MSS 資安服務

Hybrid of 24x7 and follow-the-sun delivery
Regional MSS delivery centers
400+ Tier 1 & 2 Threat Detection & Investigation analysts
ISO27001/27017, PCI DSS, SSAE 16 – SOC 2 Type 2, FFIEC, Privacy Shield

區域等級的 MSS 服務中心

Data stays in regional centers
Local governance and regulation
In-region personnel delivery
Independent from global MSS

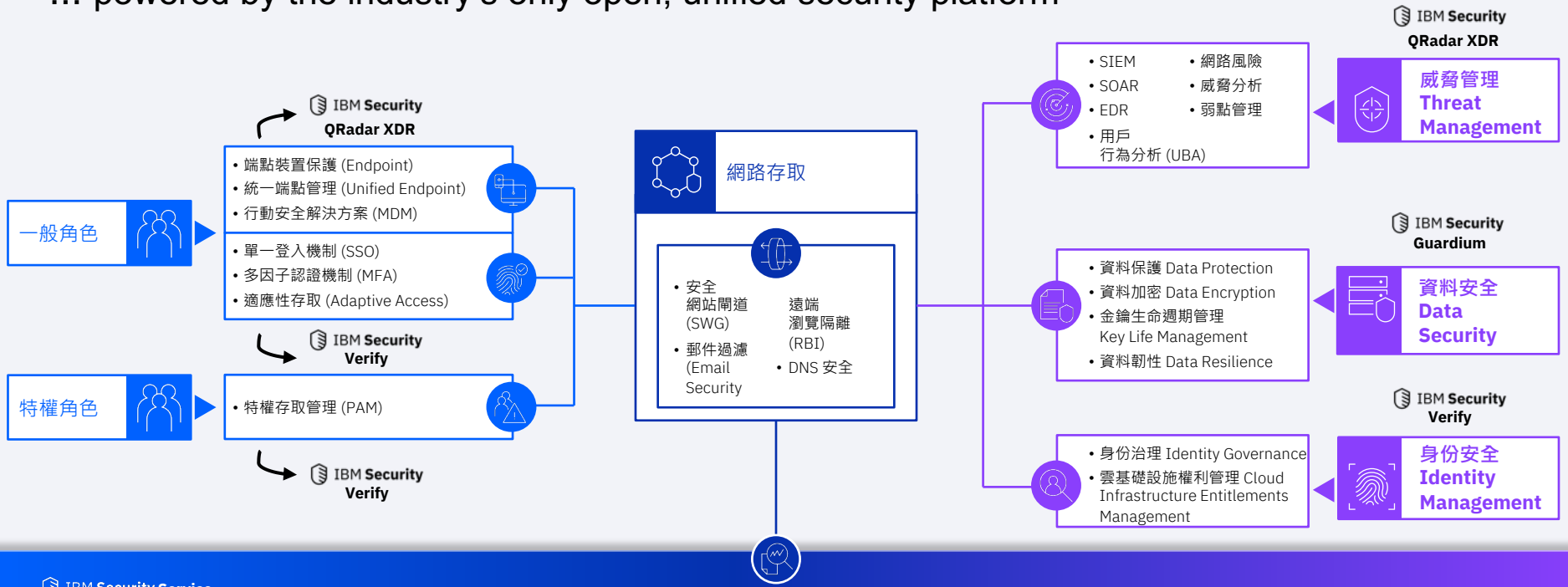
IBM Security 擁有豐富且完整的資訊安全夥伴生態系

Recent Partnerships

aws zscaler touch.io

IBM Security™ End-to-end 的零信任 (Zero-Trust) 資安解決方案

... powered by the industry's only open, unified security platform



IBM Security Service

Zero Trust Acceleration Services
Ransomware Readiness Assessment
Risk Quantification Services
Incident Response Retainer
X-Force Threat Management

支援混合雲各式工作負載環境的資訊安全保護

Data Center | IaaS and PaaS | SaaS and Web

IBM Security
框架、整合與連動聯防

1. Foundational

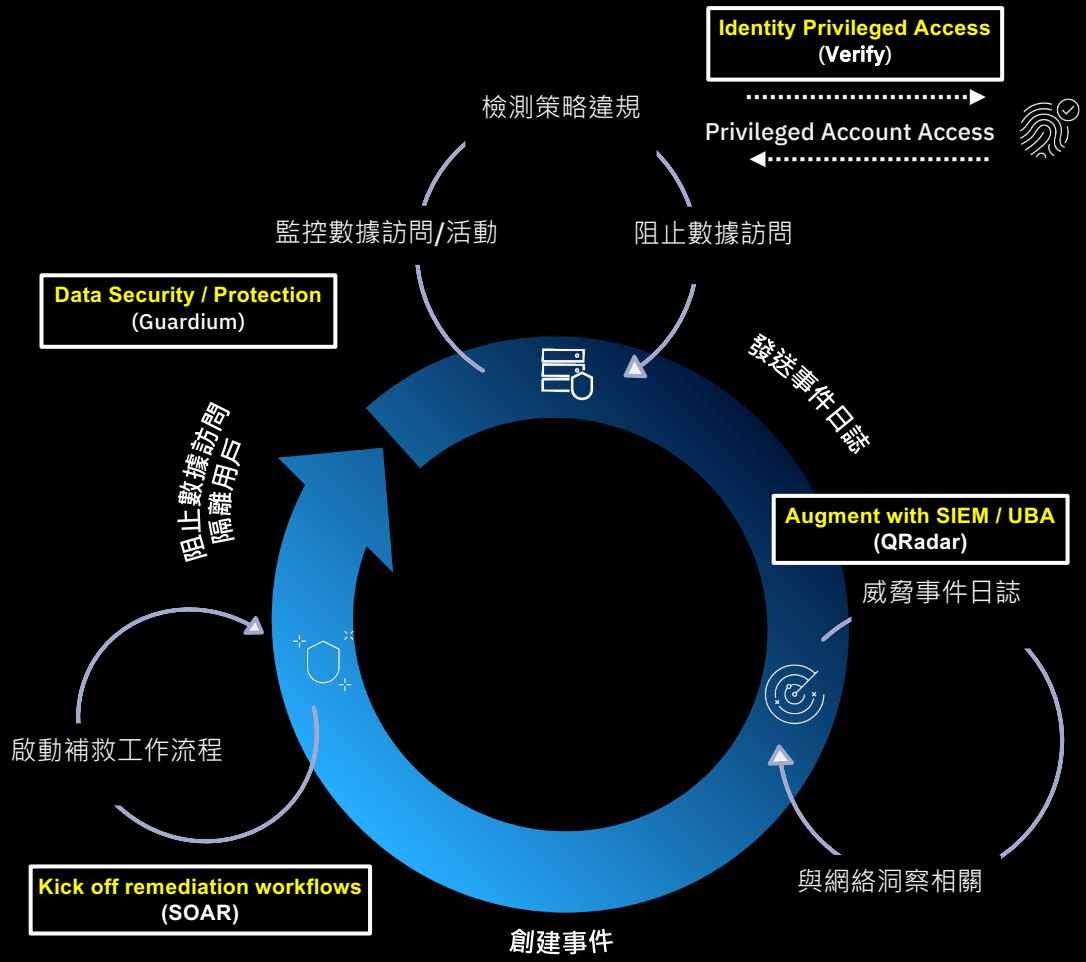
- 實施：監控敏感數據訪問和活動
- 檢測：檢測違反政策/未經授權的訪問
- 響應：確定補救措施

2. Advanced

- 實施：定義數據和用戶級別的策略
- 檢測：分析與數據和特權訪問相關的威脅
- 響應：阻止數據訪問和隔離用戶

3. Optimized

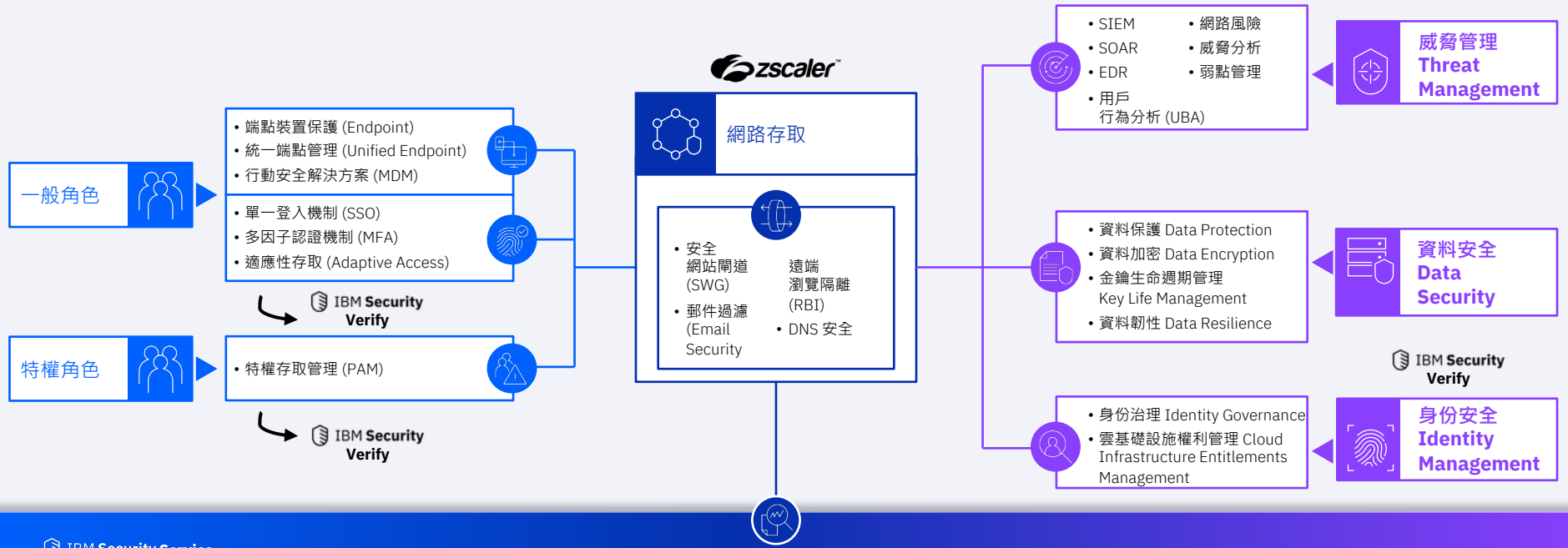
- 響應：響應事件並啟動補救措施
- 改進：根據威脅模式更新數據安全性



IAM (identity access management) , AD protection

IBM Security™ End-to-end 的零信任 (Zero-Trust) 資安解決方案

... powered by the industry's only open, unified security platform



IBM Security Service

Zero Trust Acceleration Services
Ransomware Readiness Assessment
Risk Quantification Services
Incident Response Retainer
X-Force Threat Management

支援混合雲各式工作負載環境的資訊安全保護

Data Center | IaaS and PaaS | SaaS and Web

現代化大型企業組織身份安全管理
高科技製造業的身份存取與管理的威脅挑戰

傳統機制現代化的挑戰

高科業製造業普遍採用 Active Directory 機制實現身份集中化控管，但隨著混合辦公、供應鏈管理與應用程式微服務化等異質環境的新興需求，傳統身份管理機制逐漸無法滿足企業成長實需。

身份蔓延的內部威脅風險

製造業因產業特性，內部常因業務需求而建立許多獨立、互不兼容的身份管理系統，隨著帳號數量增加，身份憑證資訊開始無法避免地在組織傳播、分散或蔓延，可能遭駭客鎖定利用，進而成為組織內部潛藏的安全風險。

帳號授權與生命週期管理

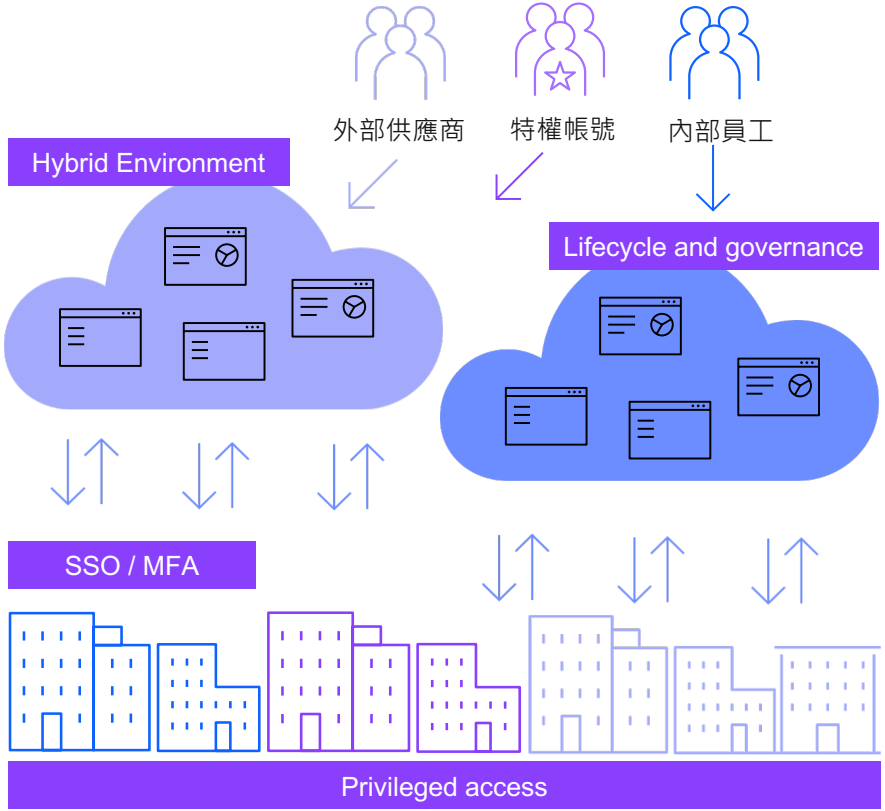
當製造業開始與時俱進引入新興科技，加上各自獨立的身份管理系統，常造成組織無法有效根據用戶、角色與職掌授予或撤銷相應權限，導致整體人員到職、調職或離職程序等員工身份帳號活動無法與企業整體身份安全管控方案相整合。

SSO與MFA的部署挑戰

現今高科技製造業均逐漸接受並實施企業單一登入 (SSO) 與雙因子認證機制 (MFA)，來強化身份存取安全，但常因組織各自獨立的應用系統，無法有效統一部署實施，導致企業需反覆投入重複資源建立個別、不連貫的身份安全管理機制。

現代化大型企業組織身份安全管理
高科技製造業的身份存取與管理的威脅挑戰

如何透過整體化身份管理解決方案於地端、雲端環境實現單一登入、雙因子登入、特權帳號控管，以及帳號生命週期管理？



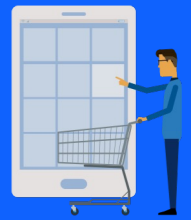
現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案

IBM Security
Verify

企業內部身份管理
Workforce Identity
推動 IT 身份管理現代化、
技術敏捷性和用戶生產力

持續性的登入存取管控 (Access Control)

- 單一登入與多因子認證
  Single Sign-On and MFA
- 帳號生命週期管理
  Lifecycle management
- 條件式存取
  Adaptive access
- 特權帳號存取管理
  Privileged access
- 無密碼式認證機制
  Passwordless authentication
- 隱私權與同意資料管理
  Privacy and consent management



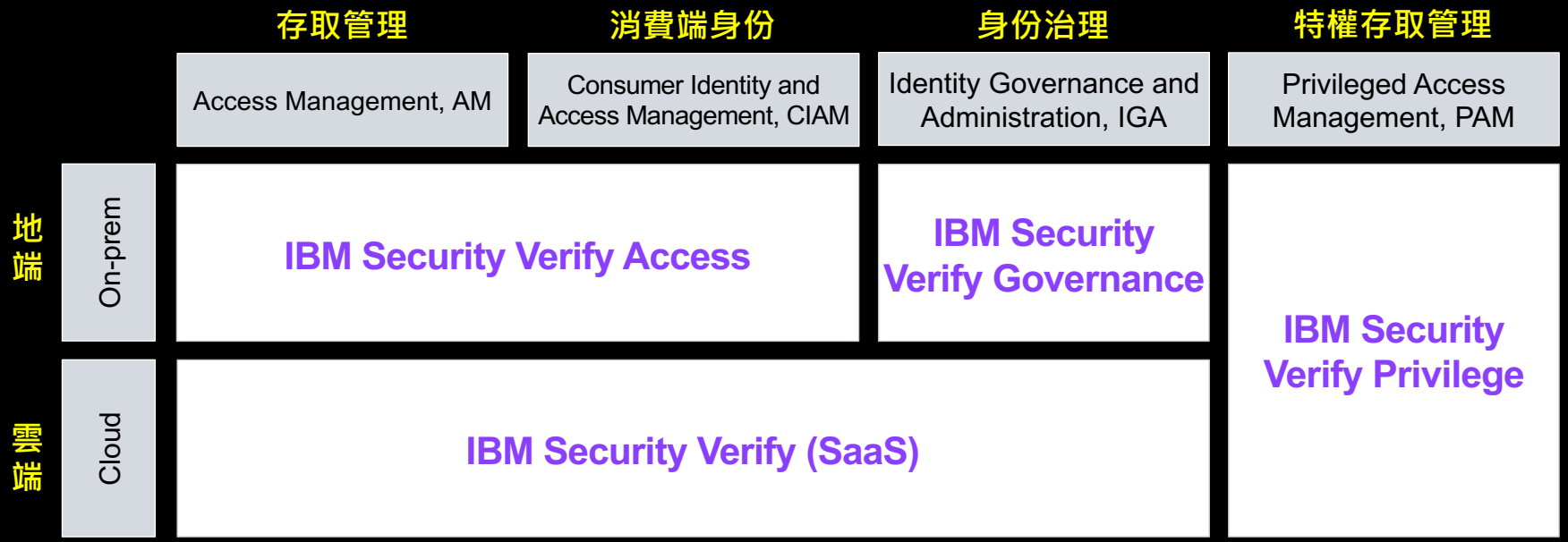
外部客戶身份管理
Consumer Identity
提供客製化、個性化和
值得信賴的操作與登入體驗

地端、雲端內、外部應用程式資源 (Hybrid Cloud Resources)

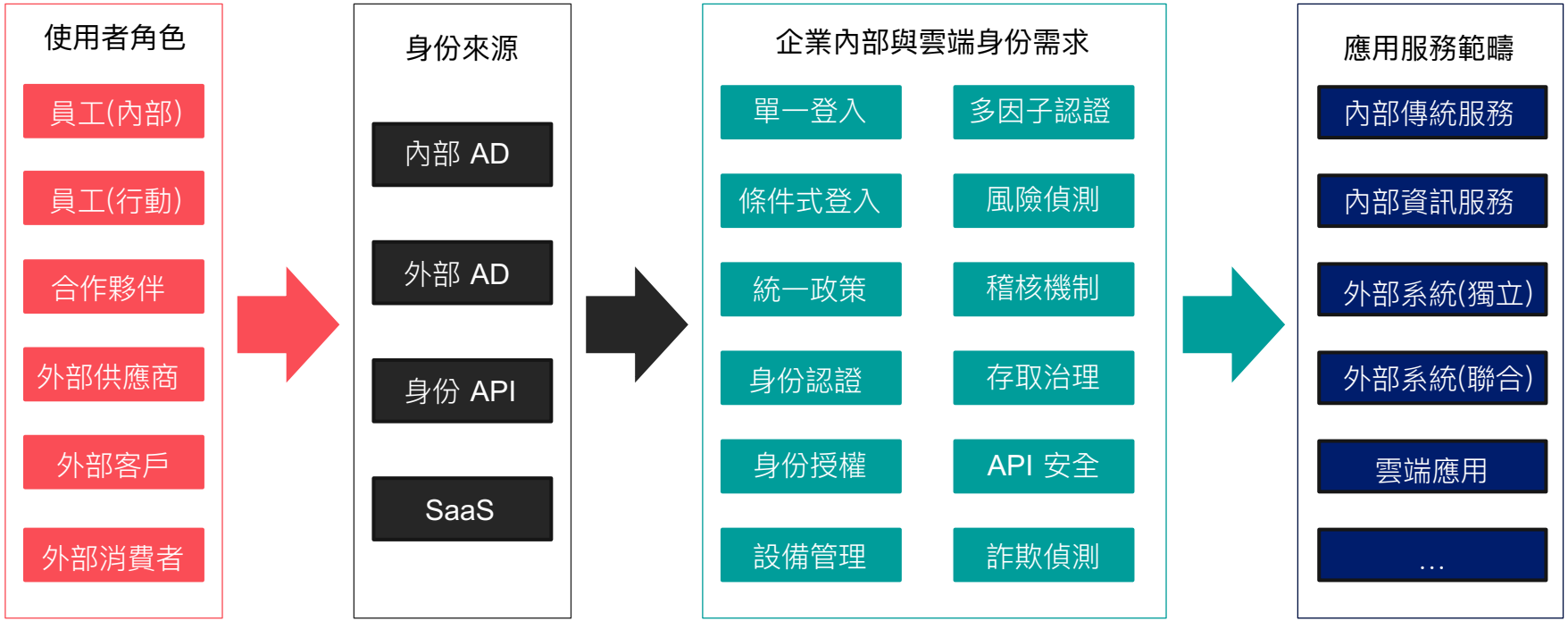
Cloud Apps | On-Prem Apps | Mobile Apps | Data

VPNs | Servers | Databases | Mainframes

IBM Security™ Verify Overview

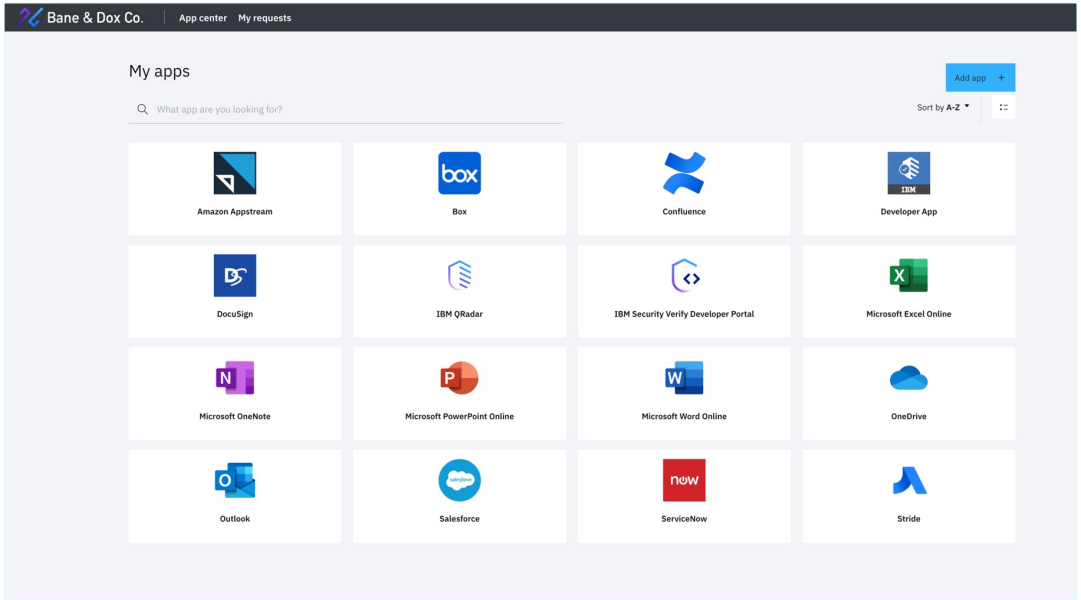


現代化大型企業組織身份安全管理
高科技製造業的身份存取與管理的威脅挑戰



現代化身份安全管理解決方案需針對所有類型的用戶、企業內、外部系統與雲端服務整體考量

現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案



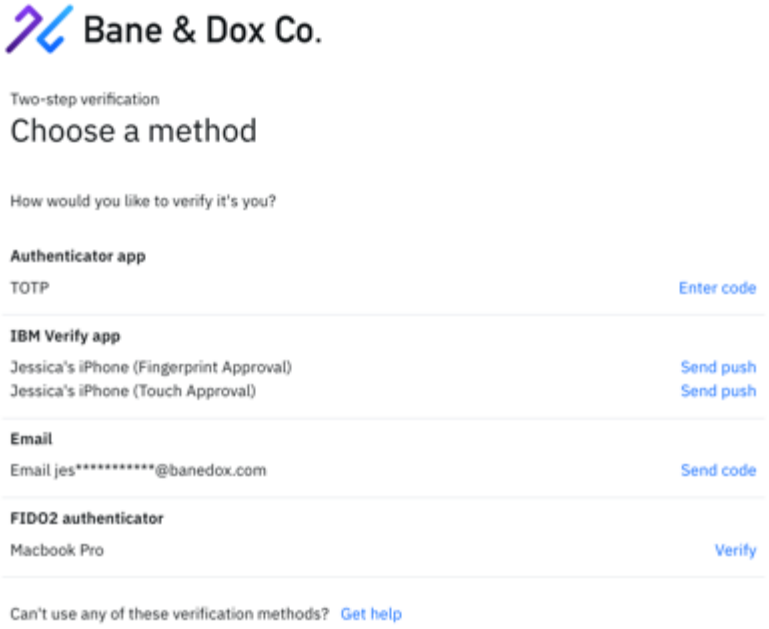
IBM **Security** Verify

SSO Launch Pad

讓員工輕鬆存取和授權企業組織內、外部工作所需的應用程序服務。

- 訪問 SaaS 或自行開發的應用服務
- 搜索與檢視企業應用服務
- 請求訪問企業應用服務
- 管理設置個人身份資料
- 註冊與啟用 MFA 設備
- 更改用戶名和密碼

現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案



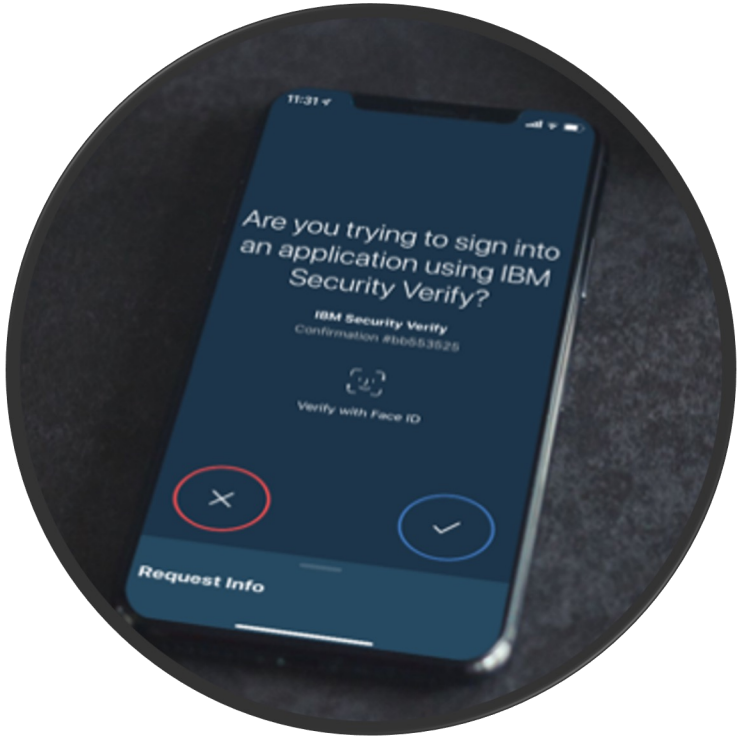
IBM **Security** Verify

MFA Options

提供企業組織或員工 MFA 的適用選項，例如 SMS OTP 或是 FIDO2

- 整合行動裝置應用程序推送基於時間的 TOTP 進行雙因子認證
- 二維碼、指紋、面部識別和 FIDO2 身份驗證器等無密碼選項 (Passwordless)
- 使用簡單、開箱即用的訪問策略或基於每個應用服務進行服務存取的政策定義
- 僅在必要時或偵測為高風險訪問時，要求用戶進行 MFA 機制認證 (條件式認證)

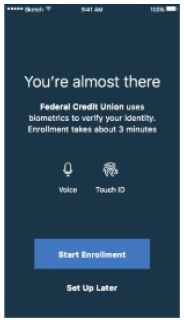
現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案

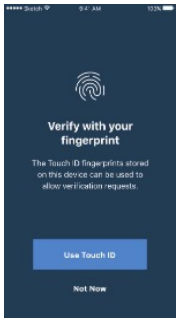


IBM **Security** Verify

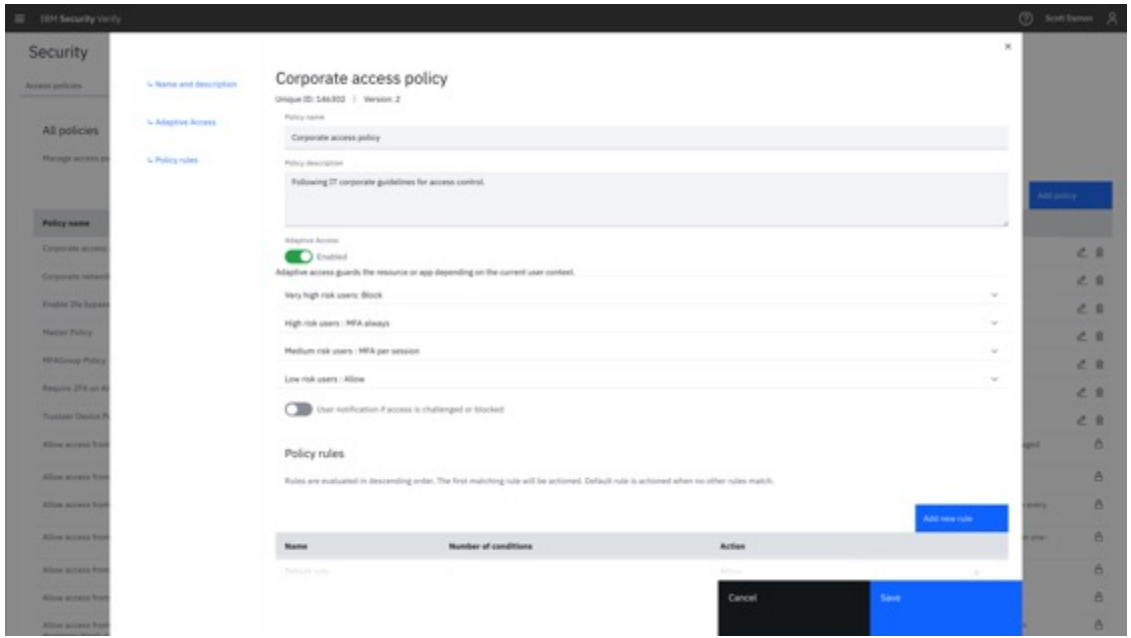
MFA Across Resources

- 在一般性平台上利用其他 MFA 方法
- 對本地或雲端應用程序進行身份驗證
- 擴展到 VPN、Linux、AIX、Windows 桌面、Windows 服務器、IBM z 等整合 MFA





現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案



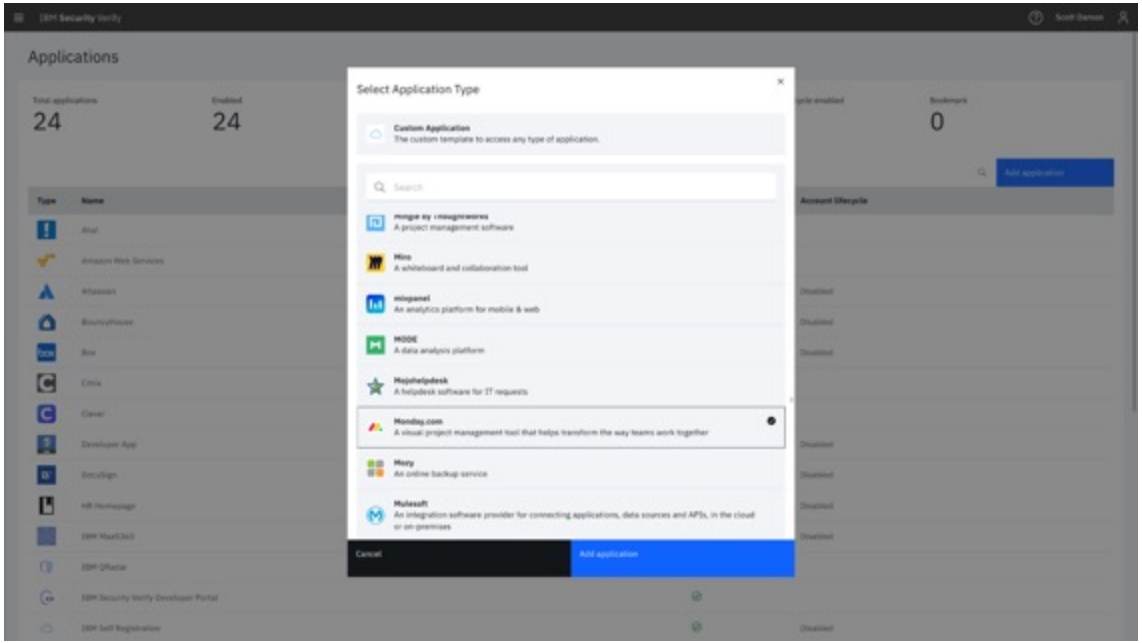
IBM **Security** Verify

Adaptive Access

基於風險的身份驗證的訪問策略

- 身份詐欺風險偵測保護機制和身份存取管理技術的整合。
- 深入結合用戶、設備和環境情境
- 人工智能驅動的整體風險評分
- 為低風險用戶提供無障礙訪問，同時防範高風險身份存取場景
- 僅需簡單的配置即可完成設定

現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案



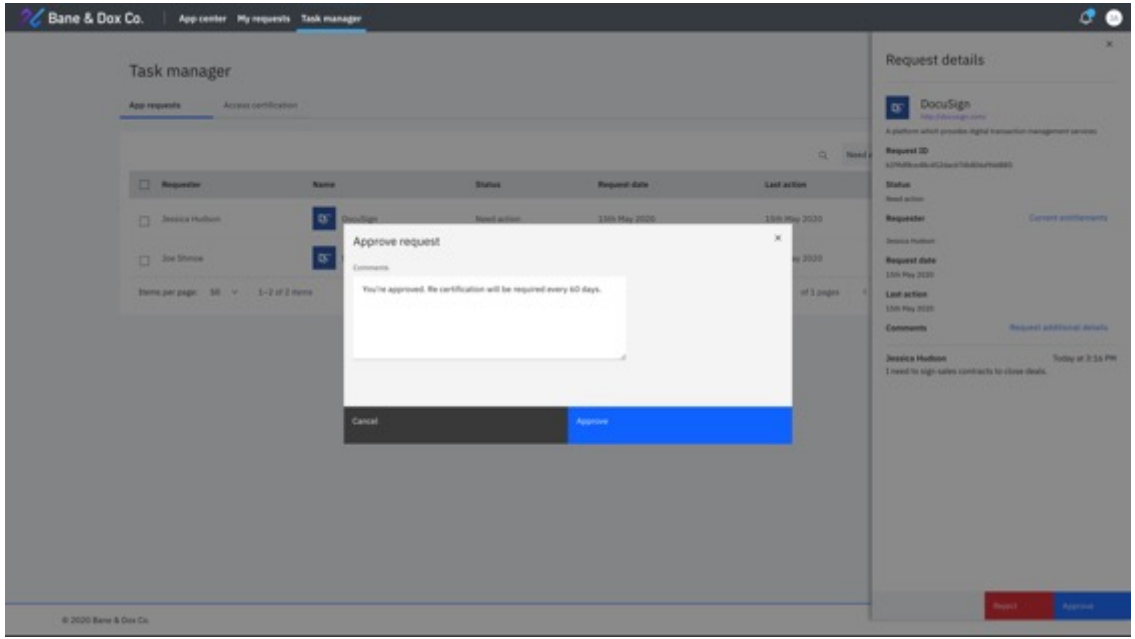
IBM **Security** Verify

Application Onboarding

在短時間內在整體身份安全管控系統內整合新的應用服務

- 內建支援數百個常見的 SaaS 應用快速連接器
- 按步驟式的整合步驟與指導
- 整合應用服務的進階屬性
- 支援各式共通的認識協定 OAuth2、OIDC 或 SAML 2.0

現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案



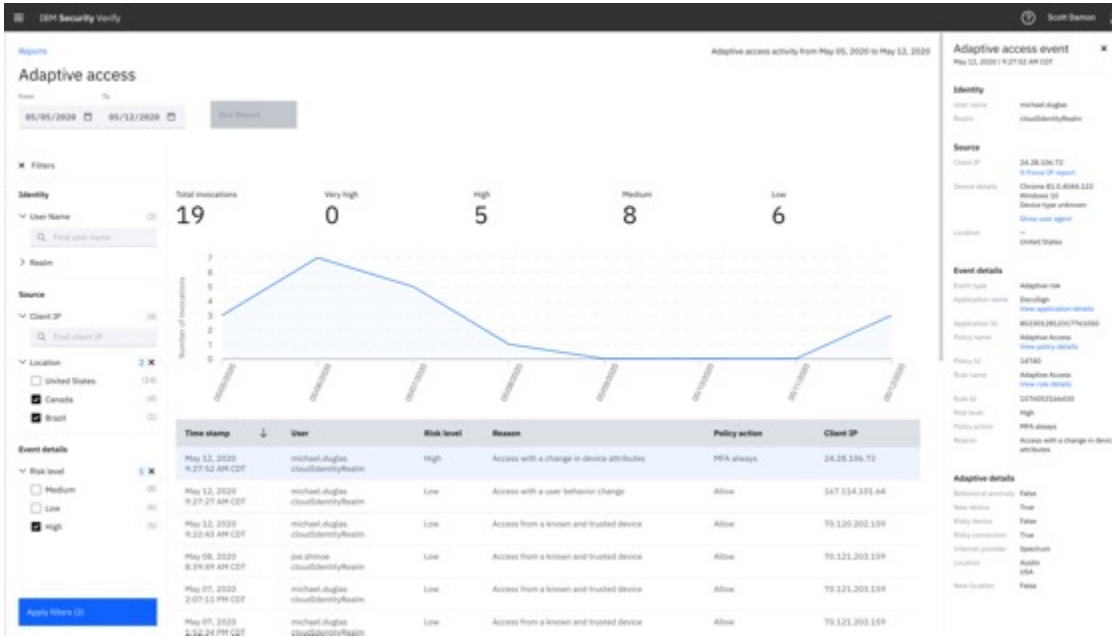
IBM **Security** Verify

Delegated Administration

釋放 IT 身份管理資源與簡化企業組織業務認證與授權流程

- 指定業務單位管理者或所有權者來管理特定應用服務的訪問權限
- 使管理人員能夠快速啟用人員加入應用系統團隊，而無需呼叫外部 IT 單位完成簡單的授權任務
- 加速新應用程序的採用與納管

