# 目錄
# CONTENT

THALES
Building a future we can all trust

# CipherTrust 資料保護平台

## 加密並控制重要資料的存取


資料外洩事件持續以驚人的速度不斷發生，機敏資料的安全維護對所有企業而言都至關重要。此外，企業積極遵循全球和區域性的資料隱私法規，並尋求在加速採用雲端技術的同時確保存取安全。資安單位需要以資料為中心的方案，藉此維護資料從網路移動到應用程式和雲端時的安全。當邊界網路控制與端點安全措施失效時，靜態資料保護便成為最後一道防線。

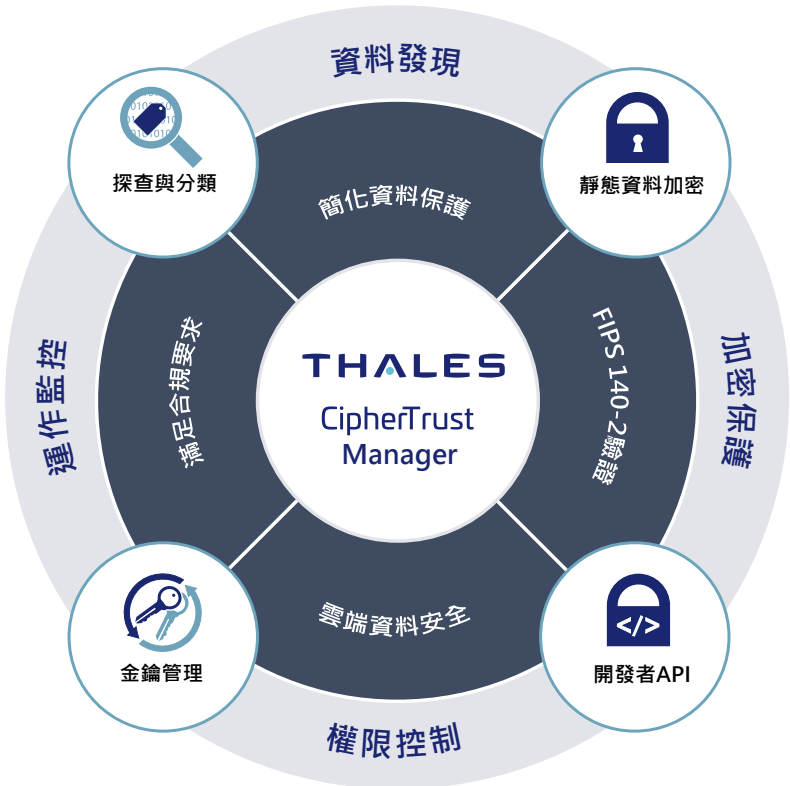
CipherTrust 資料安全平台整合了資料的發現、分類、保護，以及前所未有的分級存取控制，並提供集中化金鑰管理。CipherTrust 解決方案移除了資料保護的複雜性、加速法規遵循，並確保雲端轉移安全，減少投資資安營運所需的資源；同時提供無所不在的法規遵循控管，大幅降低企業整體風險。

## 主要特色

- 集中管理主控台
- 監控及報表功能
- 資料發現及分類
  - 以資料可視性進行風險分析
- 資料保護技術
  - 檔案、資料庫與容器的透明加密
  - L7 應用層資料保護
  - 保留資料格式的加密方法(FPE)
  - 代碼化(Tokenization)與動態資料遮罩
  - 靜態資料遮罩
  - 特權使用者存取控制
- 企業等級金鑰集中管理平台
  - FIPS 140-2 認證
  - 支援 KMIP 協定
  - 支援多雲環境的金鑰管理
  - 資料庫加密金鑰管理(Oracle TDE, big data, MS SQL, SQL Server Always Encrypted 等)

## 關於 Thales

許多企業組織在資料保護上都仰賴 Thales 的專業技術。企業在維護資料安全上，面對越來越多重要的決策，不論是加密策略建構、資料移轉至雲端，或是滿足資料法規的合規要求，在邁向數位轉型時，您都可以依靠 Thales 來保護最重要的資料。Thales 為關鍵決策提供關鍵技術。




## 法規遵循

**CipherTrust 資料保護平台支援全球安全和隱私法規，包括：**

- GDPR
- PCI DSS
- HIPAA
- SOX/GLBA
- CCPA
- FIPS140-2
- FISMA, FedRAMP
- NIST 800-53 rev.4
- 南非 POPI Act
- ISO/IEC 27002:2013
- 日本 My Number Compliance
- 南韓 PIPA
- 印度 Aadhaar Act
- 菲律賓 Data Privacy Act
- 新加坡 Monetary Act
- 澳洲 Privacy Amendment

## 關鍵效益

- **簡化資料安全**

  借助新一代資料保護解決方案，發現、保護、控管每一處的機敏資料。CipherTrust 資料保護平台透過集中管理主控台這個單一平台簡化資料安全管理，為企業提供強大的工具來發現、分類機敏資料、對抗外部威脅、防範內部人員濫用，並建立持續的控制，即便資料儲存在雲端或外部服務供應商的基礎設施內亦是如此。組織可以輕鬆查找並縮小隱私缺口、確定保護的優先順序，在實施數位轉型前就擬定正確的隱私與安全決策。

- **加速合規時程**

  監管與稽核單位要求企業必須控管那些受管制和具機敏性的資料，並提出報告佐證。CipherTrust 資料保護平台所具備的功能，如資料發現與分類、加密、存取控制、稽核日誌、代碼化及金鑰管理等，能支援這些資料安全和隱私要求。平台的集中性和模組(connector)佈署可快速延伸、增加，以因應不斷變化的合規要求。

- **安全的雲端轉移**

  CipherTrust 資料保護平台提供進階加密與集中化金鑰管理方案，讓企業能夠安全的將機敏資料儲存在雲端；同時也提供先進的多雲自帶加密(BYOE)方案，避免受限於雲端供應商的加密方案，並透過集中、獨立的加密金鑰管理功能，確保資料可以安全而有效率地跨越多重雲端環境。

  無法執行 BYOE 的企業仍可以從外部透過 CipherTrust 雲端金鑰管理(Cloud Key Manager)管理金鑰，以遵循業界最佳實務規範；且 CipherTrust 雲端金鑰管理支援在多個雲端架構和 SaaS 應用服務中自帶金鑰(BYOK)。CipherTrust 資料保護平台為企業在雲端的機敏資料和應用程式提供最強的保護，協助任何地方建立、使用或儲存的資料合規並獲得更大的資料控制權。

# CipherTrust 資料保護平台產品

## CipherTrust Manager 集中管理系統

CipherTrust Manager 是平台的中央管理系統，也是業界領先的企業金鑰管理方案，提供金鑰集中管理、分級存取控制和安全政策配置功能。CipherTrust Manager 管理金鑰的生命週期任務，包括生成、輪替、銷毀、匯入和匯出，提供金鑰和政策的 role-based 存取控制，支援強大的稽核與報告，以及易於開發、管理的 REST API。CipherTrust Manager 提供實體與虛擬版方案，並具備 FIPS 140-2 level 3 的合規標準。CipherTrust Manager 也可搭配 Thales Luna 和 Luna Cloud HSM 等硬體安全模組使用。

## CipherTrust 資料發現與分類

CipherTrust 資料發現與分類可在跨雲、大數據和傳統資料存儲途徑中找出需受監管的資料，包括結構化和非結構化的數據。透過單一管理平台可以輕鬆掌握機敏資料及其風險，進而對安全漏洞、法規遵循與修補優先順序等作業做出更好的決策。CipherTrust 資料發現與分類解決方案提供流暢的工作流程，從政策配置、資料發現、分類到風險分析與報告等，以協助排除資安盲點與複雜性。

## CipherTrust 透明加密

CipherTrust 透明加密提供靜態資料加密、特權用戶存取控制和詳細的資料存取日誌記錄。代理程式可橫跨雲端和大數據環境中的實體與虛擬伺服器，保護 Windows、AIX 和 Linux 等作業系統中的檔案及資料庫數據。CipherTrust 透明加密的 Live Data Transformation 延展功能提供免停機的資料加密與金鑰更換。此外，安全情資日誌與報告也運用了先進的 SIEM 系統，可簡化合規報告並加速威脅檢測。

## CipherTrust Tokenization 代碼化

CipherTrust Tokenization 提供 Vault 和 Vaultless 版本，協助降低資料法規遵循（如PCI-DSS）所需的成本與複雜性。Tokenization 將敏感數據替換為代碼（token），以確保機敏資料的安全，與資料庫和非授權使用者及系統保持隔離。Vaultless 版本包括基於政策的動態資料遮罩功能，兩種方案都讓應用程式的重要資料代碼化變得更容易。

## CipherTrust Database Protection 資料庫自帶加密功能整合

CipherTrust 資料庫保護解決方案透過安全、集中化的金鑰管理，整合資料庫內建的敏感欄位加密功能，且不需修改資料庫應用程式。CipherTrust 資料庫保護解決方案支援 Oracle、MS SQL、IBM DB2 和 Teradata 資料庫。

## CipherTrust 金鑰管理

CipherTrust 金鑰管理提供強大且基於標準的加密金鑰管理方案，簡化了諸多加密金鑰管理的挑戰，確保金鑰安全且僅提供給獲得授權的合法加密服務使用。CipherTrust 金鑰管理支援多種使用情境，包括：

- **CipherTrust 雲端金鑰管理**

  為 AWS、Azure、Salesforce 和 IBM Cloud 提供精簡優化的 BYOK 管理。解決方案提供完整的雲端金鑰生命週期管理與自動化，以強化資安團隊效率、簡化雲端金鑰管理。

- **CipherTrust TDE 金鑰管理**

  支援多種資料庫，如 Oracle、Microsoft SQL 和 Microsoft Always Encrypted。

- **CipherTrust KMIP Server**

  集中管理 KMIP client，如全磁碟加密(FDE)、大數據、IBM DB2、磁帶備份、VMware vSphere 和 vSAN 加密等。

## CipherTrust CTE-RWP 透明加密勒索軟體防護

CipherTrust CTE-RWP（Transparent Encryption Ransomware Protection）以低資源消耗且非侵入性的保護方式，保護文件、資料夾免受勒索軟體攻擊。CTE-RWP 使用機器學習模型來動態偵測可疑的檔案 I/O 活動，無需修改任何終端機或伺服器上的應用程式、設定對每個文件及資料夾的限制性存取控制和加密策略，即可在偵測到異常時發出警報或阻止。

# CipherTrust Manager 技術規格表

## 硬體規格（k470, k570）

| | |
|---|---|
| **尺寸** | 19.0"(寬) x 21"(深) x 1.75”（高) |
| **重量** | 12.7kg (28lbs) |
| **CPU 處理器** | Intel Xeon E3-1275v5 |
| **記憶體** | 16 GB |
| **硬碟空間** | 1 X 2TB SATA SE (Spinning Disk) |
| **Serial 序列埠** | 1 |
| **網路介面** | 4x1GB or 2x10GB/2X1GB |
| **電源供應器** | • 平均耗電量 (Watts) 0.7A @120V (84W)<br>• 最大耗電量 (Watts) 0.83A @120V (100W)<br>• 電壓: 100-240V 50-60Hz |
| **電源線** | • PSE 認證<br>• 多國規格配置 |
| **平均故障間隔時間** | 153,583 |
| **機殼入侵偵測** | 防篡改密封. k570 內建的 HSM 若偵測到破壞性侵入，將自動清空資料 |
| **運作溫度** | 0 to ~35°C |
| **非運作時溫度** | -20 to 60 °C |
| **運作相對濕度** | 5% ~ 95% 非凝結狀態 |
| **FIPS 140-2 認證** | https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3519 |
| **嵌入的 HSM 管理** | k570 (內建 HSM) , 管理介面及 REST API 都允許設定或介接 HSM |
| **硬體安裝** | 含滑軌安裝套件 |

## 軟體規格

| | | | | |
|---|---|---|---|---|
| **管理介面** | Management Console, REST API, ksctl (Command Line Interface), NAE XML | | | |
| **最大金鑰數量** | k470 | k570 | k170v | k470v |
| | 1M | 1M | 50K | 1M |
| **最大分區數(multi-tenancy)** | 1000 | | | |
| **API 支援** | REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG | | | |
| **登入認證方式** | • 本地認證 • AD/LDAP • 憑證驗證登入<br>• K570: 利用Local or Remote PED 進行主密鑰的建立及設置 | | | |
| **支援的 HSM** | Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, Data Protection on Demand, AWS CloudHSM | | | |
| **叢集支援(Cluster)** | Active/Active. Max Nodes=10 cluster<br>叢集成員可以是實體或虛擬版. k170v 僅限為 2-node clusters. | | | |
| **備份** | 手動/排程; 支援以 HSM 金鑰加密備份 | | | |
| **網管** | SNMP v1, v2c, v3, NTP, Syslog-TCP | | | |
| **日誌格式** | RFC-5424, CEF, LEEF | | | |
| **認證** | k570: FIPS 140-2 L3<br>K470, k170v 及 k470v 可介接 Luna Network HSM 確保主密鑰安全強度 | | | |

## 虛擬版硬體需求

| | k170v | k470v |
|---|---|---|
| **最小 CPU 數** | 2 | 4 |
| **最小記憶體(GB)** | 4 | 16 |
| **最小硬碟空間(GB)** | 100 | 200 |
| **最小虛擬網路埠數量** | 1 | 2 |

# Thales Luna Network HSM

在 Thales Luna Network 硬體安全模組（HSM）中儲存、保護、管理金鑰，能以效能領先業界的高安全性、防竄改、網路連結功能，保障機敏資料和重要應用程式的安全。且 Luna Network HSM 可整合各種應用程式加速加密作業、保障金鑰週期安全、為整體加密設計提供最安全的信任基礎架構。

## 主要特色

### 卓越效能

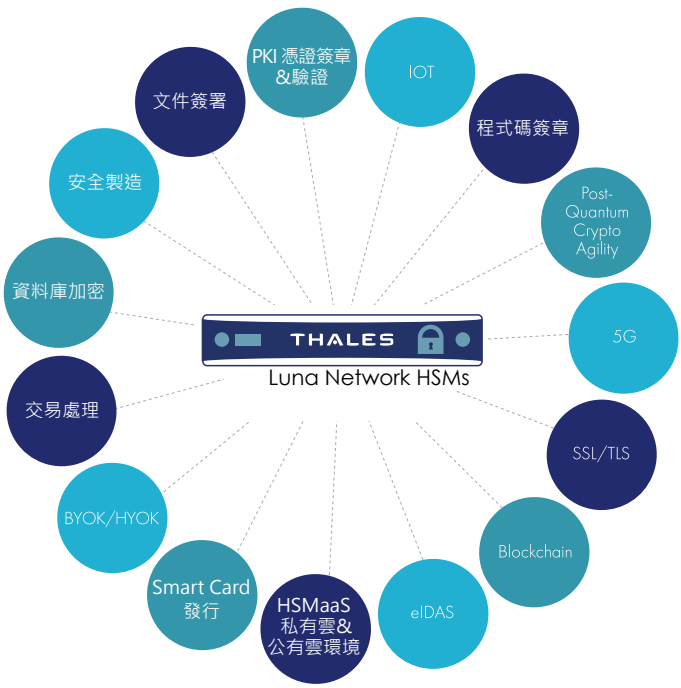
- 超過每秒 20,000 ECC 和 10,000 RSA 作業的高效運行，滿足企業對高效能的需求
- 延遲時間更短，效能更高

### 最高的安全性與合規規格

- 金鑰儲存在通過 FIPS 驗證、防竄改的硬體中
- 符合 GDPR、eIDAS、HIPAA、PCI-DSS 等要求
- 符合雲端現存標準
- 多重角色，實現高度權責分離
- M of N 多人特徵控制及多因素驗證，提升安全性
- 確保稽核記錄安全性
- 具備安全傳輸模式的高保證度傳遞效能
- 以外部 Quantum RNG 植入的高品質金鑰
- 可使用 Luna backup HSM 安全地備份、複製金鑰，或根據需要，使用資料保護將金鑰備份、複製到雲端，以實現效能運用、可靠性和災難恢復

### 降低成本並節省時間

- 支援 HSM 遠端管理，無需奔波
- 減少稽核與合規開銷負擔
- 企業系統自動化，透過 REST API 管理 HSM
- 多應用程式或租戶可共享 HSM，提高資源利用
- 彈性分割區規則，符合您的金鑰管理與合規需求




- Luna Client 可在容器中使用，便於移動、提高效率並減少經常性開銷
- 功能模組
  - 延伸原生 HSM 功能
  - 於 HSM 安全規範中建立、佈署客製化程式

## 技術規格

### 支援作業系統

- Windows、Linux、Solaris、AIX
- Virtual: VMware、Hyper-V、Xen、KVM

### 支援應用程式編程介面

- PKCS#11、Java (JCA/JCE)、Microsoft CAPI 與 CNG、OpenSSL
- REST API 管理

### 支援加密演算法

- 完整支援 Suite B
- 非對稱式演算法：RSA、DSA、Diffie-Hellman、Elliptic Curve 加密演算法（ECDSA、ECDH、Ed25519、ECIES），搭配命名、使用者自訂和 Brainpool curves、KCDSA 等
- 對稱式演算法：AES、AES-GCM、Triple DES、DES、ARIA、SEED、RC2、RC4、RC5、CAST 等
- 雜湊 / 訊息摘要 / HMAC：SHA-1、SHA-2、SHA-3、SM2、SM3、SM4 等
- Key Derivation：SP800-108 Counter Mode
- Key Wrapping：SP800-38F
- Random Number Generation：設計符合 AIS 20/31 對 DRG.4 使用以硬體為基礎的真雜訊來源，並配合 NIST 800-90A 相容 CTR-DRBG
- Digital Wallet Encryption：BIP32
- 用於用戶身份驗證的 5G 加密機制：Milenage、Tuak 和 COMP128

### 安全憑證

- FIPS 140-2 Level 3：密碼與多因素驗證 (PED)
- 針對保護規範 EN 419 221-5 的通用標準 EAL4 + (AVA_VAN.5 和 ALC_FLR.2)
- 符合 eIDAS 要求的合格簽章生成裝置 (QSCD) 清單

### 主機介面

- 2 個選項：4 個可單獨設定的 1G 自動感應 Ethernet LAN port 或 2 個 10G SFP port 和 2 個 1G RJ45 port (copper)
- 支援 IPv4 和 IPv6

### 實體規格

- 標準 1U 19 英吋機架式規格
- 尺寸：482.6 mm x 533.4mm x 43.815mm
- 重量：28 磅（12.7 公斤）
- 輸入電壓：100-240V，50-60Hz
- 耗電量：最高 110W，一般 84W
- 散熱性：最高 376BTU / 小時，一般287BTU / 小時
- 溫度：作業溫度 0°C–35°C

### 可靠性

- 雙熱插拔電源
- 平均故障間隔（MTBF）171,308 小時

### 管理及監控

- HA 災難修復
- 將硬體備份、復原到地端或雲端硬體
- SNMP、Syslog

## 硬體型號規格

### Luna A 系列 - 密碼驗證，簡易管理

| A700 | A750 | A790 |
|---|---|---|
| 2 MB 記憶體 | 16 MB 記憶體 | 32 MB 記憶體 |
| Partitions : 5 | Partitions : 5 | Partitions : 10 |
| Maximum Partitions : 5 | Maximum Partitions : 20 | Maximum Partitions : 100 |
| 標準效能<br>RSA-2048 : 1,000 tps<br>ECC P256 : 2,000 tps<br>AES-GCM : 2,000 tps | 企業效能<br>RSA-2048 : 5,000 tps<br>ECC P256 : 10,000 tps<br>AES-GCM : 10,000 tps | 最大效能<br>RSA-2048 : 10,000 tps<br>ECC P256 : 22,000 tps<br>AES-GCM : 17,000 tps |

### Luna S 系列 - 多因素（PED）驗證，最高安全性部署環境

| S700 | S750 | S790 |
|---|---|---|
| 2 MB 記憶體 | 16 MB 記憶體 | 32 MB 記憶體 |
| Partitions : 5 | Partitions : 5 | Partitions : 10 |
| Maximum Partitions : 5 | Maximum Partitions : 20 | Maximum Partitions : 100 |
| 標準效能<br>RSA-2048 : 1,000 tps<br>ECC P256 : 2,000 tps<br>AES-GCM : 2,000 tps | 企業效能<br>RSA-2048 : 5,000 tps<br>ECC P256 : 10,000 tps<br>AES-GCM : 10,000 tps | 最大效能<br>RSA-2048 : 10,000 tps<br>ECC P256 : 22,000 tps<br>AES-GCM : 17,000 tps |

tps = 每秒交易處理量

# payShield 10K 金融支付產業專用

## 專為信用卡支付系統與行動支付安全所設計的硬體安全模組(HSM)，保障全球支付安全

- 適合銀行、第三方支付業者使用，符合國際發卡機構安全稽核要求
- 擁有業界領先的效能：最高可達 2,500 tps
- 提供高可用性及完善的金鑰管理機制
- 符合 FIPS 140-2 安全等級，提供硬體強化的防竄改環境、防外力破壞


## 主要特色

- payShield 10K 是專為信用卡支付系統與行動支付安全所設計硬體安全模組(HSM)，在全球支付生態系統中受到發卡方、服務提供者、收單行、處理方和支付網路廣泛使用。對於面對面和遠端支付服務，payShield 在保護支付認證頒發、用戶身份驗證、卡片驗證和機敏資料保護的過程，提供領先的安全與支付技術。
- 擁有高可用性與高效能的金融交易專用 HSM，可同時處理最高每秒 2,500 筆交易量，滿足金融業瞬間大量交易需求。
- 與 payShield 9000 設備相容，不需要改變既有資安政策，可共用現有的 LMK IC 晶片卡，且原本的 payShield 9000 客製化功能可升級到 payShield 10K。
- 滿足零售業導入 mPOS 系統的行動支付安全，從讀卡機產生密鑰，並確保 PIN 碼全程被保護，以及解密資料必須與商家網路隔絕。確保消費者信用卡個資不外流，提升商家交易安全信賴度。
- 保護終端模擬（Host Card Emulation, HCE）模式的行動支付安全。發卡者使用 HSM 可安全地產生並集中儲存支付憑證，且能彈性決定當離線授權時在何時、有多少金鑰可被存在手機中；而在線上授權時，發卡者則可即時驗證手機支付 App 的密文。
- payShield 10K 獨特功能讓行動支付中的各環節能安全配置相關應用，包括支付 App 的發行到手機。同時也能安全配置其他使用非接觸式支付的應用，如 NFC 或 P2P 支付應用等。
- 卡片 / 行動支付支援：payShield 10K 提供全面性功能，在以下多個領域提供主要支付品牌支援（美國運通、Discover、JCB、Mastercard、銀聯和 Visa）的需求，包括：
  - 符合最新導入的支付卡系統 HSM 標準，如主要支付品牌的 PIN 碼和卡片驗證功能
  - EMV 交易授權和訊息傳遞
  - 行動支付交易授權和金鑰管理
  - ATM 和 POS 裝置遠端金鑰載入
  - 區域 / 全國金鑰管理(包括澳洲、德國和義大利)
  - Mastercard 代理金鑰管理 (OBKM) 支援
  - 支援磁條和 EMV 的資料準備和個人化，包括行動佈建方式
  - PIN 碼生成和列印

## 法規遵循

- 整機符合支付交易安全要求 FIPS 140-2 Level 3 加解密模組最廣泛採用的安全標準。
- 符合最新導入的支付卡系統 HSM 標準 Payments Card Industry Hardware Security Module standard (PCI HSM v3)。
- 加密性能與管理功能符合或超越國際支付機構安全稽核要求，包括美國運通、Discover、JCB、Visa、Mastercard 以及銀聯。
- payShield 10K 符合 Global Platform Card Specification 以及 EMV Card Personalization Specification，能建立與行動支付安全元件之間的安全對話。

# 應用 - payShield 10K 專為信用卡支付設計包含發卡與支付作業

支付方式、載具變化，從傳統 ATM、信用卡等接觸式，衍生出行動支付、NFC 等非接觸式卡片，近年來亦發展出第三方支付，收單部分有無線化、行動化的趨勢。國內甚至有第三方支付專法通過，第三方支付產業預期可蓬勃發展，國內外電商及銀行也紛紛著手建置適用的交易平台與服務。

這樣的變化回歸原點，使用者是否能接受除了考慮方便性外，最重要的還是交易是否安全可靠。因此支付交易始終遵循國內外主管機關訂製嚴格的交易機制，HSM 在其中扮演至關重要的角色，負責金鑰管理、身分驗證、密碼驗證、交易資料加密等關鍵工作，HSM 除了確保安全性之外，同時也可以簡化作業過程，降低管理複雜度。

| 接觸式支付方式 | 非接觸式支付方式 |
|---|---|
| ▶EMV | ▶TSM 金流信任管理平台 |
| ▶DUKPT | ▶PSP 支付服務業者 |
| ▶POS 收單系統 | ▶mPOS 行動支付 |
| ▶置發卡作業 | ▶NFC 近場通訊 |
| ▶PCI DSS | ▶HCEP2PE 點對點加密 |
| ▶磁條卡交易 | ▶VISA/Master/JCB/美國運通/銀聯 |
| ▶ATM 交易 | |
| ▶信用卡交易 | |
| ▶網路銀行 | |

## 技術規格

**支援加密演算法**

- DES 和 Triple-DES 金鑰長度 112 和 168 位元
- AES 金鑰長度 128、192 和 256 位元
- RSA（最高 4096 位元）
- FIPS 186-3 中定義的 ECC (P-256, P-384 & P-521)
- HMAC、MD5、SHA-1、SHA-2、SHA-224、SHA-256、SHA-384 & SHA-512

**物理安全性**

- 防篡改和回應式設計
- 一旦遭受任何竄改攻擊，機敏資料會立即清除
- 具備移動、電壓和溫度警報觸發器

**邏輯安全性**

- 本地端主金鑰 (LMK) 選項：variant 和 key block
- 資安人員須使用 Smart Card 進行雙因子身份驗證 (2FA)
- 雙重控制授權 - 實體鑰匙或 Smart Card
- 預設執行最高強度的安全設定
- 結合用戶控制事件範圍記錄的 Audit log
- 乙太網路主機 port 的 TLS 驗證 session

**金融服務標準**

- ISO：9564、10118、11568、13491、16609
- ANSI：X3.92、X9.8、X9.9、X9.17、X9.19、X9.24、X9.31、X9.52、X9.97
- ASC X9 TR-31、X9 TG-3/TR-39
- APACS 40 和 70

**產品型號和選項**

- 所有型號均標配雙熱拔插電源和風扇
- 效能等級範圍：每秒 25、60、250、1,000、2,500 和 10,000 次調用 (cps)
- 可透過 payShield Manager、payShield Monitor 和 payShield 信任管理裝置 (TMD) 實現遠端管理及監控
- 格式保留加密 (FPE) 選項
- 多個 LMK 選項：每個 HSM 最多 20 個分區
- 台灣財金資訊公司指令集選項

**主機連接**

- TCP/IP 和 UDP (1Gbps) – 雙連接埠
- 乙太網路主機連接埠上 TLS 認證工作階段的安全主機通訊管理選項

**安全認證**

- FIPS 140-2 Level 3
- PCI HSM v3

**實體規格**

- 外形規格：1U 19 英吋機架安裝
- 尺寸：482.6 mm x 736.6 mm x 44.5 mm
- 重量：35 磅（15.9 公斤）
- 電源：90-264 VAC
- 功耗：60W（最大值）
- 作業溫度：0℃ - 40℃

imperva
a Thales company

# Imperva On-Premise WAF
# 網頁應用程式防火牆

**Imperva 網頁應用程式防火牆是唯一連續 9 年位於 Gartner WAF/WAAP 領導象限的廠商**

Imperva 目前於全球超過 150 個國家有使用客戶，已有超過 6,200 家客戶使用，各個產業皆有採用 Imperva 解決方案之客戶，如政府、電信、金融、電子商務、製造業等領域。

台灣也已有超過 130 家客戶使用，且使用客戶持續快速增加中。

## 特色

- 自動學習：自動且動態白名單學習機制及政策調整，大幅減少維運人力及時間
- 彈性佈建：用戶可彈性選擇 Inline 或 sniffing 方式，不須更動現有架構及程式，並具有集中控管機制
- 使用者追蹤分析技術：讓事後的應變追查更加快速有效
- 操作簡便：不需要專業能力及可操作使用，功能分類清楚，內容詳盡
- 報表系統：內建符合國際法規的報表範本
- 分權控管：權限控管系統，各司其職
- 即時更新：由原廠維護，每周更新報表範本、政策定義、黑名單...等
- 整合弱點掃描：可匯入網頁弱點掃描報告，並提供資料庫弱點評估功能
- Threat Radar：結合第三方專業機構，及時防護最新攻擊事件
- 服務：原廠支援團隊分布兩地，真正做到跨時區，提供 7x24 小時專業服務

## 法規遵循

- Imperva 系列產品可滿足個資法施行細則第 9 條-要成立管理組織及投入適當資源保護個人資料之規定。
- Imperva WAF 可滿足政府資安等級 A、B 級單位對網頁應用程式防火牆的部署要求。
- Imperva 網頁應用程式防火牆可幫助企業滿足支付卡產業資料安全標準(PCI-DSS) 6.6 的要求，並防護 OWASP Top 10 及新興威脅的攻擊。
- 符合上市櫃公司資通安全控管指引.第十八條.第五項，如有對外服務之核心系統，具備應用程式防火牆規範

## 精確監控和保護網頁應用程式

Imperva 網頁應用程式防火牆採用多層檢查和多重安全防護來提供最安全的保護。

- **HTTP(S)協定驗證**

  HTTP(S)協定驗證可以防止包括緩衝區溢位、惡意編碼、HTTP 偽裝以及非法伺服器操作在內的協定濫用。 彈性的規則讓使用者可以嚴格遵守 RFC 標準，同時支援各種靈活多變的應用程式。

- **防止資料洩漏**

  Imperva 檢查伺服器回應資訊以識別潛在的敏感資料(如持卡人資料和身份證字號)洩漏。除了報告還在應用程式中何處發現了敏感資料外，還可以選擇讓 Imperva 阻止這些資訊從企業網站洩漏。

- **網路及平台防護**

  Imperva 針對網頁伺服器弱點、中繼軟體弱點和平台弱點中的已知攻擊提供廣泛的保護，這些已知攻擊的資訊來源是 Imperva 應用防禦中心(ADC)提供的超過 6,500 個特徵碼。ADC 特徵碼不僅包括 Bugtraq、CVE® 和 Snort® 來源發現的攻擊，還包括透過 ADC 研究發現的威脅。Imperva 還可透過檢測和識別網頁爬蟲獨特的特性組合來抵禦零時差的新爬蟲攻擊。

- **無與倫比的準確度**

  Imperva 獨特的關聯攻擊驗證技術，可準確識別最複雜的攻擊。

- **網頁服務保護**

  Imperva 透過動態學習網頁服務的行為來保護這些應用，包括 XML 檔、元件、屬性、架構、變數和簡單物件連結協定(SOAP)。Imperva 將識別並阻止任何嘗試竄改正常網頁服務的行為，還會抵禦應用程式中常見的威脅，如 SQL 注入、XSS、CSRF 等。