現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案



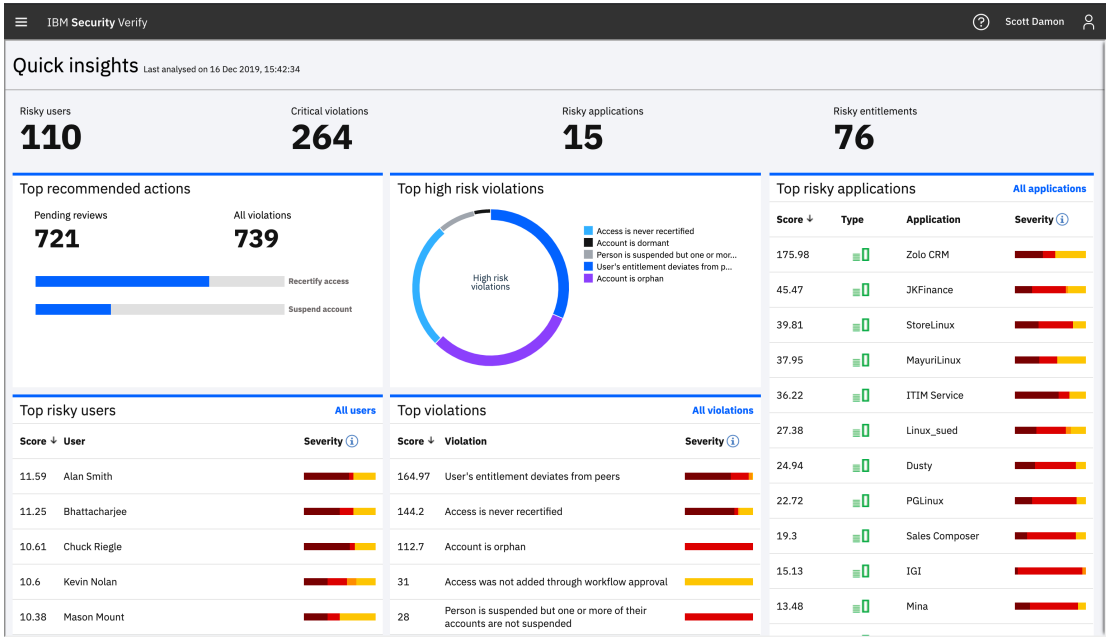
IBM **Security** Verify

Reporting

針對身份存取風險即時過濾、診斷與調查

- 認證活動 Authentication Activity
- 自適應訪問 Adaptive Access
- 應用程序使用 Application Usage
- 管理員活動 Admin Activity
- MFA 活動 MFA Activity
- 身份認證活動 Fulfillment activity

現代化大型企業組織身份安全管理
端到端 (End-to-End) 一站式的身份管理解決方案



IBM **Security** Verify

Identity Analytics

查看企業組織 IAM 整體運行狀況

- 使用 360 度視角掃描與身份相關的存取風險
- 同儕或同團體成員的群體分析
- 通過 AI 驅動的風險和可信度評分以挖掘潛藏風險異常情況
- 採取建議的緩解措施，例如重新檢查訪問權限或暫停特定帳戶活動

身份安全管控方案的導入效益

有效控管企業整體身份安全風險與強化 IT 效率

透過全面化身份安全管理降低資料外洩與資安事件發生風險

降低網路攻擊面

藉由實現 SSO 作為員工、外部供應商與合作夥伴存取企業內、外部資源的單一登入途徑。

促進企業組織資安保護

整合企業內部應用程式 MFA 機制提供第二層資訊安全保護效益。

降低用戶身份帳號風險

自動化執行身份帳號風險偵測，協助偵測或阻絕高風險帳號存取

節省與降低 IT 執行身份帳號日常管理操作與維護成本

提供身份自助管理服務

讓員工透過一定程度的自助服務解決常見的憑證管理問題，例如忘記或重置密碼，或是申請特定服務的權限開放，釋放 IT 部門日常維運。

分層授權身份存取申請

分層授權由相關部門經理批准員工特定層級的訪問請求，以加速整體身份授權流程、提升組織身份安全管理生產力。

Let IBM help you accelerate

- 借助專業資安顧問和經驗豐富的技術專家加速 IAM 計劃
- 解決方案已跟數以千計的合作夥伴整合擁有良善的技術聯盟
- 20 多年 IAM 解決方案專業知識，適合大型企業部署實施

IBM 身份認證與管理資安服務 (IBM Security IAM Services)

策略規劃與設計 Strategy & Design

Plan | Define | Design

開發合適的身份管理框架

- 使用企業營運思維設計以用戶為中心的解決方案與務實可行的遷移計劃
- 確定要配置的企業應用服務與身份功能
- 評估現有基礎設施和 IAM 流程的整合
- 使用行業最佳實務導入標準化 IAM 流程

部署實施與執行 Transformation

Build | Test | Enable

確保 IAM 專案成功實施

- IAM 技術與專案的快速部署
- 適配企業組織的商業與工作流程
- 使用敏捷方法快速測試、雛形化和迭代
- 降低基礎設施管理成本以建立管理階層或利益相關者投資信心
- 整合企業應用服務、配置認證與授權功能和最終用戶身份安全意識教育訓練
- 分階段實施、遷移以最大程度避免用戶服務存取中斷或遭受干擾

持續最佳化調適 Optimization

Operate | Enhance | Expand

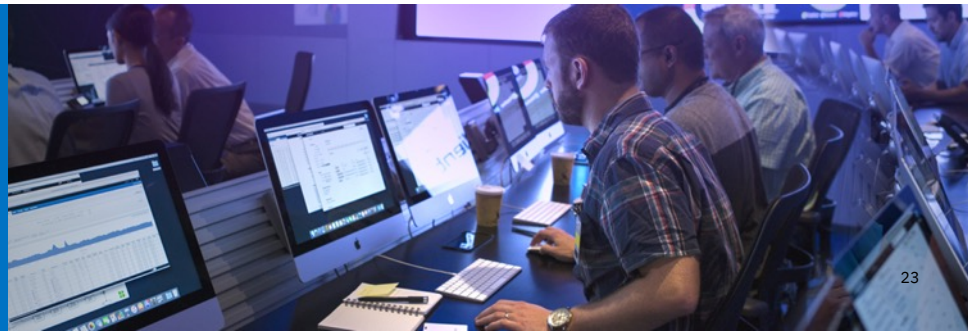
提升整體投資效益

- 將熟練的商業部門成員重新引用至企業更關鍵的營運任務中導入 IAM 專案
- 完善整合員工入職、調職與申請程序
- 通過自動化 IAM 身份安全提升管理效率
- 持續收集用戶使用反饋與持續改進
- 與時俱進支援新安全技術整合

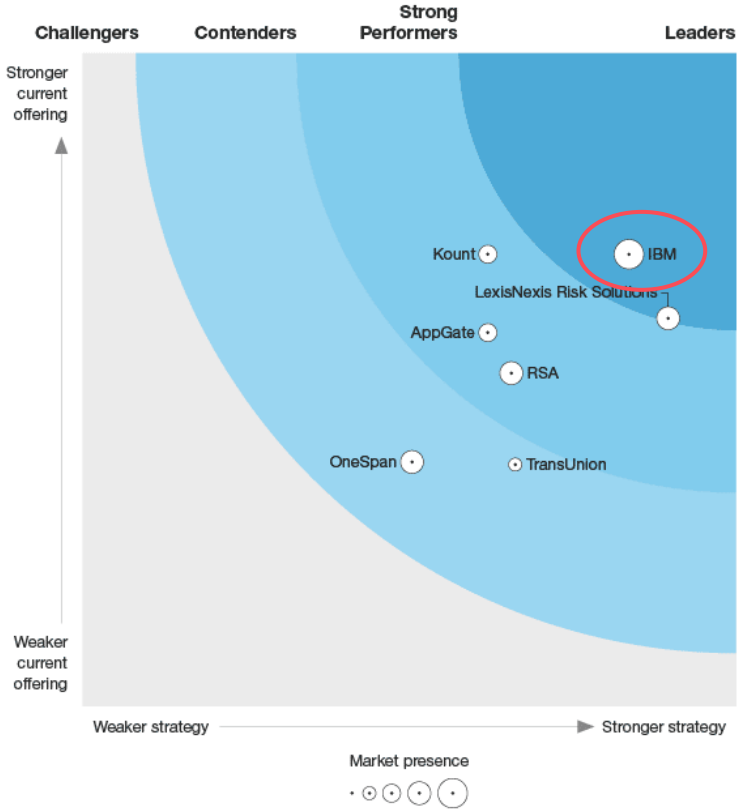
IBM Identity as a Service
LEADER

KuppingerCole's
Leadership Compass

A successful IAM program requires a security strategy that combines people, process and technology.



The Forrester Wave™: **Risk-Based Authentication**, Q2 2020



Forrester, The Forrester Wave™: Risk-Based Authentication, Q2 2020, Andras Cser, Merritt Maxim, Matthew Flug, and Peggy Dostie, May 2020

Magic Quadrant for **Access Management** (AM), Q4 2021

Gartner

“ **Access management (AM)** has become the source of trust for identity-first security. Increased dependence on identities for access anywhere, anytime, requires AM to be more reliable and easier to adopt. Identity orchestration, IAM convergence and SaaS resilience importance will increase during 2022 "

“ **IBM is a Challenger** in this Magic Quadrant. Its product is offered as software (IBM Security Verify Access) and SaaS-delivered (IBM Security Verify) options, focused on a converged approach for AM and other IBM Security products. Its operations are geographically diversified, and its clients tend to be large organizations, mostly in the banking and public sector industries, looking for on-premises and hybrid deployments. “

IBM採用現代化數位身份解決方案提供內部員工與外部客戶統一性身份認證與管理

透過 IBM Verify 身份認證
與管理解決方案，提供超過：

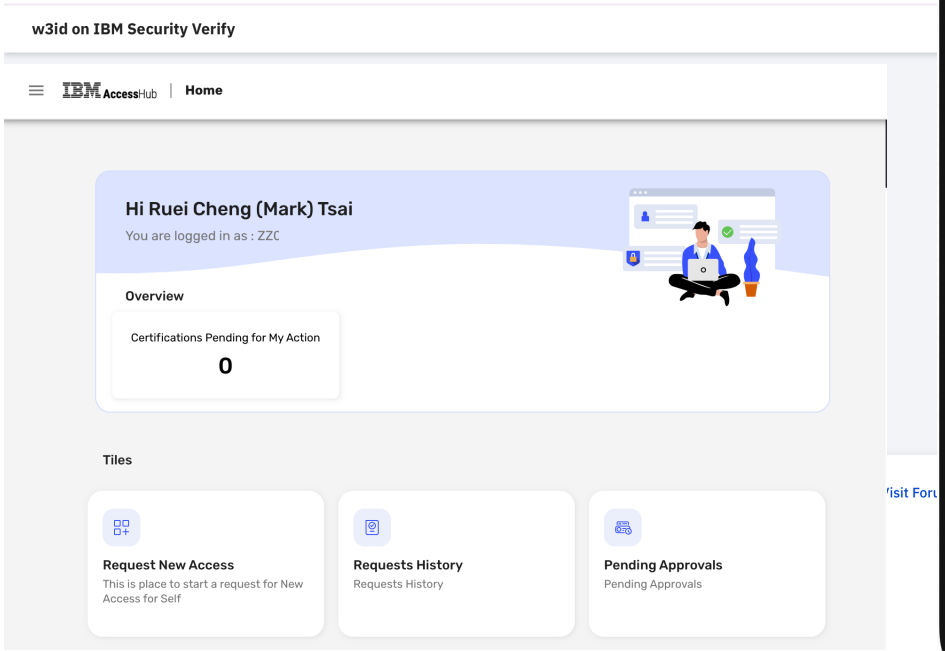
270 萬+

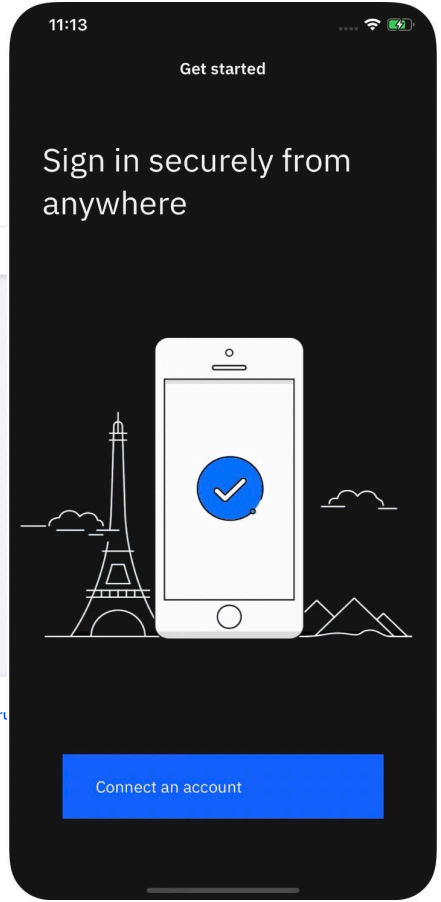
使用無密碼方式 QR 和 FIDO2 等
高級身份驗證機制進行內、外部資源存取

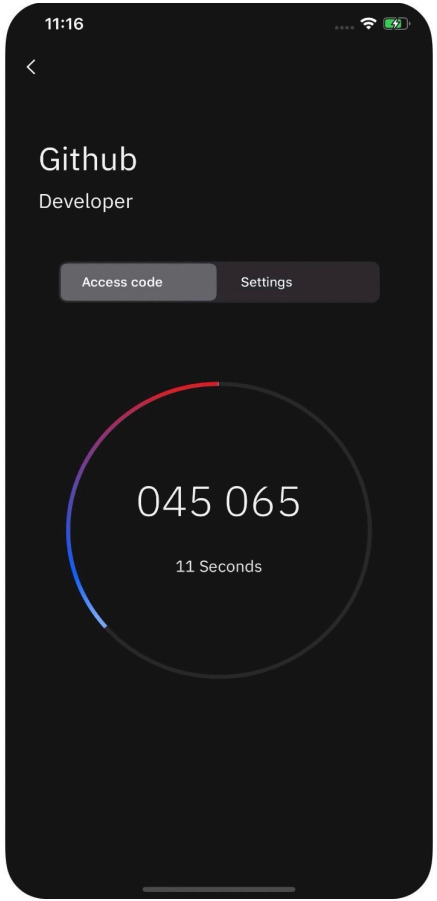
“ With IBM Security Verify, to anyone who interacts with IBM, we can now provide frictionless, secure, state of the art access to information resources.”

Gary Schmader, Sr. Manager, Assured Identity and Security Operations, IBM

IBM採用現代化數位身份解決方案提供內部員工與外部客戶統一性身份認證與管理



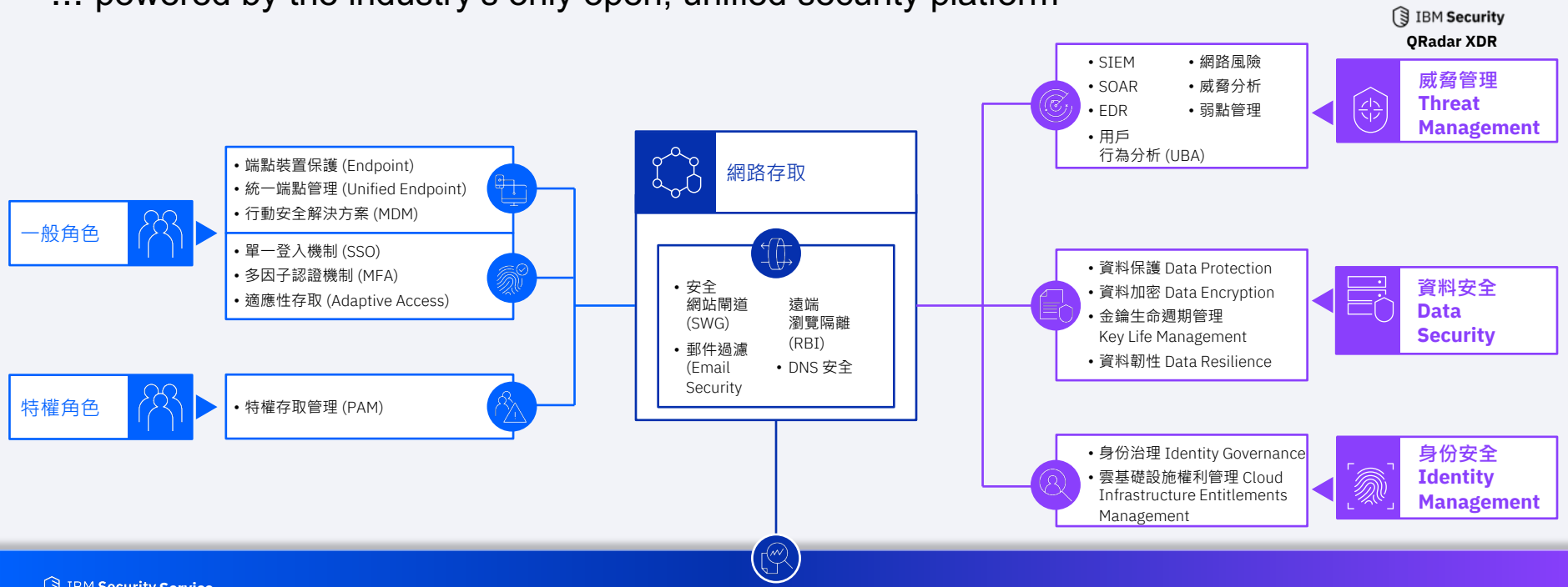




Network Protection (Threat Management)

IBM Security™ End-to-end 的零信任 (Zero-Trust) 資安解決方案

... powered by the industry's only open, unified security platform



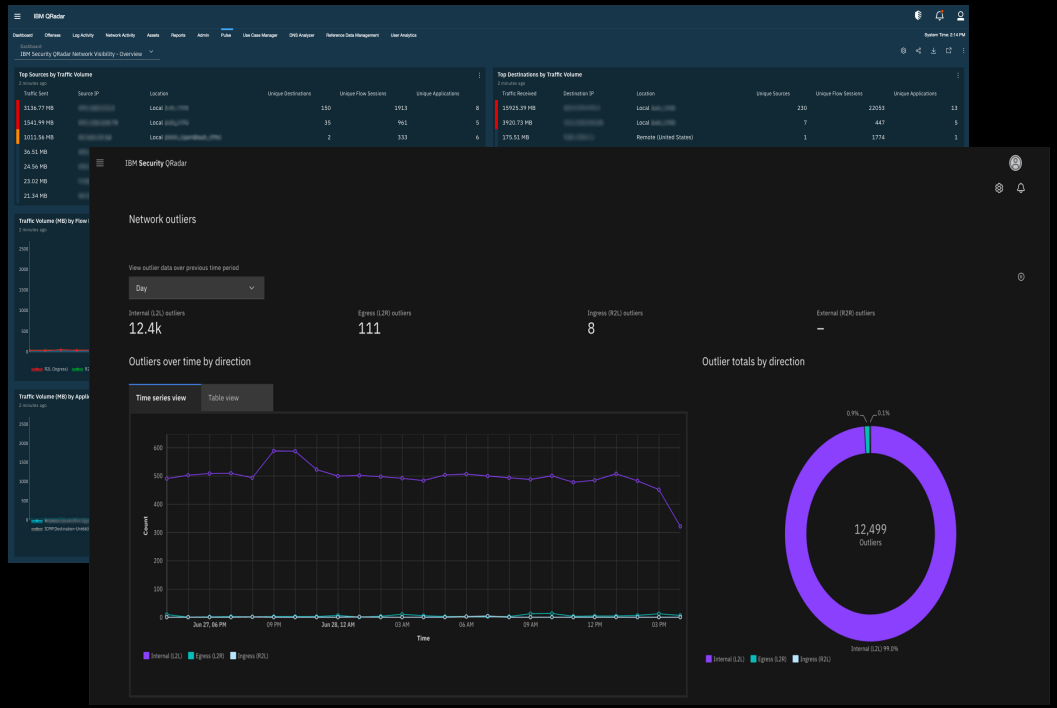
IBM Security Service

Zero Trust Acceleration Services
Ransomware Readiness Assessment
Risk Quantification Services
Incident Response Retainer
X-Force Threat Management

支援混合雲各式工作負載環境的資訊安全保護

Data Center | IaaS and PaaS | SaaS and Web

QRadar NDR 提供網路流量的可視化與網路流量異常分析 (NTA)



使用 NTA 技術偵測潛藏的威脅流量：

- 行為分析 (Behavioral analytics)
  - 透過流量偵測遭駭設備
  - 偵測 beaconing and C2 犯罪活動
  - 按會話的識別指標
- 進階鑑識分析 (Next-Gen Forensics)
  - 封包流量分析
  - 鑑識分析等級的流量調查
  - 自動化封包深度解析
- 資產識別 (Asset Aware)
  - 偵測未管制的 IT 設備資產
  - 自動建立化建立資產基準
  - 同步整合風險、CMDB 與弱點資訊

99%

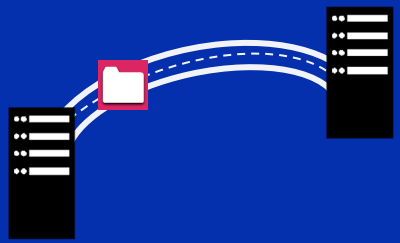
...的威脅攻擊都是以某種方式透過網路進行

流量包含我們檢測、調查和響應所需的信息

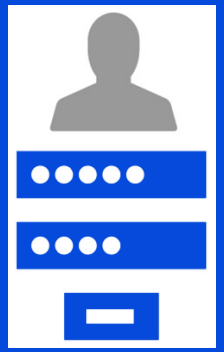
攻擊者非常聰明，
會主動隱藏他們的踪跡

隱藏在
正常流量範圍內

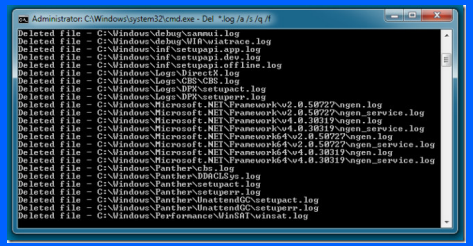
不引人注意的小型
橫向移動提取數據



竊取合法用戶憑證



刪除軌跡紀錄



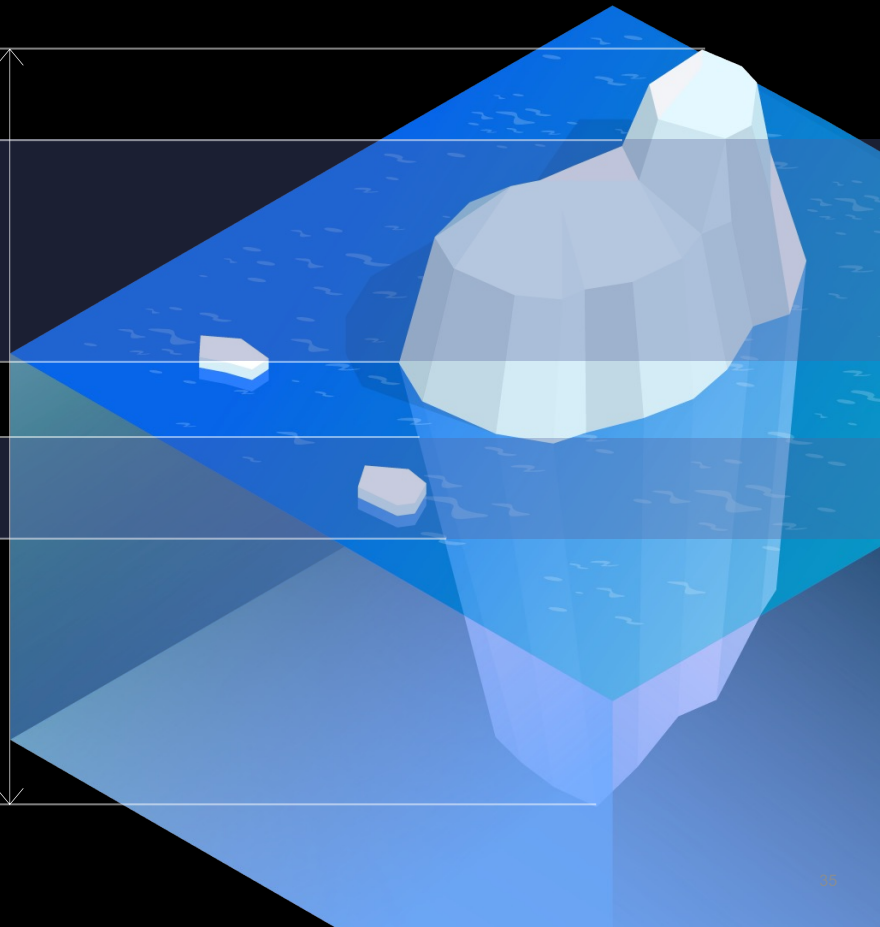
“It’s like they say… packets don’t lie.

You could make logs say whatever you want but if you’re watching the wire, then you know what’s really going on.”

Chris Elgee (SANS instructor, challenge developer and penetration tester)
GIAC Podcast – April 14th, 2020

QRadar NDR：在網路流量上能看到什麼？

What devices tell me	Logs
Basic flow visibility	Netflow
Application	QFlow
Metadata	DPI solutions
Content	QRadar Network Insights
	QRadar Incident Forensics
	QRadar Network Packet Capture



深入了解網路通訊行為

Threat Detection | Incident Response

日誌 (Log) 提供了日誌來源的可見性，並且僅限於該日誌中包含的數據

網路流量 (Flow) 提供對網路通信的全面可見性

QRadar Network Insights 分析每個網路會話及其內容，以檢測可疑行為、敏感內容等

QRadar Incident Forensics 將捕捉完整的數據包數據，重建、分析和顯示原始形式的內容

Key Network use cases

Advanced Threats

使用識別惡意軟件和網絡釣魚嘗試所需的深度和上下文分析網路數據。了解每個文件的詳細信息，文件來自哪里以及發送到哪裡。

Threat Hunting

查詢歷史網絡活動以搜索過去的活動，發現異常行為並識別所涉及的資產。

Incident Response

為分析師提供額外的上下文和元數據，以加快平均響應時間

Lateral movement

檢測指示惡意橫向移動的設備之間的偵察、旋轉和傳輸

Data exfiltration

通過電子郵件、聊天消息、文件上傳/下載或社交媒體實時發現跨網路傳輸的敏感數據

Asset profiling

在新設備連接到網絡時發現它們，並根據屬性和行為持續分析資產以發現威脅、受損設備和影子 IT

IBM QRadar Network Insights, QNI

通過即時網絡流量分析檢測高級威脅。 查看網路攻擊鏈中較早的攻擊階段，以阻止它們繼續往下執行。

Key capabilities

- 獲得深入的可見性和網絡上下文，以進行有效的檢測和響應
- 收集威脅搜尋和歷史分析所需的網絡數據
- 洞察實時威脅活動、設備通信和可疑行為
- 跨本地、虛擬和雲的靈活部署模型

Benefits

- 增強對已知和未知威脅的檢測
- 加強針對僅通過日誌無法獲得洞察的分析能力
- 使用所需數據快速自信地做出響應
- 整個企業的統一可見性

IBM Security QRadar Network Insights

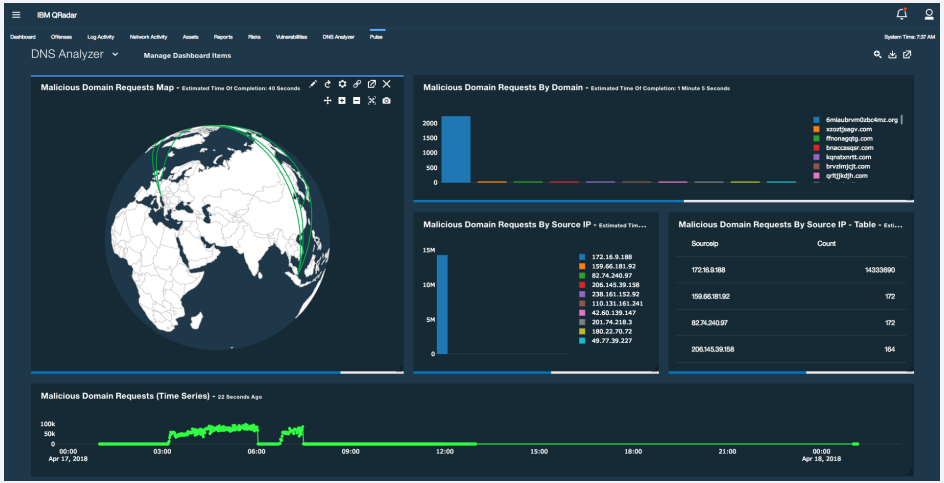
通過即時網路流量分析啟用攻擊預測。

通過 **QNI** 或 **DNS** 日誌觀察到的本地 **DNS** 活動觀察新的網域

QRadar 域分析，包括 **DGA** 檢測、蹲點和隧道檢測

在網路流量中移動時暴露威脅

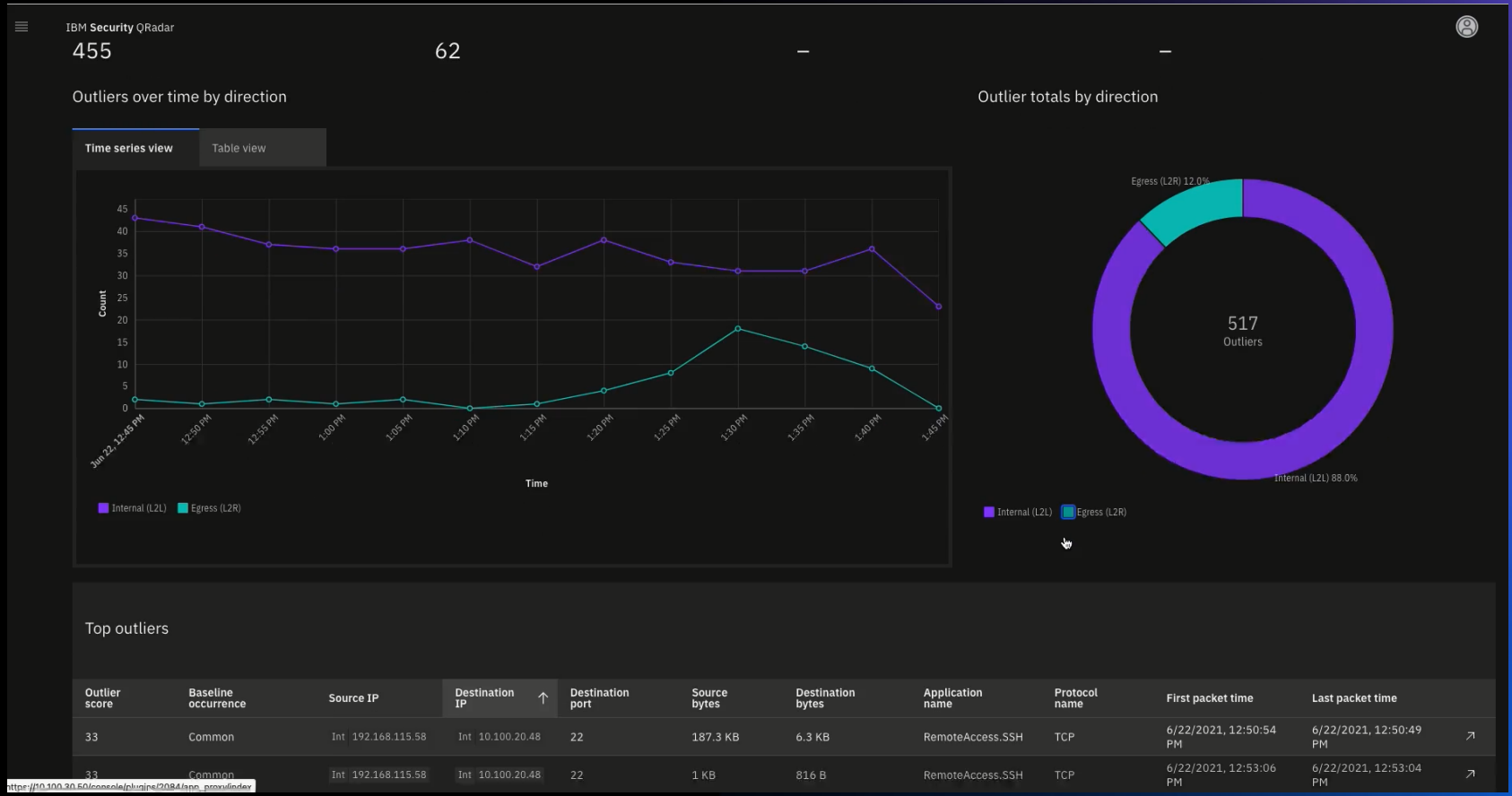
整合 **Windows Sysmon** 的端點可見性



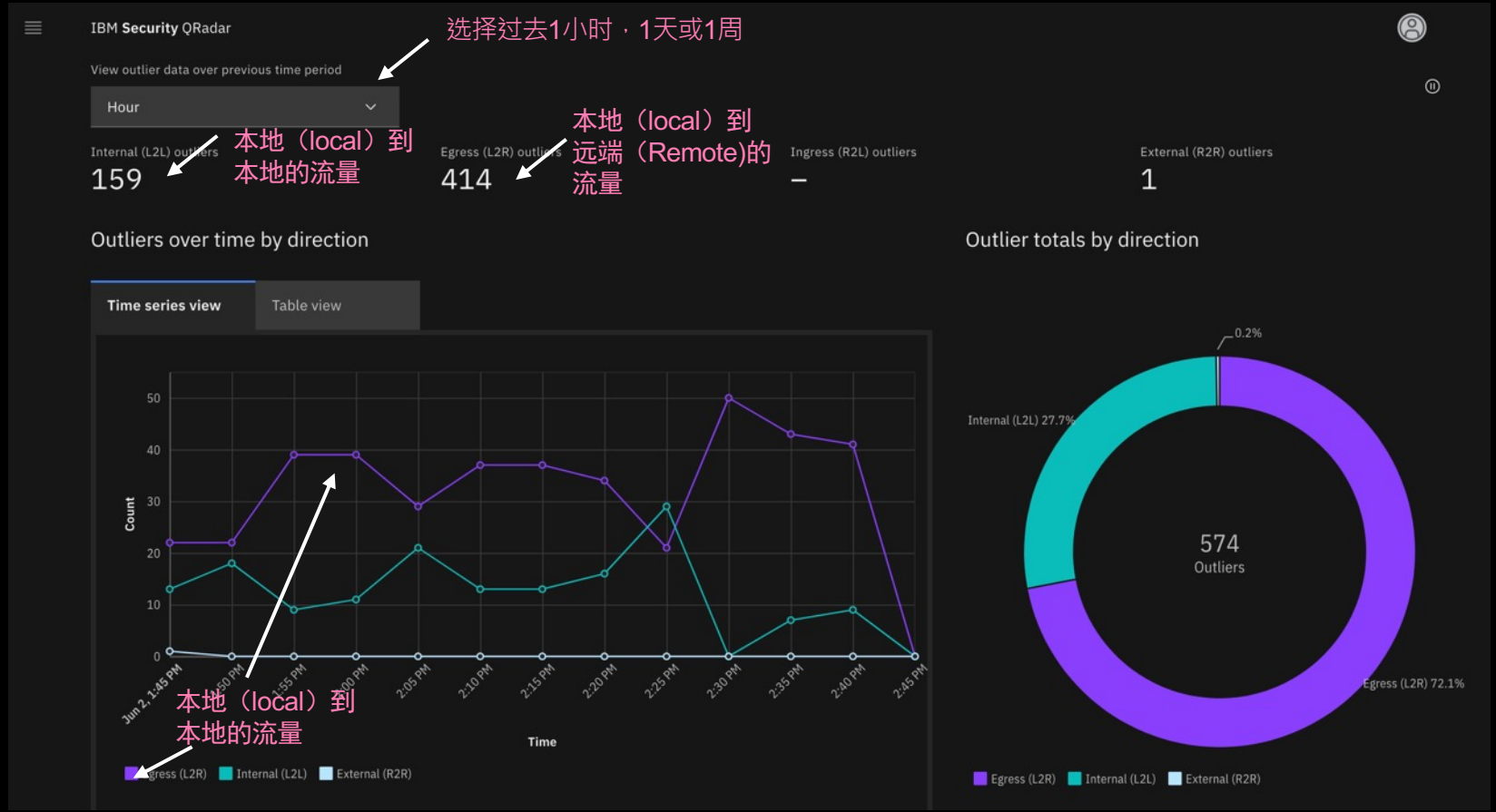
“QRadar 大大縮短了我們將 100 多個混合多雲帳戶連接到 QRadar 的時間。這使得從我們的 AWS 和其他雲環境中消費事件和網絡流量變得很容易。”

Large US-based Insurance Company

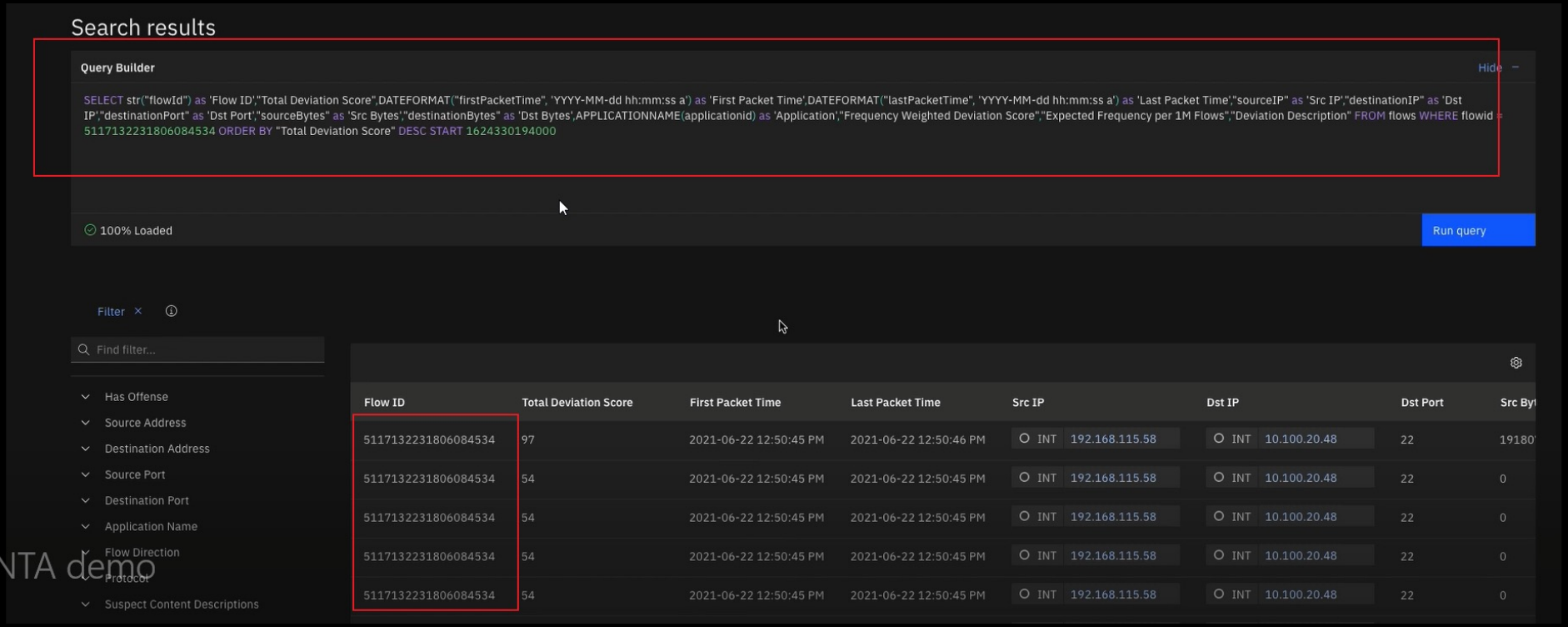
QRadar® NDR 儀表板畫面



QRadar® NDR 儀表板畫面



QRadar® NDR 儀表板畫面



NTA demo

Endpoint Protection

端點安全：
幾近即時的資安威脅挑戰

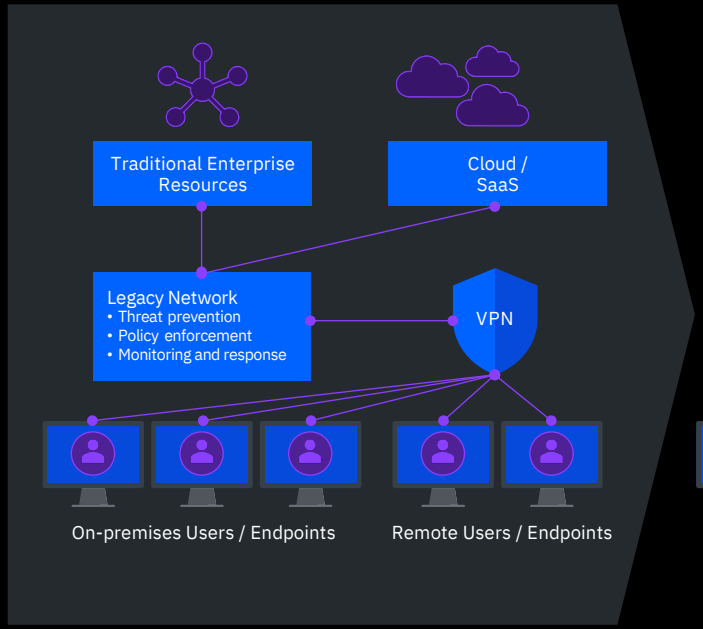
- 傳統方法仰賴查找已知內容或特徵比對 (Signature-Based)，但攻擊者已經轉向針對不固定目標的威脅攻擊 (無文件/勒索軟體) 進行進階持續攻擊 (APT)
- 端點是最常發生 Zero-day 攻擊與缺乏威脅可視化的最後一哩處
- 攻擊者利用合法軟體或文件掩飾他們的攻擊軌跡
- 惡意活動的複雜度和自動化網路攻擊活動的增加，其中最大部分都是來端點遭到第一時間滲透
- 缺乏實務經驗的資安分析師，每日需要處理與操作複雜的資安工具，伴隨過多的警報和曠日耗時的資安事件調查

"端點安全仍然是最受關注的核心主題覆蓋領域之一.....因為端點通常是最常見攻擊的目標、威脅攻擊變得越來越複雜，以及端點裝置也越來越多樣化"

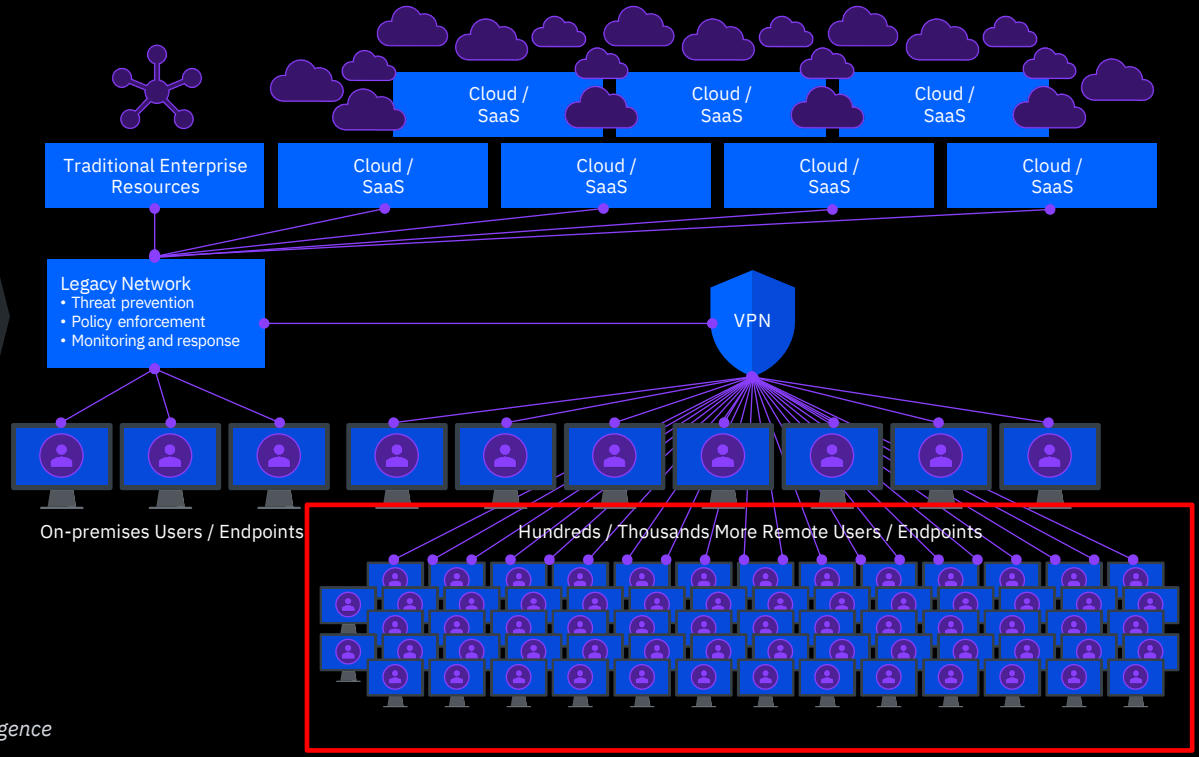
Gartner, Guide to Endpoint Security Concepts, Dec. 2020

全球疫情的流行與後疫情時代，勒索軟體的興起和零信任的採用，迫使企業重新考慮整體安全性

傳統的企業資訊架構



現代化企業日漸複雜的資訊架構



Source: Scott Crawford, 451 Research, part of S&P Global Market Intelligence

關於 ReaQta

REAQTA

- Founded in 2014 by elite cybersecurity professionals with deep AI / ML expertise
- Headquarters in **Amsterdam** and **Singapore**
  - Start-Ups with 30+ employees
- Acquired by IBM from 2021 as XDR Solution

MITRE ENGENUITY | ATT&CK Evaluations

- #1 in Attack Coverage per Alert Generated
- #2 in Alerts Actionability
- #2 in Alerts Quality
- #3 in captured Telemetry
- 90% of attack contained

European Commission

SEAL OF EXCELLENCE

Gartner COOL VENDOR 2020

FROST & SULLIVAN 2020 BEST PRACTICES AWARD

ENTERPRISE SECURITY TOP 10 ENDPOINT SECURITY SOLUTION PROVIDERS 2020

市調機構與行業評比獎項

- Gartner 網路和端點安全領域的酷供應商 (Cool Vendor), 2020
- Frost & Sullivan's European Technology Innovation Award 歐洲行為網路威脅檢測技術創新獎 - 2020
- Enterprise Security Magazine 歐洲十大端點安全解決方案提供商, 2019 - 2020
- EDR of choice from the 2020新加坡網絡安全行業網絡安全局呼籲創新 (2020 Call for Innovation)

Gartner peerinsights customers' choice 2021™

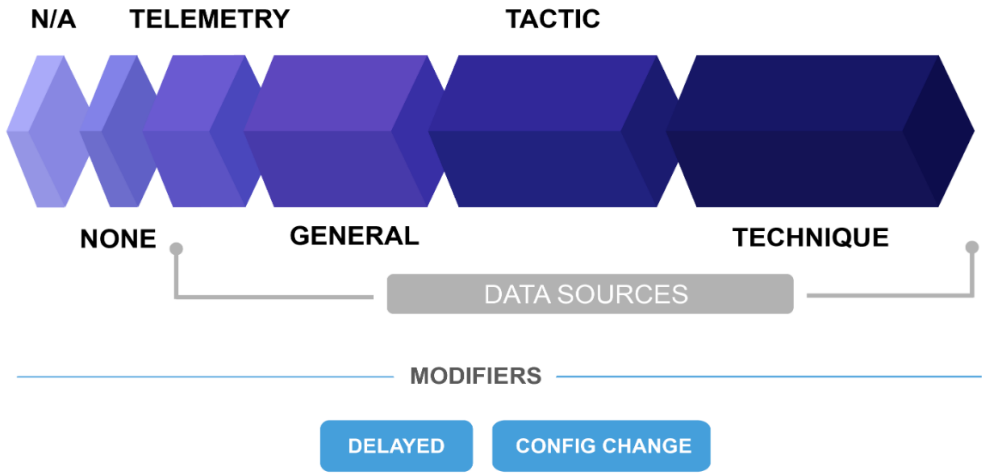
"Endpoint Security without the extra headache or headcount!"
- Energy and Utilities Company

"Great to have a silent assassin in your corner!" - Financial Company

WIZARD SPIDER AND SANDWORM DETECTION CATEGORIES

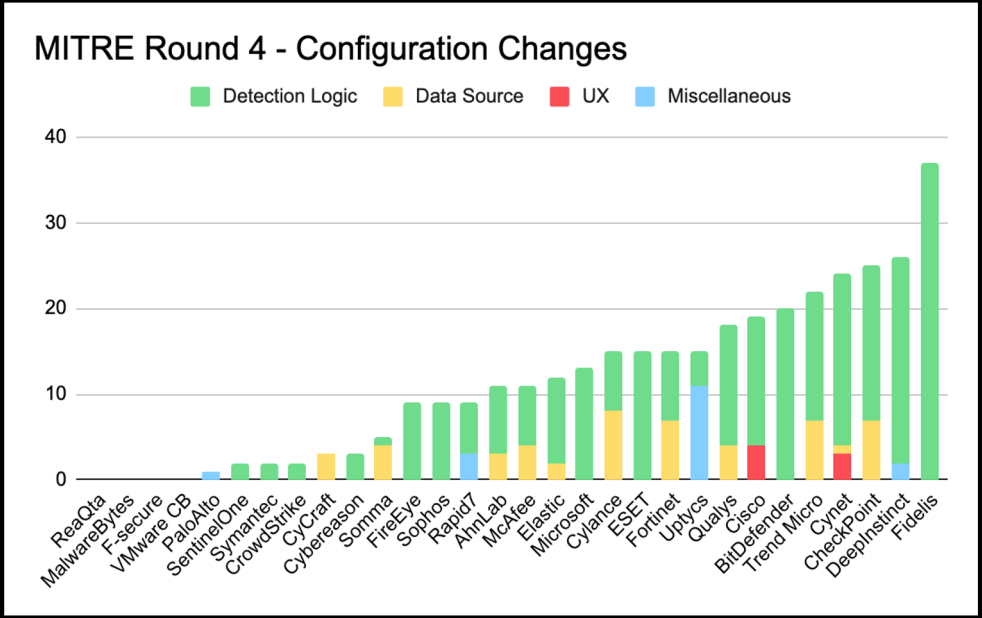
The evaluation focuses on articulating how detections occur, rather than assigning scores to vendor capabilities.

We organize detections according to each substep (i.e., implementation of a technique). For a detection to be included for a given substep, it must apply to the specific technique-under-test (i.e., the detection must apply to the one technique associated with that substep, not other or all techniques of that Step). For each detection, we require that proof/evidence be provided to us, but we may not include all detection details in public results, particularly when those details are sensitive. While we make every effort to capture all relevant detections, vendor capabilities may be able to detect procedures in ways that we did not capture.



MITRE ATT&CK 評測結果

100% 偵測整個網路攻擊鏈的攻擊測試
No configuration changes 在測試期間沒有調整相關設定



MITRE | REAQTA

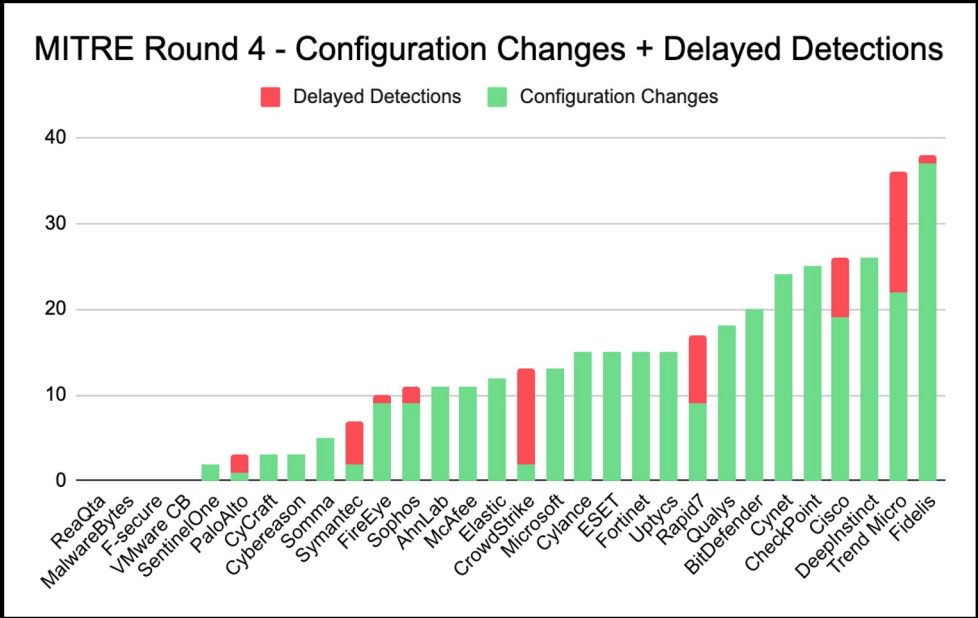
ReaQta-Hive 在**測試過程沒有更改軟體配置參數的情況，達到 100% 的檢測效果**。在一般情況，軟體的配置更改有助於供應商隨著攻擊的進展調整他們的檢測方式、機制與參數，而在這輪評比裡，大多數供應商必須多次調整他們的產品“天線”才能檢測到威脅警報。

Why is this Important ?

在現實生活場景中，配置更改通常是不切實際的。因為實際威脅在進入下一步前，攻擊者不會給防御者第二次機會來調整他們的檢測。意即，如果一個平台需要多次配置更改才能以最高效率運行——或檢測一個主動威脅——那它的自主檢測能力不可避免地會受到損害，就像它的實時響應能力一樣。

MITRE ATT&CK 評測結果

100% 偵測整個網路攻擊鏈的攻擊測試
No configuration changes 在測試期間沒有調整相關設定



在本輪的測試過程使用 ReaQta 的行為分析引擎，所有**檢測結果都是完全即時的 (Real-Time) 反映、沒有延遲的時間**。當攻擊的每一步都在發生時 ReaQta 都能夠有效進行跟踪，最大限度地降低丟失重要事件的風險，而不是因爲其他友商需要等待一些外部模組分析後才能提供偵測能力。

Why is this Important ?

隨著攻擊者的創新，自動化允許攻擊者在網路中極快地移動。 過去需要幾分鐘或幾小時的操作現在只需幾秒鐘。 立即識別和自動響應在完全受損的基礎設施和不成功的破壞之間劃清界限。

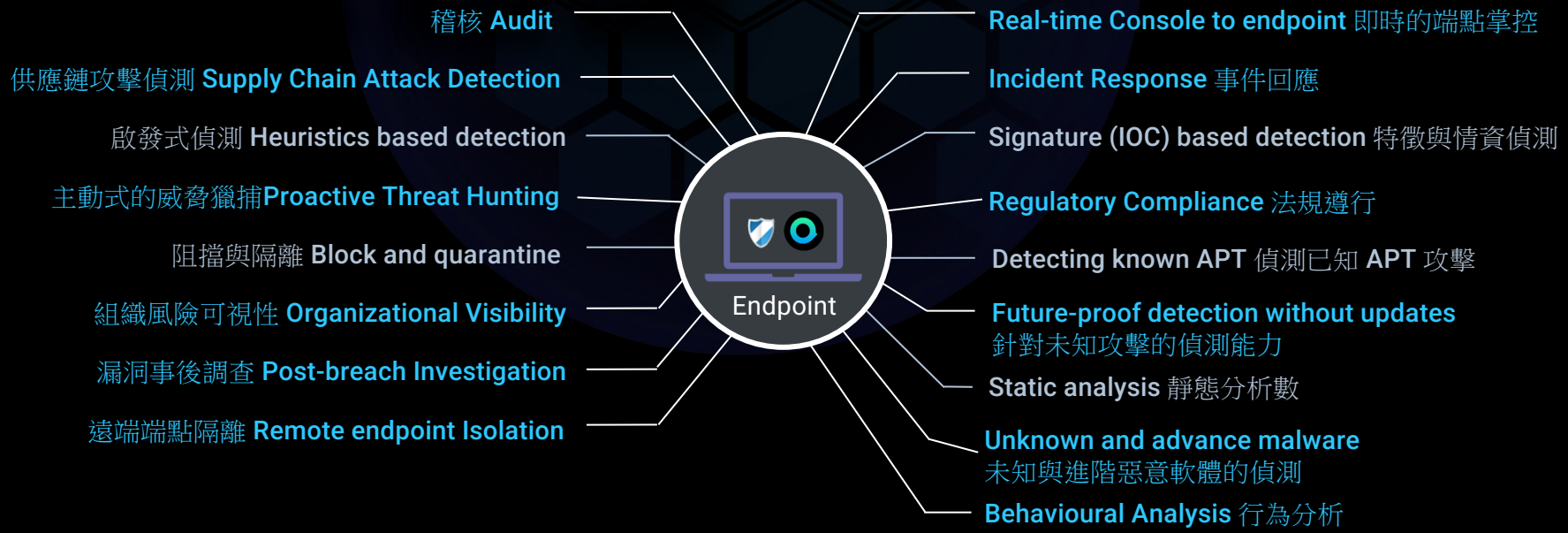
MITRE | REAQTA

Why Endpoint Detection & Response, EDR?

IBM

防毒 ANTI VIRUS + 最完善的 EDR 解決方案 BEST-IN-CLASS EDR

基本保護 Basic Protection | Behavioral Analysis | Threat Hunting | Risk and Compliance | CERT | IT Audit



REAQTA

ReaQta 採用領先的人工智慧
提供 **端點偵測與回應** 的解決方案

ReaQta 的端點安全解決方案利用 AI 自動
識別和管理威脅，同時讓對手無法檢測到

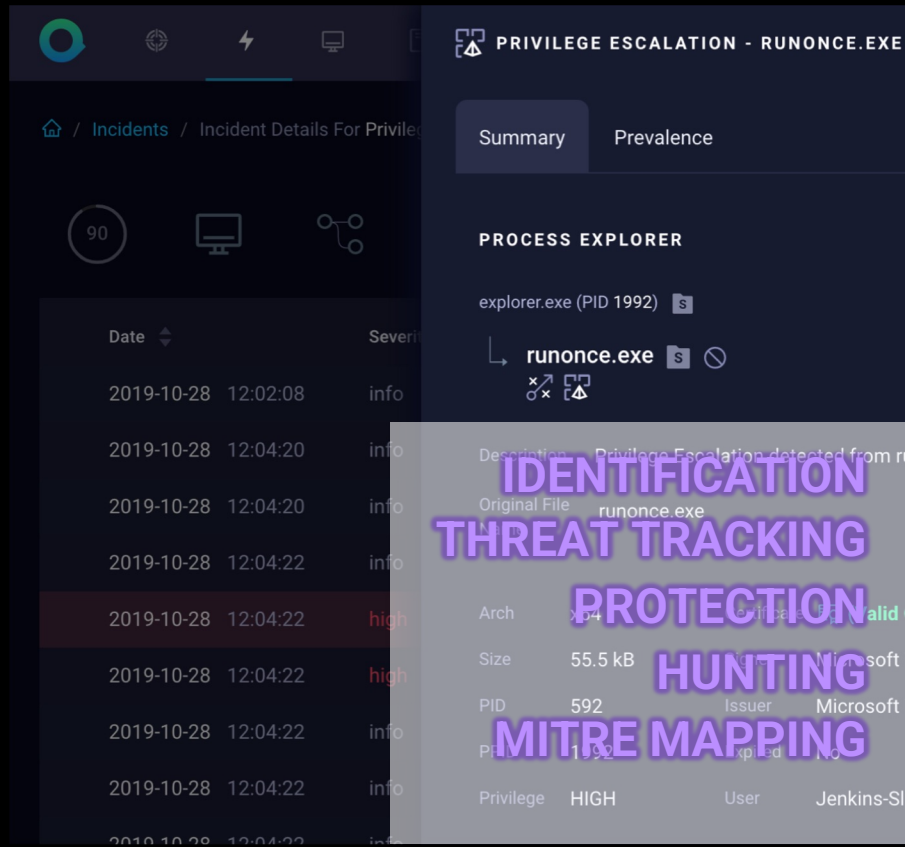
Endpoint Detection & Response, EDR
ReaQta-Hive 統一執行偵測 (detection)、回應 (response) 以及自動化威脅獵捕

Live-hypervisor based monitoring

Data-mining to find advanced threats

Managed Detection and Response (MDR) Services
24/7/365 ReaQta-MDR 服務

Single Agent, Multiple Deployment Options
支援 desktop, Server, cloud and mobile operating systems 環境，
以 SaaS, on-premises or in air-gapped environments 方式部署



Why ReaQta? 與其它 EDR 解決方案的 **優勢與差異點** 是？

世界領先與
唯一採用 **Nano OS**

NANO OS

Live-Hypervisor
based monitoring

- 從底層監控作業系統 (OS) 任何活動
- 提供對應用程式生命週期的完整可見性和洞察力
- 對惡意軟體而言是不可見，無法被駭客關閉
- 進階惡意行為的進階偵測機制：
  - 鍵盤記錄、動態模擬、憑據收集、
  - 內核漏洞利用、屏幕截圖

120+ 參數模組與
70+ 行為偵測模型

ADVANCED THREAT DETECTION

Automated AI-driven
threat detection

- 70+ 部署在端點的行為模型
- 120+ 所有檢測和狩獵需求的特定參數
- 只需單擊一下即可即時遠程移除特定程序進行修補
- 允許用戶建立自己的偵測策略和劇本

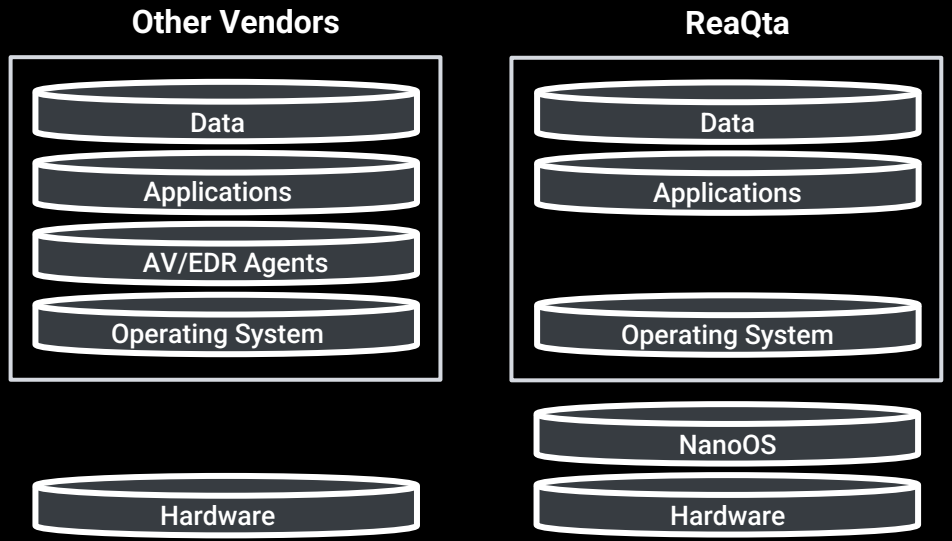
降低高達 **80%**
以上的假警報

CYBER ASSISTANT

One-shot learning system

- 從分析師的決策中學習並採取行動
- 為分析師騰出時間專注於更進階的威脅分析
- 適用於單個客戶或多租戶 (MSSP) 模式

Zooming in on NanoOS



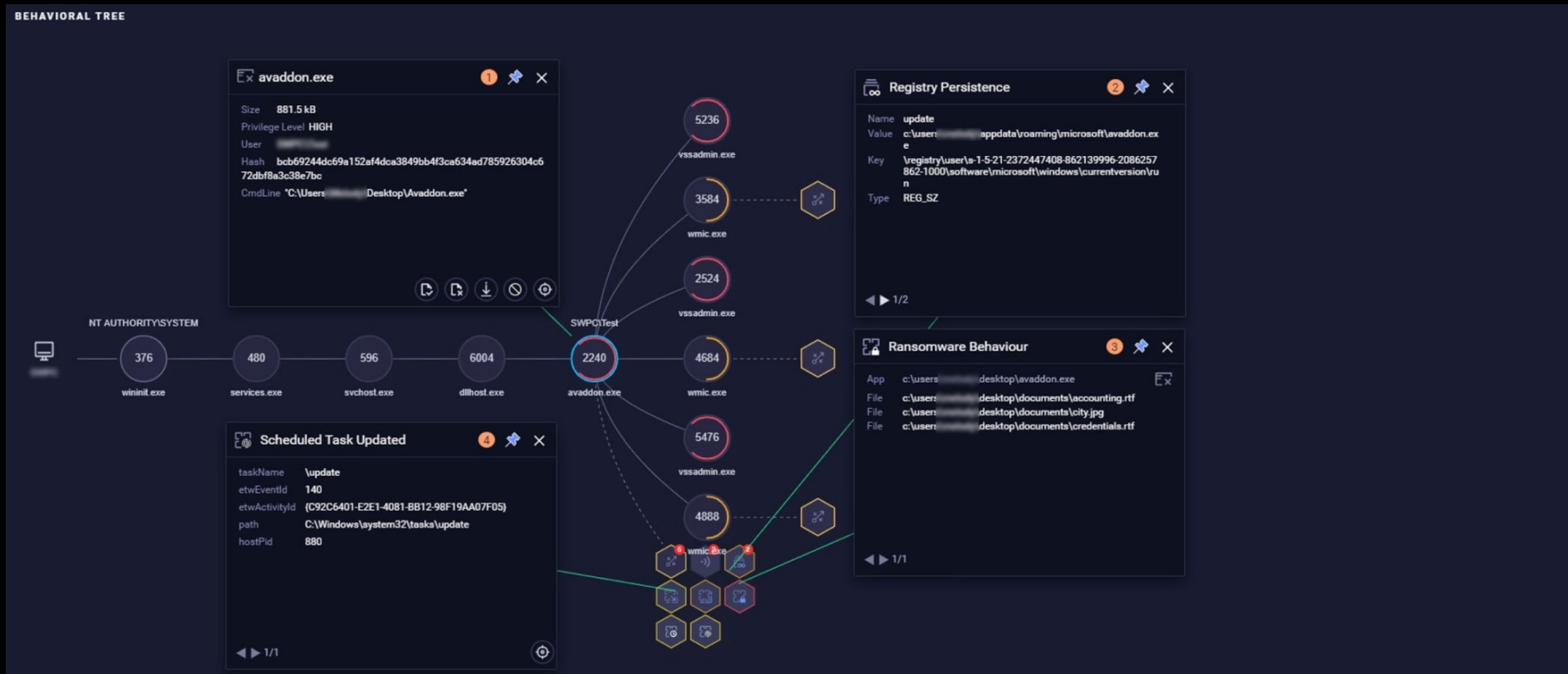
Benefits

> Protects the Whole Stack
> Invisible to Attackers
> Cannot be Shut Down

REAQTA
an IBM Company

ReaQta in action: 勒索軟體的 早期偵測 (Early-Warning)

通過直接在端點上利用人工智能和自動化，ReaQta 檢測勒索軟件行為並即時主動緩解威脅

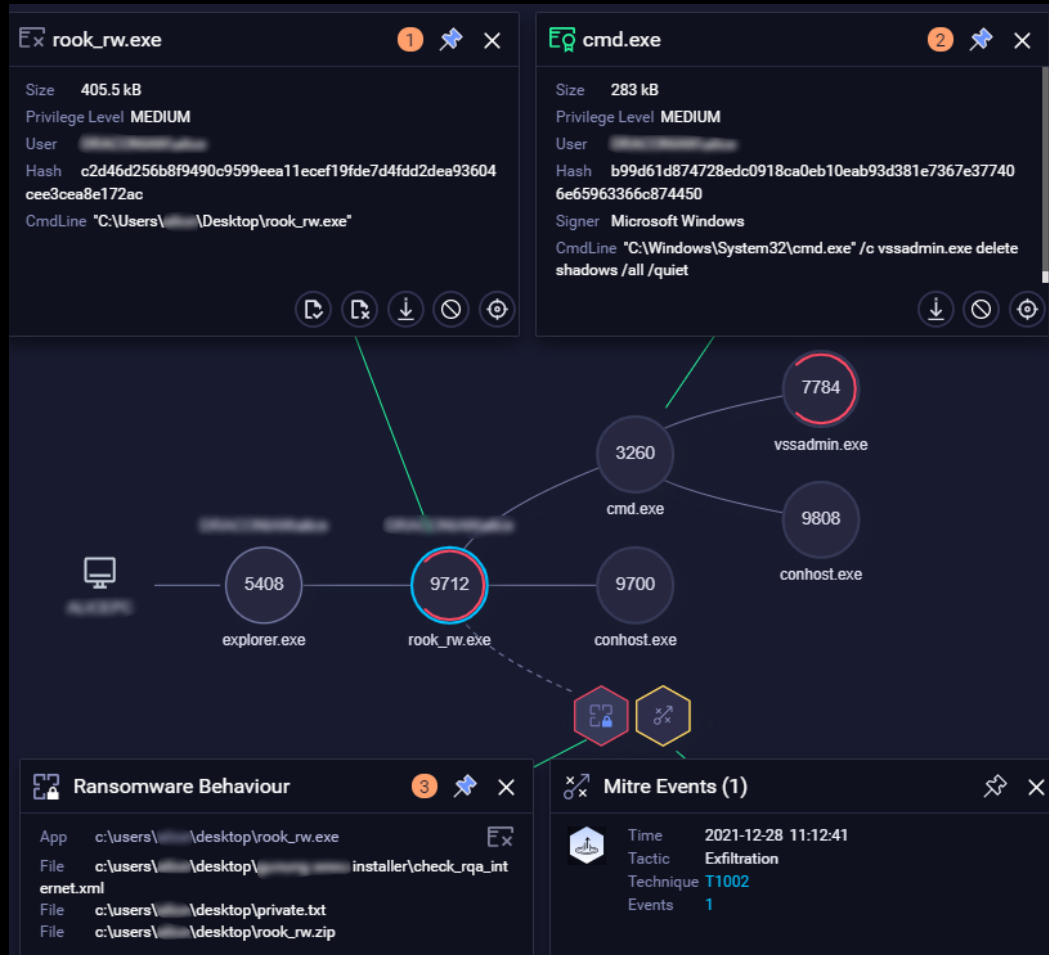


ReaQta in action: 勒索軟體的 早期偵測 (Early-Warning)

ReaQta 通過直接在端點上利用 AI 和自動化，幫助檢測 Rook Ransomware (RaaS) 並即時主動緩解。

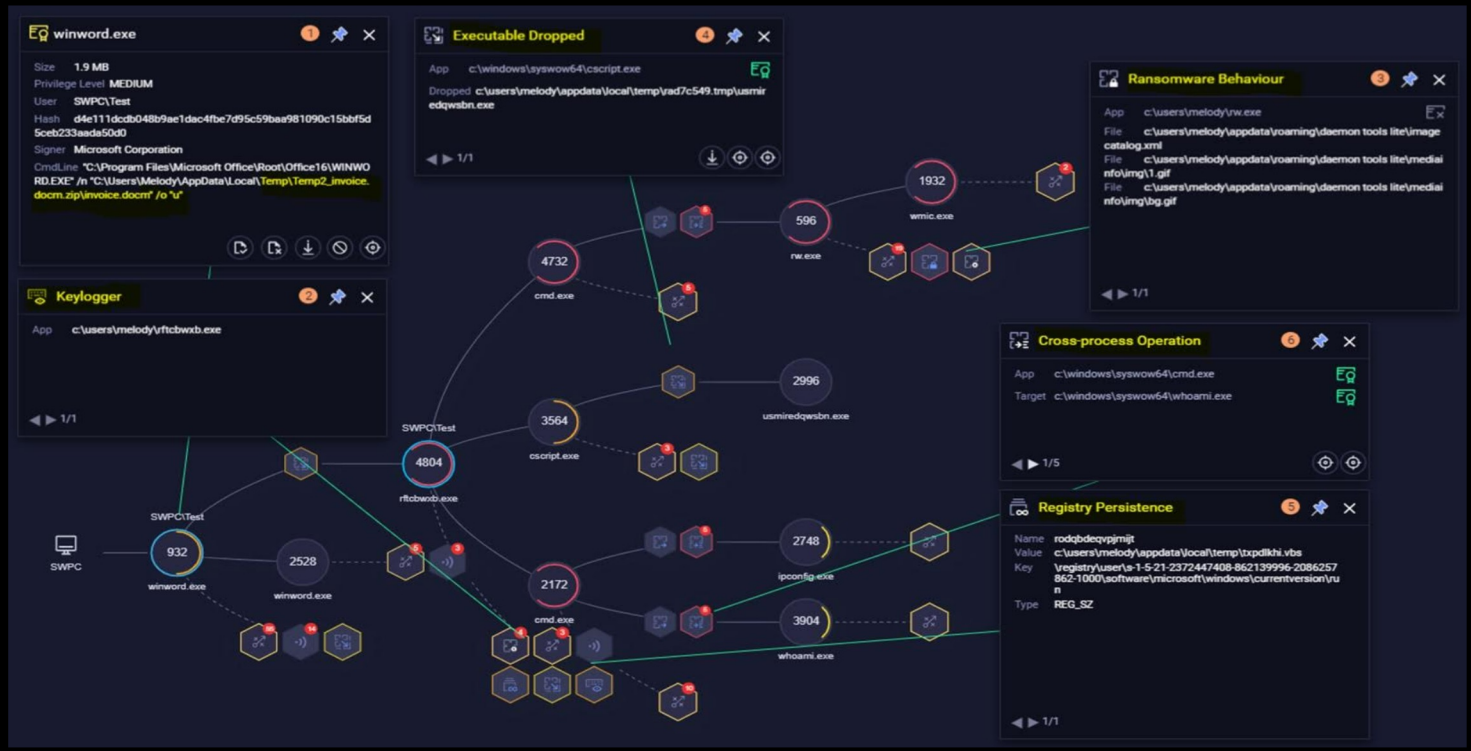
Key capabilities

- 使用行為引擎檢測未知的勒索軟件變種
- 分析文件活動和訪問，如果檢測到加密嘗試並且進程鏈可疑，則阻止程序，並即時恢復加密文件
- 針對硬碟上和內存中的已知變體使用基於簽名的資料保護



ReaQta 行為樹 (behavioral tree) 與其他 EDR 解決方案不同？

Ans: 我們在行為數（威脅拓撲）階段提供所有訊息，都可以支持
分析師進行初步調查、識別並讓分析師立即隔離機器與清除威脅。



REAQTA

ReaQta 行為樹 (behavioral tree) 與其他 EDR 解決方案不同？

Ans: 除了顯示事件情節外，它還可以隔離觸發點並且允許直接從行為樹進行補救。

* **A**ttached the screenshot (behavioral tree.jpg) to show a behavioral tree with multiple endpoints.