## 自動化安全操作

- **自動應用學習**

  Imperva 獨特的動態建模技術可自動學習被保護網頁應用的結構、元件和預期使用模式。動態建模持續自動檢測有效的應用模型中。透過對比 Web 請求與行為模型，Imperva WAF 能夠精細的檢測不可接受的行為，並防止惡意活動。

- **網頁應用程式使用者追蹤**

  Imperva 使用動態建模技術自動獲取 Web 應用的使用者名稱並將後續所有會話活動與這個使用者名稱的關係連接在一起。因此 Imperva WAF 能夠依使用者進行監控、實行策略和稽核。

- **來自 ADC 的最新安全解決方案**

  Imperva ADC 是國際知名的安全研究機構，持續調查全球各地的漏洞，分析來自眾多不同網站的非法探測流量，並進行根本性漏洞研究來識別最新威脅。研究的結果就是提 Imperva 各設備的最新防護措施，包括特徵碼更新，協定驗證規則和關係連接規則。

## 使用非入侵式的部署

- **不需要更改網路或應用程式**

  Imperva 在業界所有網頁應用防火牆中提供的建置部署選項最多，包括不需要更改任何網路應用程式的透通橋接建部署項目。

  Imperva 提供每秒數 GB 的傳輸量、數萬次的交易處理量，同時還能將延遲時間保持在低於毫秒的等級。

## 提供企業級的集中管理

- **支援分散式部署**

  Imperva 可作為獨立設備進行部署，也可進行擴展以保護大型或分散式資料中心。Imperva MX 管理伺服器提供集中式配置、監控和報表基礎架構，以便從單一控制台管理多個設備和安全政策規則。

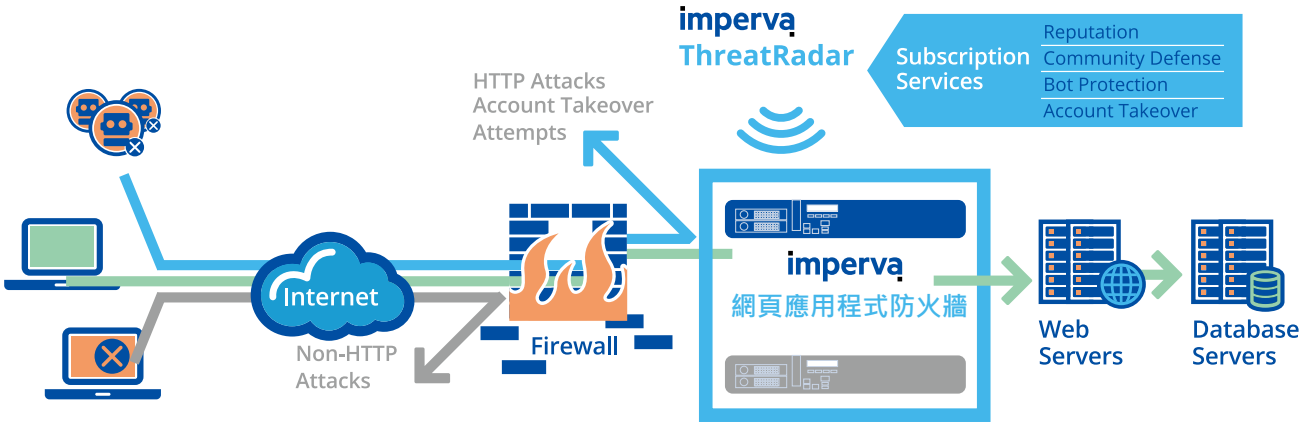
- **同等級產品最佳監控和報表功能**

  即時集中展示頁面提供一個高階的系統狀態與安全事件圖形，可以很方便地對告警進行搜尋、排序，還可以直接將其連結到相對應的安全規則。

  Imperva 提供豐富的圖形報表功能，使客戶能輕鬆地瞭解安全狀態並符合法規要求。Imperva 提供預設的報表，也提供基於 Web 應用的客製化報表。可以按需求查看報表，也可以每日、每週或每月透過電子郵件發送。

## 整合第三方應用程式

Imperva 整合大型企業 Web 應用程式防火牆的整體安全活動，包括 SIEM 和日誌管理的領導解決方案、基於角色進行身份驗證和用於弱點評估的網頁應用掃描解決方案。



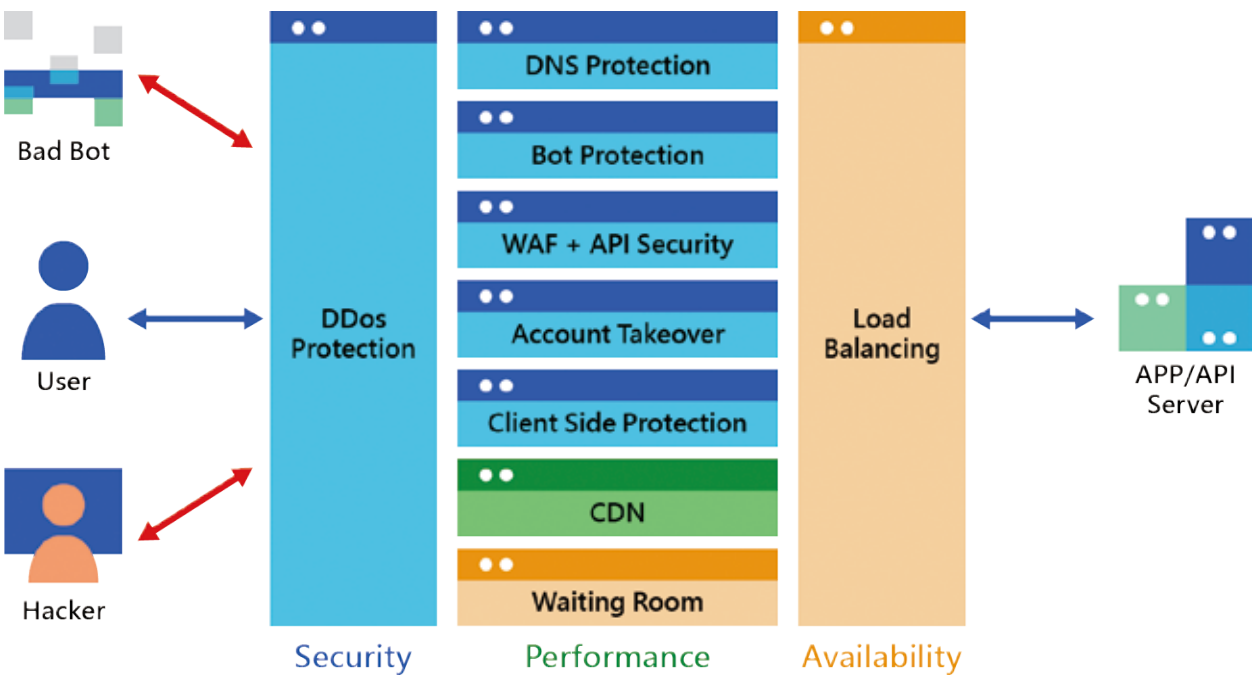

Imperva 可支援多種部署設定選項，包括 Layer2 Bridge、Proxy 和 Non-Inline 方式。

imperva
a Thales company

# Imperva Application Protect
# 將安全整合一體

Imperva Application Security 防護技術，是 100% 基於雲端的安全解決方案，提供不同等級的服務內容，能同時滿足各種客戶的需要， Imperva 的防護功能有 DDoS、WAF、CDN、API 安全、ATO 帳戶竊取和 Advanced Bot Protection 進階機器人檢測保護，產品獲得 PCI 認證，可用於保護網站和應用程式免受外部威脅，包括：OWASP 十大威脅、駭客攻擊、惡意機器人、漏洞掃描、DDoS 緩解、SQL Injection 、XSS (Cross-Site Scripting)、撞庫攻擊等各種惡意攻擊。

Imperva 防護的核心是透過客戶執行簡單的 DNS 變更，將所有網站流量導向部署在全球的 Imperva 雲端處理中心，透過獨特的檢查技術，將發送到網站的每個請求都進行過濾，處理任何類型的惡意活動，保護網站免受已知和未知的威脅。Imperva 以接近零的誤報率來阻擋這些惡意攻擊行為，確保您的設備在受到攻擊後的幾分鐘內就能受到完整防護。




Imperva Application Security 完整防護解決方案

## 高可用性的全球雲端處理中心

Imperva 為安全而建立的全球雲端處理中心，包含台灣在內，共有 56 個雲端處理中心 (PoP)，每個處理中心都具備 Application Security 全部功能，確保您的網路流量可以從最近的雲端處理中心進行清洗，不必從一個 PoP 跳到另一個。

鄰近的日、韓、新加坡、香港與泰國都有設置處理中心，Imperva 透過先進的軟體開發技術創建了一個 DDoS 清理中心虛擬池，可以在需要時進行全自動分配流量，並相互調用資源來應對惡意流量攻擊。

**Imperva 全球雲端處理中心**

○ Operational ○ Planned

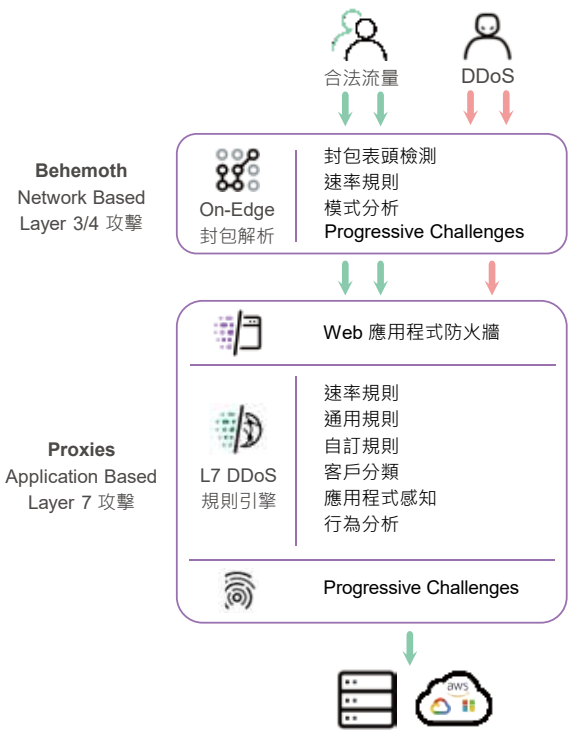
- 99.999% 的正常運行時間
- 全球 95% 區域存取低於 50 毫秒延遲
- DDoS 提供 SLA 保證 3 秒內完成清洗
- 每分鐘阻擋 25,000,000 個惡意請求

## 3 秒內完成各種 DDoS 清洗處理的信譽保證

Imperva DDoS 透明緩解防護技術，可以讓使用者免受任何類型的 DDoS 攻擊，不論是網路第 3 層、第 4 層或是應用程式第 7 層的攻擊行為，都能保證您的網路存取者和您的設備在 DDoS 攻擊中永遠不會受到影響，不論主機是設置在地端或是雲端，都只有合法的連線能被轉發到服務主機。

防護的目標可以是網站、DNS、網段，甚至單一 IP，並支援多種網路協定和部署方式，包括 GRE 路由、Cross Connect 和 Equinix Cloud Exchange 等。Imperva 提供每秒 10+ Tbps 和 650 億個封包的清理能力，並使用先進的來源識別技術，以保證 3 秒內啟動防護，完成任何攻擊行為的阻擋。

Imperva 有經驗豐富的網路維運中心（NOC），工程師團隊也提供 7x24 的技術支援，能不間斷進行實時監控與策略調整。



## 針對最複雜的安全威脅提供企業級保護

Imperva Cloud WAF 提供業界領先的 Web 應用程式安全防火牆，針對最複雜的安全威脅提供企業級保護。作為基於雲的 WAF，無論您的網站及應用程式是託管在公有雲還是本地端，Imperva Cloud WAF 都能確保您的關鍵資產一直受到保護，免於各種應用程式層的駭客攻擊。Imperva Cloud WAF 是 Imperva 全方位應用程式安全與服務交付解決方案的關鍵要素，可將企業組織的縱深防禦提升到新的水平。

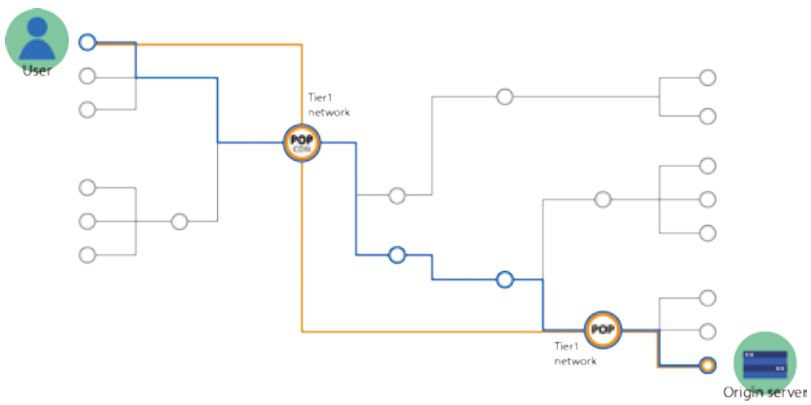
Imperva 數據整合平台的分析內容覆蓋範圍超越 OWASP Top 10 ，提供最好的網站防護，將網站風險從邊緣網路開始進行緩解，因此您的網站只會接收到安全的存取流量。

您可以透過 Imperva 保護最新的服務，無論是舊版應用程式、第三方應用程式、微服務 API、雲端應用程式、容器 (Container) 及虛擬機 (Virtual Machine) 等，都能以接近零的誤報率和全球 SOC 阻擋這些攻擊，確保您的組織在受到攻擊後的幾分鐘內就能受到保護，並符合 PCI 6.6 的規範。

## 完整的邊緣網路安全 CDN 解決方案

安全 CDN 會自動快取一份網站內容在各地的節點上，當不同區域的用戶向網站發出請求時，使用者可以就近取得服務，提升服務遞送速度及品質，提高網站效能並降低頻寬用量，最大程度地減少將內容下載到存取者瀏覽器所需的時間，並預防頻寬濫用可能導致的停機風險。

**使用 Imperva 的網站平均速度能提高 50%，頻寬消耗減少 60%。**




Imperva CDN 提升網站和應用程式效能，進而為您的客戶提供更好的體驗，包括更快的載入時間、更好的內容交付和更低的頻寬成本。

- 進階快取，提升網站速度
- 降低延遲、自動故障移轉
- 自訂快取規則，降低延遲並改善效能
- 基於雲端技術的網路第 7 層服務和數據中心負載平衡
- 傳輸內容和連線優化技術
- 支援 IPV6 和 HTTP/2 效能強化
- 與 ISP、雲端託管供應商、一級網路供應商為合作夥伴關係
- 提供流量監控與即時分析

## 更好的網路流量控管，更好的客戶體驗

網站存取量在尖峰或特殊期間可能忽然大增，除了讓主機花費變高外，IT 人員也很難評估網站所需的硬體需求。網站效能中斷不僅會影響客戶體驗，並可能導致客戶流失並損害企業品牌聲譽。

Imperva Waiting Room 功能可讓您為網站預設一個最大存取量，當訪客數超過該數量時，客戶將被導向虛擬等候室中的排隊系統，以先進先出的方式進行處理，依序讓客戶訪問網站。這意味著網站可以保持在線狀態，不會讓客戶收到 "無法存取" 的訊息，相反地，客戶可以在 Waiting Room 的虛擬等候室內持續更新預計等候時間，藉此獲得更令人滿意且無縫的使用者體驗，降低離開網站的機率。