REAQTA

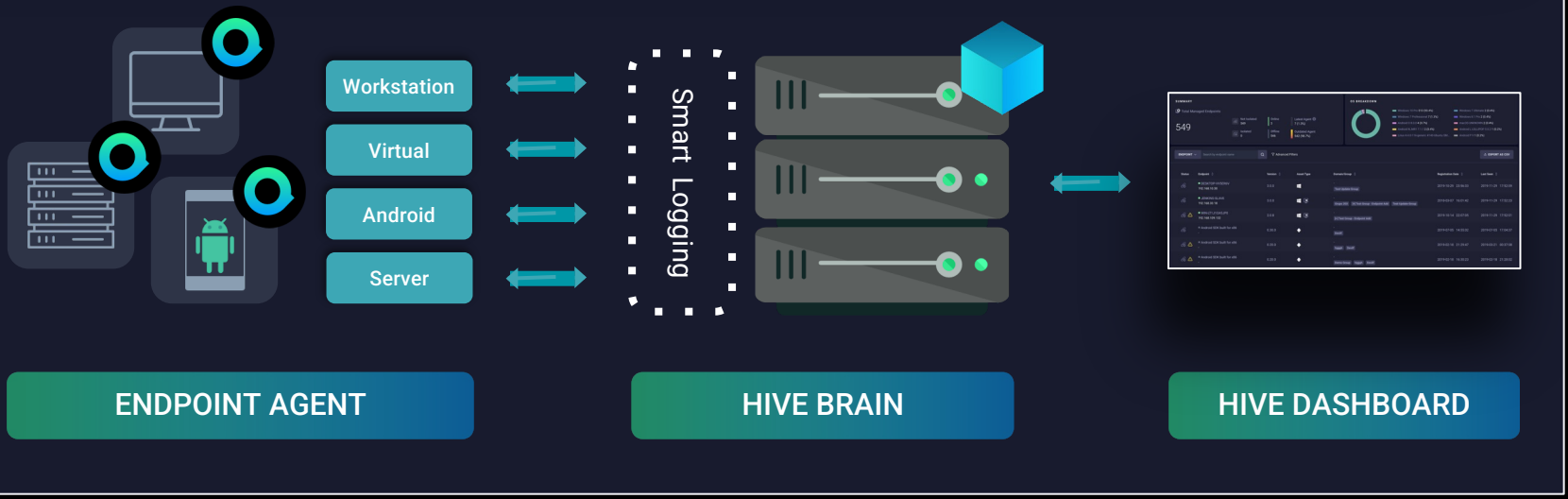
ARCHITECTURE

Learn • Detect • Track • Respond • Protect

Endpoint AI & Nano OS
Real-Time Coverage

Infrastructural AI
Data Collection & Behavioral Analysis

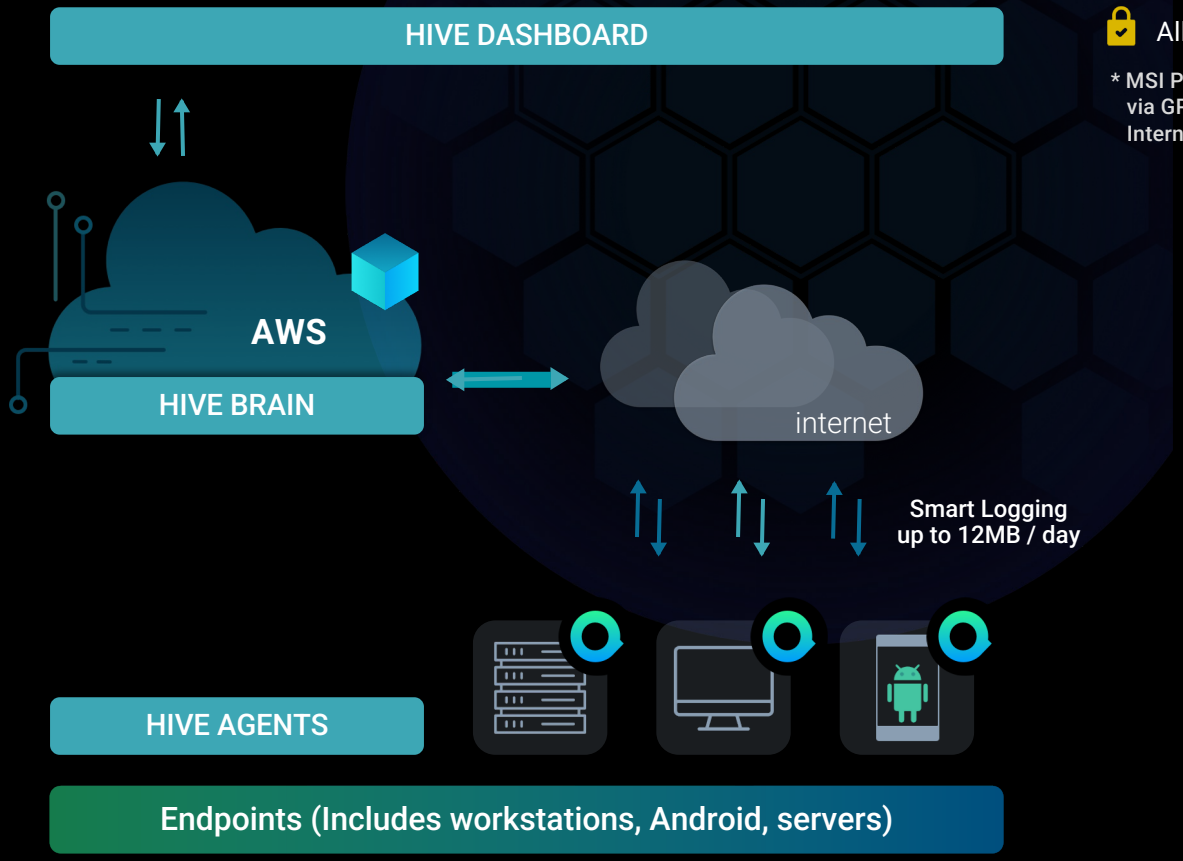
Single Console
Optimised Remediation Workflow



REAQTA

DEPLOYMENT

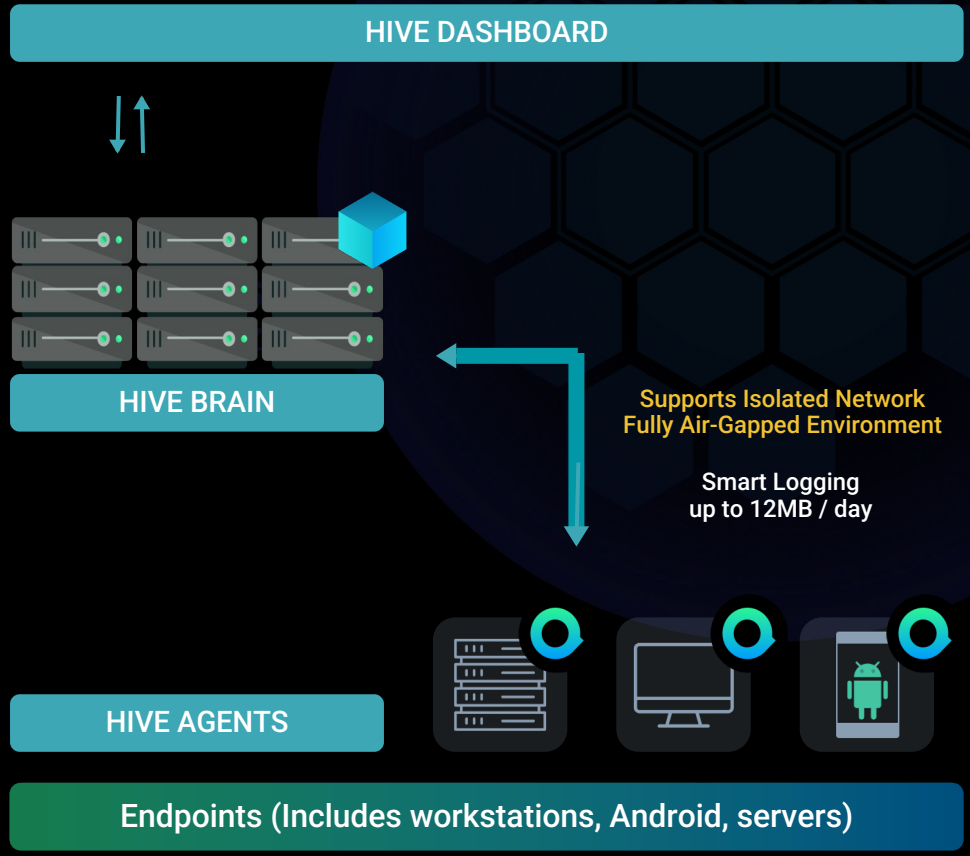
CLOUD



REAQTA

DEPLOYMENT

ON-PREM



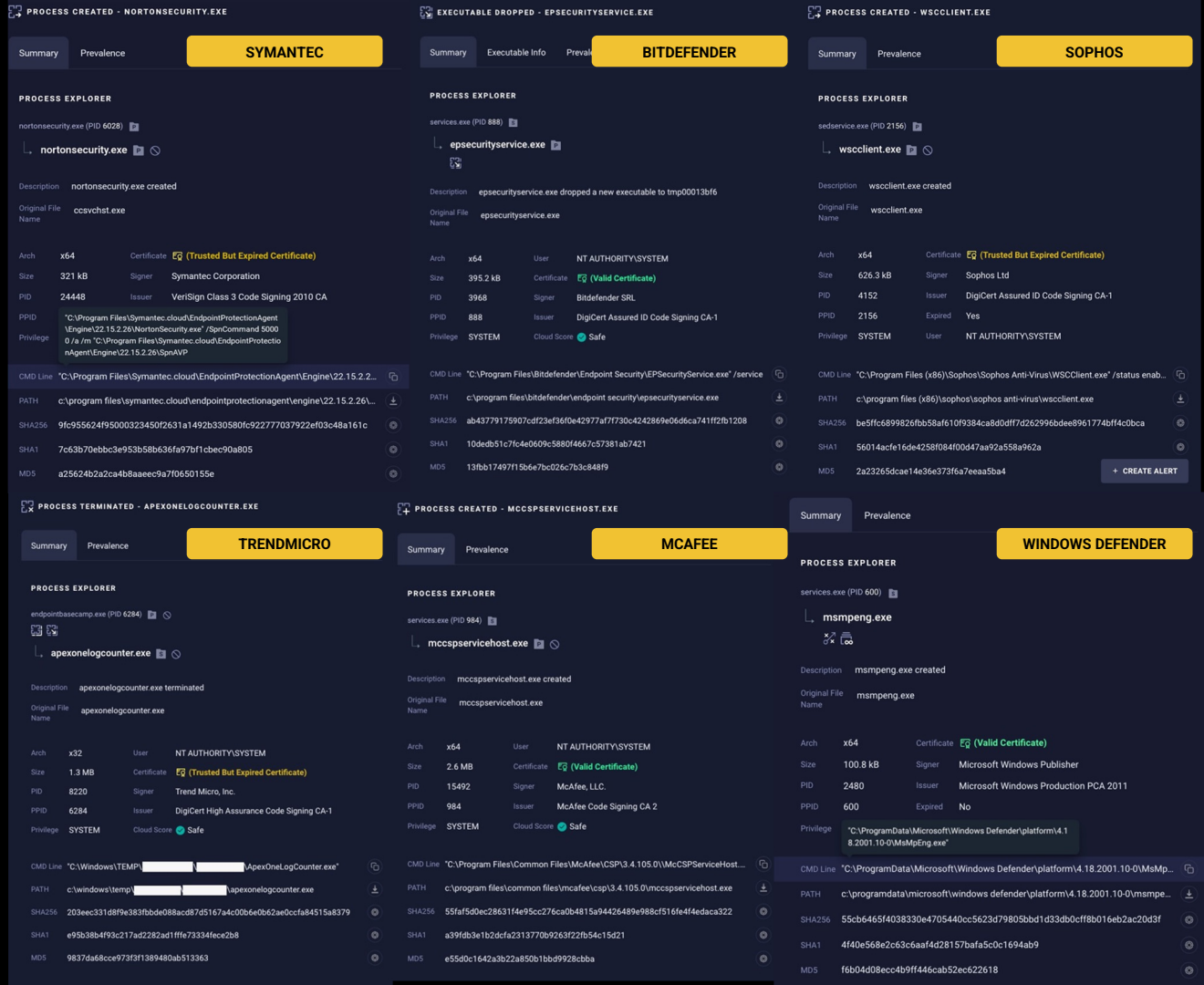
All Network Traffic

* MSI Package Deployment via GPO (15Mb) with no Internet required

REAQTA

ReaQta-Hive coexists with **any** Antivirus solutions to provide an enhanced layer of **security**, **visibility** and **control**.

REAQTA



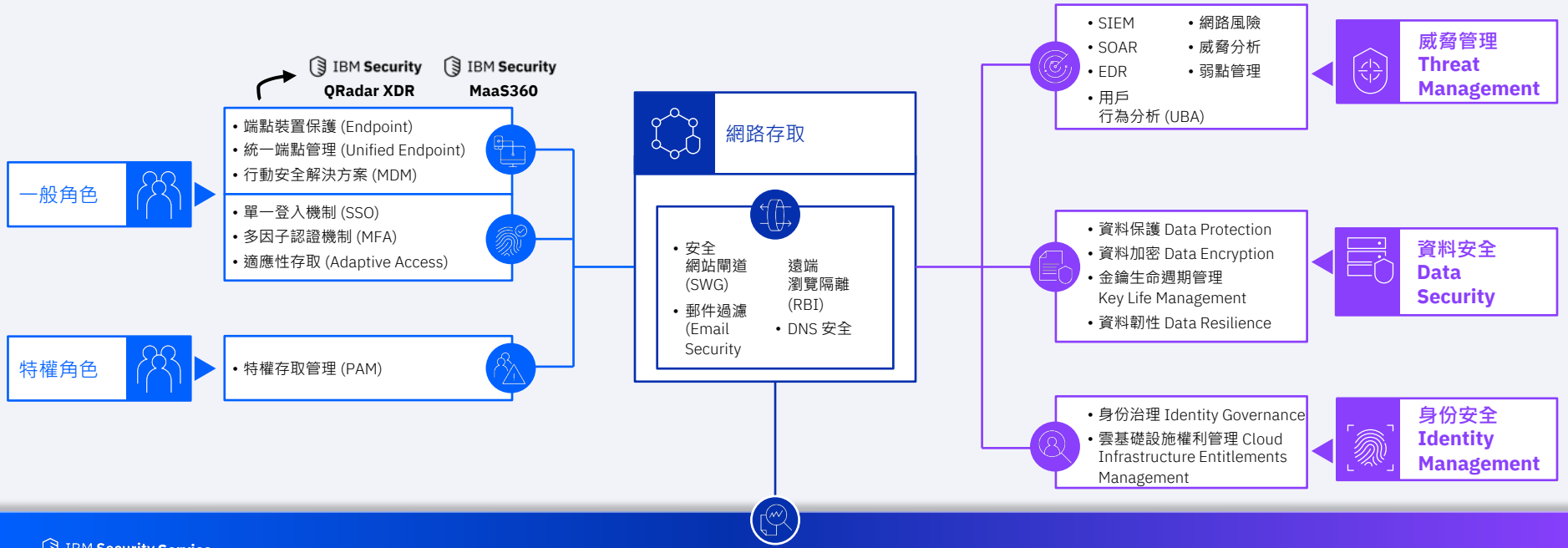
ReaQta 支援的作業系統類型？

Windows	7 (SP1), 8, 8.1, 10, 10-POS, 11
Windows Server	2008R2(SP2), 2012, 2016, 2019
Linux	Ubuntu (16 / 18), Centos 7, Debian 8.10, RedHat 7, Mint 18+
Mac OS	Sierra+
Android	4.2+

MDM (asset management / BYOD)

IBM Security™ End-to-end 的零信任 (Zero-Trust) 資安解決方案

... powered by the industry's only open, unified security platform



IBM Security Service

Zero Trust Acceleration Services
Ransomware Readiness Assessment
Risk Quantification Services
Incident Response Retainer
X-Force Threat Management

支援混合雲各式工作負載環境的資訊安全保護

Data Center | IaaS and PaaS | SaaS and Web

Unified endpoint management, or UEM, has evolved from EMM and MDM and...

...helps IT and security teams improve user productivity, reduce threats, and maintain compliance

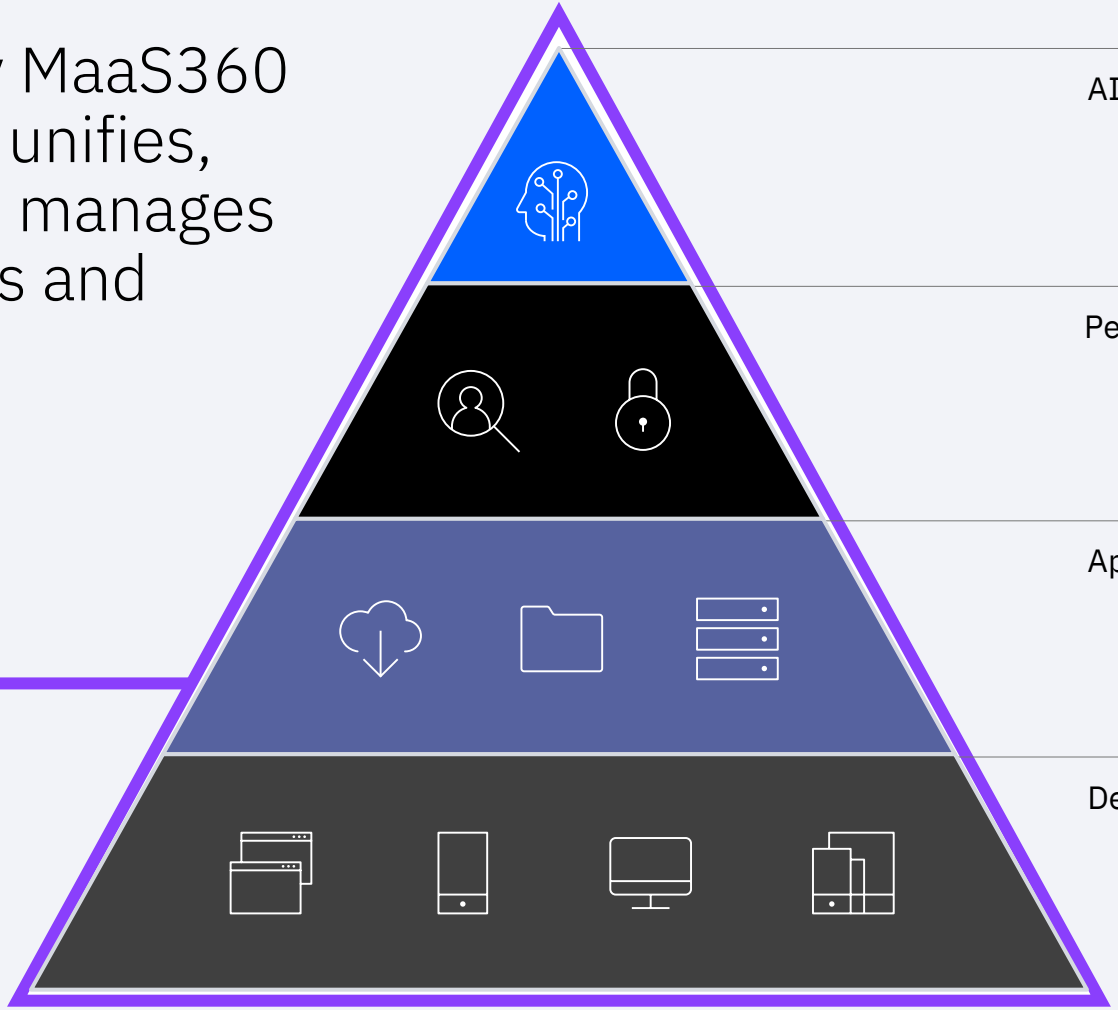
A single console to configure and manage smartphones, tablets, laptops, kiosks and IoT

Unify the application of:
- Device configuration
- Data protection
- Usage and security policies
- UX and productivity

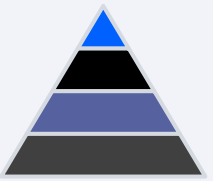
A single, user-centric view to enhance end-user support and gather workplace analytics

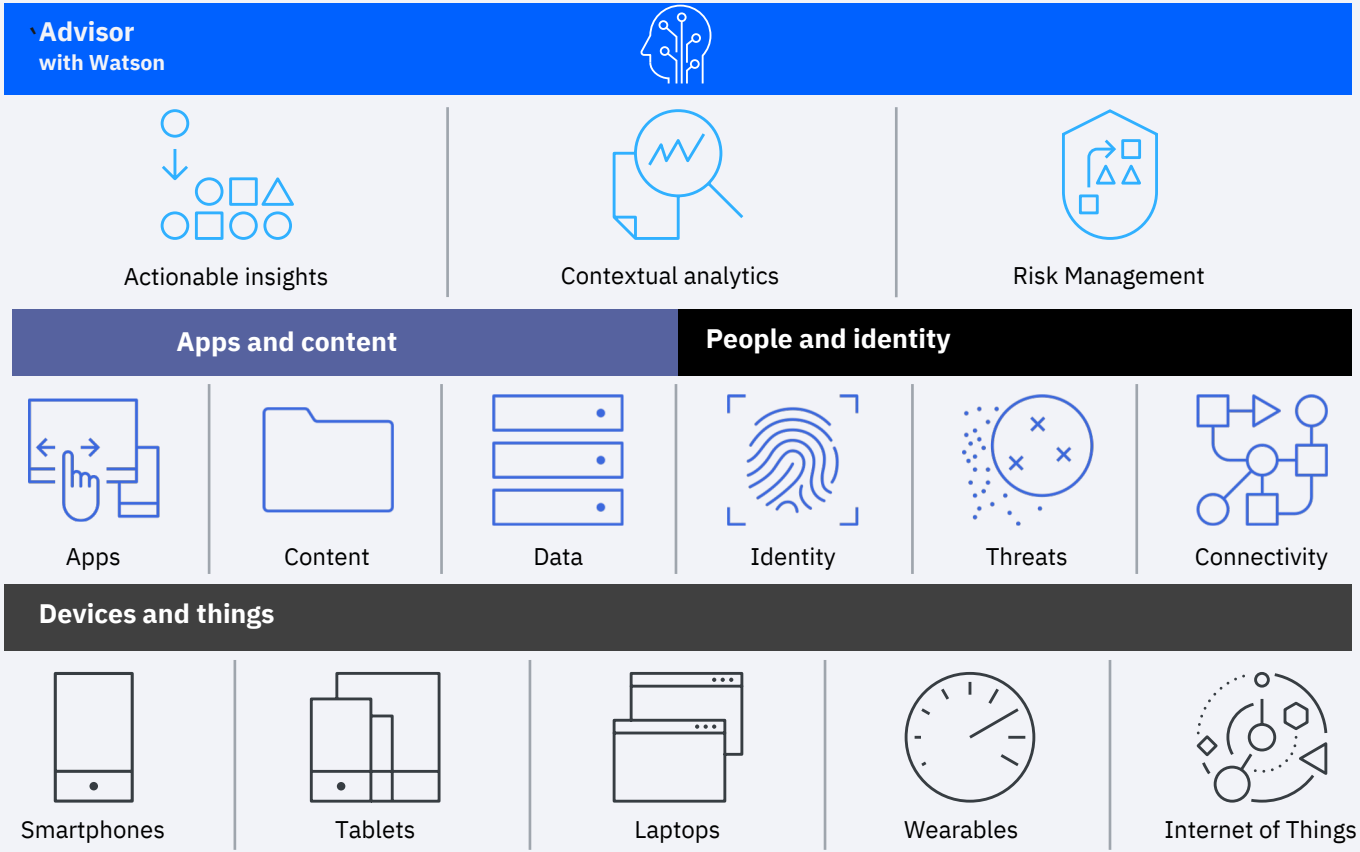
integration point with key related technologies (SIEM, IAM, CMT)

IBM Security MaaS360 with Watson unifies, secures, and manages devices, apps and users

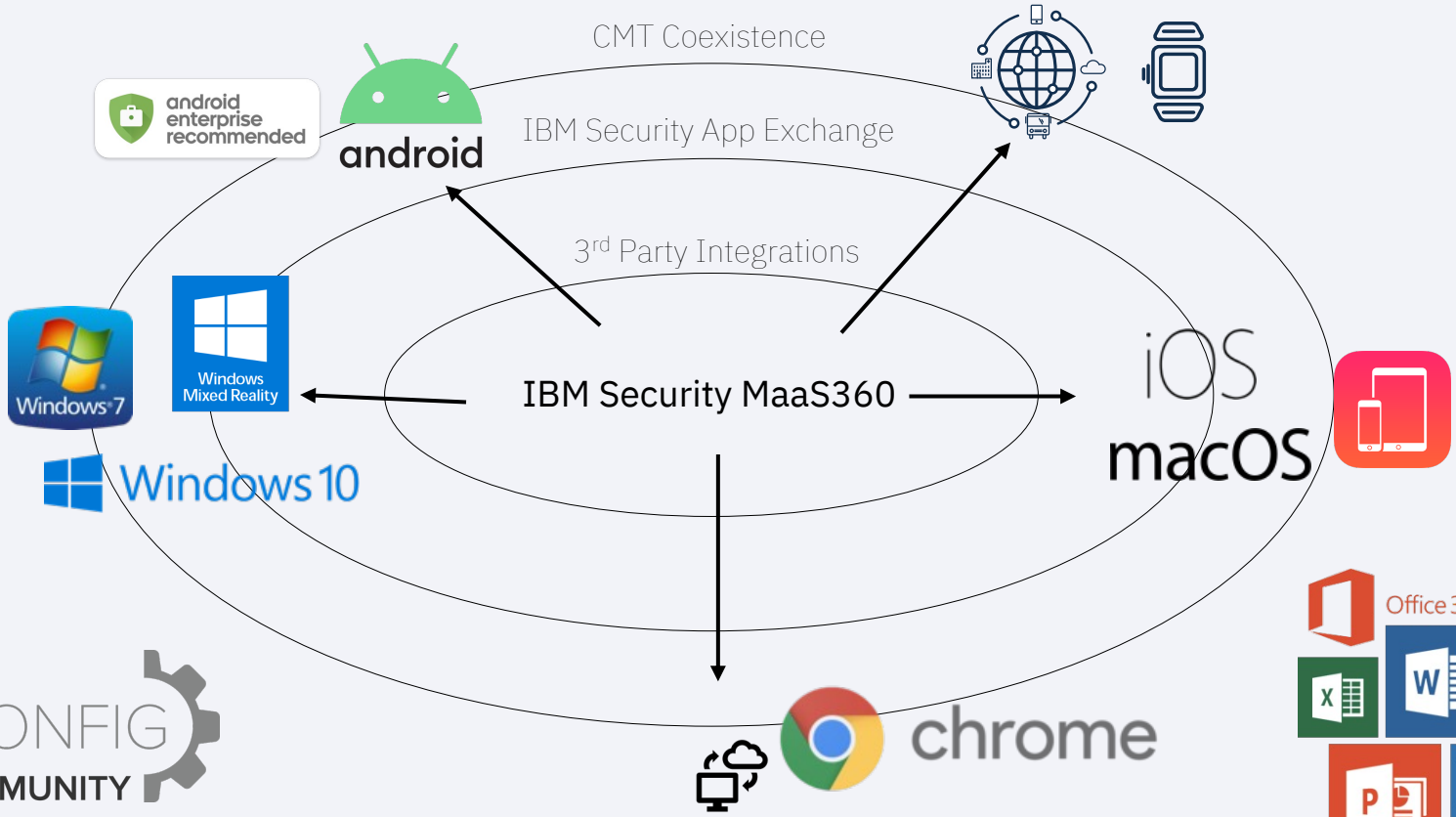


IBM Security MaaS360 with Watson



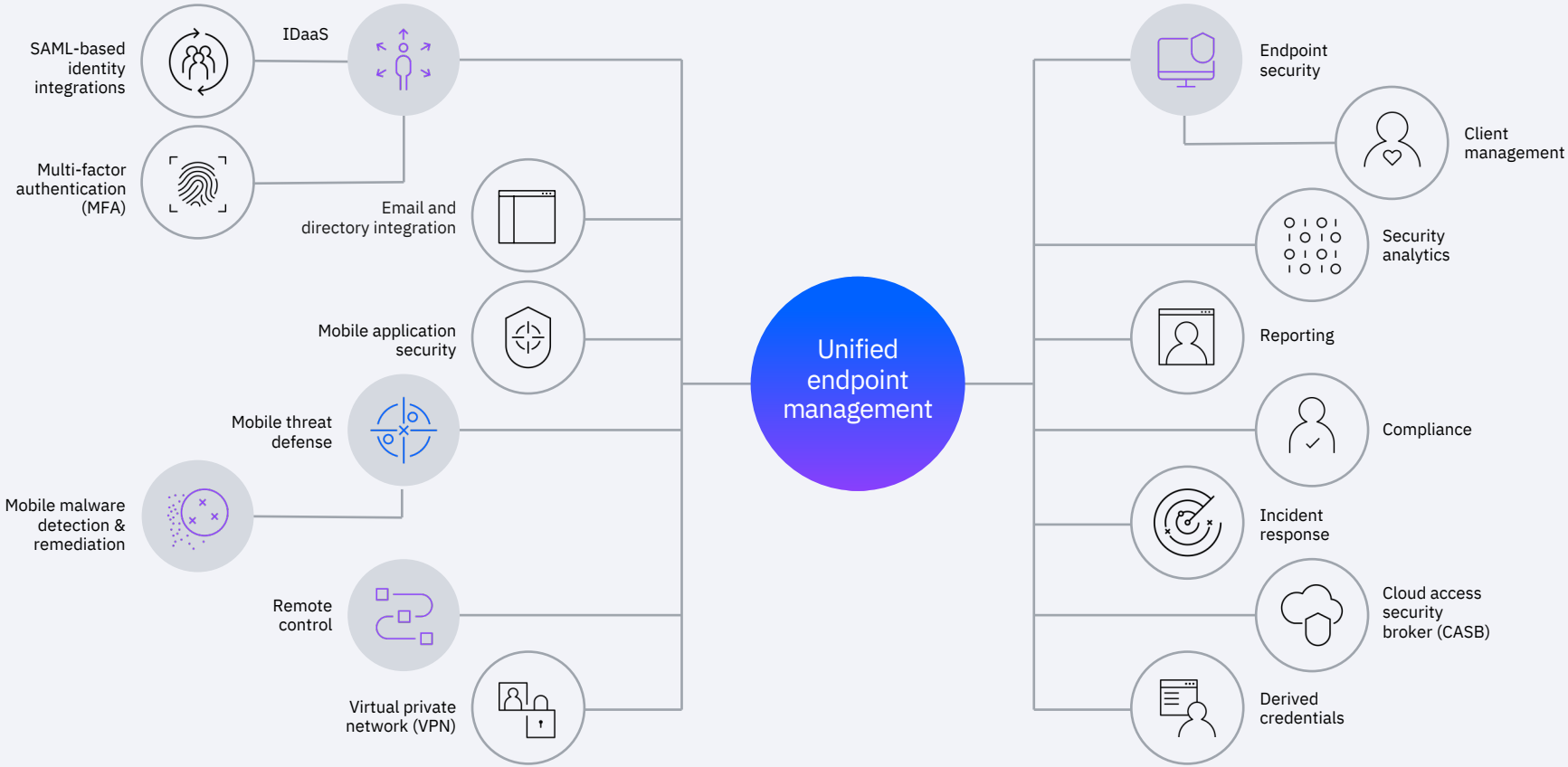


IBM MaaS360 is *Open* for Business



APPCONFIG COMMUNITY

Integrated with your enterprise security tools



iOS / iPhone MaaS360 操作示範

IBM Security MaaS360 + Apple Business Manager

Power on device

IBM Security MaaS360 + Apple Business Manager

決定哪些初始化步驟要省略：

- iCloud
- Apple Watch migration
- Siri
- Passcode
- Location
- Home button sensitivity
- Android migration
- And more...