## 超越 OWASP API 十大資安威脅範疇

Imperva API Security 雲端應用程式安全套件預設的安全規則，涵蓋 OWASP API Top 10 攻擊手法，並使用自動化的積極安全模型，同時採用 API Discovery 持續學習機制，會在 API 更新時不斷學習它們的結構，透過檢測應用程式並阻止漏洞利用來保護您的 API 免遭利用。

在新的應用程式的開發架構裡、自動化 B2B 的運用流程、物聯網設備連接等系統架構都廣泛被使用，隨著 API 使用激增，對 API 的攻擊也呈現上升趨勢，需將您的防禦縱深提升到一個新的水準。

## 卓越的自動化爬蟲檢測技術

唯一擁有全球最大的已知違規者設備指紋實時更新資料庫，讓您由全球主動防禦態勢實時分析的機器學習基礎設施，主動防禦特定領域風險並快速進行更深度的生物特徵檢測分析，使您的用戶能進行有效的搜索並找到您提供的內容。

有效識別任何惡意行為並提供最深入的進階爬蟲機器人洞察力，包含通過 IP、用戶代理、載入 JavaScript，支援 cookie、滑鼠游標移動和頁面時間改變等 100 多個數據維度的分析，在機器人爬蟲的戰爭中最大程度地控制您的惡意流量，將駭客工具、帳戶接管、密碼撞庫、漏洞掃描等機器人惡意行為屏除在流量之外。

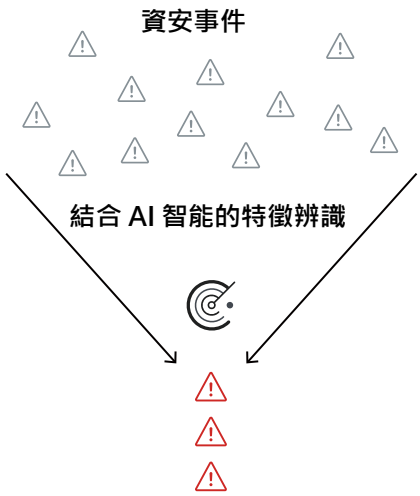
Imperva 優異的爬蟲檢測能力也榮獲 Forrester 自動化爬蟲解決方案評估報告中的領導者品牌 。

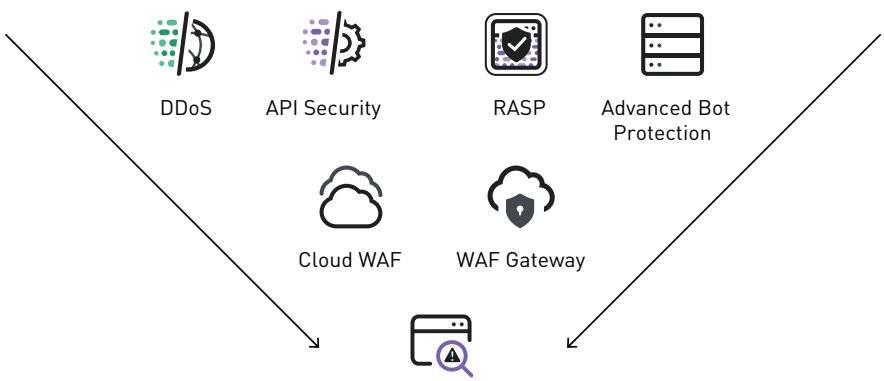
## 雲端 AI 告警分析系統 - 在眾多告警事件裡找出真正的威脅

Imperva 雲端 AI 告警分析系統 (Attack Analytics) 是 Imperva Application Security 解決方案之一，透過機器學習和領域專業知識來檢測應用程式攻擊，將大量資安事件分類和分組呈現去蕪存菁的結果，並為每個事件分配一個嚴重級別並提供額外的聲譽情報，提供資安事件所需的統一監控及統整分析。這讓資安團隊可以用簡單的方式，專注在少數幾個真正重要的事件分析上，而不必在成千上萬的事件告警裡大海撈針。

Imperva 解決方案整合各大 SIEM 系統，並藉由 Attack Analytics 的 AI 人工智慧過濾告警資訊，降低隱藏在大量告警事件下的威脅風險，實現完整的可見性，減少資安事件分析所需的時間，進而顯著提升安全營運中心 (SOC) 的效率。

Attack Analytics 是基於雲的解決方案，可一鍵部署，因此具備無限的可擴充性和企業所需的大量事件處理能力。




Attack Analytics 分析、過濾 Imperva 多項解決方案中成千上萬的告警事件訊息

## 高智能全自動撞庫防護

Account Takeover(ATO) 為暴力帳密填充技術，非法獲得的帳號密碼被用於未經授權存取的線上帳戶，攻擊者可以從中執行惡意操作，例如資料竊取、身份盜用或執行詐欺性電子商務交易。

Imperva 的核心 ATO 檢測機制使用其風險引擎中定義的因素（例如每台設備的登錄率、用戶名和登錄失敗的數量）來識別攻擊，根據攻擊的嚴重性和客戶定義的政策採取相對應的緩解措施。

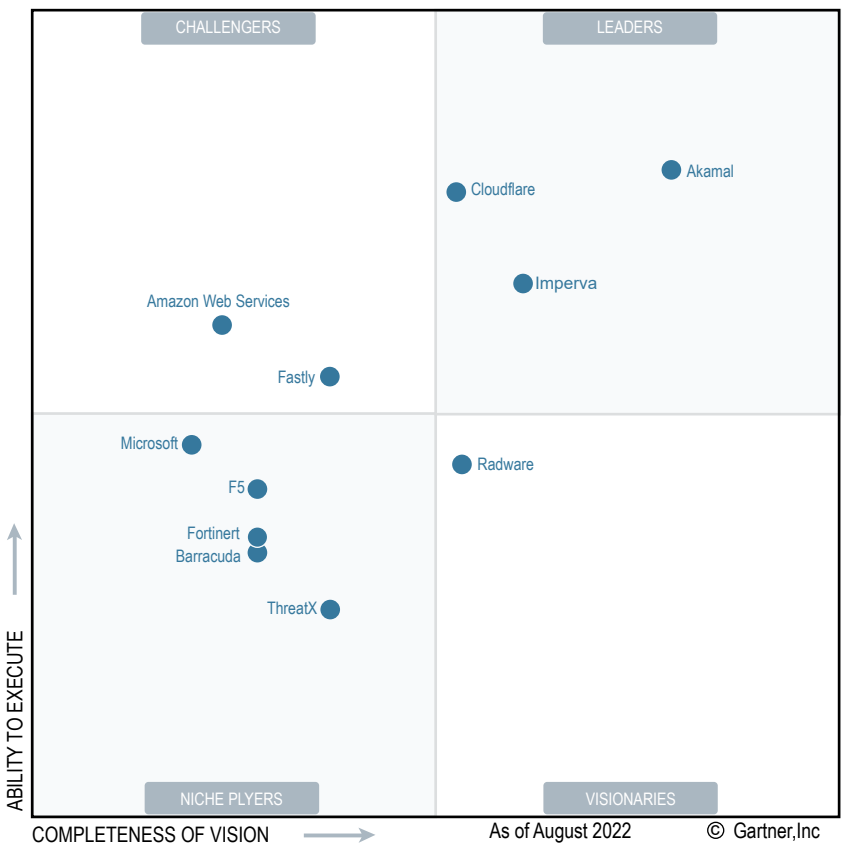
## 實時洞察分析第三方 JavaScript 套件

JavaScript 服務在 Web 應用程式上呈現爆炸式成長，並廣泛被嵌入使用，當第三方套件在不知情的情形下被更新或劫持，將導致客戶在不知情的狀態下成為表單劫持攻擊的受害者，對於企業造成的嚴重的影響。

Imperva Client-Side Protection 讓您在不需要更改套件或增加延遲的情形下，即可查看、控制嵌入在 Web 應用程式中的所有第三方 JavaScript 套件，並持續監控所有 JavaScript 服務。Client-Side Protection 只允許執行預先批准的服務，這意味著在網站中任何 JavaScript 服務在套件被劫持或獲得授權前將數據發送到其他地方都會被阻擋。

## 多重榮譽的安全解決方案領導品牌

Gartner 將 WAAP（Web 應用程式和 API 保護）定義為 WAF 的進化，並將原本 WAF 的功用擴展至 4 個面向：WAF、DDoS 防禦、機器人管理、API 保護。在 Gartner WAAP Report 中，Imperva 是唯一連續 9 年位於領導象限的品牌，除了提供強大的混合雲資安防護功能：包括資料安全產品、RASP、實體或虛擬設備的 WAAP (Imperva WAF Gateway)，以及雲端 WAAP 服務 (Imperva Cloud WAF) 等，近期更收購 API 資安公司 CloudVector ，進一步拓展 API Security 領域的資安防護。




Imperva 是業界專家認可的網路安全領導品牌，致力提供資料和應用程式所需的各種保護，無論是地端、雲端或是混合架構環境

imperva
a Thales company

# Imperva Data Security
# 資料庫安控稽核系統

» 取得完整的資料庫活動細節(5W)留存存取資料庫的行為軌跡
» 利用靈活的視圖和稽核分析使稽核資料容易取得
» 產生對資料庫攻擊和欺騙性活動的即時警告，以善盡保護資料庫重要資料(如個資)的責任
» 建立資料安全、遵守法規週期
» 自動化與集中化的資料庫稽核與報告
» 加密與加註簽章的稽核資料，具有資料不可被竄改與不可被否認性

## 特色

- 持續稽核、分析所有資料庫流量：詳細稽核並持續監控所有資料庫的操作，提供每筆事件的稽核紀錄，包含：「何人、何時、何處、如何連線資料庫及做什麼(5W)」。同時能擷取所有資料庫活動，包括 DML、DDL 和 DCL 活動、查詢活動(SELECT)、對儲存程序、觸發程序和資料庫物件的修改及 SQL 錯誤的資料庫登入活動，並監控(可選擇稽核)資料庫回應以確保不會洩漏敏感資料。
- 驗證及控制特權資料庫活動：Imperva 利用閘道設備來監控網路流量，利用輕量化 Imperva Agent 來擷取本機活動並消除問題點。確保全面瞭解和保護所有網路與本機特權使用者的操作，包括資料定義語言(DDL)命令、資料控制語言(DCL)命令、資料操作語言(DML)命令和 SEELECT。
- 防止竄改的稽核紀錄：監控詳細的稽核資料會儲存在安全的外部硬體處存設備中，可透過唯讀方式存取。該儲存設備中使用以角色為基礎的存取控制(RBAC)，為了確保稽核資料的完整性，還可以對其進行加密。
- 即時資料庫保護（※僅適用 DBF/Bridge)：監視即時資料庫活動時會於作業系統、通訊協定及 SQL 活動層檢查各種資料庫攻擊，以提供準確的即時保護。未授權更改、欺騙性活動以及資料庫攻擊可以在到達受保護系統之前從網路上阻擋或在系統自身上阻擋。
- 靈活的部署與集中管理架構：提供包括通透網路監視、輕巧的 Agent 監視、自身稽核收集或混合模式。這種非入侵性的體系結構使企業能以任一方式混合部署，以滿足客戶特有的拓樸與需求。集中管理伺服器可對多 Gateway 及 Agents 進行統一管理。

## 法規遵循

- Imperva DAM 可滿足新版個資法施行細則第 5 條 - 要對個人資料之處理留有軌跡紀錄之規定，且提供稽核資料具有不可被竄改、不可否認性，可滿足個資法採舉證責任倒置原則。
- Imperva DAM 提供資料庫加密的補償性控制（PCI-DSS 3）。它還啟用關鍵性對存取持卡人資料的監控和跟蹤（PCI-DSS 10）。其它 PCI-DSS 要求符合以下措施：1.內建評估工具確保不使用廠商提供的帳號和密碼 2.對非法存取持卡人資料進行智慧型告警 3.使用內建和客制報表來衡量控制的有效性。 12項 PCI-DSS 要求中共有 7 項可由 Imperva DAM 來完成。
- Imperva 使企業能夠保持獨立的稽核線索，該稽核線索中包括與財務資料相關活動中的「何人、何時、在哪裡、如何及做什麼?」詳細資料，符合沙賓法案（SOK）要求實施適當的步驟和控制以確保可靠財務資訊的一致性(第 302 條)以及內部控制的可靠性(第 404 條)。

## 探索和弱點管理

**• 資料庫探索和分類**

Imperva 可確保企業能夠保護所有敏感資料並區分其優先順序。基於整個網路的探索可了解資料庫伺服器間的資料。基於資料庫中包含的資料類型對資料庫進行分類可幫助企業對應所發現的伺服器並區分其優先順序，從根本瞭解哪些伺服器屬於法規監管的範圍。

**• 廣泛的弱點評估**

Imperva RDBMS 弱點評估和最佳作法有助於企業修正、控制其資料庫的設定配置並實現整體弱點管理策略。這些評估測試會與 Imperva 應用防護中心(ACD)研究小組的最新研究保持即時更新。

## 自動稽核和安全保護

Imperva 包含一套完整的預設稽核與安全政策，可以迅速監測任何資料庫的環境。這些規則基於＂黑名單＂和＂白名單＂安全模組，這些模組可透過 Imperva 已申請專利的動態建模技術以及 Imperva ADC 不斷更新的研究成果得以持續更新。動態建模技術(Dynamic-Profiling)可持續自動檢測並納入有效的更改，使管理員不必再手動新增和更新包含了成百上千個資料庫物件、使用者和 SQL 查詢的冗長白名單。

## 持續稽核與分析所有資料庫流量

詳細稽核並持續監控所有資料庫操作，提供每筆事件的詳細稽核紀錄，包含：「何人、何時、何處和如何連線資料庫及做什麼(5W)」。
Imperva 擷取所有資料庫活動，包括 DML、DDL 和 DCL 活動、查詢活動、對儲存程序、觸發程序和資料庫物件修改以及 SQL 錯誤和資料庫登錄活動。
Imperva 並監控(可選擇稽核)資料庫回應以確保不會洩漏敏感資料。

**• 管理安全對策和更改**

Imperva 即時監控資料庫活動並檢查各種作業系統、協定層級 SQL 層的資料庫攻擊。透過詳細的行為更改稽核可以準確地針對欺騙性活動、資料庫修改和攻擊進行告警、發送即時告警、分配後續任務以及確保變更的控制。

**• 原始資料保存與回復**

資料庫稽核軌跡原始資料(Raw Data)，可透過加密、數位簽章等方式，安全備份存放於本機硬碟，或搭配外部儲存空間，以 NFS、FTP、Mount Point、AWS S3 等方式，備份存放於指定外部儲存空間，避免歷史紀錄遭受竄改或刪除。
Imperva 操作介面提供匯入功能，可將歷史紀錄匯入回復，以供查詢、產製報表等作業。

**• 加密解析**

若資料庫本身啟用如 SSL 加密傳輸等機制，僅須利用安裝 Agent 或匯入憑證等方式解析出資料庫帳號，不影響稽核紀錄完整性。

## 簡化工作流程，並符合法規要求

**• 互動式稽核分析**

Imperva 提供圖表及統計數據列表兩種分析，透過互動式稽核分析可以全面瞭解所有稽核活動，這讓不了解技術的資料庫稽核人員只需點幾下滑鼠即可從多個角度深度分析、關聯和查看資料庫活動、從而簡易識別可能隱藏了安全風險或法規問題的趨勢和模式。

**• 同級產品最佳報表功能**

Imperva 提供內建的圖形報表，可以圖形、統計數據列表方式，呈現完整資料庫存取紀錄，並支援 UTF8、BIG5 等中文編碼，可正確呈現中文內容。排程自動產生報表，發送 PDF 或 CSV 格式的結果，以及與 SIEM、問題處理系統和其他第三方解決方案的整合，提供相關稽核及告警訊息。

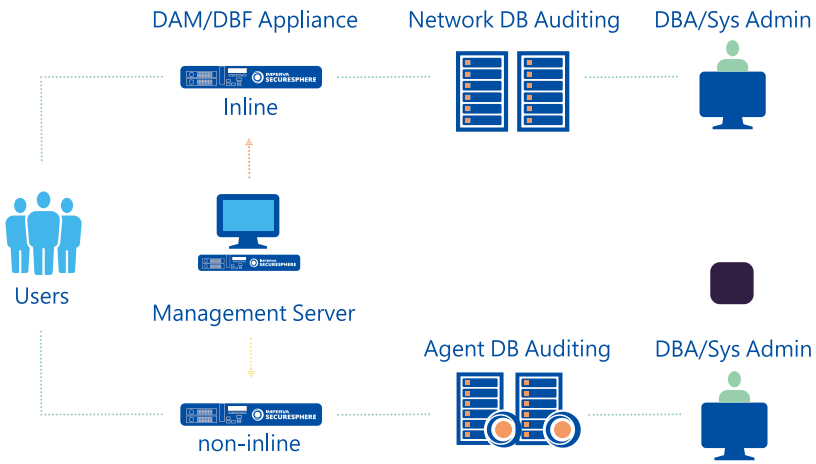
## 靈活的部署、較低的建置成本

**• 靈活的部署模式：網路、Agent、內建稽核或混合模式**

Imperva 提供最簡單的部署選項，包括網路監控、Agent 監控、內建稽核日誌收集或混合模式。這種非侵入性的體系結構使企業能夠以任意方式混合部署，滿足客戶特有的拓樸和需求。
Agent 可在下列情況下獨立運作：
(1)不使用資料庫帳號安裝
(2)不啟動資料庫內建之稽核日誌功能
(3)不更動資料庫設定
(4)Agent 故障不影響資料庫運作
(5)可調整占用之系統資源

## 效能和可擴展性

Imperva 提供即時的保護和完善的稽核功能，可以輕鬆支援任何環境，從中小企業到大型企業，這是其它資料庫防護解決方案難以與之匹敵的。




Imperva 可部署在 inline 或 non-inline 網路監控環境，控管特權及使用者帳戶的資料庫行為

# imperva Data Security 訂閱制方案

| | Data Secure | Data 360 | Sonar Reporting Add-on | Sonar 360 Add-on |
|---|---|---|---|---|
| 地端虛擬版 DBF | V | V | | |
| 可部署在 AWS 及 Azure | V | V | | |
| Clustering | V | V | | |
| 使用者權限管理(URM) | V | V | | |
| 資料庫弱掃功能(DAS) | V | V | | |
| 資料庫風險 AI 智能分析(DRA) | V | V | | |
| Jsonar Reporting/Data Environment | V | V | V | V |
| Sonar Agentless Collection | V | V | | |
| 資料保留時間 - 13 個月 | V | V | V | V |
| Data SOAR | | V | | V |
| Advanced Data Enrichment | | V | | V |
| Compliance and Security Automation | | V | | V |
| Splunk SOC Advanced Workflow | | V | | V |
| Self Service | | V | | V |
| 資料保留時間 - 3 年(37 個月) | 選購 | 選購 | 選購 | 選購 |
| 資料保留時間 - 不限時間 | 選購 | 選購 | 選購 | 選購 |
| Cloud Data Security for AWS DBaas | 不包含在方案中，可單獨購買 | | | |

# Qualys 雲平台

一切可見，一切安全

Qualys 雲平台可讓您對全球 IT、安全及合規狀態進行持續、always-on 的評估，並能在 2 秒內查看所有 IT 資產，無論它們位於何處。透過自動化的內建威脅排序、修補和其他回應功能，提供用戶一個完整的點到點安全解決方案。

Qualys 創新的雲端架構，為您的資訊安全和合規需求提供快速部署、易於擴充、實時防護，且不需硬體設備的解決方案，無論是機房端設備、容器、雲端服務或移動終端，都能透過單一平台進行實時管理與分析。

在本地端、終端、移動設備、容器或雲端環境中，Qualys 雲平台的感測器(Sensor)會保持 always-on 的狀態，讓您能在 2 秒內連續查看所有 IT 資產。感測器提供硬體、虛擬設備或代理程式(Agent)版本，可遠端部署、集中管理及自動更新。

## Qualys 雲平台優勢

- 不需添購、管理硬體設備
- 降低營運成本
- 易於執行分散式站點及網段的掃描
- 滿足快速擴充的需求
- 實時進行資訊更新
- 漏洞資訊經過層層加密保護

Qualys 雲平台可直接以 Web 瀏覽器操作，不需安裝任何軟體。強大的儀表板方便在單一畫面中檢視各式統計數據，並可依需求提供儀表板客製化編排。

Qualys 在全球 130 多個國家擁有 11,000 多個客戶，包括富比士全球 100 大及財富 100 強中的大多數公司。

Qualys 幫助企業在單一平台上簡化並整合他們的安全與合規解決方案，將安全納入數位轉型計畫中，以提升資訊敏捷性、強化業務成效並節省大量成本。


Qualys 雲平台提供多種安全防護

為強化您的資訊安全資產管理與合規需求，Qualys 提供以下功能模組：

## Asset Management 資產管理

**CASM網路安全資產管理**

查看整個攻擊面，持續維護您的 CMDB ( 配置管理資料庫 )，並追蹤 EOL/EOS 軟體

**EASM 外部攻擊面管理-New**

從攻擊者視角持續查找面向互聯網的資產與未經授權的軟體，並快速進行修復，實現可見性與風險追蹤

## Vulnerability & Configuration Management 弱點及配置管理

**VMDR 弱點管理、檢測與回應**

讓 IT 資產環境中的發現、評估、優先排序和漏洞修補效率提升 50% 以上

**ETM 企業 TruRisk 管理平台-New**

整合第三方工具的安全與漏洞資訊，將網路風險的衡量、管理、緩解集中至單一平台

**WAS 網頁應用程式掃描**

透過 Shift left DAST ( 動態應用程式安全測試 ) 在 CI/CD 環境中自動掃描

**CWP 雲端 workload 防護**

掃描、排序並修復雲端環境裡 VM、容器和無伺服器 workload 的漏洞

**CS 容器安全**

發現、追蹤並持續保護容器從建置到實際運行時的安全

## Risk Remediation 風險修復

**PM Patch 管理**

簡化並加速 IT 資產弱點與 Patch 的關聯性管理

**CAR 客製化評估與修復**

提供可快速建立的客製化自動工作流程腳本及控件，以實現企業所需的安全性及合規性

## Threat Detection & Response 威脅偵測與回應

**EDR 多向量端點偵測與回應**

進階端點威脅防護、優化的威脅上下文資訊及告警排序

**XDR 上下文關聯延伸偵測及回應**

將偵測和回應擴展到企業端點之外

## Compliance 合規管理

**PC政策合規**

評估網路 IT 系統的安全配置，降低風險，輕鬆遵循內部政策和外部規範

**FIM檔案完整性監控**

記錄、追蹤全球 IT 系統的檔案變更，減少告警並保護檔案免於惡意用戶和網路威脅侵害

## Cloud Security 雲端安全

**Total Cloud CNAPP 雲端原生應用防護平台**

發現、評估、優先排序、防禦和修復多雲環境的漏洞、威脅和錯誤配置

**CSPM 雲端安全狀態管理**

提供公有雲 workload 和基礎設施的統整清單，可持續發現、監控、分析雲端資產是否有錯誤配置和非標準部署

**IaC 基礎設施即程式碼安全**

偵測並修復 IaC 範本中的安全性問題，以消除雲端基礎設施的潛在安全威脅

**SSPM SaaS 安全態勢管理-New**

管理整個 SaaS 應用程式堆疊 ( stack ) 的安全狀況及風險

**CWP 雲端 workload 防護**

掃描、排序並修復雲端環境裡 VM、容器和無伺服器 workload 的漏洞

**CDR 雲端偵測與回應**

結合人工智慧和深度學習演算法進行實時多雲威脅偵測，持續保護多雲環境免受主動利用 ( active exploitation )、惡意軟體和未知威脅。

**CS容器安全**

發現、追蹤並持續保護容器從建置到實際運行時的安全

# VMDR 2.0 with TruRisk™ 全方位弱點管理、檢測和回應

## 透過單一管理介面，實時發現、評估、確認優先順序並修補重要漏洞

風險成長的速度超出了傳統 VM 和 SIEM 工具的管理能力。資安與 IT 團隊需要新的方法來因應網路威脅，清楚掌握網路安全風險並自動化工作流程以實現快速回應。

借助 VMDR，企業能獲得對網路風險的可見性和洞察力，進而根據風險確認資產或資產群組的弱點優先順序。安全團隊可以採取行動來降低風險，幫助企業衡量其真實風險，並隨時間追蹤風險降低的情況。

Qualys VMDR 2.0 提供基於風險的弱點管理解決方案，根據風險和業務關鍵性對漏洞和資產進行優先排序，確定漏洞、錯誤配置和資產的優先處理等級，透過大規模修復漏洞來降低風險，並透過時間追踪幫助組織衡量安全防護的有效性。Qualys VMDR 2.0 還與 ServiceNow 等資訊服務管理系統整合，實現點到點弱點管理的自動化和運作。


**了解、管理網路安全風險**
使用 Qualys TruRisk ™ 量化漏洞和資產的風險，幫助組織主動降低風險並追踪風險隨時間降低的情況。

**使用無程式碼工作流程自動修復**
透過 Qualys Flow 實現弱點管理和修補的操作任務自動化與編排，以節省寶貴的時間。

**防止攻擊持續發生**
Qualys 威脅資料庫整合來自 25 個來源以上的 18 萬個漏洞分析，提供對潛在攻擊的預先告警。

**識別環境中的所有資產**
檢測所有 IT、OT 和 IoT 資產，提供完整且分門別類的資產清單，並包含供應鏈生命週期資訊等詳細訊息。

**以 6 sigma 的準確度分析漏洞和錯誤配置**
根據互聯網安全中心(CIS)基準，自動檢測資產漏洞和重大錯誤配置。

**快速且大規模的修復威脅**
與 ServiceNow、JIRA 等資訊服務管理系統(ITSM)整合，自動分配案件並啟用修復排程以降低平均修復時間(MTTR)。

### 資產管理 - 自動資產識別與分類

VMDR 讓用戶能自動發現已知和未知資產並對其進行分類，持續辨識未託管資產，並建立自動化工作流程以有效進行管理。完成資料收集後，用戶可以立即查詢資產和相關屬性，以深入了解硬體、系統配置應用程式、服務、網路資訊等。

### 弱點管理 - 即時偵測漏洞及錯誤配置

VMDR 可讓用戶根據 CIS 基準自動偵測資產的弱點和嚴重錯誤配置。藉由 Qualys 對 86,000 以上個漏洞的支援以及對 CIS 基準的全面覆蓋，組織可以更快地回應威脅。VMDR 與 TruRisk 持續識別 IT 環境面臨的重大風險，包含業界廣泛使用的裝置、作業系統和應用程式上之關鍵漏洞及錯誤配置。

### 威脅優先排序 - 根據風險自動排定弱點修復順序

VMDR 運用即時威脅情報、進階關聯和強大的機器學習模型，自動對關鍵資產上風險最高的弱點進行排序，並透過對每項資產的業務影響評估，進一步確認修復的優先順序。

### 修復管理 - 修補（Patch）與修復（Remediation）唾手可得

在依風險對弱點進行優先排序後，VMDR 整合相關 Patch 資源，在不同規模的環境中快速修復目標弱點。此外，基於策略的自動化作業可讓系統保持最新狀態，為安全性和非安全性 Patch 提供主動式管理。

# CSAM 網路資安資產管理 (含外部攻擊面管理)

## 以駭客視角檢視您的攻擊面

傳統攻擊面管理和弱點管理解決方案難以看見現今駭客所瞄準的外部資產和軟體全貌。為了降低網路風險並整合資安差距，必須實現內外部面向互聯網資產的完全可見性。

攻擊面正急速擴大，為攻擊者提供了新的目標。超過 30% 的地端、雲端資產和服務未進行盤點，這是網路安全可見性的巨大落差！

網路安全資產管理 (CSAM) 是 Qualys 一項雲端服務，能像攻擊者一樣查看您的攻擊面，並整合資安與 IT 的資產管理。CSAM 可以持續發現、分類、修復和改善其內部和外部 IT 資產的網路安全狀況，同時查找所有已知和未知、面向互聯網的資產，以實現 100% 的可見性和風險追蹤。


Qualys CSAM 2.0 包括外部攻擊面管理，增加了“縱深防禦”以更新組織的網路安全狀態。CSAM 2.0 透過具有紅隊型態的資產及漏洞管理解決方案，提供持續發現、分類未知資產的能力，以實現 360 度的全面性涵蓋。

## 特色與效益

基於風險的網路安全建立在攻擊面管理（ASM）基礎上。透過網路安全資產管理（CSAM），資安和 IT 營運人員可以獲得攻擊者和防禦者對其環境全面、完整的可視性，包括資產、資產群組、網域、子網域、生命週期（EOL/EOS）等。結合外部攻擊面管理（EASM），CSAM 可以幫助組織發現、偵測、確認資產風險的優先順序，並編排資安和 IT 團隊之間的工作流程，以消除作業摩擦、改善修復成效並降低網路風險。

透過統一的盤點和資產目錄（包括第三方資產情資以及內對外與外對內的數據）來降低網路風險。

透過 EOL/EOS 盤點、未經授權軟體查找和關鍵 agent 覆蓋等功能，找出資安弱點並監控資產運作狀況。

透過本機整合的工作流程簡化、改善弱點管理、AppSec 和 Patch 管理程式。

透過與 ITSM、CMDB 和 Ticket Tool 的雙向整合，提升 90% Patch 速度，更快完成事件處理。

Qualys

# Web Application Scanning 網站弱點掃描服務

## 查找、修復網站應用程式與 API 弱點

Qualys 雲平台提供針對網站應用程式的弱點掃描及錯誤配置管理服務，可直接透過雲端服務，快速、方便完成佈署準備。立即管理您的網站資產、掃描弱點與錯誤配置、修復追蹤，並透過惡意軟體掃描，讓網站更加安全，且無需花費建置任何硬體設備。

WAS 掃描企業的網站並識別、報告感染的情況，如經過行為分析找出的零時威脅。詳細的惡意軟體感染報告內也包含了須修復的程式碼。中控儀表板可顯示掃描活動、受感染頁面和惡意軟體感染趨勢，並允許用戶直接從介面採取行動。惡意軟體檢測功能為選用的附加模組。

- **全面查找**

  搜尋企業內存在的網站，建立網站資產清單。

  Qualys WAS 透過查找整個網路後可得到的資訊包括：

  - 已確認及未確認的網站
  - 可使用標籤或群組方式管理網站資產

  分類弱點風險等級，讓資安人員優先修復重要問題。

- **深入掃描**

  WAS 的動態深度掃描涵蓋邊界、內部環境和正在開發中的所有應用程式，並可支援移動設備的 API。WAS 還涵蓋公有雲實例，為您提供 SQLi 和 XSS 等弱點的即時可見性。

  透過深入、完整、精確的掃描查找網站弱點，並以近趨於零的誤報率保護您的網站應用程式。可漸進式逐步掃描並繞過阻擋掃描整個應用程式的限制。

- **DevOps 安全工具**

  WAS 可提升 DevOps 環境中應用程式開發和部署的安全性，檢測程式碼安全問題、測試品量保證(Quality Assurance)並產出統整報告。WAS 也與 Qualys WAF 高度整合，可持續監控並虛擬修補應用程式，快速防禦尚未修復的弱點。