IBM Security MaaS360 + Apple Business Manager

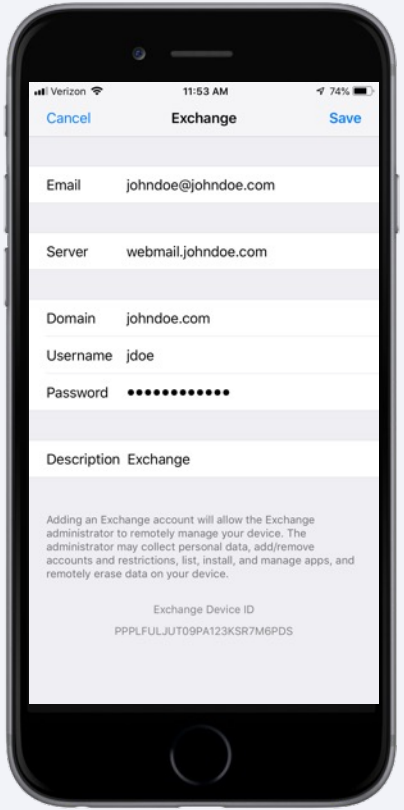
自動安裝企業允許的應用程式白名單

Automatically install applications

IBM Security MaaS360 + Apple Business Manager

自動設定電子郵件相關帳號資訊

Automatically configure email



IBM Security MaaS360 + Apple Business Manager

限制或移除企業機構不允許的應用程式
Restrict/Remove unwanted applications

IBM Security MaaS360 + Apple Business Manager

尚未套用安全政策之前相機 App 功能存在

IBM Security MaaS360 + Apple Business Manager

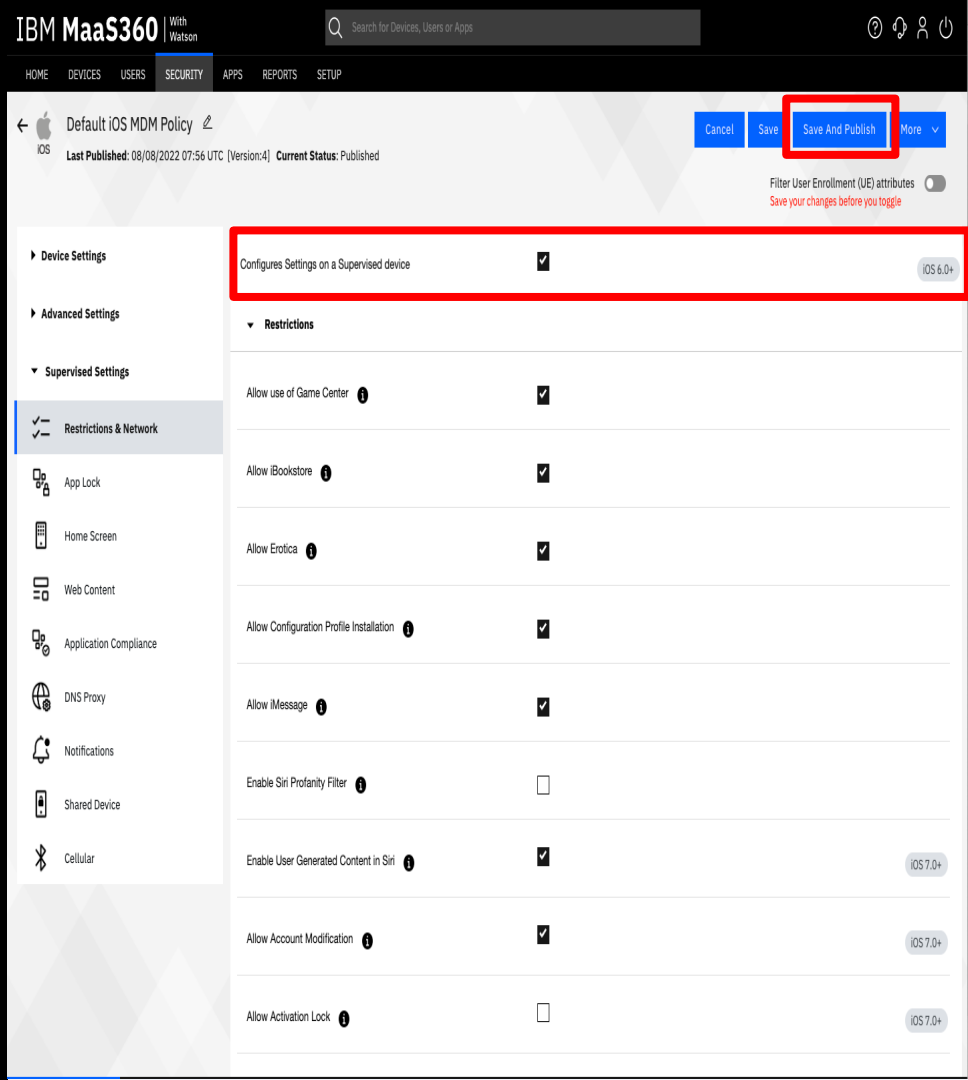
行動裝置下載與安裝企業專屬的 MaaS360 App

IBM Security MaaS360 + Apple Business Manager

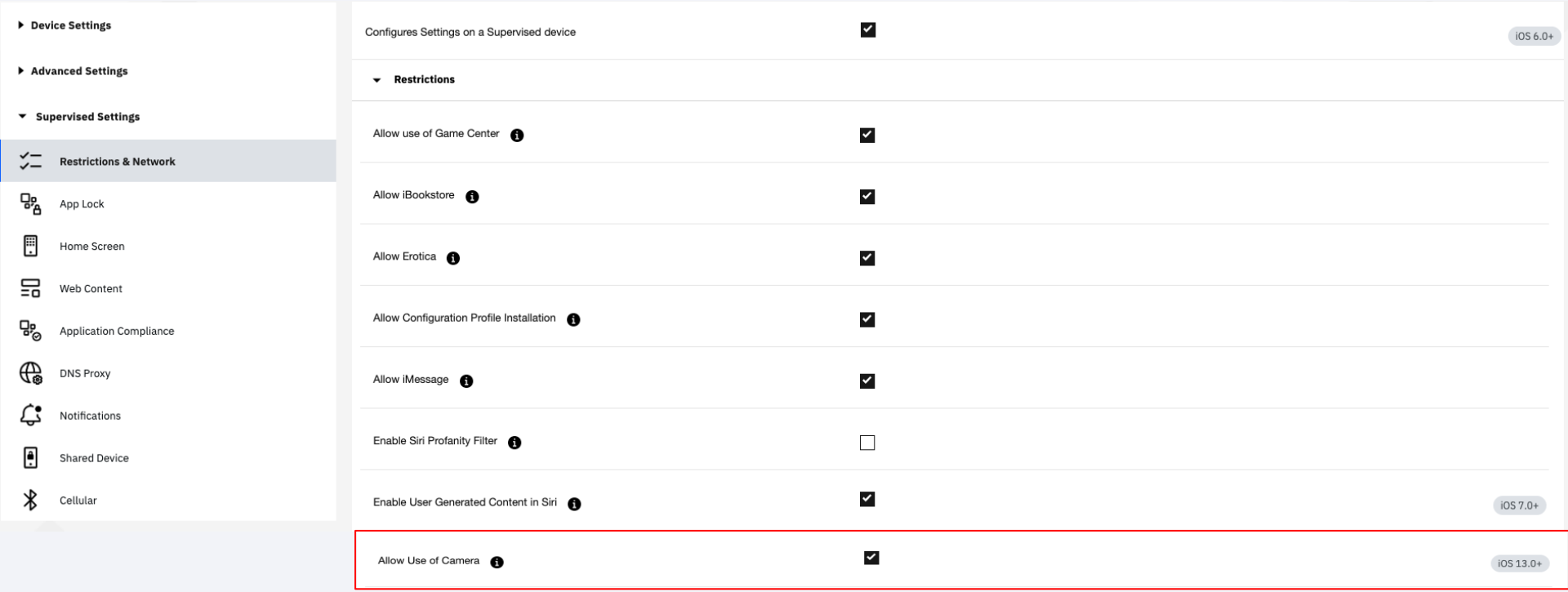
登入 MaaS360 App 主畫面，查看相關資訊

IBM Security MaaS360 + Apple Business Manager

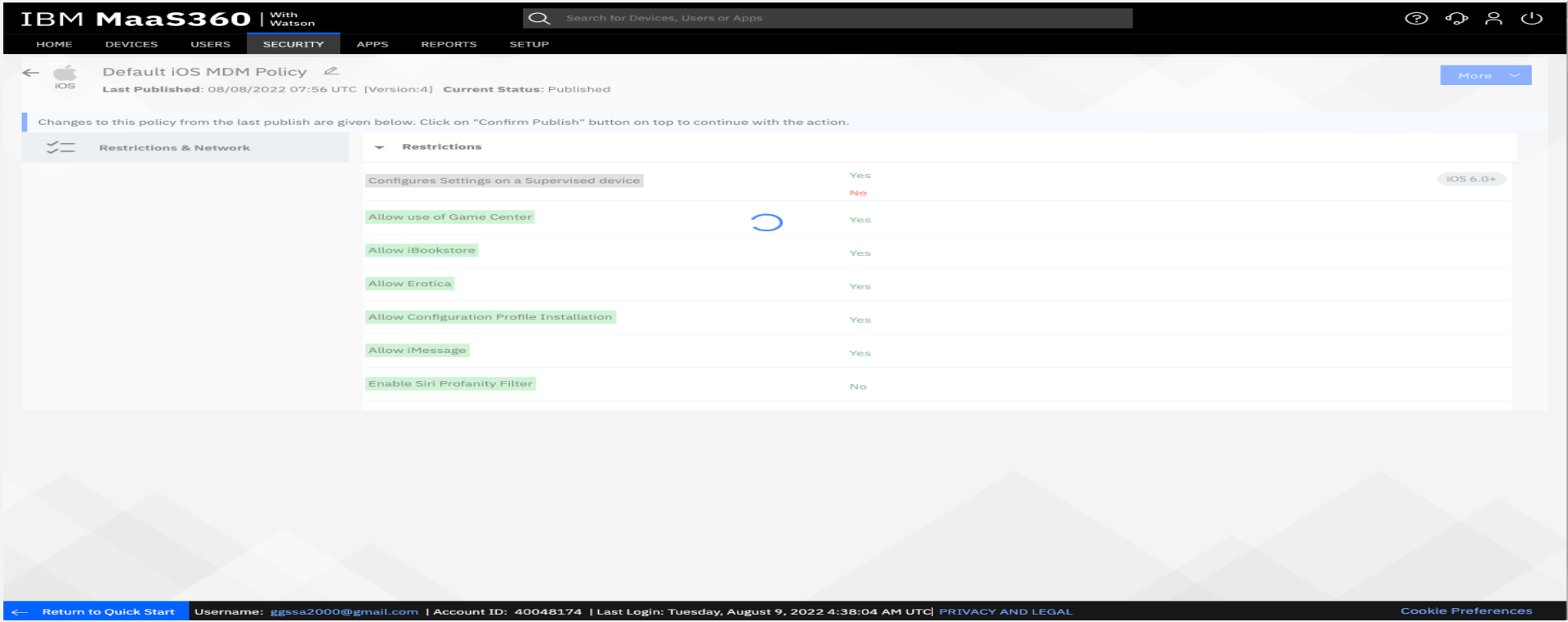
在 Web 端管理中心設定安全政策（關閉相機功能）



行動裝置管理解決方案 (MDM)
限制 iOS 裝置是否允許/關閉相機功能

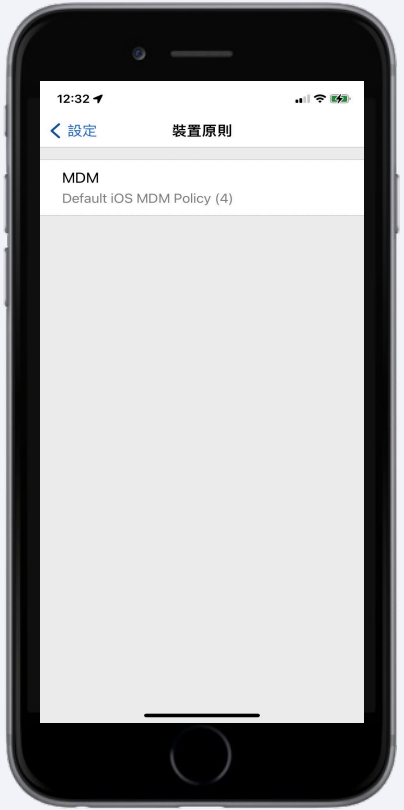


行動裝置管理解決方案 (MDM)
新的安全政策派送中的過程畫面



IBM Security MaaS360 + Apple Business Manager

確認最新版本的安全政策已派送至手機端



IBM Security MaaS360 + Apple Business Manager

iOS / iPhone 的相機功能App已消失

IBM Security MaaS360 + Apple Business Manager

其他 App 在存取相機時會提示「提供權限」字樣。

IBM Security MaaS360 + Apple Business Manager

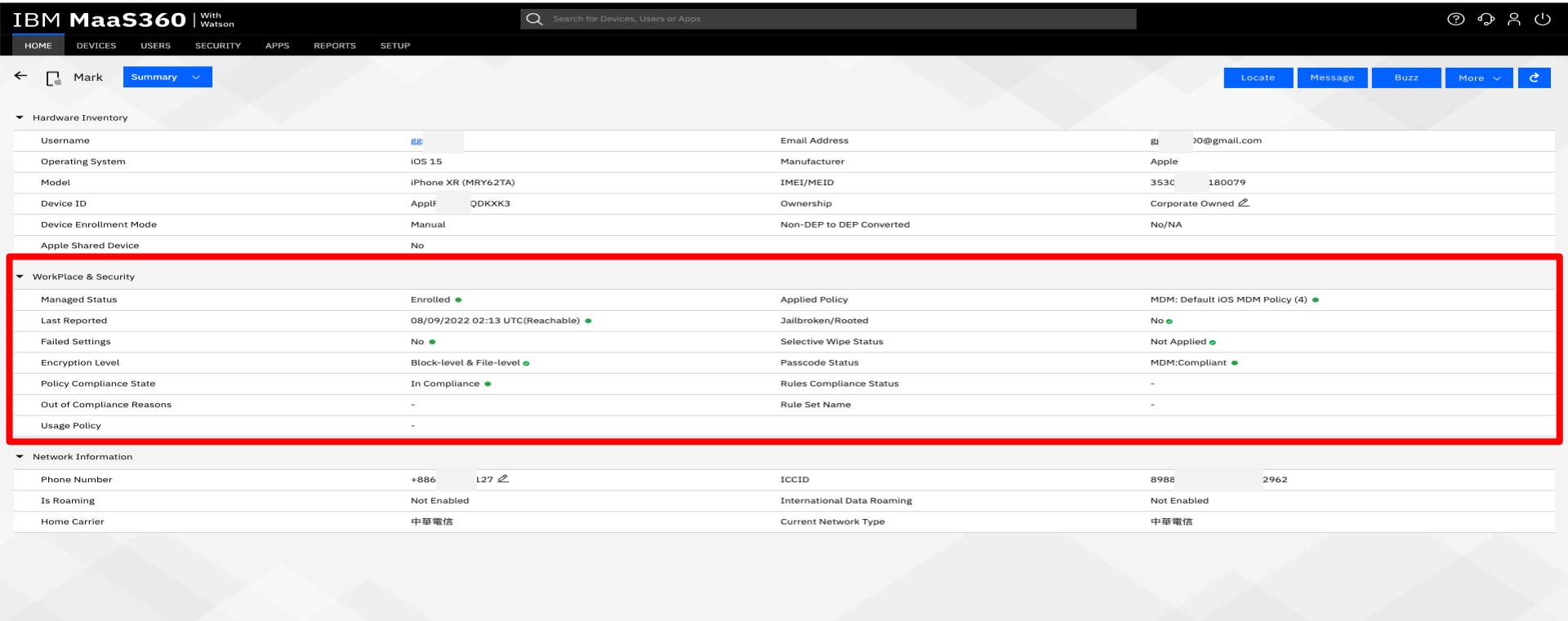
其他 App 在存取相機時會提示「提供權限」字樣。

IBM Security MaaS360 + Apple Business Manager

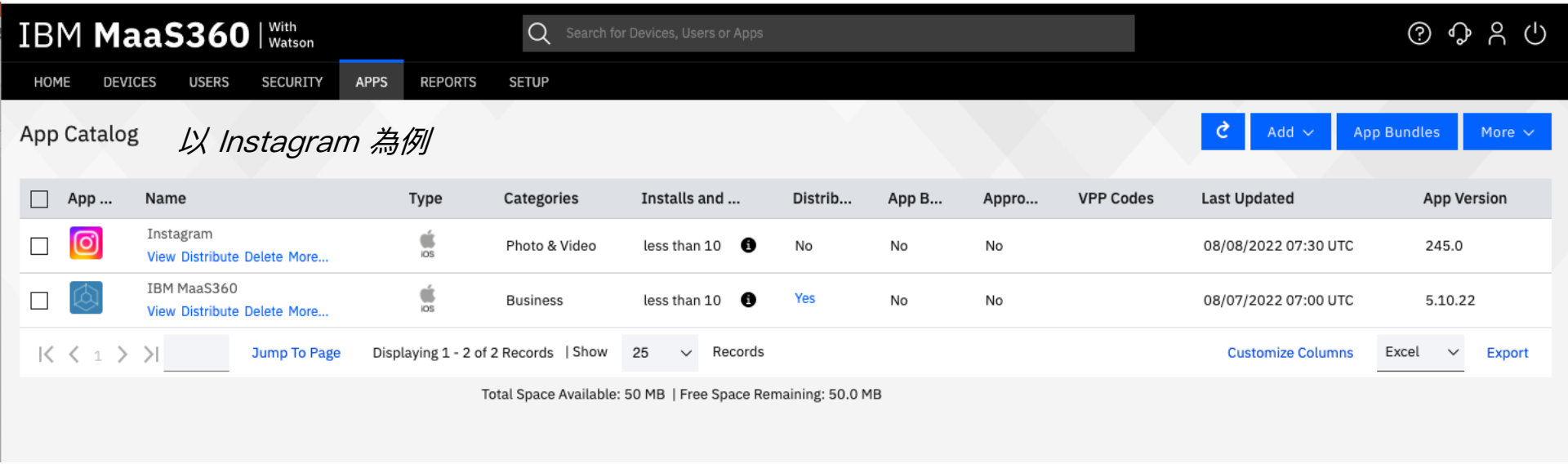
既使 該 App 本身相機權限有開啟，但 Global 層級的相機功能已經關閉，故相關 App 即無法使用相機功能

MaaS360
管理介面說明

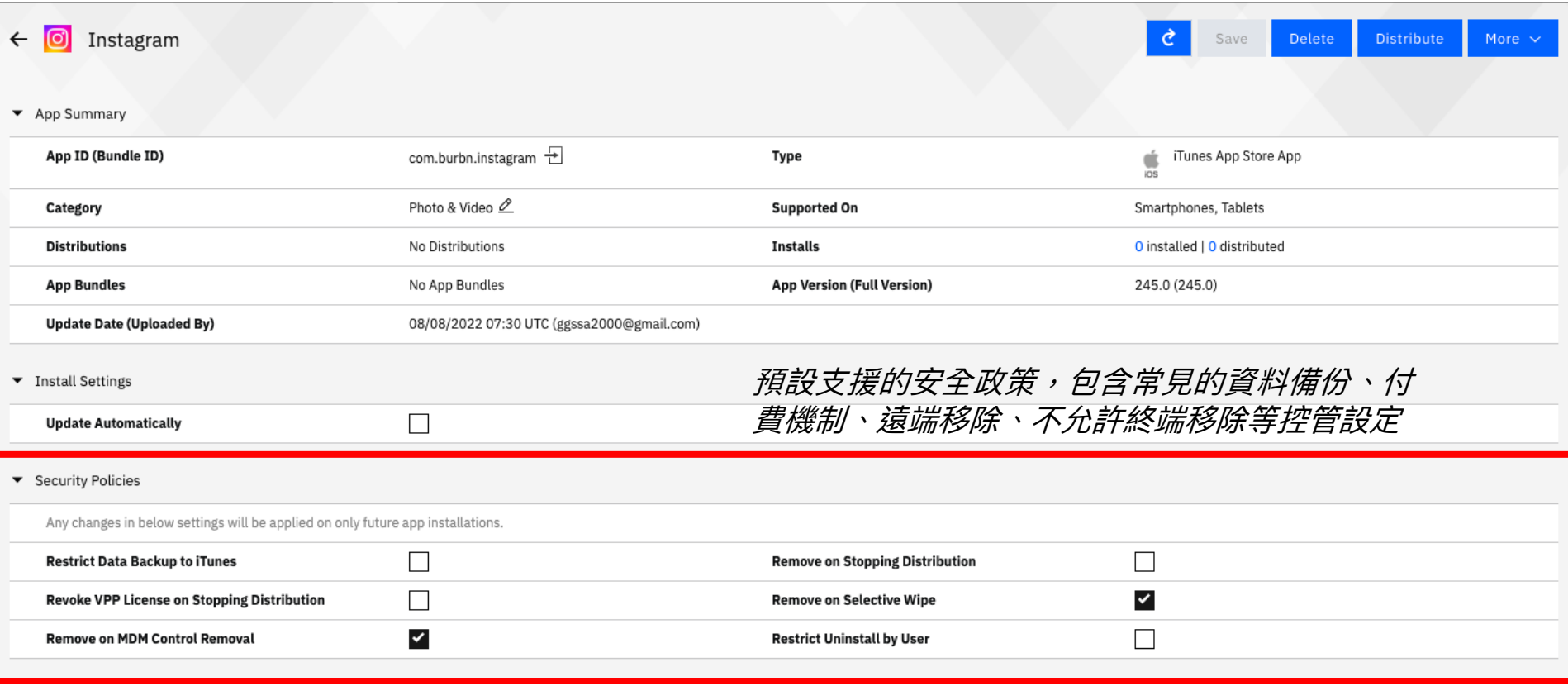
行動裝置管理解決方案 (MDM)
行動裝置資產管理 (iPhone XR for example)



行動裝置管理解決方案 (MDM)
行動裝置應用程式白名單 (App Catalog)

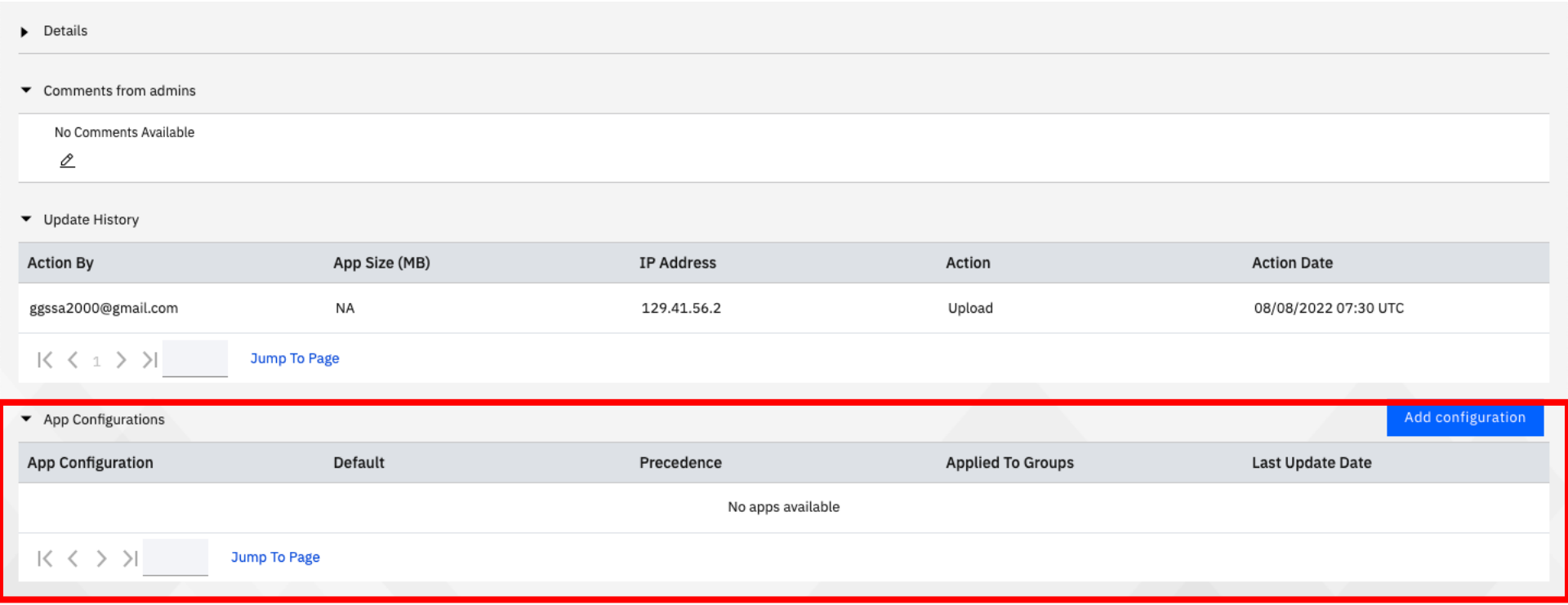


行動裝置管理解決方案 (MDM)
行動裝置應用程式管控細節 (App Security Policies)

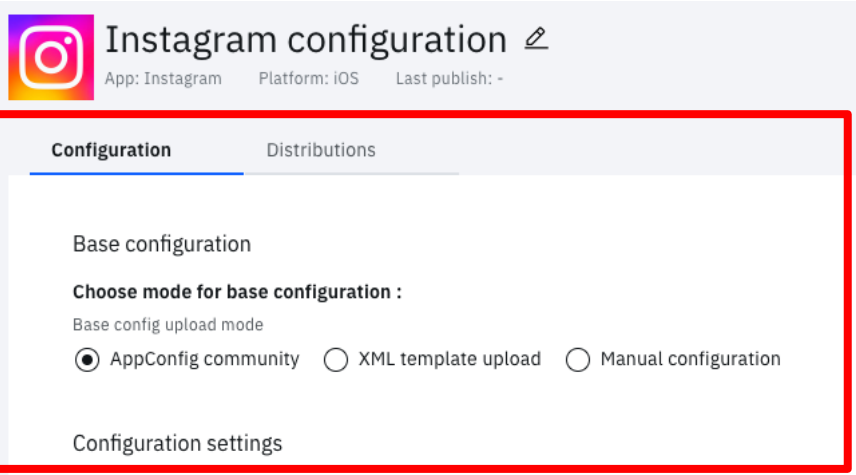


預設支援的安全政策，包含常見的資料備份、付費機制、遠端移除、不允許終端移除等控管設定

行動裝置管理解決方案 (MDM)
行動裝置應用程式設定管理 (App Configurations)

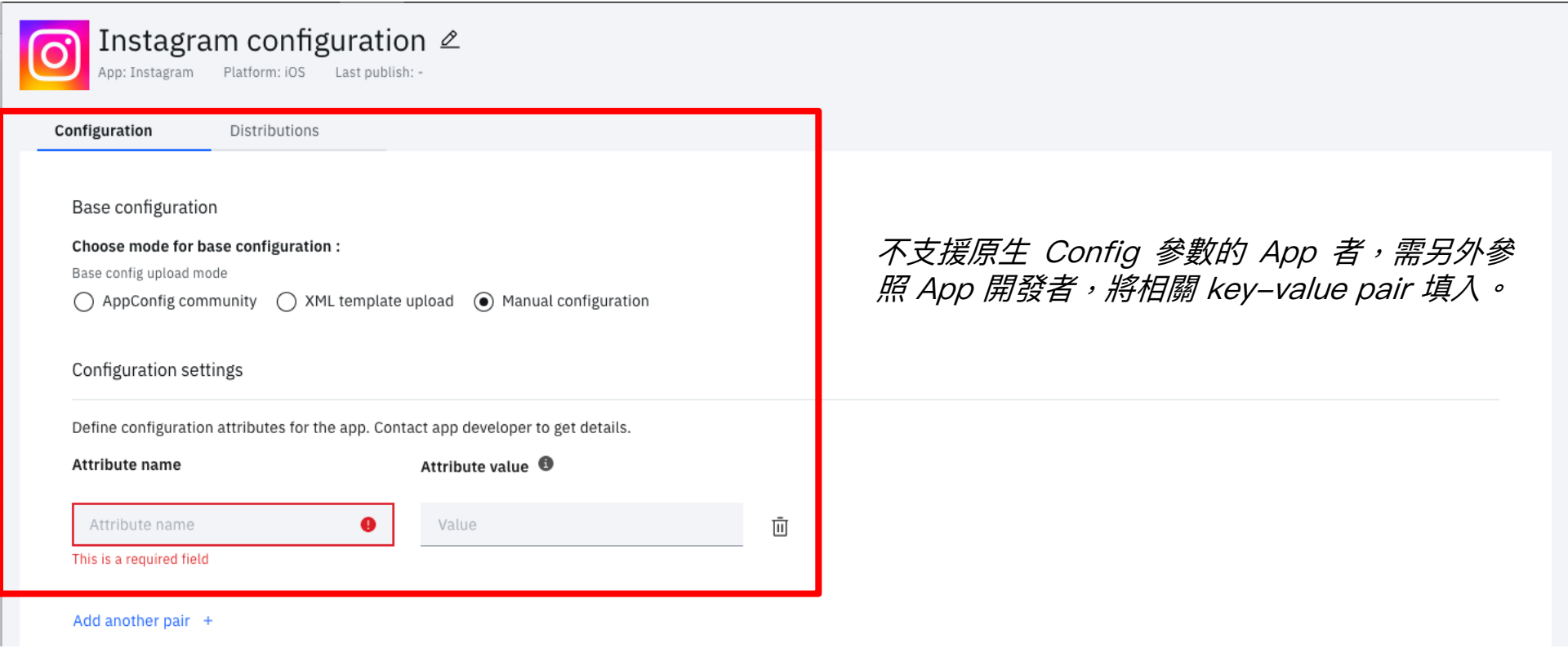


行動裝置管理解決方案 (MDM)
行動裝置應用程式設定管理 (Instagram for example)



原則上可以在 MaaS360 設定行動終端允許的應用程式白名單，並且在安裝前設定好相關 App Configuration 參數，來決定初始化安裝時，該 App 相關的設定參數應 On/Off

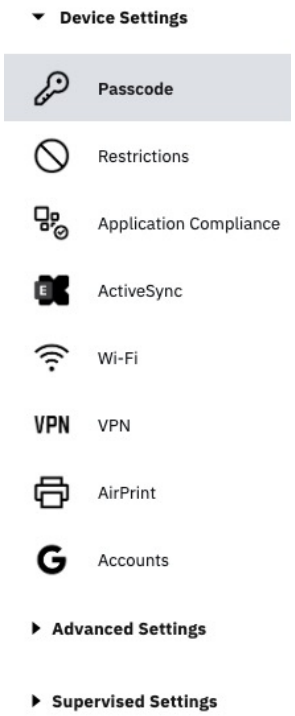
行動裝置管理解決方案 (MDM)
行動裝置應用程式設定管理 (Instagram for example)



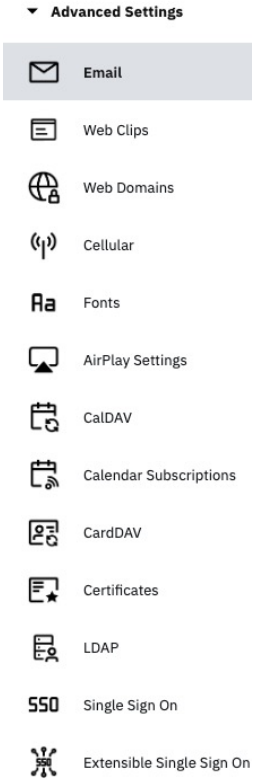
不支援原生 Config 參數的 App 者，需另外參照 App 開發者，將相關 key-value pair 填入。

行動裝置管理解決方案 (MDM)
MaaS360 支援的行動裝置安全政策類別 (Security Policy)

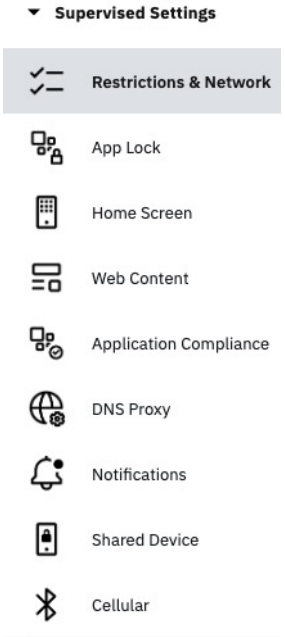
Device Settings (Click)



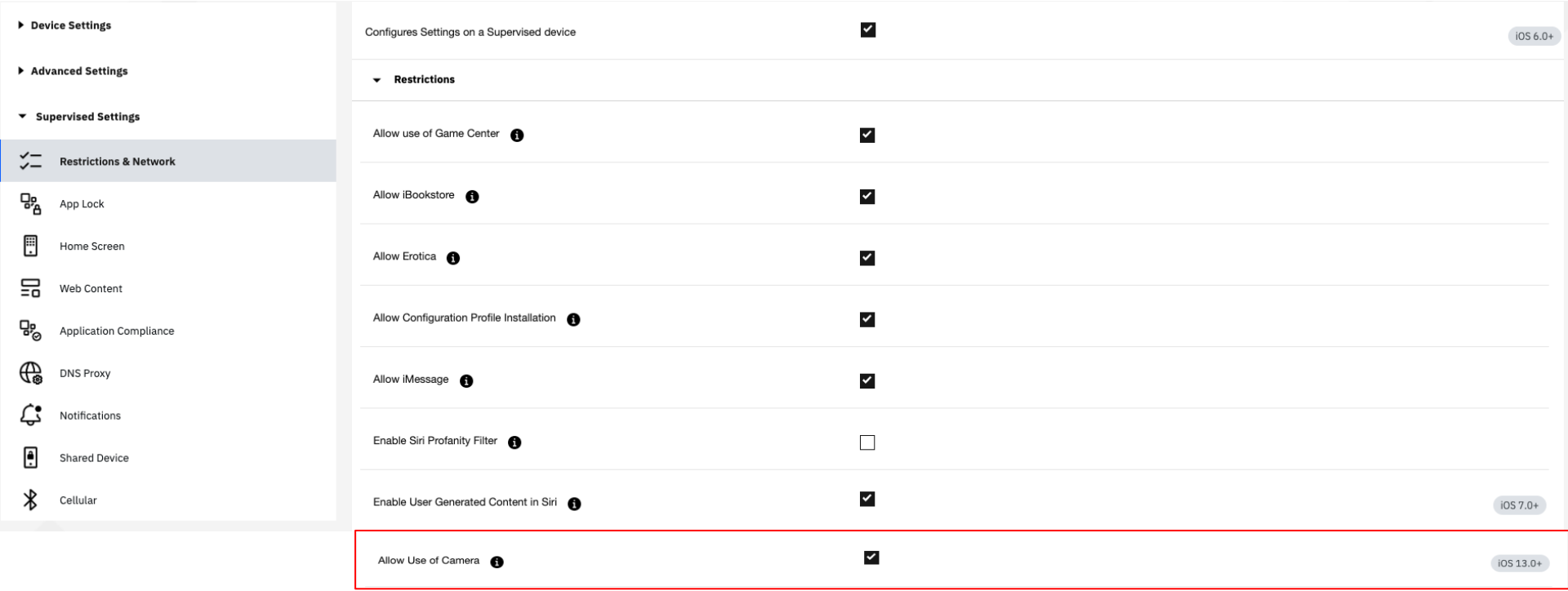
Advanced Settings (Click)



Supervised Settings



行動裝置管理解決方案 (MDM)
限制 iOS 裝置是否允許/關閉相機功能



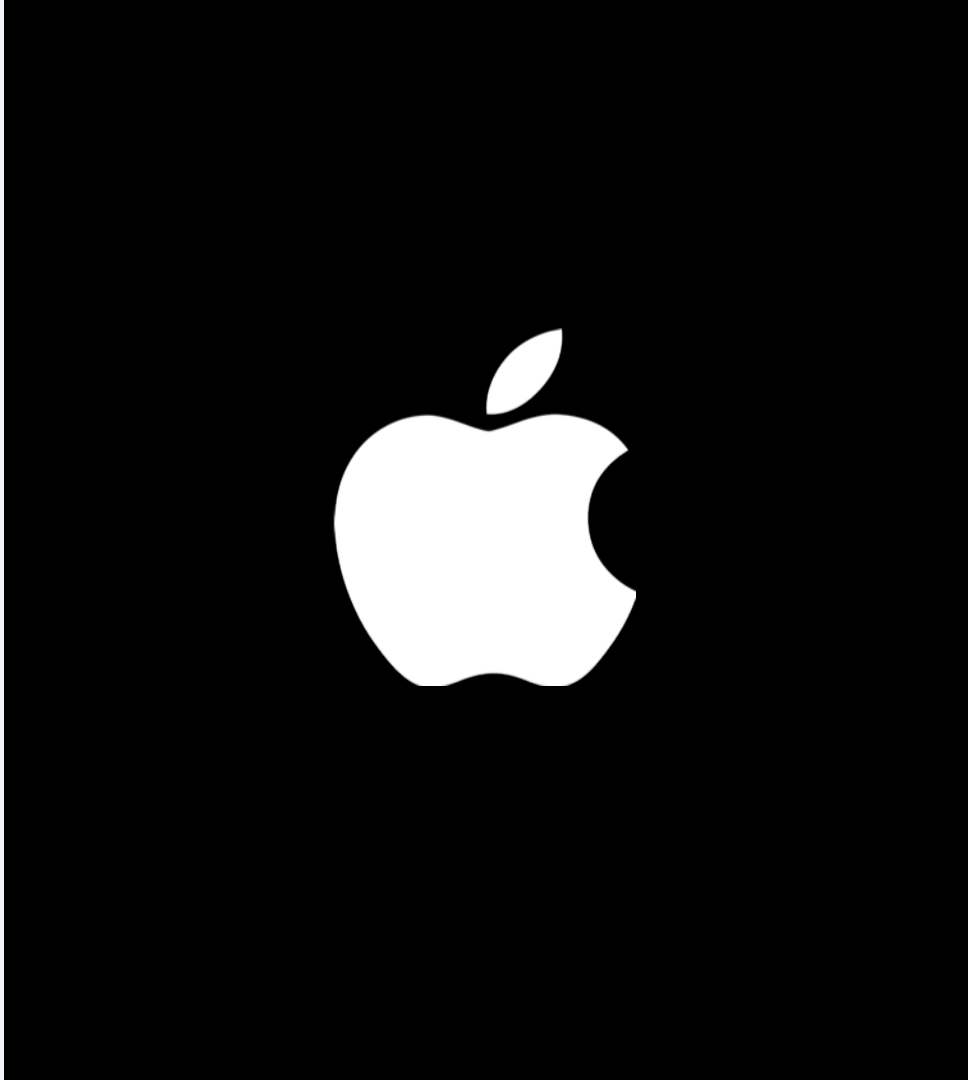
行動裝置管理解決方案 (MDM)
限制 iOS 裝置是否允許/關閉相機功能細節說明

Allow use of camera	Users can use the camera app on the device. If this setting is disabled, the camera app is hidden from the user and the user cannot access the camera app from other apps. **Allow use of FaceTime**: Allows the FaceTime app on the device to make audio and video calls from the device.	iOS 12.0 and earlier

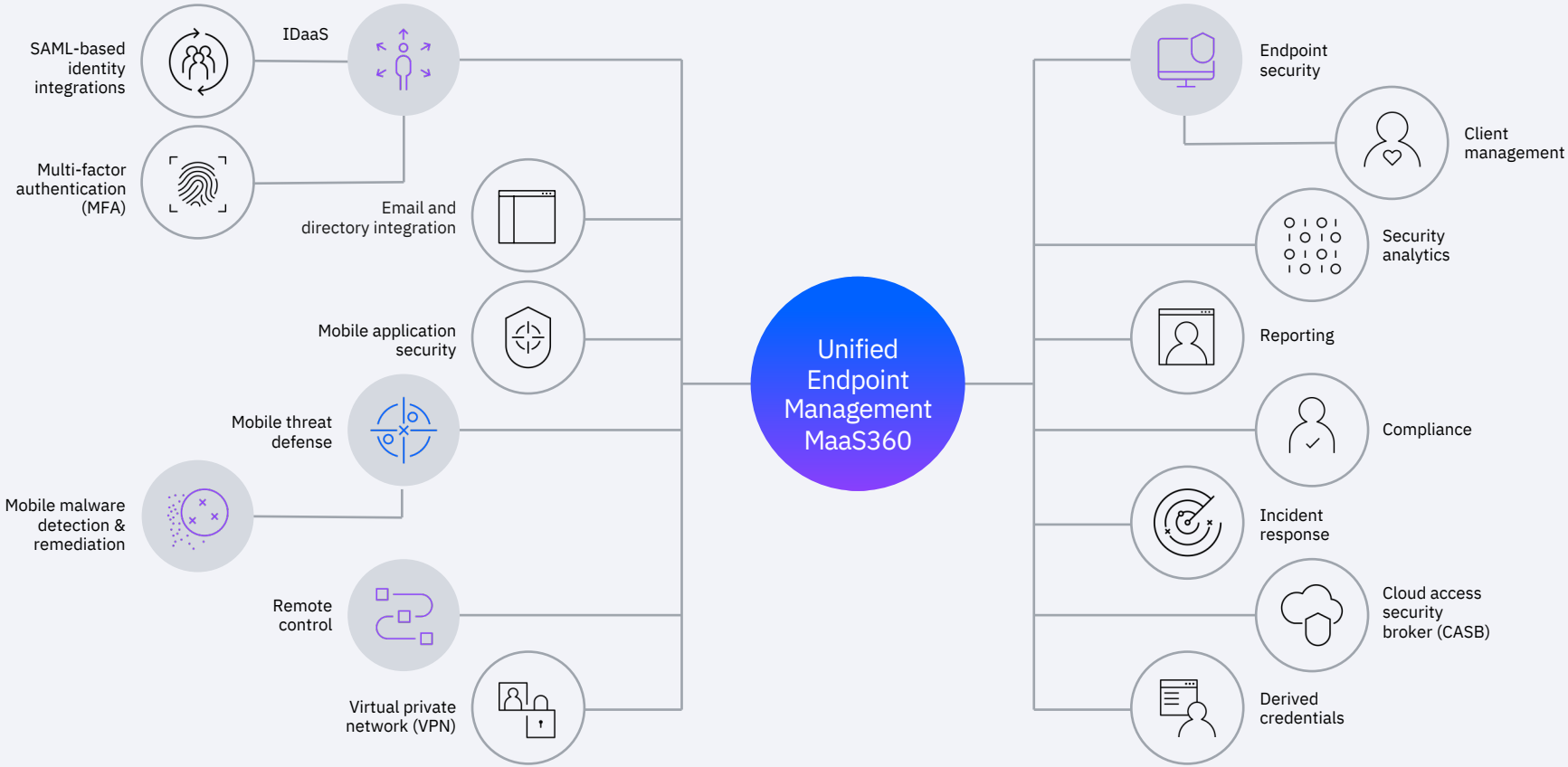
Doc: https://www.ibm.com/docs/en/maas360?topic=device-restrictions-network

UEM for personal Apple devices

- **Multi-persona enrollment** option focusing on personal devices
- **Increase user acceptance** by focusing on user privacy at an OS level
- **Secure data** by separating personal & Managed Apple IDs
  - Divide business and private data
  - Separate storage volume for corporate data
  - Managed Apple ID used for Work Identity
  - Managed Apps deployed via Managed Apple ID
  - Unenrolling removes Corporate apps and content
- **Protect privacy** & personal data
  - Cannot fully wipe device, clear passcode, or access *any* personal data or PII
  - Can configure settings, VPN, install corporate apps



Integrated with your enterprise security tools



2020 Gartner Magic Quadrant for Unified Endpoint Management

Gartner, Magic Quadrant for Unified Endpoint Management, Dan Wilson, Rich Doheny, Rob Smith, Chris Silva, Manjunath Bhat, 11 August 2020

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from IBM. G00450413

Source: Gartner (August 2020)

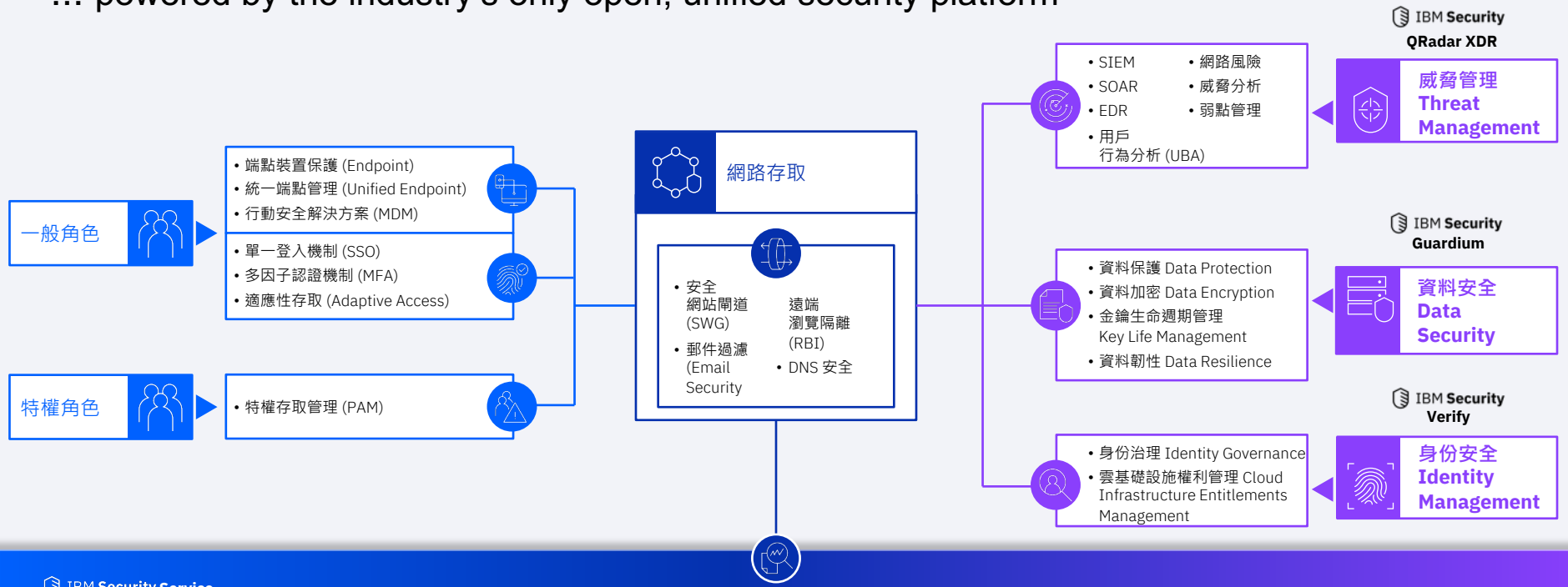
The Forrester Wave™: Unified Endpoint Management, Q4 2019

Forrester, The Forrester Wave™: Unified Endpoint Management, Q4 2019, Andrew Hewitt, Stephanie Balaouras, Renee Taylor, and Diane Lynch, November 2019

Surveillance/Data protection for remote workers / home workers

IBM Security™ End-to-end 的零信任 (Zero-Trust) 資安解決方案

... powered by the industry's only open, unified security platform



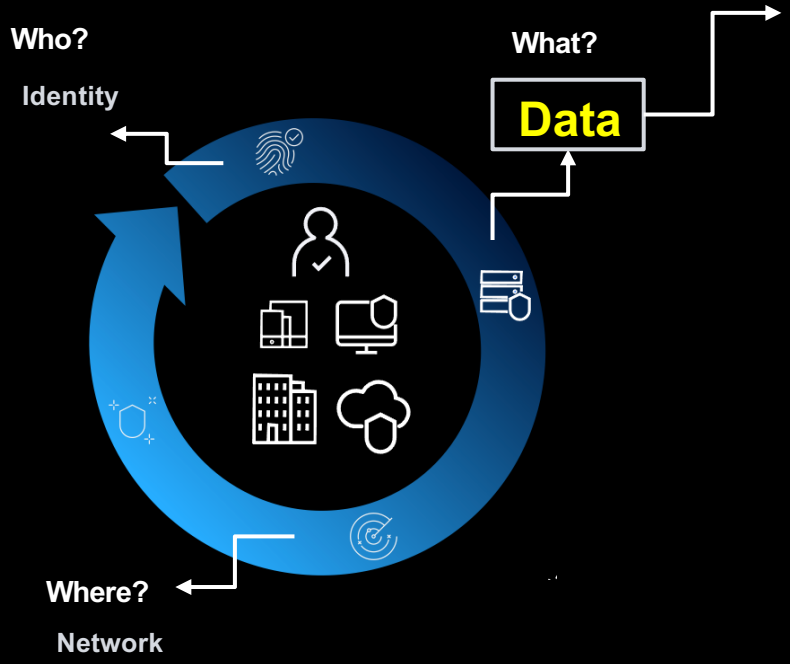
IBM Security Service

Zero Trust Acceleration Services
Ransomware Readiness Assessment
Risk Quantification Services
Incident Response Retainer
X-Force Threat Management

支援混合雲各式工作負載環境的資訊安全保護

Data Center | IaaS and PaaS | SaaS and Web

Guardium® 資料層級的零信任保護措施與威脅可視化



What *data* needs protection?

- 隱私相關數據：PII 和 PHI
- 監管與合規數據：PCI、HIPAA
- 公司營業秘密：知識產權、商業秘密

How do organizations gain *visibility*?

透過 Guardium 可以允許組織 “觀察” 和 “分析” 誰在訪問數據以及如何存取數據，達到像 “監視器” 一般地即時 監控 資料存取與稽核保護。

Data is everywhere, security is not.

企業組織與資料安全防護
持續發生的資料洩漏威脅與挑戰

組織內部資料外流

企業經常遭遇資料外洩風險，常見原因多是**資料存取管控不當**或遭受**勒索病毒攻擊**，因此科技公司、金融機構或醫療院所等產業均常見資料外流的重大資安事件。

企業營業秘密竊取

常見員工為有利至競爭公司，透過竊取原公司營業秘密獲取相關利益。通常會在離職前從**大量存取公司內部資料**，均會直接或間接造成企業嚴重的營運風險與商譽損失。

客戶個資隱私洩漏

企業或公部門單位委託資訊業者建置、實施與管理相關資訊系統，常因**系統管理不當或防護程度不足**，導致大量的客戶資料洩漏，導致企業與客戶均蒙受相關損失。

法遵與合規需求

各領域產業均有相關法遵與合規需求，常見 **金融業的 PCI 、醫療機構的 HIPAA 或一般性的 ISO 27001**，均針對個資與隱私等資料規範相關控制措施。

企業組織與資料安全防護
現代化核心指導原則與方針

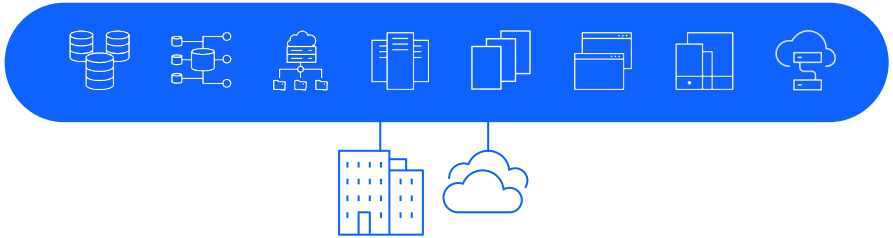
1. 關鍵數據的儲存位置、存取方式，
以及設計兼顧使用與安全的資料保護方案。

2. 全面性的發掘組織內、外資料風險，
同時針對動態和靜態資料建立與執行保護策略。

3. 降低法規遵循與合規性稽核成本，
並且能夠週期性監控與稽核控制項目實施情形。

4. 自動化實施資料保護與威脅即時偵測與緩解，
且能連接與整合企業既有資安防禦策略。

現代企業組織資料主要使用與保存在
內部環境 與 **混合雲** 環境



資料通常會被 **個別** 或 **分散** 的團隊存取
且資料保護相關工具通常是 **孤島式方案**

IBM 現代化資料安全保護策略
提供資料存取威脅的可視化、優先級與風險緩解

風險合規管控 (Compliance)

資料存取管理 (Access)

資料數據隱私 (Privacy)

Guardium® Data Protection
資料保護方案與應用情境

資料庫存取活動
(Database Activities)

Client/Server network connections

Session Starts (log in)

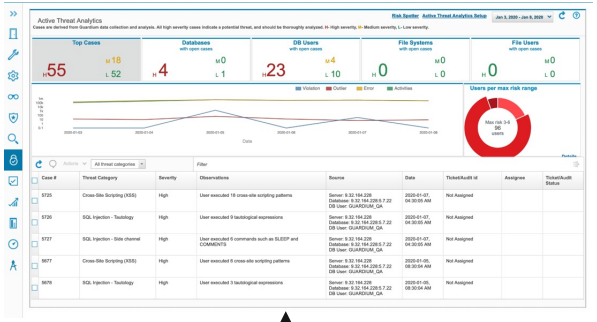
SQL Requests (commands)

Session Ends (log out)

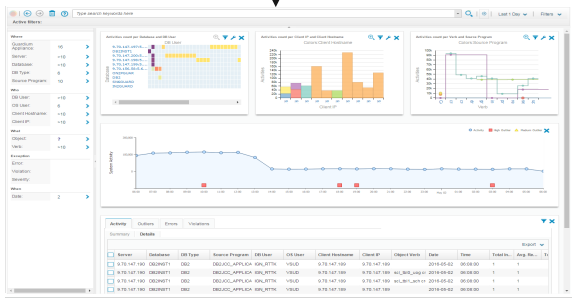
資料庫伺服器
(Database Server)

- 系統登入失敗
- SQL 語法錯誤
- 回傳敏感資料
- 異常活動存取

0101
0001
0101
1110
1110
1101
1001



Guardium



0001
1001
0001
1110
1110
1101
1101

檔案系統
(File System)

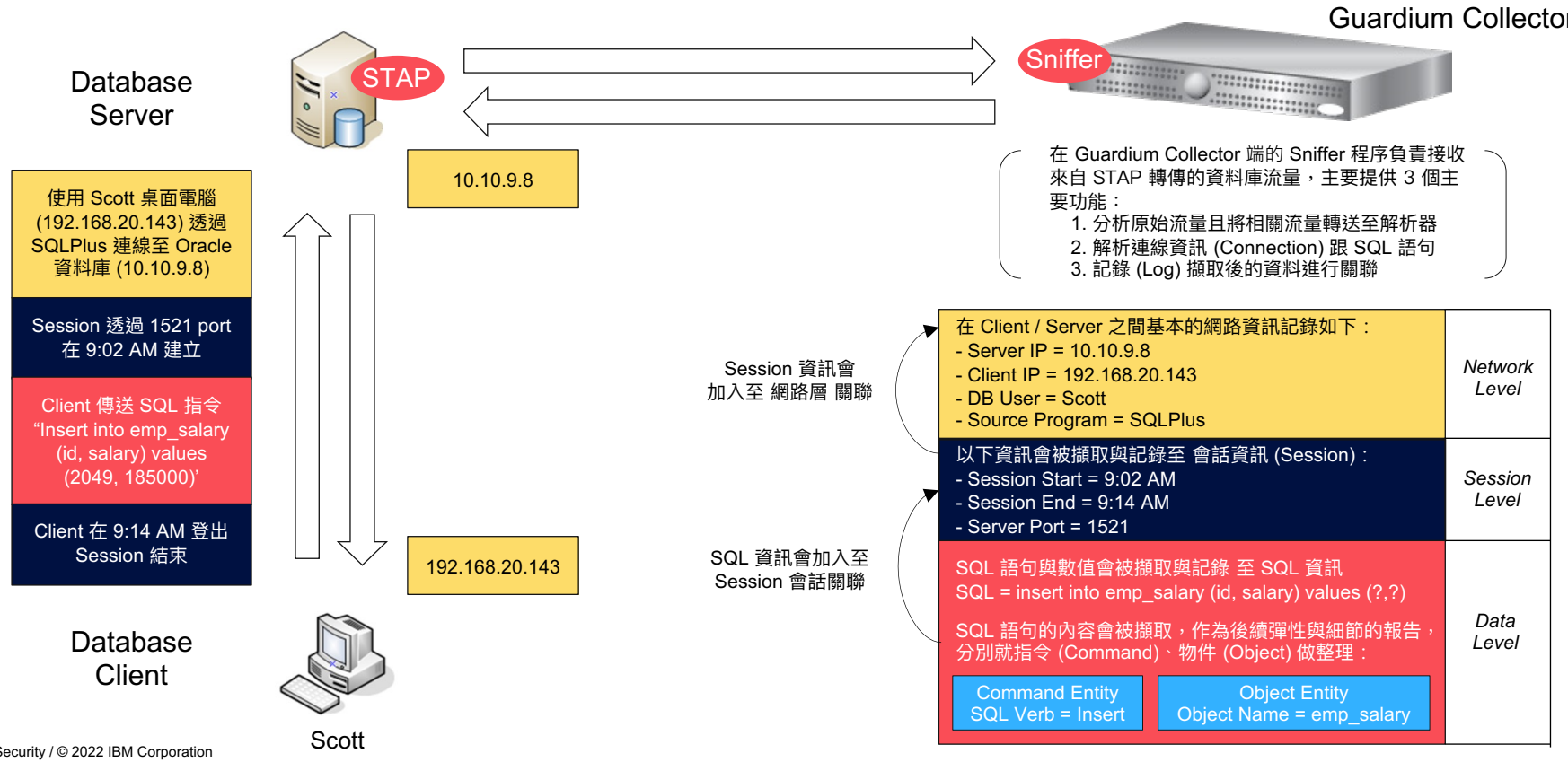
- 檔案活動監控
- 敏感資料發掘
- 檔案屬性授權
- 日誌紀錄稽核

資料庫連線終端
(Database Client)

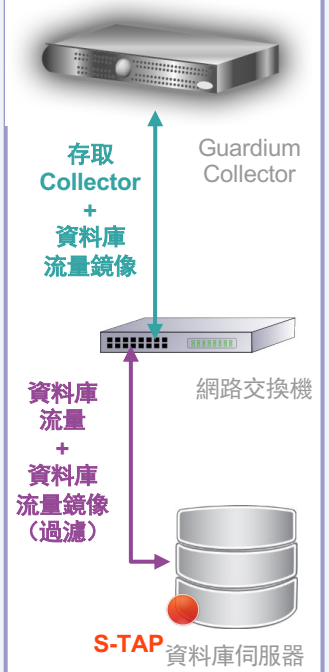
用戶連線終端
(User / Client)

Guardium® Data Protection
資料保護方案與應用情境

發現 Discover ▶ 保護 Protect ▶ 分析 Analyze ▶ 回應 Respond ▶ 稽核 Comply



Guardium® Data Protection S-TAP 監控機制



軟體代理 (S-TAP) 位於主機 OS 層，不依賴資料庫管理系統同時發送網路和本地流量到 Guardium Collector：

- 在作業系統層 (OS) 監控所有資料庫活動：TCP, Shared Memory, Named Pipes, Bequeath
- 處理加密流量：SSH/IPSEC, Oracle ASO, SQL Server SSL
- 不需要牽涉與修改既有資料庫環境
- 無論有多少個、不同類型的資料庫實例，每個系統只需安裝一個S-TAP
- 無需額外硬體配置，降低建置成本
- 可以對流量進行過濾，無需將所有流量（左圖示意）發送給 Guardium Collector，顯著降低網路負載
- 對資料庫伺服器平均低於 3% 的性能影響

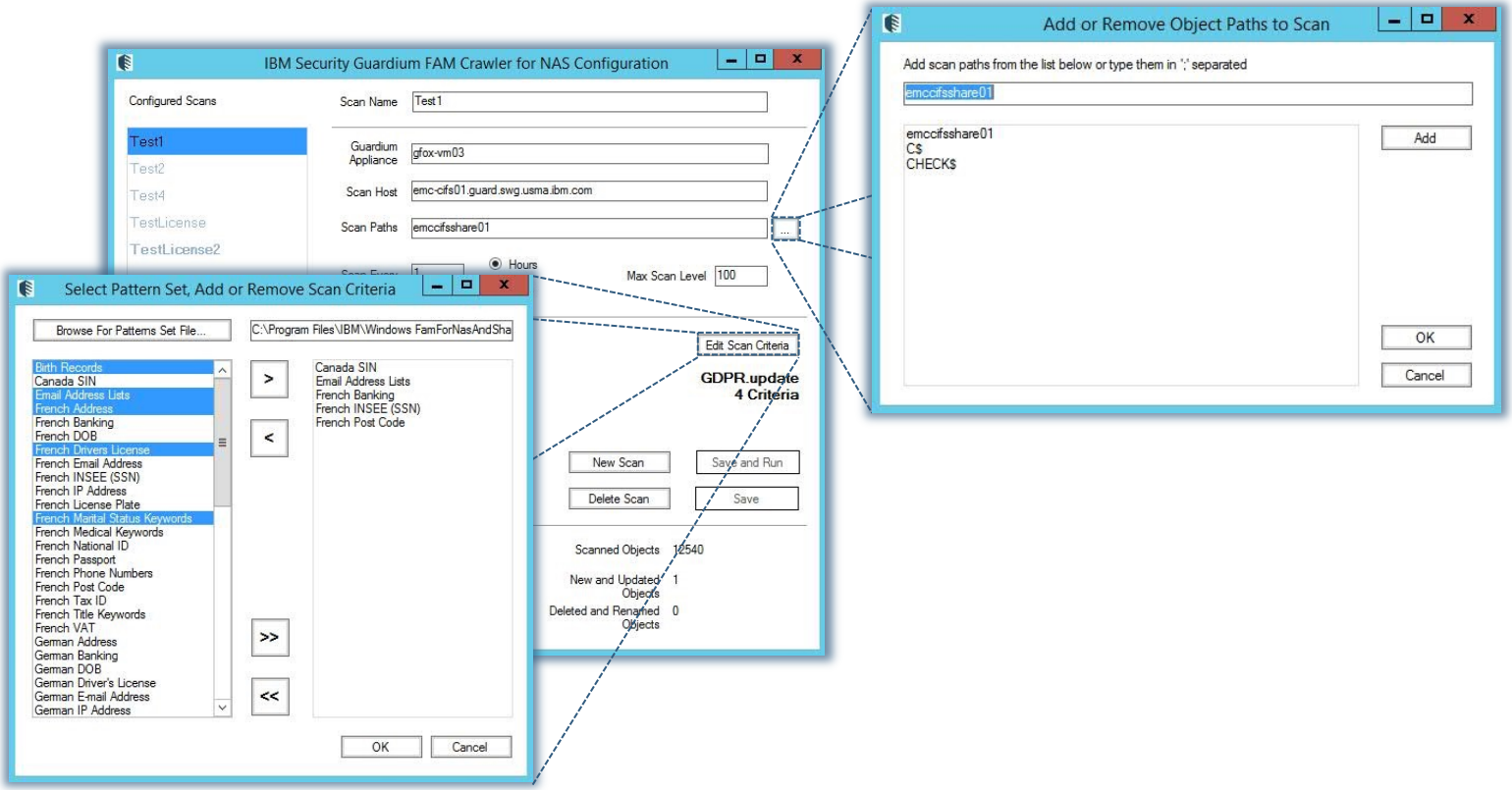
Guardium Data Protection for File 檔案系統 (File System) 活動保護與監控

在不影響您的業務的情況下保護敏感和關鍵檔案/文件數據。

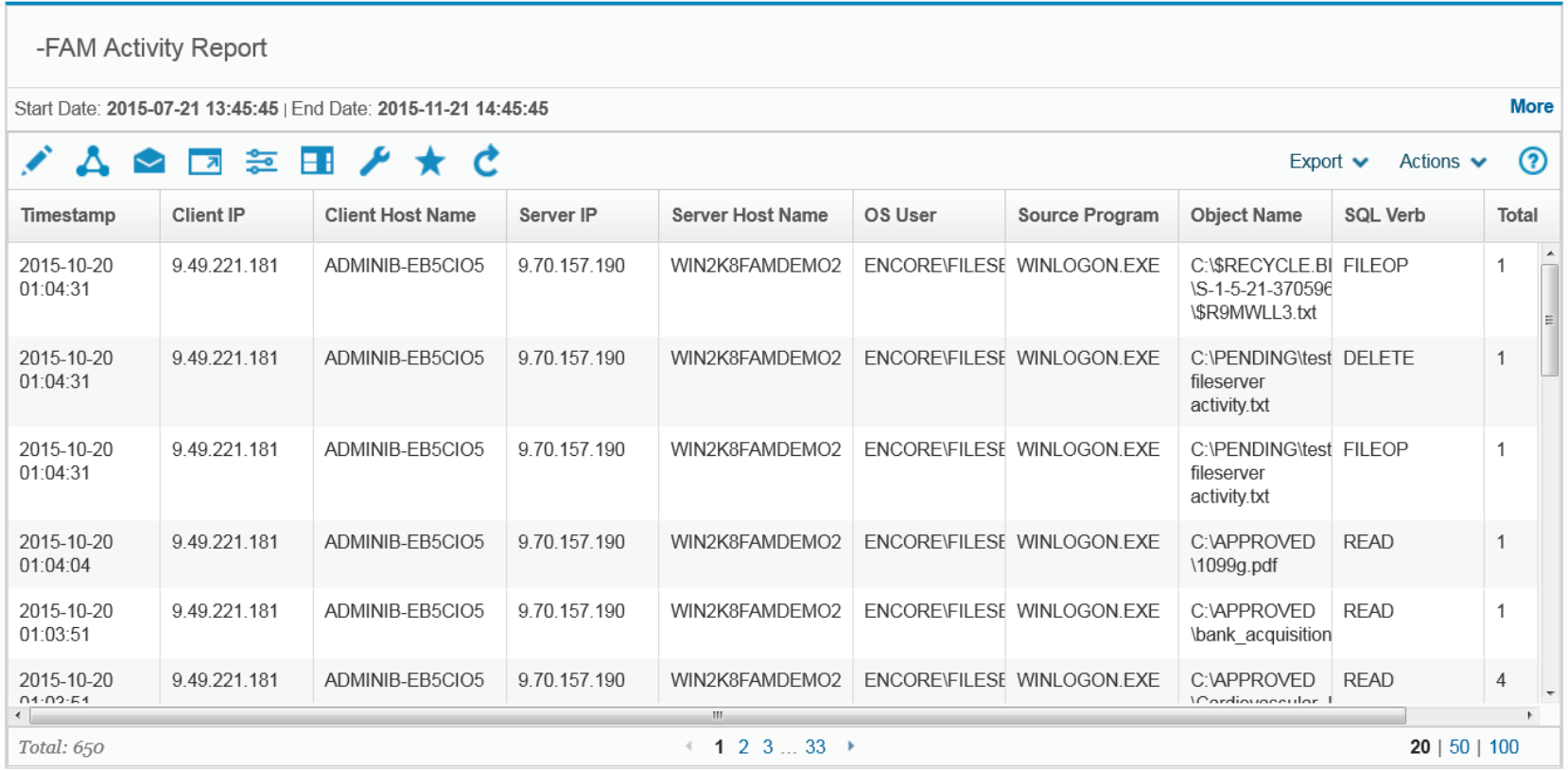
保護關鍵配置和應用程序文件	保護對包含 PII 訊息的文件訪問	保護對應用程序文件從後端訪問	保護程式碼
需要保護可以通過直接訪問應用程序或數據庫服務器來訪問、修改甚至破壞的關鍵應用程序文件。	需要保護包含 PII 數據的文件，同時不影響日常業務運營。	需要阻止對企業應用程序管理的文檔的後端訪問。	需要保護源代碼和其他知識產權。

Guardium Data Protection for File 檔案系統 (File System) 活動保護與監控

Guardium Data Protection for File 檔案系統 (File System) 活動保護與監控



Guardium Data Protection for File 檔案系統 (File System) 活動保護與監控



-FAM Activity Report

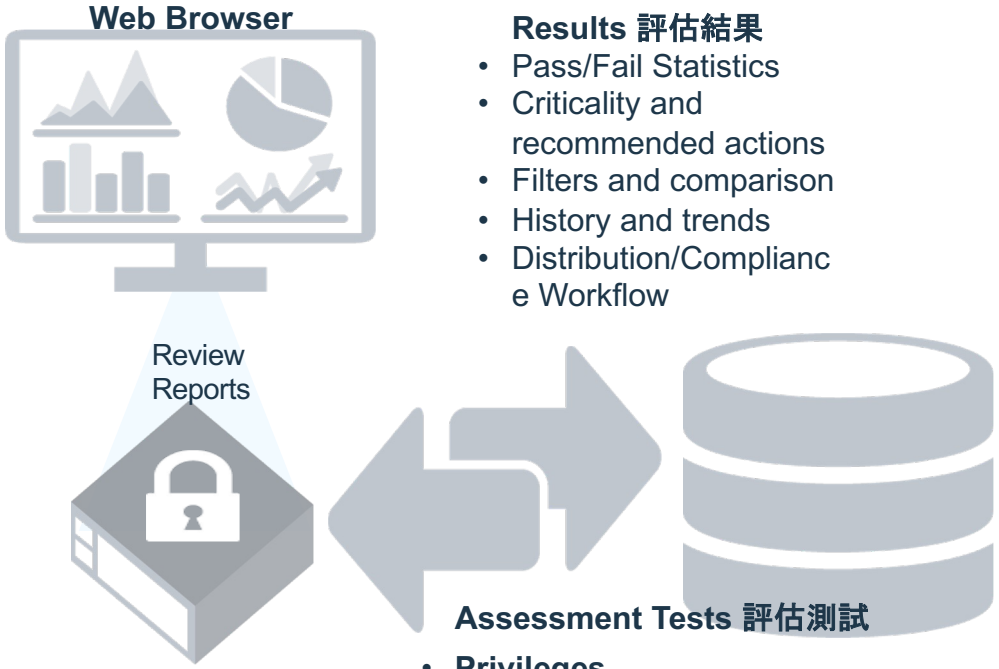
Start Date: **2015-07-21 13:45:45** | End Date: **2015-11-21 14:45:45** More

Export Actions

Timestamp	Client IP	Client Host Name	Server IP	Server Host Name	OS User	Source Program	Object Name	SQL Verb	Total
2015-10-20 01:04:31	9.49.221.181	ADMINIB-EB5CIO5	9.70.157.190	WIN2K8FAMDEMO2	ENCORE\FILESE	WINLOGON.EXE	C:\$RECYCLE.BI \S-1-5-21-370596 \$R9MWLL3.txt	FILEOP	1
2015-10-20 01:04:31	9.49.221.181	ADMINIB-EB5CIO5	9.70.157.190	WIN2K8FAMDEMO2	ENCORE\FILESE	WINLOGON.EXE	C:\PENDING\test fileserver activity.txt	DELETE	1
2015-10-20 01:04:31	9.49.221.181	ADMINIB-EB5CIO5	9.70.157.190	WIN2K8FAMDEMO2	ENCORE\FILESE	WINLOGON.EXE	C:\PENDING\test fileserver activity.txt	FILEOP	1
2015-10-20 01:04:04	9.49.221.181	ADMINIB-EB5CIO5	9.70.157.190	WIN2K8FAMDEMO2	ENCORE\FILESE	WINLOGON.EXE	C:\APPROVED \1099g.pdf	READ	1
2015-10-20 01:03:51	9.49.221.181	ADMINIB-EB5CIO5	9.70.157.190	WIN2K8FAMDEMO2	ENCORE\FILESE	WINLOGON.EXE	C:\APPROVED \bank_acquisition	READ	1
2015-10-20	9.49.221.181	ADMINIB-EB5CIO5	9.70.157.190	WIN2K8FAMDEMO2	ENCORE\FILESE	WINLOGON.EXE	C:\APPROVED	READ	4

Total: 650 1 2 3 ... 33 **20** | 50 | 100

Guardium® 提供對資料庫可能存在的弱點和配置進行弱點掃描



Results 評估結果

- Pass/Fail Statistics
- Criticality and recommended actions
- Filters and comparison
- History and trends
- Distribution/Compliance Workflow

Assessment Tests 評估測試

- **Privileges**
- **Authentication**
- **Configuration**
- **Patch levels**

Data sources 資料來源

- Oracle
- SQL Server
- DB2, DB2 z, DB2 i
- Sybase
- Teradata, Aster
- Informix, Netezza
- MySQL
- Postgres
- MongoDB,
- SAP HANA

Guardium® 提供對資料庫可能存在的弱點和配置進行弱點掃描

Guardium® Risk Spotter 風險綜合觀測

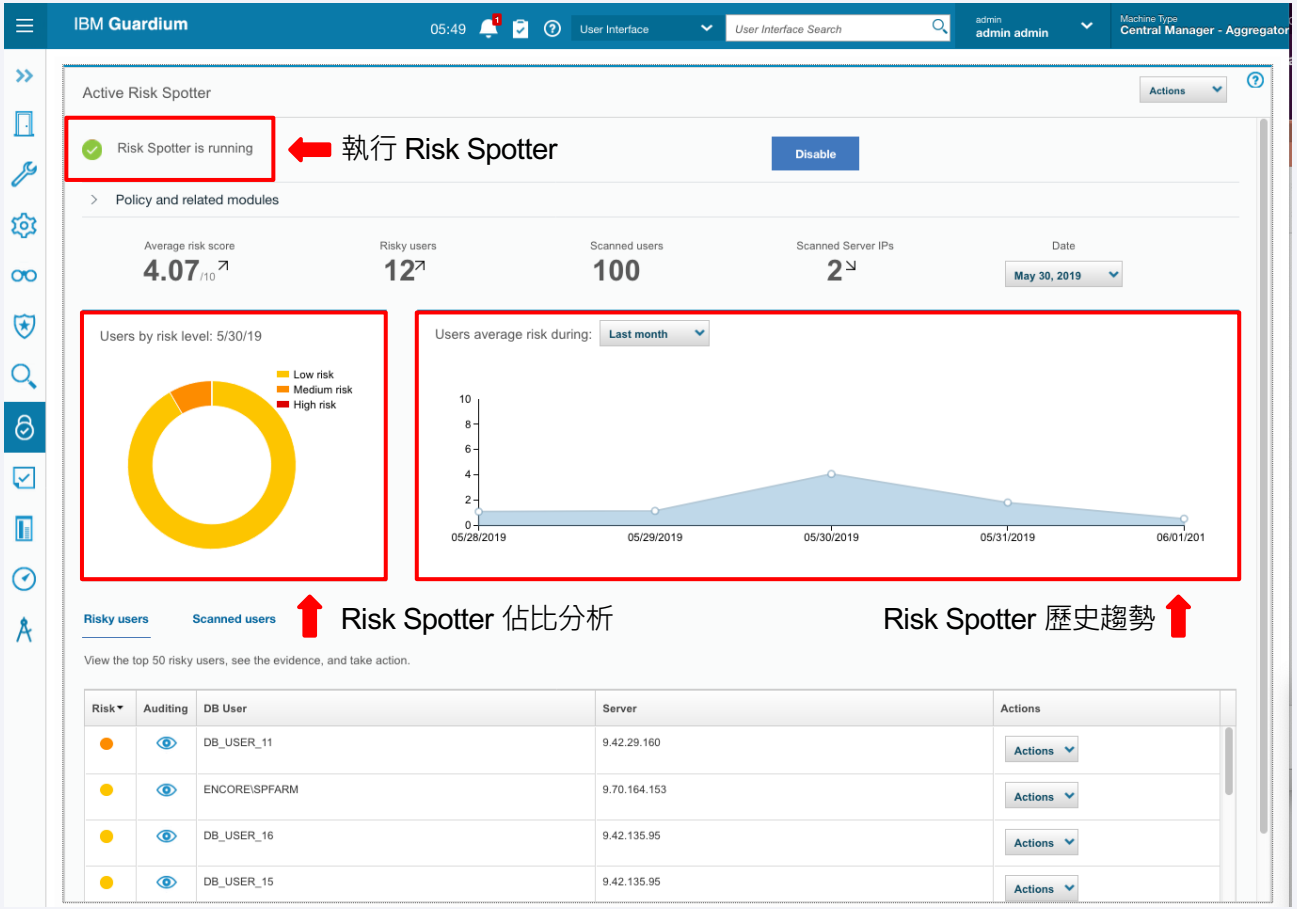
- 動態風險評估

基於 outliers, vulnerability, volume of activities, access to sensitive data, 等因子進行綜合風險評估