  檢測 OWASP Top 10 風險，如 SQL 注入、跨站腳本(XSS)、跨站請求偽造 (CSRF) 和無效重定向等。

  可檢測具身分認證的網站應用程式，還可用自動執行腳本的方式登入系統，擴大掃描覆蓋率。

- **惡意軟體檢測**

  可手動執行掃描，亦可透過排程自動執行網站掃描，確認是否受惡意軟體感染。

# PCI Compliance & SAQ PCI 合規掃描與自我審查評估表模板

## 簡單、快速、自動化完成 PCI 合規檢查

Qualys PCI 政策合規提供企業、網路商家和服務供應商最簡單、最具成本效益和高度自動化的方式來實現PCI DSS (信用卡行業資料安全標準)合規性。

除了以 PCI ASV 進行掃描外，透過完整的 Qualys PCI 合規解決方案，更能滿足 97% 以上的 PCI DSS 要求。在資產管理、弱點檢測和回應、支付網站應用程式安全、安全配置管理和安全評估問卷等方面，都能獲得安全性和合規性。

PCI DSS 要求企業每 90 天要對所有面向 Internet 的網路和系統執行一次有既定流程的網路安全掃描。為實現合規性，企業必須識別、修復在掃描過程中檢測到的所有重大弱點。

Qualys PCI ASV 應用程式提供：

- 自動化並大幅簡化的掃描與修復流程
- 易於使用的 PCI DSS 合規弱點掃描報告
- 透過 Qualys 雲平台準確掃描弱點
- 為每個檢測到的弱點提供詳細說明，並提供驗證過的修補連結以進行快速修復。

當您完成各項驗證操作後，Qualys PCI ASV 應用程式可透過以下兩種模式執行 “自動提交” 功能，完成合規流程：

√ 自動將合規報告直接提交給收單銀行

√ 可下載 PDF 格式的 PCI 合規報告再另行提交給收單銀行

可加購自我審查評估表模板(SAQ)，內含多種合規所需的自我審查評估表，包含 ISO、PCI-DSS、HIPAA、NIST、GDPR 等各種法規型式及版本的模板。PCI 審查評估表提供直接填寫問卷並寄發給收單銀行或下載 PDF 格式報告兩種模式。

# 雲端原生應用程式防護平台(CNAPP)

## 無代理雲端安全的先驅

Orca Security Platform 是業界領先的雲端安全平台，可辨識、確認優先等級並引導修復跨 AWS、Azure、Google Cloud、阿里雲等雲端平台、容器和 Kubernetes 的資產安全風險和合規問題。透過 Orca Security 解決方案，能以單一、完整的方式實現雲端環境 100% 的覆蓋率和可見性。


Orca 改變雲端安全的專利技術-SideScanning™，不需安裝任何代理程式，可直接從雲端配置和工作負載(workload)運作區塊儲存的頻外(out-of-band)收集資訊，進而對原本難以察覺的重大風險採取行動，包括漏洞、惡意軟體、錯誤配置、橫向移動風險、身分識別和存取管理(IAM)風險、錯置的敏感資料和 API 風險等。

所有資產相關資訊都可整合到單一平台中，透過 Orca 上下文感知引擎詳細了解 AWS、Azure 和 Google Cloud 等雲端環境中的資產風險，並讓資安團隊依據風險嚴重程度的排序，專注處理 1% 的重大關鍵問題。

Orca Security Platform 持續維持雲端合規性並提供漏洞管理、惡意軟體掃描和文件完整性監控等多種工具。Orca 支援 40 多個網路安全基準(CIS)和關鍵資產的合規框架，如 PCI-DSS、GDPR、NIST 和 SOC 2，並具有內建及自定模板，可滿足不同用戶的特定需求。

借助 Orca Security Platform 直觀且具彈性的查詢功能，每個用戶都可以快速搜尋雲端數據以獲取可用情報，同時也可透過整合的工作流程立即將問題分配給負責的團隊成員，以提高效率、加快修補速度，實現更好的投資報酬率。

### 雲端安全狀態管理 (CSPM)

傳統的 CSPM 解決方案可幫助組織保持合規性並解決雲端風險，例如錯誤配置和過於寬鬆的身份驗證。但是，這僅涵蓋攻擊面一部分的風險，且將雲端工作負載、事件監控和機敏資料發現排除在外。

Orca 將雲端工作負載、配置、身份和權限安全、容器安全、機敏資料發現、檢測和回應整合到單一平台中，並橫跨整個生命開發周期(SDLC)。這讓 Orca Security Platform 能了解風險的前後脈絡，並識別看似無關的問題何時會產生危險的攻擊路徑。運用這些洞察，Orca 能有效確認風險的優先順序，確保資安團隊可以優先處理最關鍵的告警。此外，Orca 也會持續檢查多雲端資產中的錯誤配置，確保設置的安全性並遵守最佳實務及產業合規標準。

### 雲端工作負載保護平台 (CWPP)

與其他 CWPP 不同，Orca 不需安裝代理程式，可在幾分鐘內以 100% 的覆蓋率提供對雲端工作負載及雲端資產風險的可見性，並能橫跨雲端 VM、容器、無伺服器應用程式、Kubernetes 以及雲端基礎設施，而不影響效能和營運成本。此外，Orca 還可掃描雲端配置和用戶身份，提供完整的上下文分析和告警優先排序。

## 雲端基礎設施授權管理 (CIEM)

Orca 將身份風險與其他風險數據（漏洞、錯誤配置、惡意軟體、機敏資料的儲存位置和橫向移動風險）結合起來，以幫助您優先考慮環境中的風險。若發現過於寬鬆的身份認證時會發出告警，並能根據潛在的業務影響進行風險優先排序。

## 雲端原生漏洞管理

Orca 為您的雲端環境建立完整漏洞清單，並結合 20 多個漏洞資訊來源，以發現、評估整個雲端資產中的漏洞。

- 資產清單包含操作系統、應用程式、函式庫、版本和其他識別特徵的資訊。
- 將雲端資產的上下文、相關連接和風險分數納入評估，以評估須優先解決哪些漏洞。
- 如遇到 Log4Shell 等需要快速回應的問題，Orca 能快速識別易受攻擊的雲端資產，並優先修補會對營運構成最大風險的資產。

## 保護您的機敏資料

Orca 掃描雲端資產的每一處，搜尋有風險的機敏資料，從個人身份資訊 (PII) 到受保護的醫療保健資訊等。

- 檢測雲端資產中每個工作負載內具風險的機敏資料，無論資產是運作中、閒置、暫停或停止狀態。
- 告警會指出機敏資料的確切位置，並提供遮罩樣本以進行有效的分類和修復。
- 機敏資料檢測含括各種個人身分資訊(PII)，如地址、Email 信箱、信用卡號和身分證字號等。

## 檢測已知和未知的惡意軟體

Orca 將 SideScanning 結合多種惡意軟體檢測技術，以找出雲端工作負載和資源中的已知及潛在惡意程式碼。

- 基於特徵碼的檔案 hash (特徵)掃描 - 檢查已知的惡意軟體。
- 啟發式檔案分析(Heuristic file analysis) - 詳細檢查檔案以確定其用途、目標和意圖，進而標註是否為惡意軟體。
- 動態掃描 - 在受控制的虛擬環境中執行檔案以觀察其動向及表現是否為惡意軟體。
- 基因特徵碼偵測 - 比對過往的惡意軟體資訊以發現相同來源的惡意軟體。


## 身份認證風險 - 集中式的多雲查找和合規

Orca 支援跨多個雲端平台，以追蹤雲端資產、角色和權限，確保符合法規標準和網際網路安全性(CIS)基準。

- 獲得雲端中所有身份、配置、存取策略、權限和活動的精確上下文可見性。
- 查看所有雲端資產中的網路存取和公開資源。
- 提供 20 多個類別，1,300 多項存取控制，包括身份驗證、資料保護、日誌記錄和監控、IAM 錯誤配置及系統完整性。

## API 風險優先排序及合規

Orca 掃描整個雲端資產並發現潛在危險的 API 安全風險，包括來自 OWASP API Security Top 10 告警，並提供可執行的資料和修補建議。

- 運用重要程度評分和基於上下文的資料（例如 PII 位置、API 公開顯示等）排定風險的優先順序以加速修補行動。
- 藉由自動建議輕鬆識別 “不應暴露在外的資產” 。
- 採取預防措施來減少 API 攻擊面。搜尋與特定網域或子網域相關的風險，或特定期間內的告警。
- Orca 提供帶連結的告警，高於稽核標準並遵守合規性架構（如 PCI-DSS）。

proofpoint.

網路攻擊者主要鎖定三件事：勒索軟體、資料勒索和金融詐騙。他們會遵循一套「攻擊鏈」的標準步驟，Proofpoint 的方法就是破壞攻擊者所採取的關鍵步驟。攻擊鏈可能很複雜，但我們將之歸納在三個關鍵領域並進行破壞。

## 破壞攻擊鏈

保護您的員工免於進階電子郵件攻擊和基於身分的威脅；保護機敏資料，避免竊取、遺失和內部威脅。

### 一、防止初始入侵 - 阻擋攻擊者侵入您的組織

- 阻擋針對性的網路釣魚、惡意軟體、社交工程和冒名攻擊。
- 檢測並回應雲端帳戶接管，包括對第三方供應商和合作夥伴的攻擊。


## Aegis 威脅防護平台

**停止電子郵件攻擊和初始詐騙**

保護員工、阻止攻擊者入侵，您就能從攻擊鏈的源頭中斷它。Proofpoint Aegis 威脅防護平台 是業界最有效的電子郵件解決方案，由 AI 支援，而且「以人為本」。為您的員工提供安全意識計畫，並使用真實的威脅數據以貼合您的風險環境。

**全面的可視性**

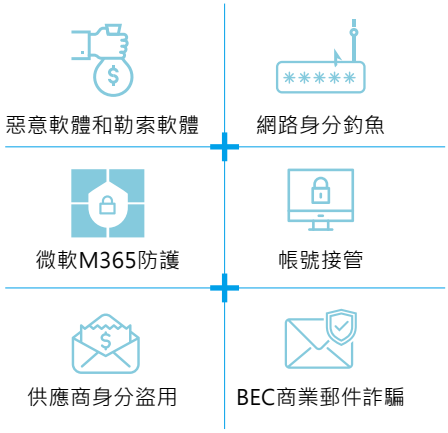
了解誰遭受攻擊以及如何受到攻擊。辨識組織內的「重點受攻擊人員」（Very Attacked People™, VAP）。

**無與倫比的效益**

透過機器學習和行為分析準確檢測出更多威脅。

**營運效率**

減少資安團隊工作負擔。




### 二、防止橫向移動及權限提升 - 檢測在組織內部移動的攻擊者，並阻止他們獲得存取權限

- 阻斷常見的攻擊路徑並實施誘捕。
- 阻止攻擊者利用特權身分取得存取權限。


## Identity 威脅防禦平台

**檢測並防止身分風險以阻擋橫向移動**

超過 90% 的攻擊仰賴身分資料外洩。Proofpoint ITD 身分威脅防護目前已在 150 次紅隊演練中維持不破（紀錄增加中）。

**持續發現**

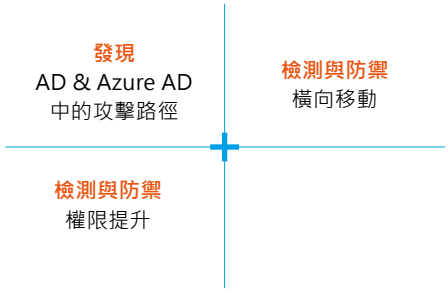
發現並確認身分漏洞優先排序。

**自動修復**

自動清除端點和伺服器中的風險。

**實時檢測**

部署誘捕系統（Deception）以維持安全可靠的入侵偵測。



## 三、減少對關鍵資料的影響 - 防止保護您的資料遭外洩或被盜用

- 檢測並阻擋企圖竊取資料的嘗試。
- 深入了解具風險的使用者行為和資料活動。


## Sigma 資訊保護平台

**阻止資料遺失和內部威脅**

Proofpoint Sigma 是唯一將內容分類、威脅遙測（Threat Telemetry）和跨管道使用者行為整合到單一、雲端原生介面的 DLP 資料保護平台，並受到 45% 《財富 100 》企業的信賴。

**強大的上下文關聯**

有效運用資料、行為和威脅之間的上下文關係（context）。

**統一的可見性**

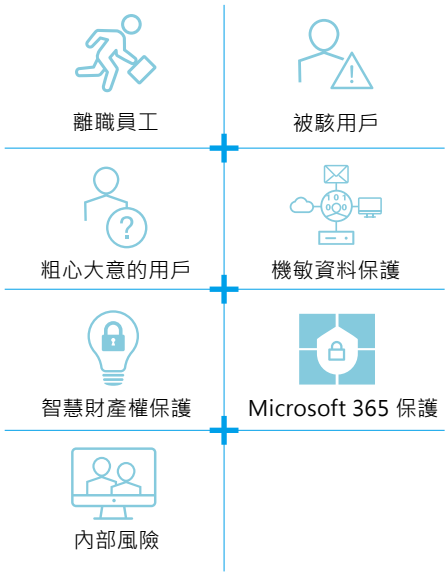
獲取對跨管道資料外洩及內部風險的可見性（visibility）並加以防範。

**內部調查**

調查內部人員，同時保護他們的隱私。

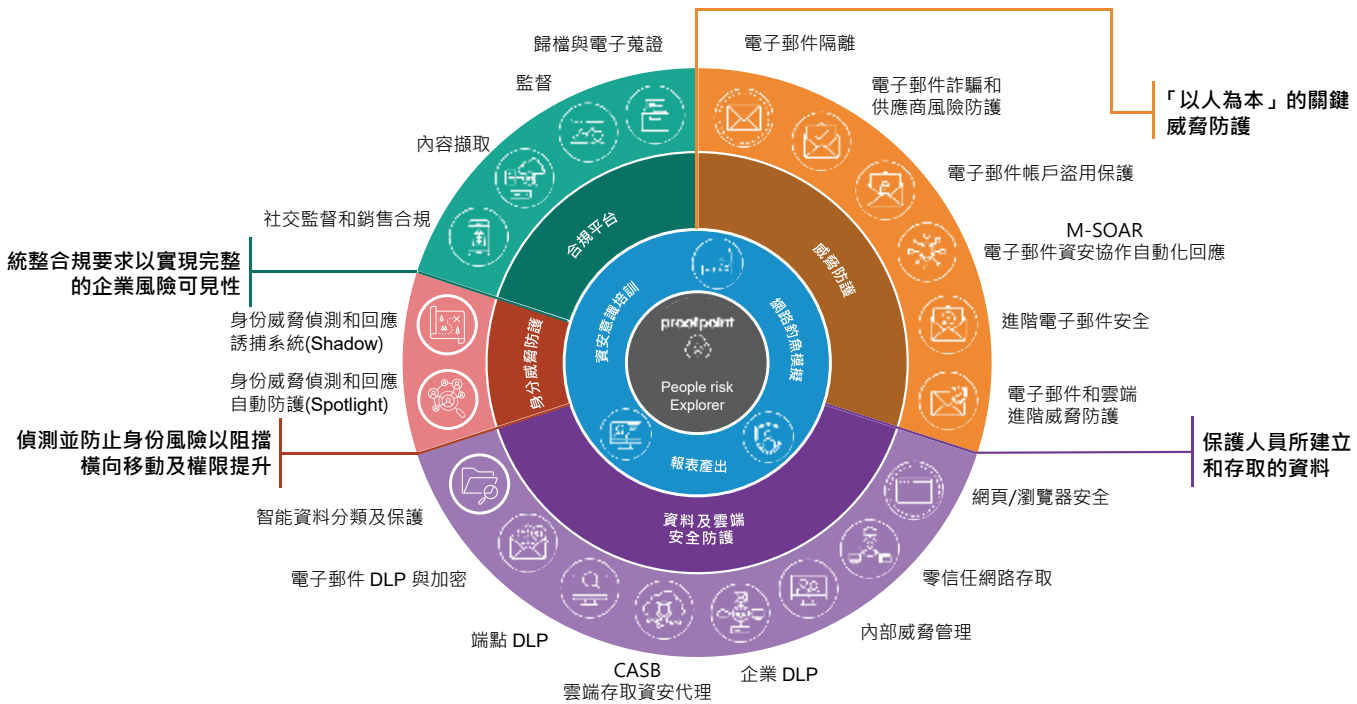
**加速實現價值**

實施簡化且具高可擴充性的雲端原生（cloud-native）部署。




## 以人為本的網路安全解決方案

確保您的業務安全、合規並蓬勃發展。



proofpoint.