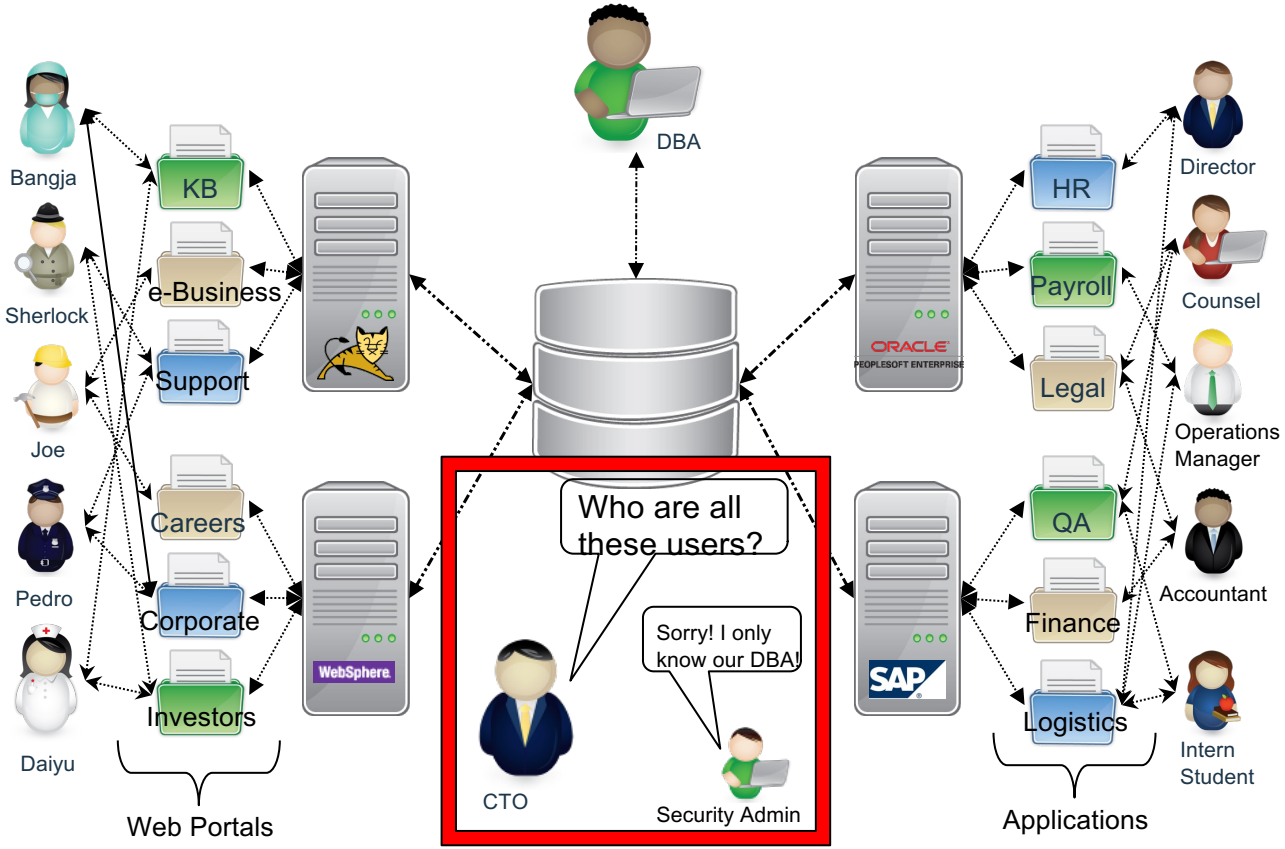
Risk assessment 風險評估的元素

Outliers	與用戶相關的異常的數量和嚴重程度。
Violations	高度或中等程度的違規數量。
Vulnerability	沒有通過漏洞評估的數量。
Sensitive objects	敏感數據查詢次數。
Off-work activity	在非工作時間發生的與用戶相關的活動。
DDL queries	總活動數量裡 DDL 查詢的相對數量
DML queries	總活動數量裡 DML 查詢的相對數量
Administrative queries	總活動數量裡管理查詢 (Administrative) 的相對數量。
Select queries	在總活動中與用戶相關的選擇查詢的相對數量。
High volume activity	與用戶的平均活動相比較的高度活躍的活動量。

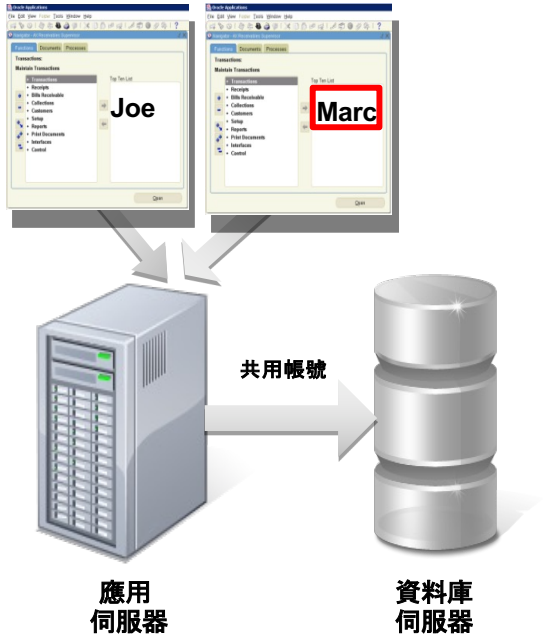
Risk assessment 風險評估的結果



Guardium® 提供應用程式層級的使用者識別



Guardium® 提供應用程式層級的使用者識別



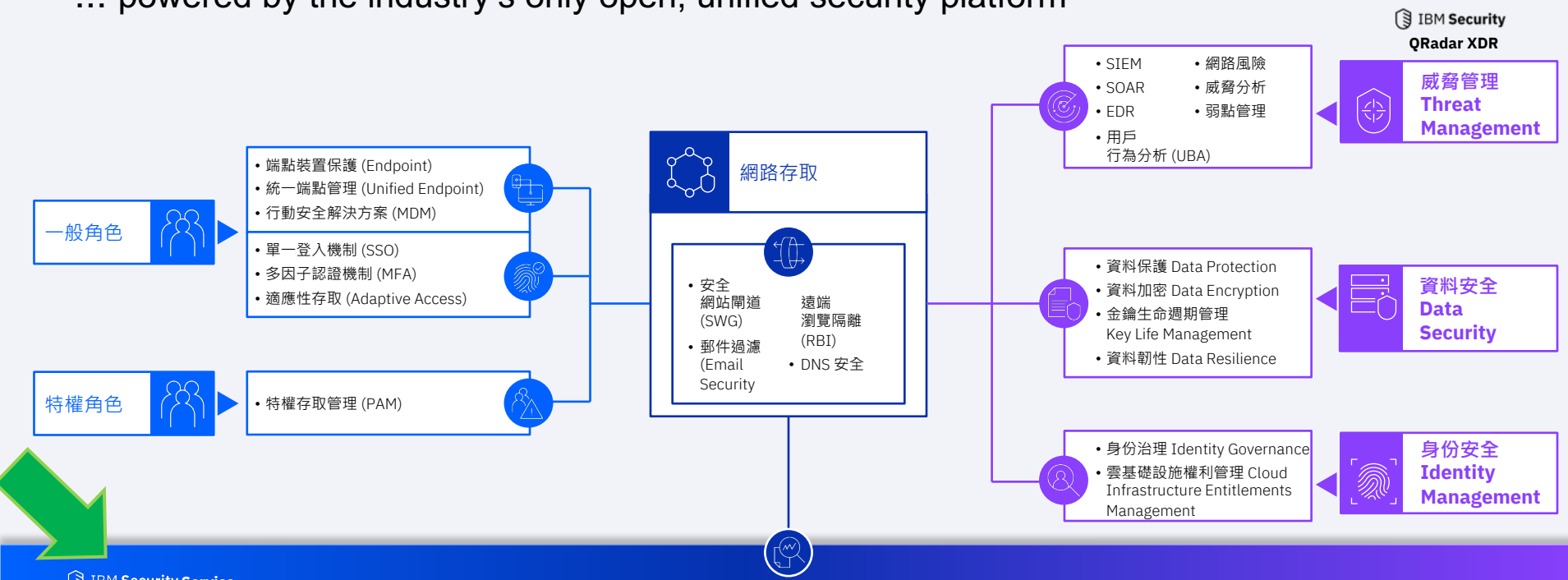
DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

- ***問題: A應用伺服器一般使用一個能用的服務帳號來存取資料庫 – 這樣就不能識別出究竟是 誰 發起的交易 (連接池的應用環境中)***
- ***解決*: 跟蹤與SQL命令相關的實際應用使用者**
  - 原生支援所有主流的企業級應用 (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos, etc.)
  - 直接支援主流的中介軟體平台應用 (WebLogic, WebSphere)
  - 提供簡單的API
    - select 'GuardAppEvent:Start', 'GuardAppEventUserName:USERID' from dual;
    - -- USERID 執行的 SQL 交易語句;
    - select 'GuardAppEvent:Released' from dual;

CIRC (Cyber Incident Response)

IBM Security™ End-to-end 的零信任 (Zero-Trust) 資安解決方案

... powered by the industry's only open, unified security platform



X-Force Threat Management

透過 AI-Powered 的資訊安全框架保護您的企業環境

持續性調整的資安保護機制框架與完整成熟的方法論

與全世界資安專家合作，提供**可信賴的資安服務與解決方案**

資安成熟治理框架

整合與持續營運模式

評估資安成熟度作為發展路線調整與修正

透過現代化與進階威脅管理的平台提供威脅保護與落實

Watson AI for Cybersecurity

X-Force Exchange

Cloud Pak for Security

OCP Platfrom

QRadar SIEM

QRadar SOAR

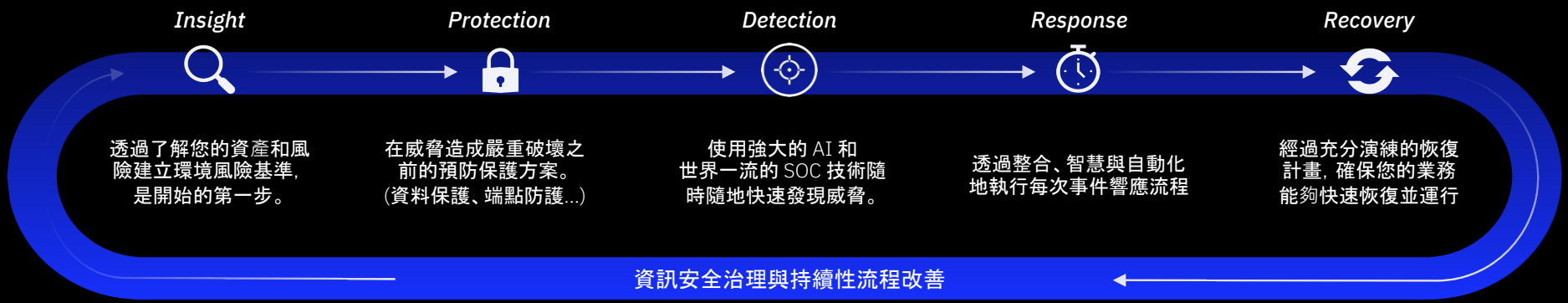
QRadar EDR

Out-of-box Use Cases Library

Modern and intuitive UI

IBM Security 提供完善地資訊安全生命週期管理

End-to-end offering powered by NIST Cyber Security Framework (CSF)



識別和保護關鍵資產，檢測高級威脅，更快地響應中斷並從中斷中恢復

- **Threat intelligence**
- Baseline Maturity Assessment
- Asset Identification
- Risk assessment
- Ransomware Readiness Assessment

- **Protection technology**
- Policy management
- Policy optimization
- Endpoint and Network Security Management
- Vulnerability management

- **SIEM | NDR | EDR management**
- Advanced analytics
- Alert enrichment
- Rule optimization
- 24x7 monitoring
- Use cases
- Threat Hunting

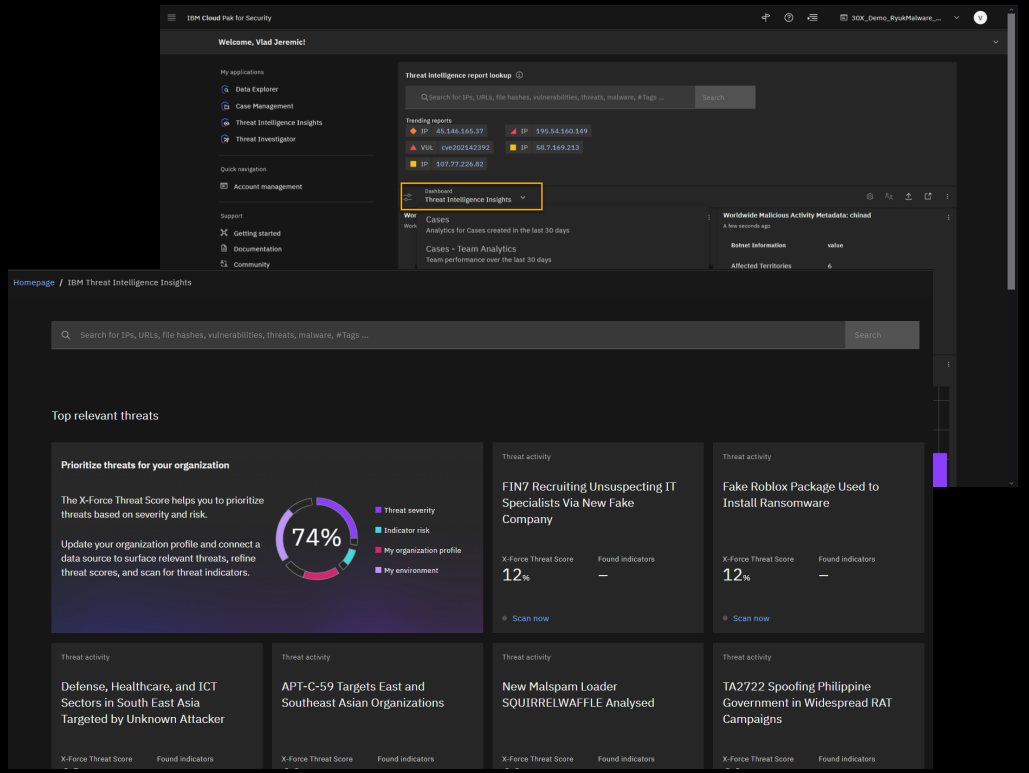
- **Incident Response planning and Execution**
- Incident Management
- SOAR Playbooks
- Endpoint and Network Response
- Crisis communication

- **Recovery & Remediation plans**
- BC / DR Program integration
- After action review

Insight: Threat Intelligence

以情資為中心的威脅偵測與響應服務

- 通過全球 IBM X-Force 團隊打造包含情境的威脅分析引擎獲取全球化且針對產業領域的威脅情資 (Threat Intelligence)。
- 使用 X-Force Threat Score 為您的組織確定威脅的優先級，這是一個彈性分數，根據組織的相關性、嚴重性、滲透性、影響和實際外部環境觀察計算得出。
- 使用 Am I Affected 識別內部環境中的活躍威脅並採取行動，它在連接的數據源中運行連續和自動搜索，並自動為威脅攻擊創建調查案例。
- 整合既有或第三方情資來源，通過單一平臺配置，有效在調查與回應過程豐富化威脅事件調查內容。
  - 支援預先整合的第三方情資來源：AlienVault OTX, Cisco Threatgrid, MaxMind Geolocation, SANS Internet StormCenter and Virustotal



IBM Security™ QRadar® SOAR

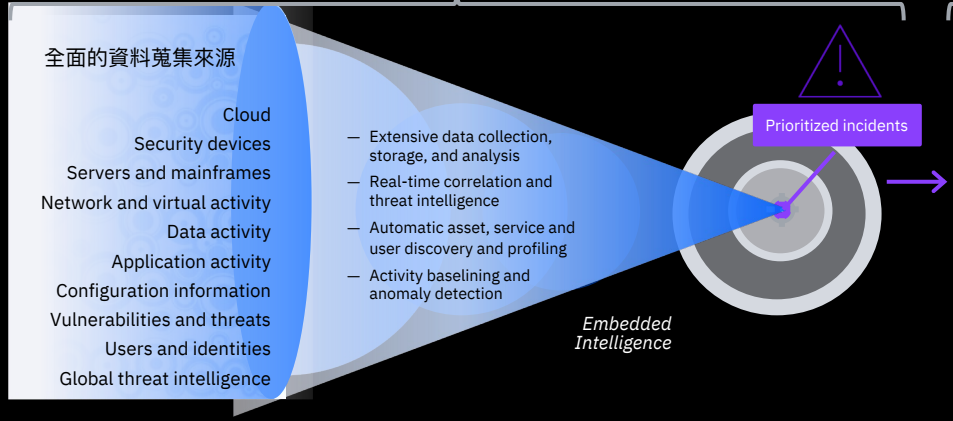
QRadar® SIEM + SOAR 涵蓋資安事件生命週期

Security Intelligence and Event Platform (SIEM)

從 Logs, Flows, Vulns, User, Config Data 等資料來源分析、排序、偵測威脅事件

Security Orchestration, Automation and Response (SOAR)

透過資安運維機制回應資安事件威脅與相關漏洞與弱點事件



資安事件開立

- 基於事件類型分類
- 基於事件風險決定是否通知相關層級

蒐集事件背景內容

- 蒐集相關證據
- 套用與遵守法規要求
- 指派相關處置任務

緩解措施與關單

- 與團隊溝通修補任務
- 確認執行修補任務
- 關閉事件與禁行通知

資安事件分類與歸檔

資安事件知識庫 (Knowledge Base)

資安事件通報 (Incident Report and Notify)

持續進行資訊安全威脅偵測與分析

資訊安全程序與偵測機制改善

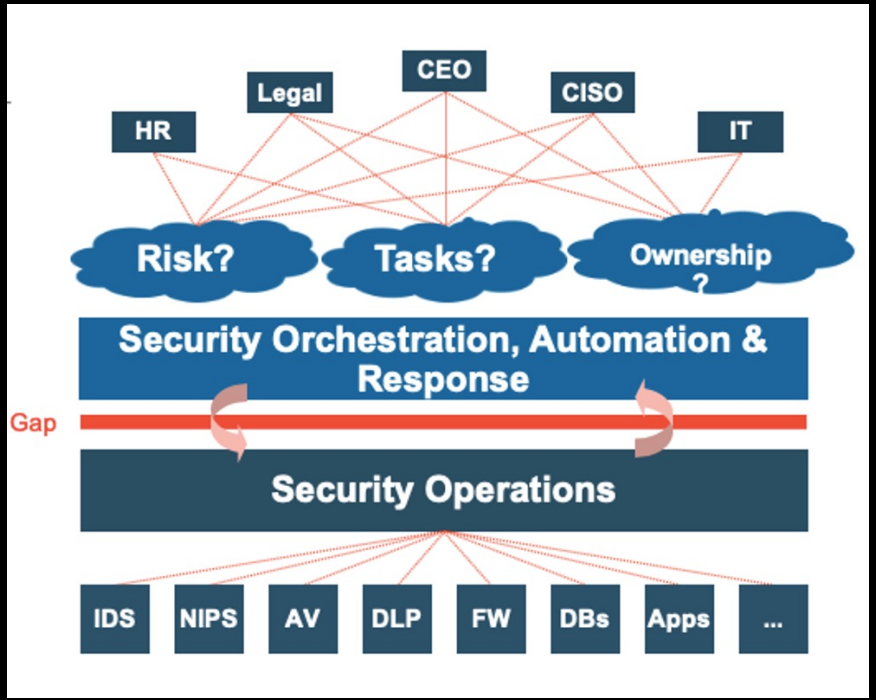
Why Security Orchestration Automation Response (SOAR) ?

1. 未定義或規範的事件處理流程導致預期外的攻擊事件處理時效 (People, Process, Procedure)

2. 未協同一致運作的資訊安全工具導致需要人工手動事件回應 (Siloed Security Tools)

3. 不熟悉法規與合規性遵循要求，導致違反隱私或義務性要求 (Compliance and Regulation)

4. 缺乏資訊安全專業人才與技能導致無法有效執行事件回應 (Professional skill shortage)

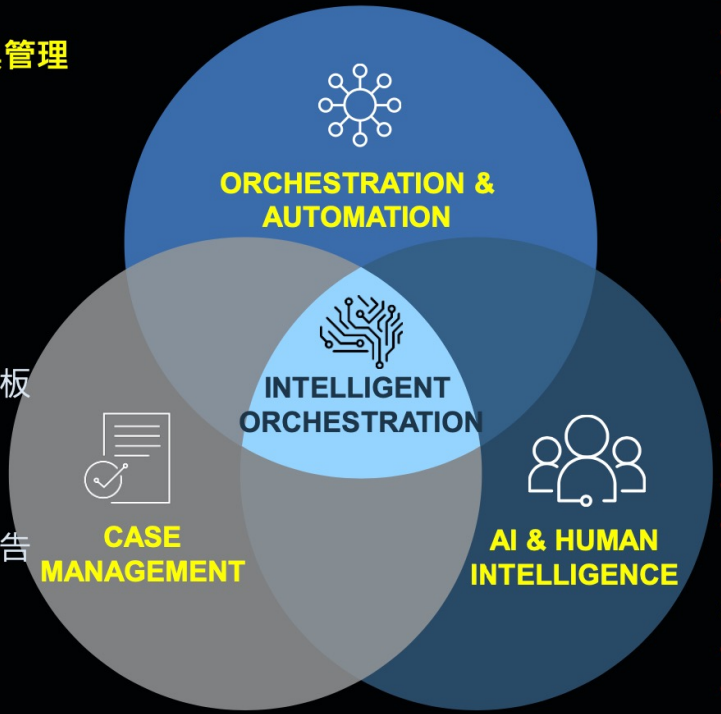


QRadar® SOAR Overview

事件上報、建立與管理
- 事件提取與上報
- 事件管理
- 集中管理平台

協同合作
- 電子郵件協作
- 任務指派與問責
- 訊息提要與儀表板

團隊管理
- 指標與 KPI
- 分析儀表板與報告
- 模擬
- 工作區
- RBAC



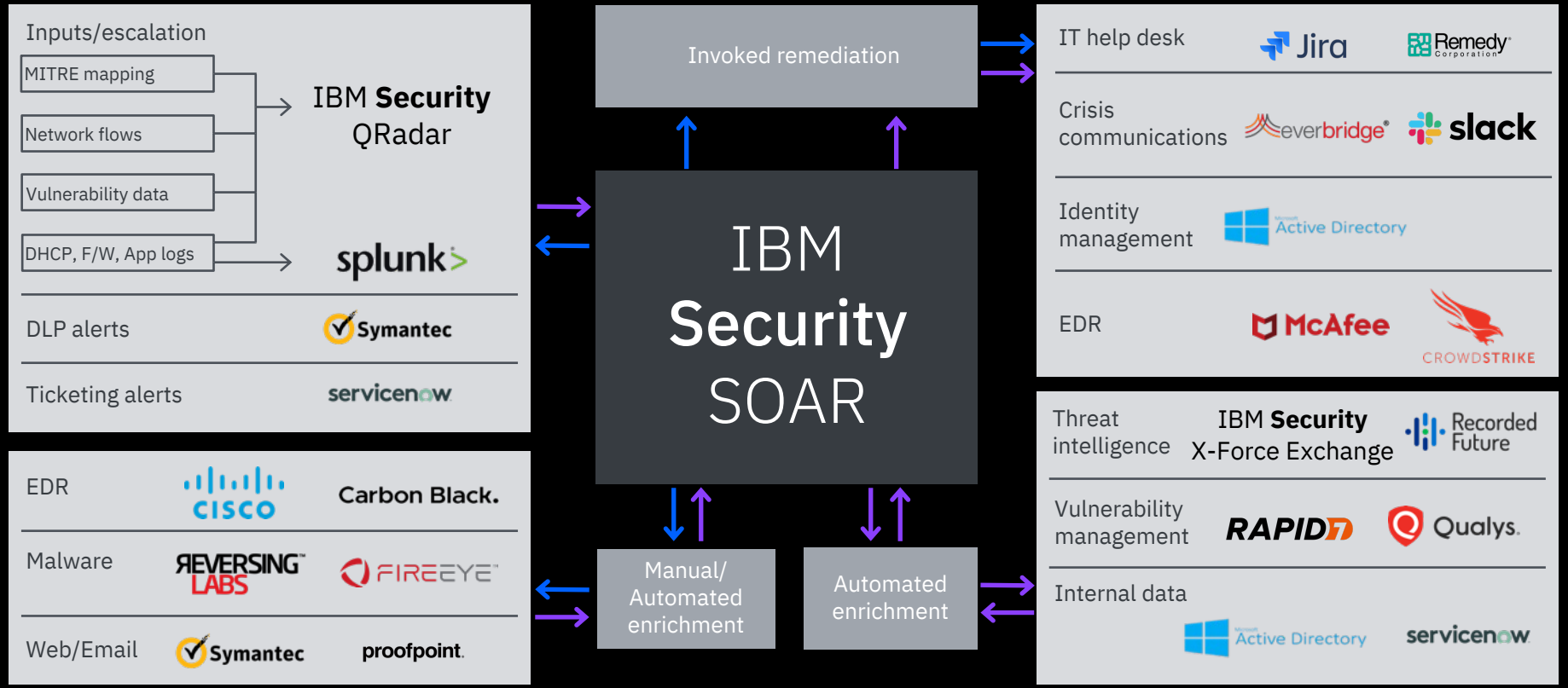
編排與自動化
- 指導回應
- 動態劇本
- 客製化業務邏輯
- 拖拉視覺化工作流程編輯平台

編排生態系統
- IBM Security AppExchange
- Community 提供整合、劇本與最佳實踐
- Developer community

威脅情報與資料豐富化
- 整合威脅情報
- 事件與構件的視覺化呈現
- 透過 SIEM、EDR 等的資料豐富化

最佳實踐與 IR 專業知識
- 隱私與合規性法規
- 資料洩漏通知
- 可自訂的標準劇本 (NIST, CERT, SANS)

QRadar® SOAR 整合協作 (Orchestration)



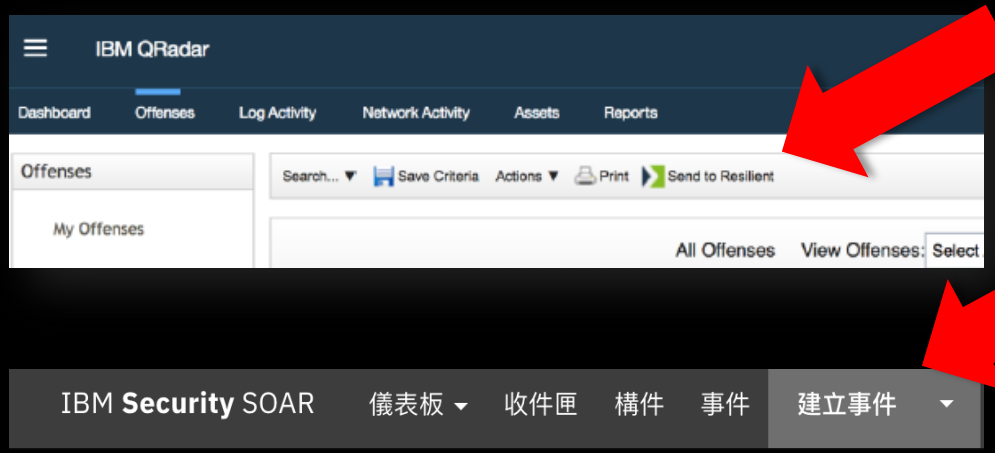
Manual

Automatic

QRadar® SOAR **Case Management** 案件管理

Incidents can be created via “Out of the box” integrations

- Integration with QRadar
- Integration with ArcSight
- Integration with Splunk
- Integration with ServiceNow
- Integration with JIRA



Or through custom integration

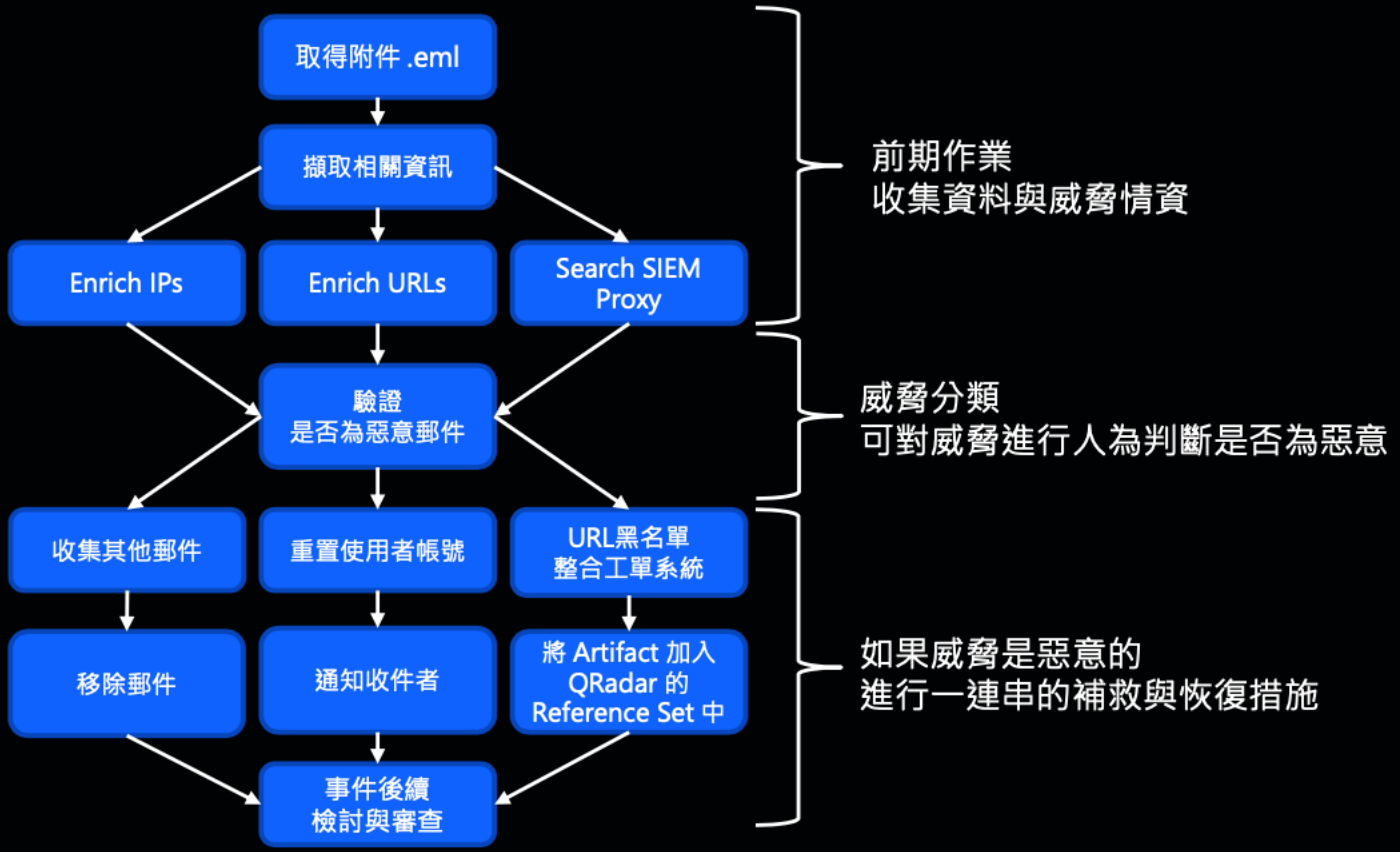
Or manually created using the New Incident Wizard

- Selecting the New Incident from the menu bar

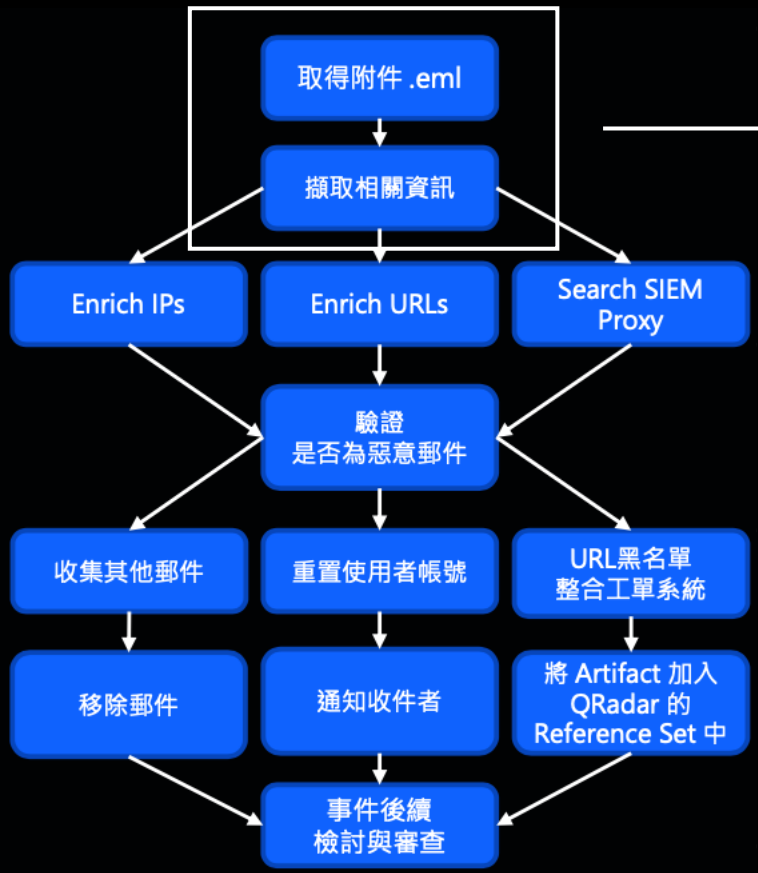
or

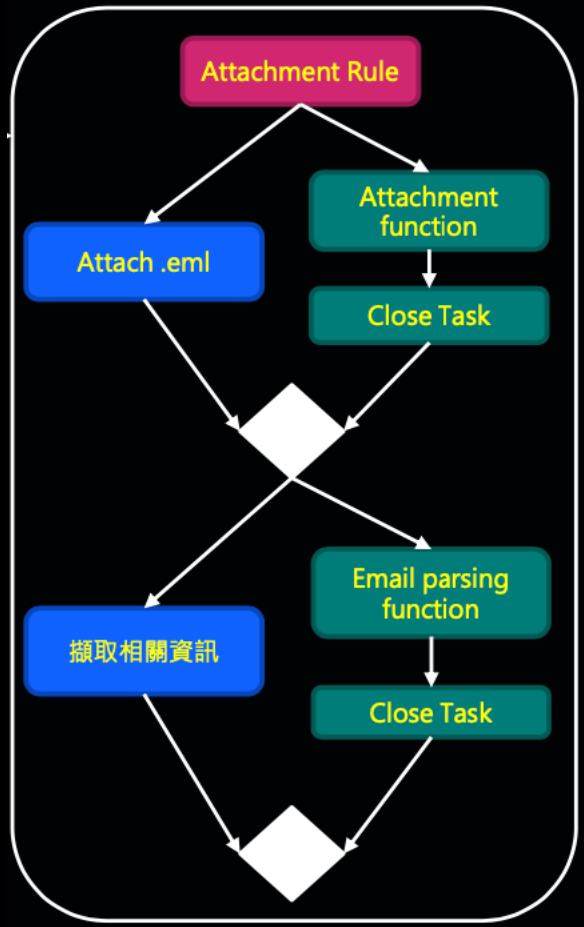
- Started by Web URI **https://<your.ip>/#external/new_by_url**

QRadar® SOAR 自動/半自動化腳本 (Automation)

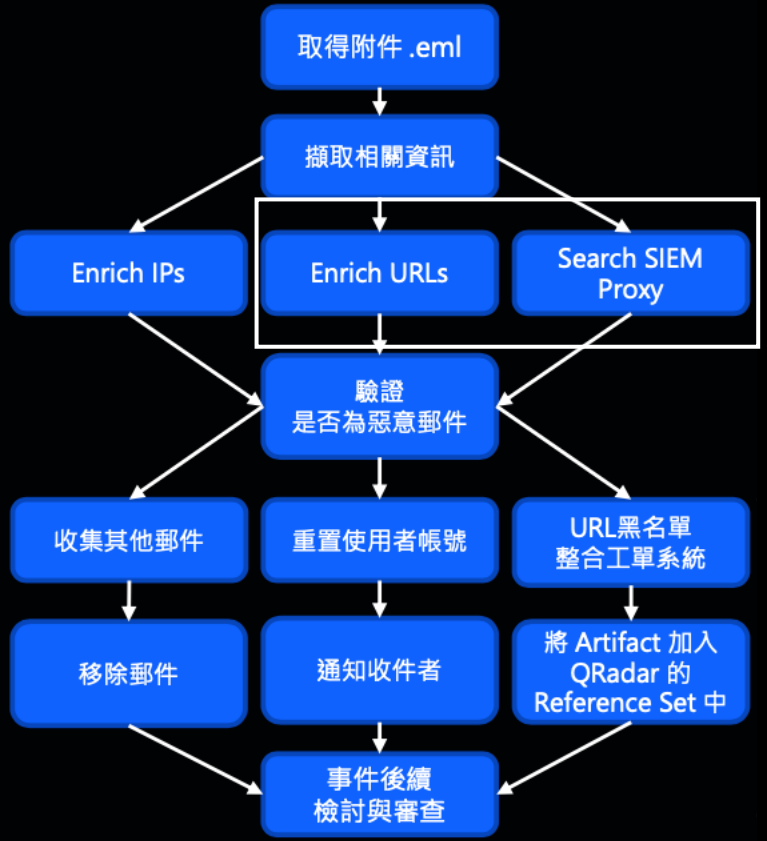


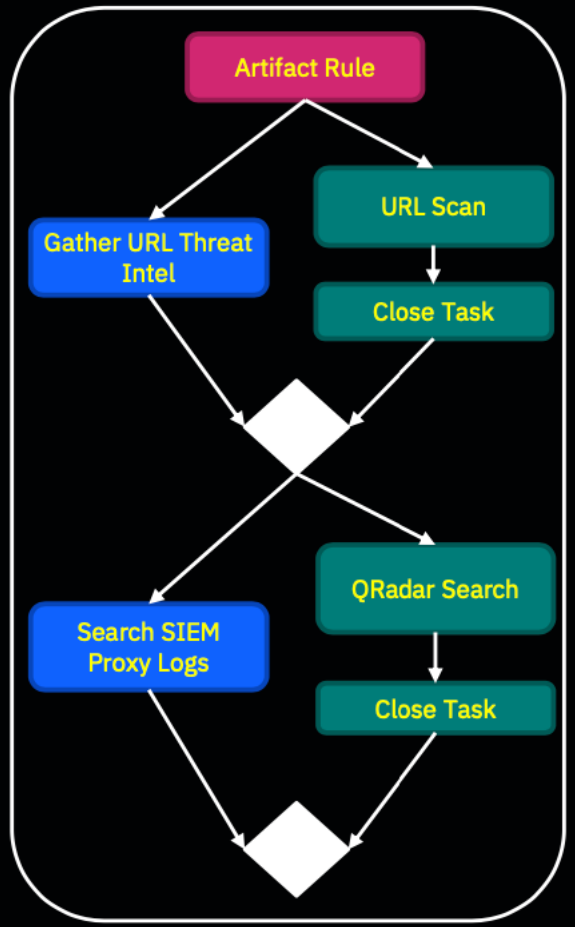
QRadar® SOAR Dynamic Playbook 動態劇本：釣魚郵件範例





QRadar® SOAR Dynamic Playbook 動態劇本：釣魚郵件範例

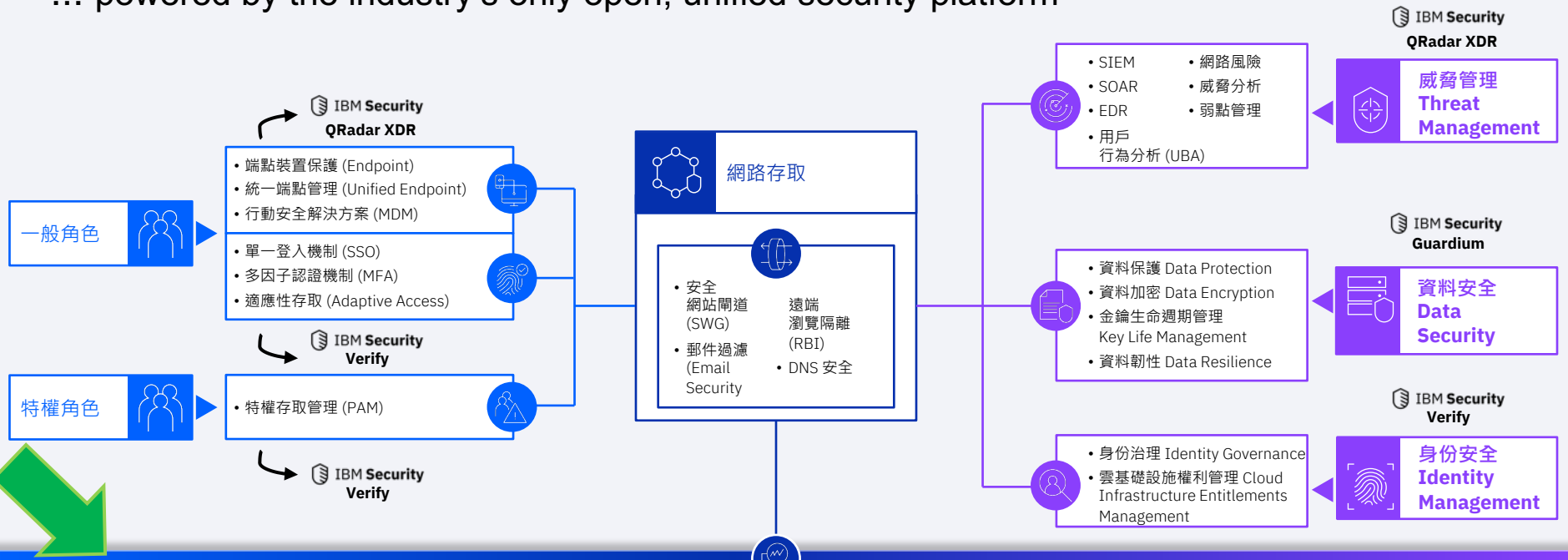




Malware protection

IBM Security™ End-to-end 的零信任 (Zero-Trust) 資安解決方案

... powered by the industry's only open, unified security platform



IBM Security Service

Zero Trust Acceleration Services
Ransomware Readiness Assessment
Risk Quantification Services
Incident Response Retainer
X-Force Threat Management

支援混合雲各式工作負載環境的資訊安全保護

Data Center

IaaS and PaaS

SaaS and Web

IBM Security X-Force Threat Intelligence Index 2022

Key findings

Ransomware the top attack type

21%
Percentage of attacks that were ransomware

17 months
Average time before a ransomware gang rebrands or shuts down

Phishing and vulnerability exploitation the top attack vectors

41%
Percentage of attacks that used phishing for initial access

3X
Click effectiveness for targeted phishing campaigns that add phone calls

33%
Increase in the number of incidents caused by vulnerability exploitation

Threats to manufacturing, OT and IoT

#1
Manufacturing's rank in top attacked industries

61%
Manufacturing share of compromises in OT-connected organizations

2,204%
Increase in reconnaissance against OT

74%
Share of IoT attacks originating from Mozi botnet

Cloud, Linux threats rise

146%
Increase in Linux ransomware with new code

Asia becomes top attacked geo

26%
Share of global attacks that targeted Asia

2022 IBM Security X-Force Cloud Threat Landscape Report

IBM

Key findings

1. Cloud Vulnerabilities Rise in Numbers

28%

increase in new cloud vulnerabilities in the past year and their severity is increasing.