## Email Security and Protection 電子郵件安全與保護

電子郵件是第一大威脅媒介，網路釣魚和電子郵件詐騙等社交活動 96% 都是透過電子郵件進行，且方式不斷在演變。Proofpoint 提供最有效的解決方案，保護您的員工和機敏資料免於進階電子郵件威脅。Proofpoint 完整且可擴充的電子郵件安全平台提供進階 BEC 防禦功能，可阻擋惡意和非惡意軟體的電子郵件威脅，讓您掌握最大的風險來源 — 您的員工，更全面了解所面臨的風險並快速回應各項威脅。

| | |
|---|---|
| 防止電子郵件詐騙<br>**防範 BEC 威脅** | 您可以透過 Proofpoint 先進的機器學習技術 NexusAI 對 BEC 和網路釣魚電子郵件、惡意軟體、垃圾郵件等威脅進行準確分類，並對所有寄件者進行身份驗證，讓合法電子郵件正常傳遞，以確保您的組織在電子郵件詐騙攻擊中的商譽。Proofpoint 電子郵件安全解決方案可自動識別您的供應商及其對企業組織的風險。 |
| 進階 BEC 防禦<br>**防範電子郵件和供應商詐騙** | 保護您的電子郵件免於各式各樣的詐騙，例如付款時遭重新導向至惡意網站，或是供應商發票詐騙等。面對這些威脅，您需要更精細的檢測技術。進階 BEC 防禦所運用的檢測引擎結合 AI 和機器學習，是專為發現、阻擋 BEC 攻擊而設計，能夠分析多種訊息屬性，藉此確認該訊息是否為 BEC 威脅。分析內容包括：<br>■ 訊息標頭資料<br>■ 寄件者的 IP 位址（x-originating IP 和商譽）<br>■ 緊急郵件內容和文字、句子等訊息<br>進階 BEC 防禦還可檢測各種攻擊者策略，例如回覆地址不一致( reply-to pivots)、使用惡意 IP 或類似供應商網域，並且可以讓您詳細了解 BEC 威脅資訊、提供 BEC 主題（例如，供應商發票、禮品卡、變更薪資轉帳帳戶等）、訊息相關的可疑原因觀察及訊息範例。這些詳細資訊可協助資安團隊更了解攻擊並進行因應。 |
| 威脅防護<br>**檢測並阻擋進階惡意軟體** | Proofpoint 電子郵件安全解決方案透過多層次內容分析、信譽分析和 Sandbox 分析來分析電子郵件，可檢測帶有惡意 URL 或附件的電子郵件，並阻擋勒索軟體和多種型態的惡意軟體。重寫 URL 可以保護所有網路和裝置上的用戶，並協助檢測訊息在發送後是否已被武裝化。 |
| 修補措施<br>**一鍵自動收回惡意郵件** | 您可以刪除寄送後中毒的 URL 網路釣魚電子郵件或被駭者不需要的電子郵件。即使電子郵件被其他使用者轉發或接收，也可以一鍵自動執行。 |

## | Proofpoint 電子郵件安全產品

### 電子郵件保護 Email Protection

Proofpoint 電子郵件保護 (EP) 是業界領先的電子郵件安全閘道，允許您保護、控制您的收信和發信。Proofpoint 特有的機器學習和多層次檢測技術有助於動態識別並阻止網路釣魚和 BEC 威脅。

### 針對性攻擊防護 Targeted Attack Protection

針對性攻擊防護 (TAP) 可協助您領先攻擊者。它為您提供一種創新方法，可以在進階威脅到達您的收件匣前對其進行檢測、分析和阻檔，進而保護您的電子郵件。TAP 可顯示重點受攻擊人員的可見性，並提供可行的建議和攻擊活動的詳細取證資訊。

### 電子郵件詐騙防禦 Email Fraud Defense

超越電子郵件身份驗證，掌握供應商詐騙行為。透過電子郵件詐騙防禦，您可以簡化 DMARC 實施。Proofpoint 為您提供工作流程指導及顧問支援，全面保護您的組織在電子郵件詐騙攻擊中的信譽。

### 威脅回應自動收回 Threat Response Auto-Pull

透過威脅回應自動收回，使您的訊息傳遞和安全管理人員能夠分析電子郵件，並在寄送後將惡意或不需要的電子郵件移至隔離區。

### 內部郵件防禦 Internal Mail Defense

擴展您的電子郵件安全解決方案，協助內部郵件防禦檢測出遭盜用的帳號。IMD 自動掃描所有內部電子郵件流量，提供一種多層次方法來識別透過遭盜用帳戶所發送的垃圾郵件、惡意軟體或網路釣魚攻擊，刪除這些電子郵件並提供報告以顯示哪些帳戶已遭盜用。

### 電子郵件持續性 Email Continuity

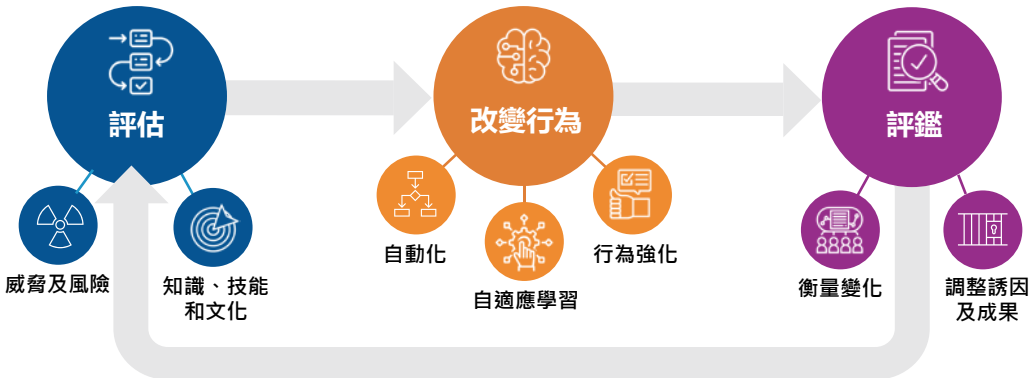
電子郵件系統停機可能會嚴重影響員工的工作效率。借助企業持續性，即使電子郵件系統停擺，仍可確保電子郵件始終可用。它透過 Outlook 整合、Web 入口網站或本機行動支援為您的使用者提供完全存取權限，EC 會在斷線時自動啟動，並於上線時自動回復。

proofpoint.

# Security Awareness Training 資安意識培訓

現今駭客比以往任何時候都更直接地以人為目標，95% 的網路安全問題都可以追溯到人為錯誤。透過為用戶提供具目標性、以威脅為導向的教育，可確保您的用戶知道在面臨真正威脅時該怎麼做。Proofpoint 資安意識培訓使您的員工能透過完整解決方案保護您的組織，進而有效減少 30% 現實世界的惡意連結的點擊次數。

Proofpoint 資安意識培訓方案採用整合性方法進行資安教育和意識培訓，提供經過驗證的框架，推動行為改變和真正的安全成果，因此連續 6 年在 Gartner 魔力象限中被評為領導者。透過 Proofpoint 資安意識培訓，您可以針對使用者弱點、角色和能力客製資安教育，實施簡短且聚焦的課程，進而持續讓員工培養習慣，確保在面臨複雜的攻擊時能做出正確回應，同時也提供 CISO 所需要追蹤的各項指標。




## 評估

第一步是建立組織的基準並了解使用者網路安全知識和計畫間的差距。Proofpoint 資安意識透過威脅情資驅動的知識評估、文化評估和網路釣魚模擬測試，幫助您了解計畫重點，並可與 Proofpoint TAP 針對性攻擊防護平台整合，讓您掌握實際攻擊中的經常點擊者和 VAP 重點受攻擊人員。Proofpoint 協助您確認使用者面臨威脅時會做什麼以及對安全的認知，進而調整培訓計畫，滿足使用者的個別需求。

- 基於實際威脅的網路釣魚、USB 模擬
- 知識評估
- 文化評估
- 識別組織內的 VAP 和點擊次數最多的項目/用戶報告

## 改變行為

提高資安意識的下一步是改變不安全的行為。借助 Proofpoint 獨特的自適應學習框架，您可以為使用者分配具針對性、威脅驅動的培訓。這種量身定製的線上資安教育可著重用戶需求及其薄弱環節來幫助企業推動行為改變，建立資安意識的知識基礎。Proofpoint 支援 40 多種語言的用戶培訓教材，減少語言障礙，並能與電子郵件安全解決方案整合。您可以提供上下文提示，提醒使用者有問題的電子郵件，並允許他們使用電子郵件警告標籤提報可疑訊息，透過自訂報告統整用戶回饋的可疑消息，強化積極回報行為。

- 微學習內容
- 自適應學習框架
- 威脅導向的教育訓練
- 電子郵件警告標籤
- 閉環電子郵件分析和回應（CLEAR）流程

## 評鑑

最後，您可以衡量您的安全意識培訓計畫績效，了解使用者的電子郵件準確率、點擊率和模擬 / 真實攻擊的報告資訊，並透過擷取重要指標來與產業同行比較。資安意識培訓可以提高安全計畫的可見性，以便更好地展現成效，並幫助您專注於須改進的地方。

- 使用 CISO 儀表板進行基準測試和其他關鍵指標確認
- 即時報告
- VAP 重點受攻擊人員的可見性

## 擴充和規模

Proofpoint 資安意識培訓為您提供靈活的導入方式，甚至應用至全球規模。您可以依計畫職責進行委派，同時監督整個計畫，並透過 Proofpoint 的多租戶管理做出集團規模的決策。

- 適用於具有全球或分散式的大型組織
- 了解全公司內的教育活動
- 針對在地用戶和客製化培訓需求
- 打造您的資安意識品牌內容
- 可支援擴充至 40 多種語言

# Insider Threat Management & Endpoint DLP 內部威脅管理與端點資料外洩防護

隨著遠距辦公形成，讓員工、第三方廠商及供應商可以存取比以往更多的資料 - 無論這些資料是在他們的筆記型電腦、電子郵件還是雲端。因此，資料遺失的風險也隨之增加。然而，資料不會自己遺失，往往都是「人」所造成的；而資料外洩又分為三種類型：粗心、惡意或被駭。在制訂適當的策略之前，必須先了解使用者背後的行為，這能幫助您在內部事件發生時以更好的方式回應。

Proofpoint DLP 端點資料外洩防護和 ITM 內部威脅管理，提供了一種「以人為本」的方法來管理內部威脅並防止端點資料外洩。

- 識別具風險的使用者行為和機敏資料的相互影響
- 檢測並防止內部人員的資安事件和端點資料外洩
- 快速回應使用者引起的事件

Proofpoint DLP 端點資料外洩防護和 ITM 內部威脅管理都能防止用戶資料外洩，並透過對使用者活動的深度分析來防禦高風險用戶的威脅。這兩個解決方案隸屬於 Proofpoint 資訊保護和雲端安全平台 - 一個全面、情境化的雲端原生平台。它允許您從中控台設定策略、分類告警、尋找威脅並回應事件，協助您快速有效地阻止資料外洩並調查內部違規行為。

## 監控日常用戶和有風險的用戶

Proofpoint 開發了一種輕量的端點 agent，可以防止資料外洩並提供對使用者活動的深入分析。透過對策略配置的簡單變更，您可以依每個使用者或使用者群組設定所需收集的資料量和類型，這種自適應方式可以更有效地調查、回應告警，且無須收集大量資料。

一般用戶通常風險較低，可以用 Proofpoint DLP 端點資料外洩防護對其進行監控，以深入了解資料活動及關聯性。對於高階管理者或具有風險的用戶，則需要更深入了解他們的動機和意圖，監控他們的行為或情境。Proofpoint ITM 內部威脅管理收集關於這些使用者活動的深入分析資料，提供在事件發生的前、中、後，用戶的意圖關聯分析。

## 提供使用者資料活動的可見性和關聯性

Proofpoint DLP 端點資料外洩防護收集使用者與端點互動的資訊，包括使用者何時操作檔案或重新命名機敏資料檔案，以及嘗試移動機敏資料時的記錄。Proofpoint ITM 解決方案提供基於端點活動的完整視圖，以便監控具風險的使用者。它收集 Proofpoint 端點 DLP 的資料，提供應用程式使用的可見性、端點活動的截圖和其他風險行為，包括安裝、執行未經授權的工具。ITM 有助於掌握風險事件相關的人員、內容、地點和時間。借由上下文的分析洞察，您可以在資料外洩或不符規範的行為發生時，更快辨別使用者的意圖。

## 即時檢測有風險的用戶行為和資料的相互影響

您可以從頭開始建立適合您的環境規則和觸發設定，或者調整 Proofpoint 預設的威脅腳本。依使用者群組、應用程式和日期/時間以及資料敏感度、分類標籤、來源和目的地、移動路徑和類型進行腳本修改。

Proofpoint 端點 DLP 和 Proofpoint ITM 包含預設的告警庫，可以輕鬆設定並快速執行。Proofpoint 端點 DLP 和 Proofpoint ITM 都能提醒端點上具風險的資料移動及使用；Proofpoint ITM 還能針對更廣泛的內部威脅危險行為進行告警。

## 端點 DLP 和 ITM 告警庫

| 資料活動 | | 使用者活動(僅限 ITM) | |
|---|---|---|---|
| 資料使用及外洩相關告警，包括 ( 超過 40 個警報 )： | | 全方位端點用戶活動相關告警 ( 超過 100 個警報 )： | |
| • File upload to web<br>• File copy to USB<br>• File copy to local cloud sync<br>• File printing<br>• File activities (rename, move, delete)<br>• File tracking (web to USB, web to web, etc.) | • File download from web<br>• File sent as email attachment<br>• File downloaded from email/endpoint | • Hiding information<br>• Unauthorized access<br>• Bypassing security control<br>• Careless behavior<br>• Creating a backdoor<br>• Copyright infringement<br>• Unauthorized comm tools<br>• Unauthorized admin task | • Unauthorized DBA activity<br>• Preparing an attack<br>• IT sabotage<br>• Privilege elevation<br>• Identity theft<br>• Suspicious GIT activity<br>• Unacceptable use |

## 防止未經授權的資料從端點外洩

只檢測具風險的用戶和資料活動是不夠的，您還必須主動阻止資料外洩。透過 Proofpoint 平台，您可以防止使用者與機敏資料進行不當的行動。這些行動包括：

- 與 USB 裝置之間的傳輸
- 將檔案同步到雲端資料夾
- 上傳到未經授權的網站
- 文件列印

可依據使用者、使用者群組、端點群組、程式名稱、USB 裝置/序號/供應商、資料分類標籤、來源 URL 和內容掃描等項目自訂防護。

proofpoint.