26%

of cloud incidents X-Force responded to were due to vulnerability exploitation – the most prominent cause of cloud compromises.

2. More Access – More Problems

99%

IBM Security X-Force was able to compromise cloud environments through users' excess privilege and permissions in 99% of penetration testing engagements.

3. Cloud Accounts Gain Grounds in Dark Web Marketplaces

200%

increase in cloud accounts now being advertised on the dark web, reaching 100,000 accounts.

76%

remote desktop protocol (RTP) most popular cloud account sales.

19%

compromised credentials second most popular cloud account sales.

4**. Manufacturers Feel Brunt of Cloud Attacks**

1 in 4

cloud attacks X-Force responded to were against manufacturing organizations – attackers are leveraging various avenues to compromise these highly sought-out targets.

Cost of a Data Breach Report 2022

IBM

Key findings

1. Average cost of a data breach reached a record high in 2022

USD 4.35 million
average cost of a data breach in 2022

60%
of organizations had to increase prices of products and services due to the data breach (contributor of inflation)

2. Deploying incident response, XDR, and AI/automation produced the largest savings in the study

USD 2.66 million
in savings for organizations with an incident response (IR) team and regularly tested IR plan vs. no IR team or IR testing

29 days
in saved breach response time for organizations with extended detection and response (XDR) technologies, compared to those without XDR

USD 3.05 million
in savings for organizations with fully deployed security AI and automation compared to organizations with no security AI or automation deployed

3. More organizations deploy zero trust in 2022 than 2021, with cost savings of about USD 1 million

41%
of organizations have deployed a zero trust security approach in 2022, compared to 35% in 2021

USD 1 million
in savings for organizations with zero trust deployed, compared to breaches at organizations without a zero trust security approach

4. Ransomware attacks were more expensive than the average breach, and more common in 2022

41%
increase in percentage of breaches that were ransomware from 2021-2022

USD 4.54 million
average cost of a ransomware breach, excluding the cost of the ransom

IBM Security™ QRadar® XDR 開放與完整的平台策略
... XDR is e**X**tended **D**etection and **R**esponse

IBM Security QRadar XDR 結合 IBM 與 第三方 資安解決方案達到全面 可視性 與 自動化 資安維運

QRadar **XDR Connect: Open Integration**

EDR	SIEM	NDR	SOAR	Threat Intel	Open Integrations
IBM Security QRadar EDR (ReaQta)	**IBM Security QRadar SIEM**	**IBM Security QRadar NDR**	**IBM Security QRadar SOAR**	**IBM Security X-Force**	aws
CROWDSTRIKE	splunk>	DARKTRACE	paloalto NETWORKS	Alien Vault, CISCO	Microsoft Azure
vmware Carbon Black	Azure Sentinel	ExtraHop	splunk> phantom	MANDIANT A FireEye Company, MAXMIND	MySql
TREND MICRO	MICRO FOCUS ArcSight	IronNet Cybersecurity	servicenow	REVERSING LABS, SANS	BIGFIX
Windows Defender	Elastic Search	Vectra	SWIMLANE	THREATQUOTIENT, VirusTotal	tenable
More EDR Integrations		*Requires QRadar SIEM to integrate*		*More Threat Intelligence Integrations*	*Many More Open Integrations*

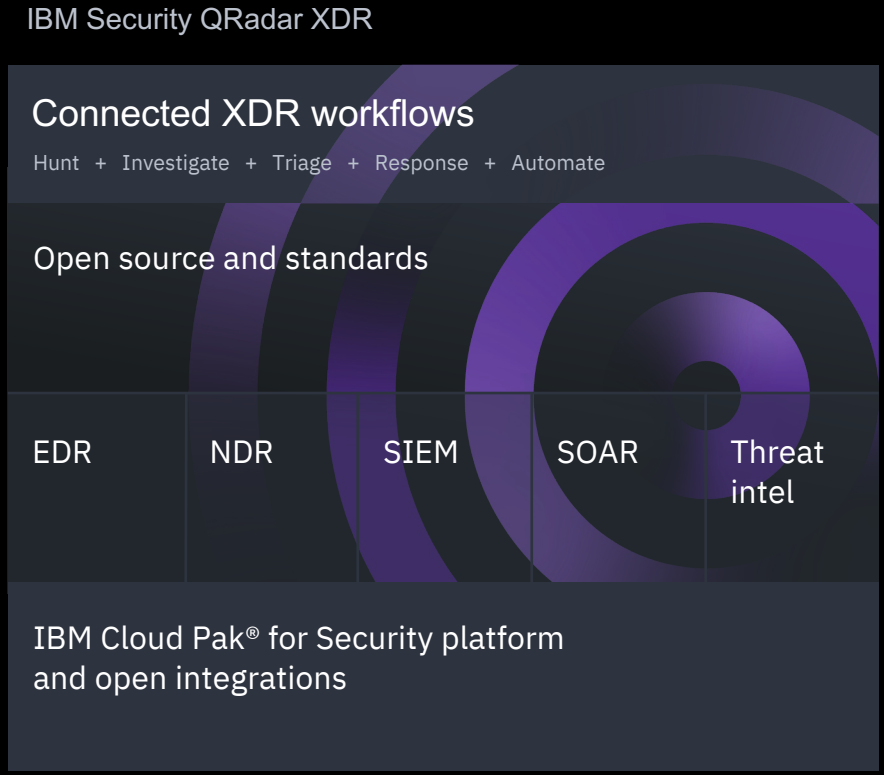
IBM Security QRadar XDR 完整且開放的連接平台

連接性：整合既有 IBM 或 其他資安工具
業界最大的開放式 XDR 生態系統可以整合您的 EDR、SIEM、NDR、SOAR 和威脅情報 (TI)，同時實現將資料留在原處、而無需重新搬遷原有資料，以實現完整的 XDR 偵測方法

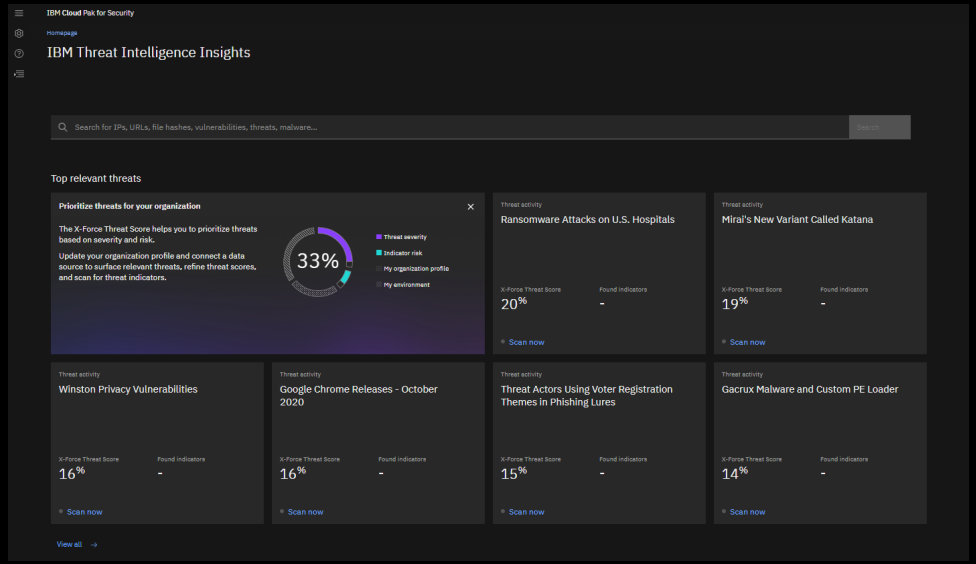
統一性：使用統一介面整合不同工具與團隊
透過統一與整合的 XDR 工作流程，有助於加快警報分類、威脅搜尋與事件調查和響應

智能輔助：使用 AI 技術提升資安分析師生產力
使用專門的 AI 和開箱即用的動態劇本 (Playbook)，包括自動化根因分析和 MITRE ATT&CK 攻擊威脅對應，以豐富、關聯和調查威脅整體工作

開放性：彈性的架構來避免特定廠商鎖定
基於 IBM Cloud Pak for Security (CP4S) ，滿足可部署在本地或雲端環境，提供企業等級的一站式安全服務



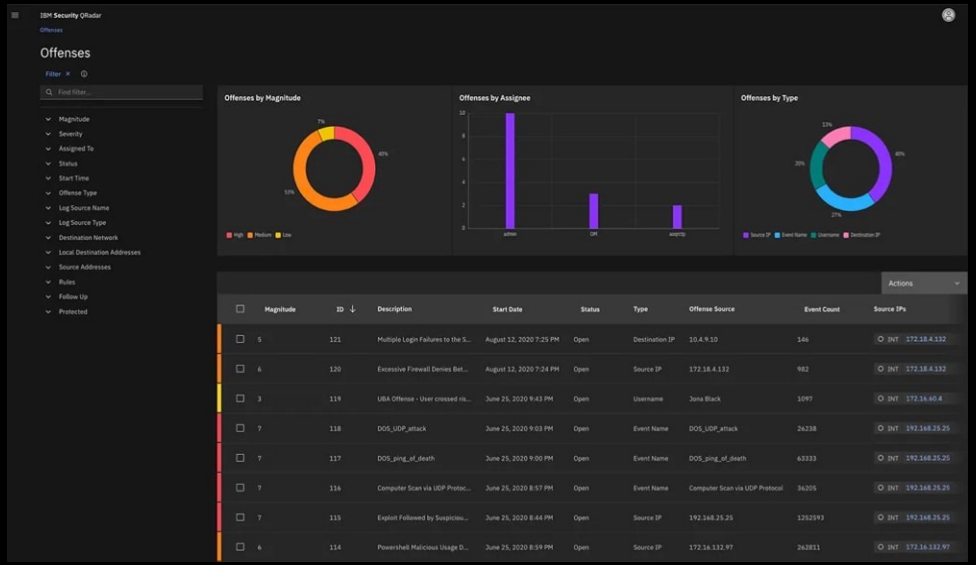
QRadar XDR 整合 Threat Intelligence Insight 提供以企業為中心的威脅偵測機制



整合與拓展威脅情資整合至 XDR 平台

- 更快速地偵測資安事件 (Detection)
  - 持續進化的進階威脅偵測技術
  - “Am I Affected” 的檢測分析
  - 自動化的威脅獵捕 (Threat hunting)
- 更快地告警分類機制 (Triage)
  - 誤告警的分析機制
  - 3rd Party SIEM 分類與分析
  - 3rd Party EDR 分類與分析
- 更快的回應時間 (Respond)
  - 萃取與應用 ATT&CK insights
  - ATT&CK 以時間軸方式呈現的分析

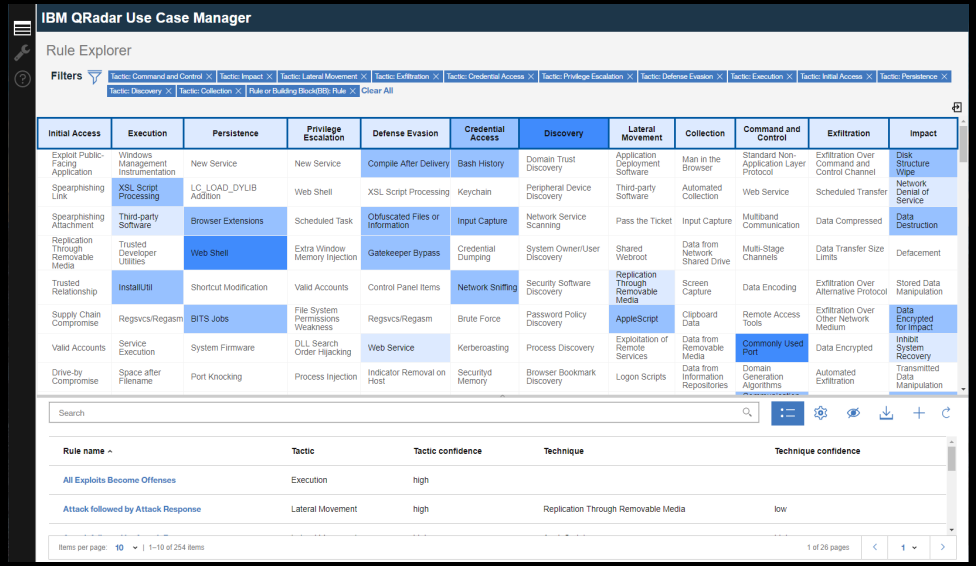
QRadar SIEM 透過整合事件 (Event) 與流量 (Flow) 提供威脅分析機制



擴展和簡化企業組織的威脅可見性：

- 簡化、有效的工作流程 (Workflow)
  - 以分析師為導向的威脅機制
  - 直覺、整合的 1 - Click Reach
- 強大的資料搜集與正規化 (Normalization)
  - 600+ 開箱即用的分析工具
  - 開放平台整合上百家夥伴的豐富生態系
  - 自動化的資料剖析與正規化
- 直覺、全面的威脅可視化 (Visibility)
  - MITRE ATT&CK 框架對應
  - 豐富的既有 Use case 管理
  - In 5-minute Use case 建立

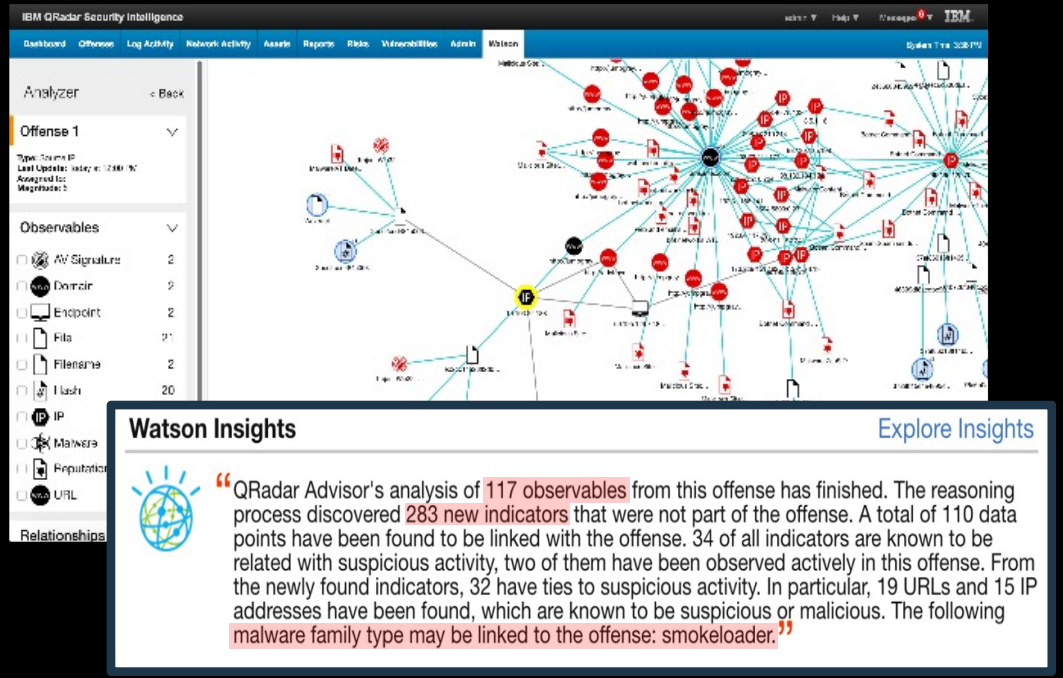
透過 QRadar SIEM 對應 MITRE ATT&CK 攻擊框架提供企業等級威脅可視化與進階威脅資訊



透過 QRadar XDR 同時對應威脅攻擊框架：

- 進階威脅分析 (Advanced analytics)
  - 1200+ 開箱即用的 use cases
  - 對應 MITRE ATT&CK 攻擊框架圖
  - 簡易高效的查詢語言
- 進階關聯分析 (Advanced correlation)
  - #1 關聯分析引擎機制
  - 偵測內部威脅與異常行為模式
  - 減少噪音與改善偵測可信度
- 整合用戶行為分析 (UBA)
  - 開箱即用的內部威脅偵測機制
  - 基於歷史與同儕團體比較演算法
  - 整合至整體 XDR 平台與軟體的偵測機制

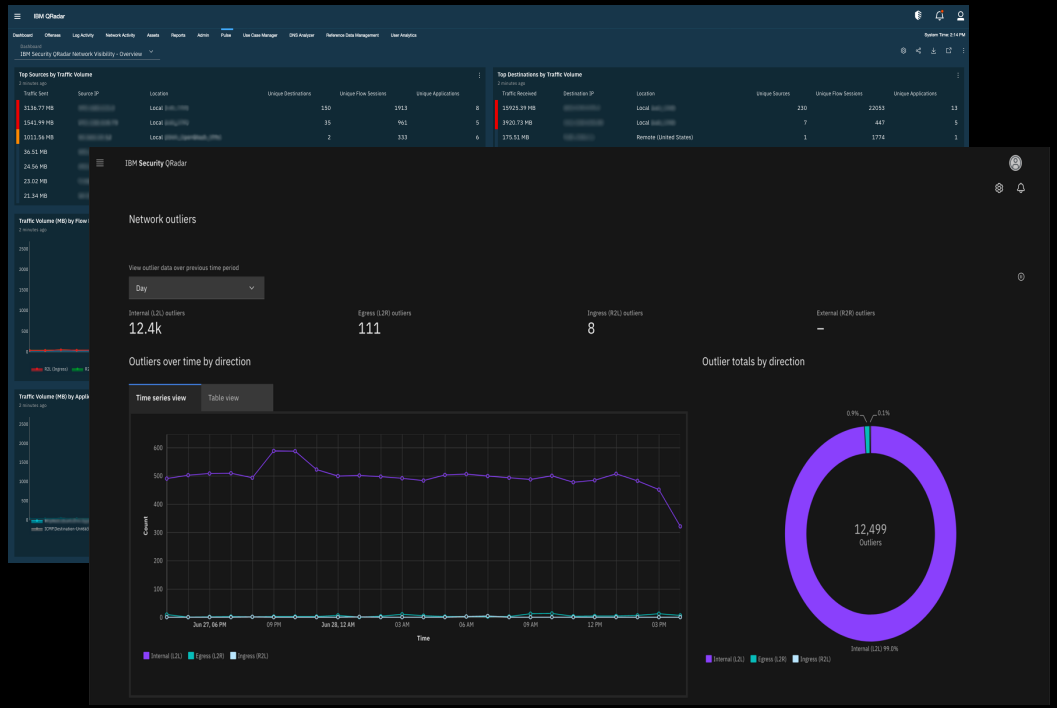
QRadar SIEM 整合 AI Watson for Cybersecurity 持續瞭解整體威脅



XDR 整合 Watson for Cybersecurity

- 自動發現安全事件的上下關聯，提供安全事件的完整輪廓
- 執行認知探索可疑活動及識別安全事件原因及其他的指標行為
- 迅速精准的安全性威脅分析，大幅節省威脅研究的時間與資源

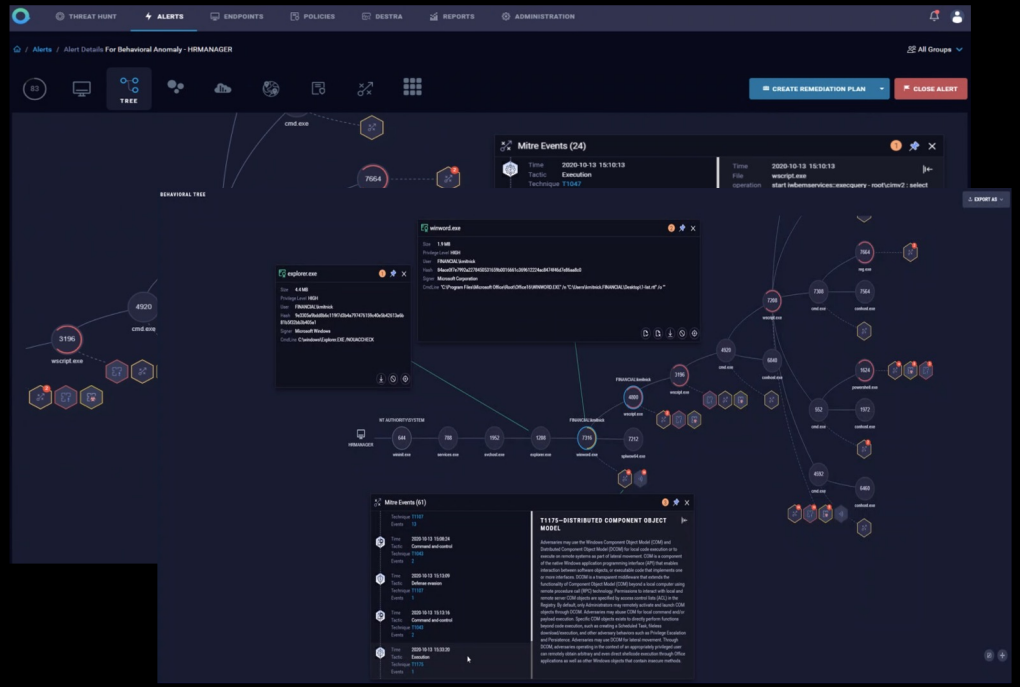
QRadar NDR 提供網路流量的可視化與網路流量異常分析 (NTA)



使用 NTA 技術偵測潛藏的威脅流量：

- 行為分析 (Behavioral analytics)
  - 透過流量偵測遭駭設備
  - 偵測 beaconing and C2 犯罪活動
  - 按會話的識別指標
- 進階鑑識分析 (Next-Gen Forensics)
  - 封包流量分析
  - 鑑識分析等級的流量調查
  - 自動化封包深度解析
- 資產識別 (Asset Aware)
  - 偵測未管制的 IT 設備資產
  - 自動建立化建立資產基準
  - 同步整合風險、CMDB 與弱點資訊

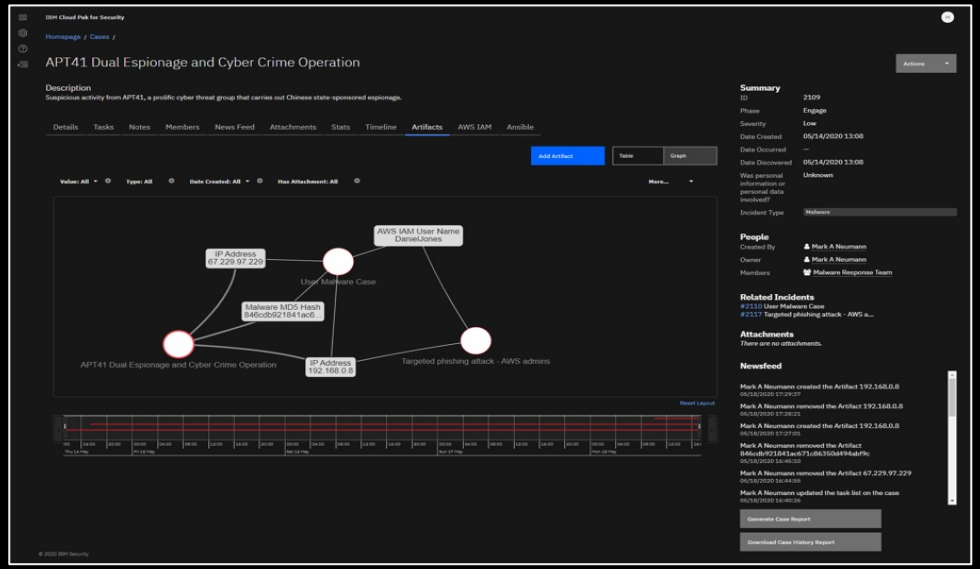
QRadar EDR (ReaQta) 端點提供威脅可視化與進階威脅分析調查



擴展和簡化端點 (Endpoint) 可見性：

- 統一的端點保護機制
  - 進階的 EDR 解決方案 with AV 防毒引擎
  - 支援整合 3rd-party AV
  - 輕量級的部署與安裝
- 整合零信任 (Zero-Trust) 機制
  - 保護終端用戶與設備
  - 支援在地端與不連網 (Air-Gap) 環境運作
- 整合即時性的 AI 技術
  - 自動化使用進階的威脅獵捕技術
  - 有效減輕資安威脅分析負擔

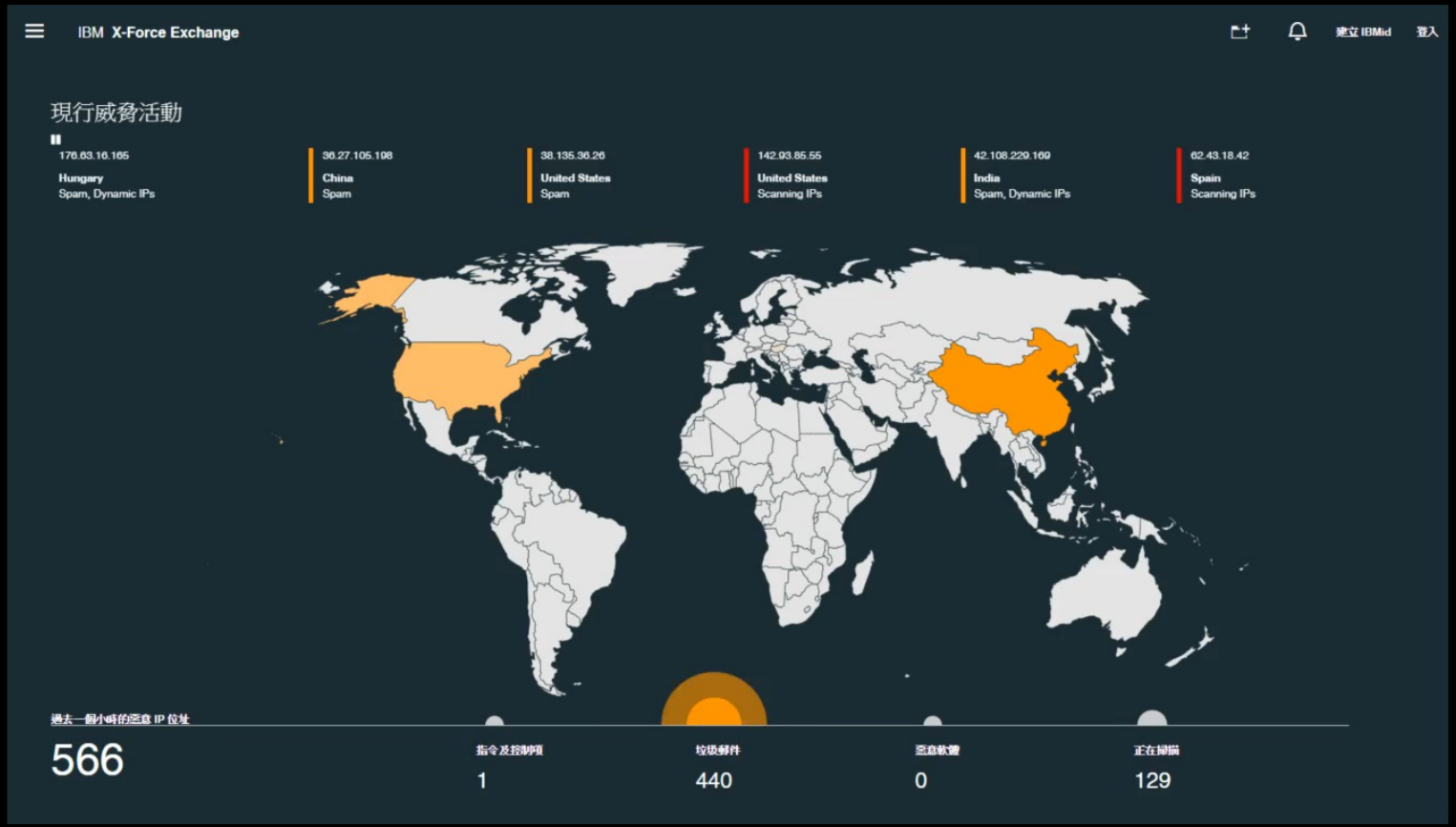
QRadar SOAR 提供整合、協作與自動化事件響應流程



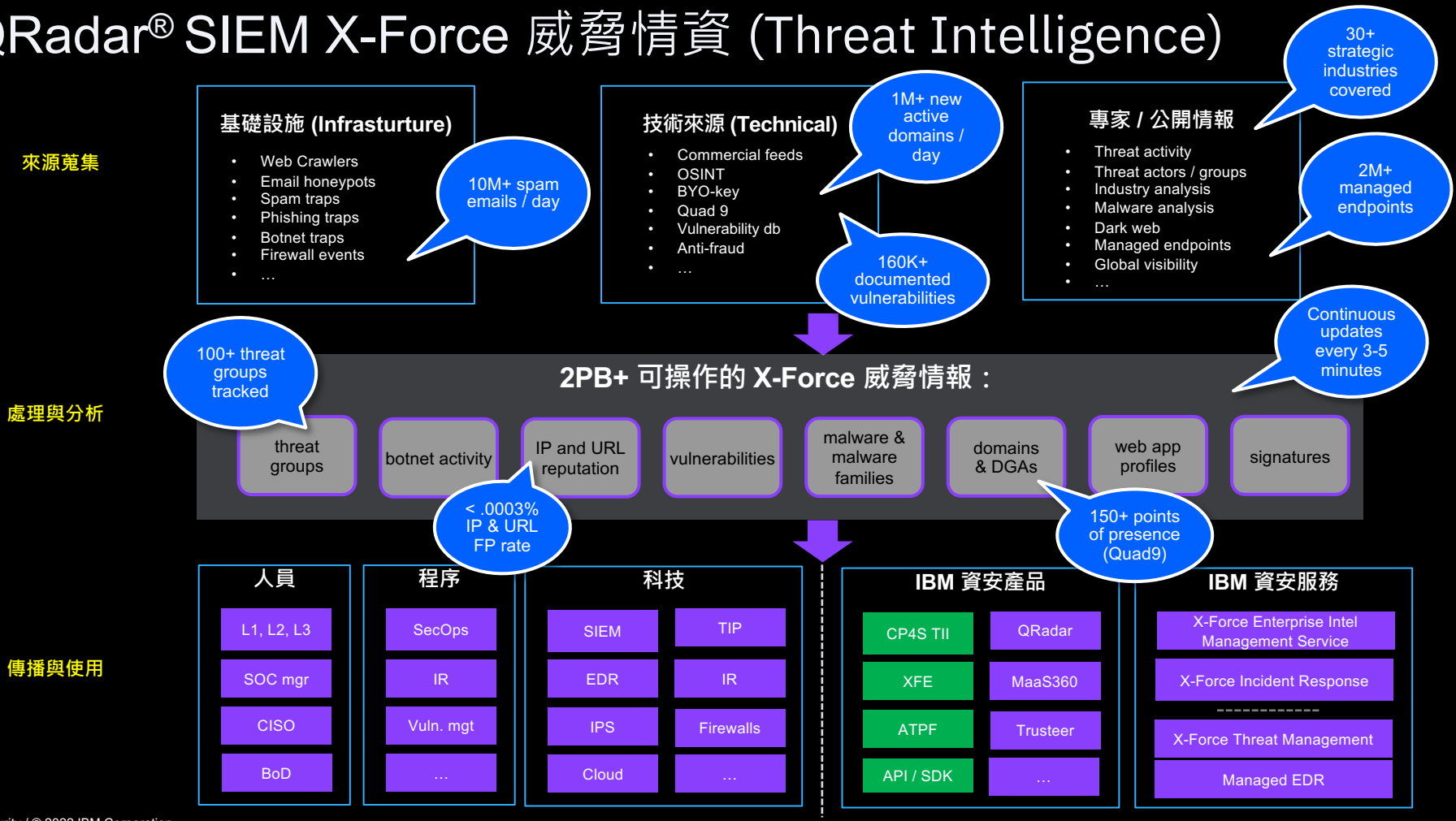
整合各式資安工具提供自動化響應：

- 整合人員、工具與機制 (Orchestration)
  - 整合調度現場與遠端工作流程
  - 自動化重複性與持續的流程
  - 企業級的事件構建 (IoCs) 指標分析
- 資安事件場景的流程自動化 (Automation)
  - 拖曳式的 劇本 (Playbook) 建立與編輯
  - 提供強大的資安事件調查自動化工具
  - 支援整合 Red Hat Ansible (ITOps)
- 同步整合法律與合規機制 (Compliance)
  - 提供法規面的影響分析與建議決策
  - 提供風險與合規面洞察意見回饋

QRadar® SIEM X-Force 威脅情資 (Threat Intelligence)



QRadar® SIEM X-Force 威脅情資 (Threat Intelligence)



Insight: Threat Intelligence

DNS 早期示警惡意網域進行阻擋 (Early Warning)

Early Warning Feed 透過 IBM Security 與 Quad9 的協作，每天能夠針對數百個新惡意網域提供預警，能夠讓安全分析人員更快的因應隨時來臨的攻擊

透過網域的深層生命週期及其活動的大量資料，提供即時與可採取行動的情報，可幫助分析師防禦 DNS 攻擊，例如網絡釣魚、網域搶註以及 DGA 演算法

1,000萬

每天由 Quad9
阻止惡意 DNS 請求

Quad9

識別惡意網域時間平均比其他威脅情報供應者早

8 天