# Identity Threat Detection and Response 身份威脅檢測及回應

## 檢測、預防身分風險，以阻止橫向移動和權限提升

身分竊取是現今數位環境中日益嚴重的威脅。駭客能突破既有防禦，在幾天內完成攻擊。Proofpoint ITDR 解決方案，可提供防禦攻擊時所需的身分威脅防護及回應。即使駭客正在行動並在環境中橫向移動，ITDR 解決方案也能持續發現並修復您的即時漏洞。

- 服務帳號
- 舊版應用程式帳號
- 影子管理者帳號
- Kerberoastable 憑證
- 快取憑證（Windows、瀏覽器等）
- 未正確斷開的 RDP session
- 雲端服務Token

ITDR 解決方案可發現並消除的特權身分風險如左圖所示：

**Spotlight - 透過自動修復預防身分風險，並檢測橫向移動與即時威脅**

當駭客第一次入侵時，很少直接執行他們的最終目標，這意味著他們需要提升權限並透過橫向移動來實現目標。駭客快速、輕鬆且有效地利用特權帳號，組織也很難檢測到。透過 Proofpoint Spotlight，您可以檢測環境中的權限提升和橫向移動。

## 發現並修復特權身分漏洞和政策違規行為

| AD 持續發現和檢查 | 自動風險修復 | 準確檢測並回應 |
|---|---|---|
| Spotlight 會持續檢查 Enterprise AD、Azure AD 和 PAM，以發現組織的身分漏洞並確定其優先順序。Spotlight 可檢測：<br>■ Enterprise AD 與 Azure AD 設定錯誤<br>■ 特權存取管理（PAM）漏洞<br>■ 端點暴露（Exposure）<br>■ 權限提升和橫向移動 | 簡化身份漏洞修復：<br>■ 自動修復端點和伺服器風險<br>■ 提供身份風險儀表板，完整了解自動修復的風險及告警<br>■ 輕鬆強化組織的身分安全態勢<br>■ 有效評估新環境風險 | 檢測規避防禦的身份威脅：<br>■ 用於部署失效安全（Failsafe）對入侵者的檢測誘捕<br>■ 超過 75 種誘捕技術用於無代理檢測和保護<br>■ 從攻擊者角度提供攻擊的可見性<br>■ 針對不同端點客製化的自動誘捕<br>■ 在攻擊鏈中自動收集證據以進行稽核和合規 |

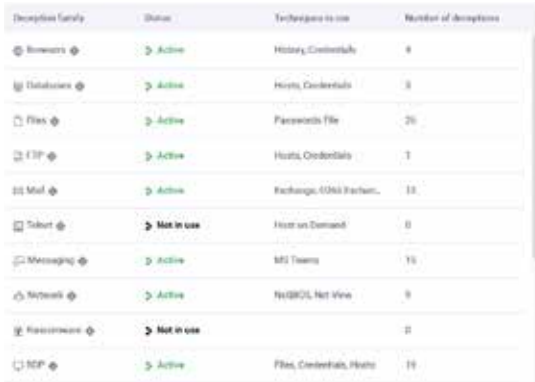
**Shadow - 透過誘捕技術，在駭客意識到前進行阻擋**

用傳統特徵碼或行為分析進行檢測，很容易讓資安團隊因為誤報和告警疲勞而不知所措。為了持續檢測新形態的網路攻擊，您需要誘捕技術來提供對權限提升和橫向移動的實際檢測。Proofpoint Shadow 與傳統方法不同，以無代理方式（Agentless）在您的正式環境中主動吸引攻擊者，並檢測出他們的存在。

## 將每個端點變成誘捕網，阻止攻擊者橫向移動

| 無代理檢測及保護 | 超過 75 種誘捕技術 | 自動誘捕 | 從攻擊者角度出發 | 自建誘捕文件檔案 |
|---|---|---|---|---|
| Shadow 獨特的無代理方式建立在智慧自動化的基礎上，減少營運足跡，最大幅度地降低對 IT 的影響，且無法像基於代理的解決方案那樣被攻擊者停用或規避。 | Shadow 提供主動誘捕技術來模仿對攻擊者有用的憑證、連接、資料、系統和其他文件。無論從何處開始被駭，組織都能在最短時間內發現內外部攻擊者。 | Shadow 智能自動化系統可建立高度真實的誘捕環境，並隨時間進行擴充和改變，而且幾乎不需要人為操作。Shadow 分析端點情況並為每台機器量身定製誘捕技術。可一鍵進行流程部署，並持續自動調整、管理誘捕的過程。 | 透過 Shadow 中控台，您可以了解攻擊者與關鍵資產的距離，一旦發生誘捕，就能取得攻擊活動的完整時間軸，還能了解攻擊者如何取得誘捕資料，以及更多與攻擊活動有關的情報。 | 透過 Shadow，您可以自建數十萬個誘捕用的 MS Word 和 Excel 檔案。這些檔案與真實檔案沒有差別，甚至連公司商標和信箋都一樣。這些仿真檔案會載入假數據，一旦駭客試圖用這些資訊來獲取存取權限，系統就會立即發出告警。 |

Spotlight 身分風險儀表板



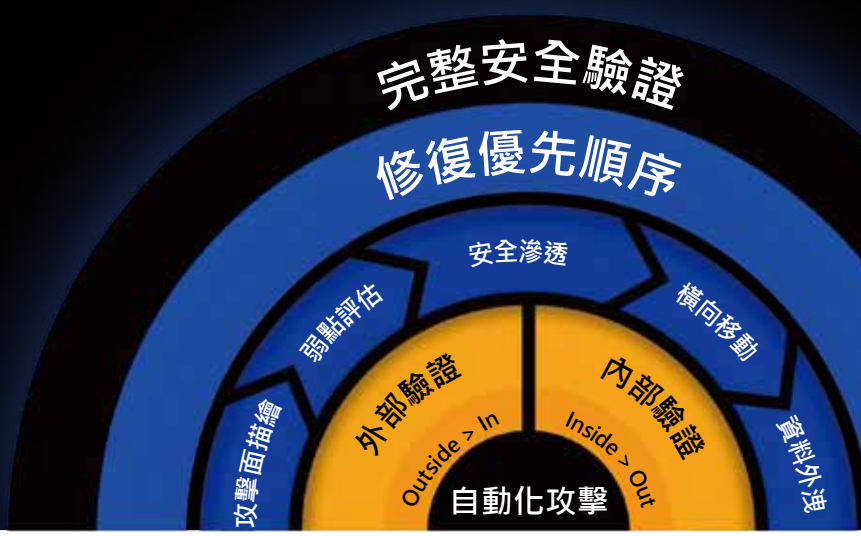
Shadow 誘捕狀態

PENTERA

PENTERA AUTOMATED SECURITY VALIDATION™ PLATFORM

# 自動安全驗證平台

模擬真實世界的攻擊
降低曝險可能




## 單一平台，提供所有您需要的安全驗證

Pentera 是自動安全驗證領域的領導者，讓每個組織都能輕鬆測試網路安全層的完整性，無論何種規模，隨時都能呈現真實、即時的資安漏洞。全球眾多資安人員及服務供應商均使用 Pentera 來導引修復，並在漏洞被利用之前進行修補。Pentera 平台能持續發現企業內外部攻擊面，安全而自動地驗證所有風險，以確保隨時準備好面對各種新型威脅。Pentera 平台能證明每個資安漏洞的潛在影響，並確認相對應的修補優先順序。

## ASV自動安全驗證三大特色

**低接觸**
無論何時何地都能以無代理程式(agentless)的方式進行安全驗證

**持續覆蓋**
隨時可用、涵蓋所有內外部攻擊面

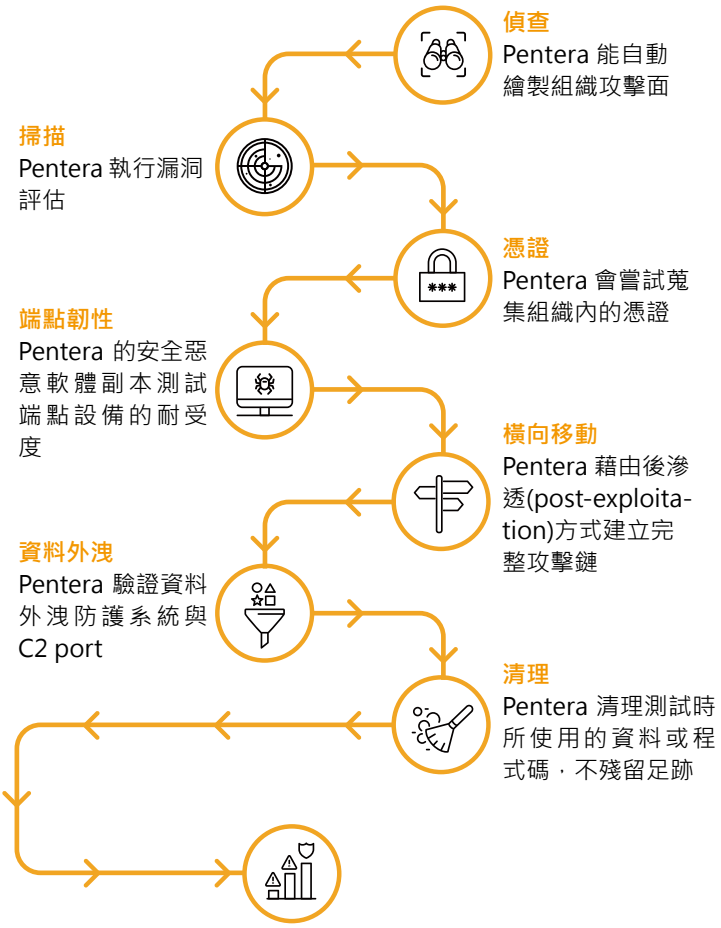
**真實攻擊**
模擬最新的戰術、技術和流程(TTP)

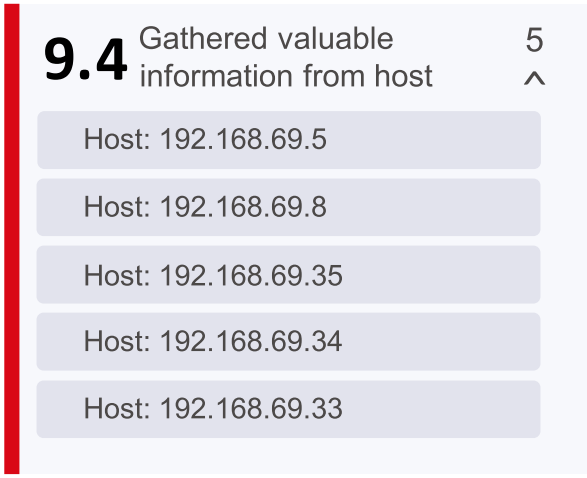
## ASV 與類似產品的比較

| | 自動安全驗證 | 弱點評估 | 入侵和攻擊模擬(BAS) | 滲透測試 | 外部攻擊面管理 |
|---|---|---|---|---|---|
| 弱點掃描 | ✓ | ✓ | ✗ | ✓ | ✓ |
| 控制驗證 | ✓ | ✗ | ✓ | ✓ | ✗ |
| 100% 自動化 | ✓ | ✓ | ✓ | ✗ | ✗ |
| 無代理程式 | ✓ | ✗ | ✓ | ✗ | ✓ |
| 真實驗證/非模擬 | ✓ | ✗ | ✓ | ✓ | ✗ |
| 基於風險的補救 | ✓ | ✗ | ✓ | ✗ | ✗ |
| 完整的攻擊面管理 | ✓ | ✓ | ✓ | ✗ | ✗ |

## ASV 運作方式

Pentera **安全地執行**攻擊者的所有行動




顯示修復的優先順序及其資訊


Pentera 進一步清楚地描繪攻擊路徑，以及漏洞將如何導致更重大的攻擊與事件

## ASV Dashboard

## ASV 效益

**以既有資源最大化資安防護**

持續的安全驗證可讓最重大的安全漏洞優先進行修補。

**縮短修復時間**

找出重大資安漏洞，並在被利用前就加以緩解，降低風險。

**減少對第三方團隊的依賴和費用**

最小化對第三方滲透測試服務的成本與依賴度。

**提高資安團隊的效率**

將資安人員對整體攻擊面的驗證效率，提升10倍以上。

IONIX

# Attack Surface Management
# 攻擊面管理 - 揭露真實攻擊面中的威脅

EASM 外部攻擊面管理已成為網路安全標準，是現代網路安全的核心組成之一。IONIX 是外部攻擊面管理的先驅，可提供您暴露在互聯網中資產的可見性、風險評估和主動保護，消除數位供應鏈風險，保護您的外部攻擊面。
EASM 是一個新興的產品，Gartner 將 EASM 定義為 “為發現企業面向外部的資產和系統可能存在的漏洞而部署的流程、技術和專業服務” ，並將 EASM 定位為 CTEM 持續威脅暴露管理（Continuous Threat Exposure Management）主要框架。

## 什麼是外部攻擊面？

其實您的攻擊面不僅包括您的組織與您的第三方供應商，您的客戶和員工在與公司連線存取的每一項資產都是構成外部攻擊面的一部份。所以，這些資產可能是您的組織所有，或是由第三方供應商擁有和營運，或者是您的 N 級供應鏈中的某個供應商，這些都可能構成組織的外部攻擊面。
簡而言之，外部攻擊面管理即是對攻擊媒介的持續發現、監控、評估、優先排序和修補。

## EASM 提供五種主要功能：

- 監控 - 持續掃描外部各種環境（如雲端服務和面向外部的本地基礎設施）、分散式生態系統（如物聯網基礎設施）
- 資產發現 - 發現未知的外部資產和系統，並將其對應到組織
- 分析 - 評估和分析資產屬性，以確定資產是有風險的、易受攻擊的，還是行為異常的
- 優先排序 - 優先考慮風險和漏洞等級，排定優先順序提供警告
- 補救 - 提供緩解首要威脅的行動計畫，以及補救工作流程或與事件系統、事件回應工具、SOAR 解決方案等系統的相互整合

EASM 應成為廣泛漏洞和威脅管理工作的一部分，以強化發現、管理內外部資產及其潛在的漏洞。
EASM 工具最常用於發現未知的面向外部資產和網路，並識別基於基礎設施的漏洞。EASM 還可以協助支援一些功能，如漏洞評估和雲端安全狀態管理（CSPM），以確定漏洞和配置錯誤的優先順序並進行補救。

## 第三方 Dependency 削弱您的網路安全防禦

一個網頁通常有數十個（或是數百個）從第三方主機提取的資源依賴項。例如：

**HTML 或 JavaScript Dependency**

Dependency 產生一個龐大的攻擊面，其中最普遍的連接是由 HTML 或 JavaScript 所產生的。這些連結可以在 HTML 圖像置入標籤、腳本標籤、CSS 和其他從第三方供應商和網站中取得資訊的標籤中找到。IONIX 可提供 Dependency 的查找和完整攻擊面的可見性。

**轉址(Redirect)**

轉址可建立使用者對網站的信任感，但需要對其進行監控和管理。IONIX 的攻擊面可見性能在單一中控台上自動顯示線上狀態中的所有轉址，不必讓資安團隊手動搜尋網站上每個頁面和每個轉址。

## 外部攻擊面可見性：第三方連接之外

在許多情況下，資源的相互依賴形成一條長鏈，而這龐大的攻擊面中的每個連接資產都可能是潛在的漏洞。透過控制單個第三方資產，攻擊者可以利用該資產的直接或間接連接來瞄準所有客戶。由於這種存取來自第三方供應商或合作夥伴，因此攻擊者可以避開組織複雜的防火牆、日誌、病毒掃描程式或其他檢測工具。如 Magecart 攻擊或是雲端資產盜用，都是第三方 JavaScript 的錯誤雲端配置所造成的漏洞，但這些可能都只是遭利用資產的冰山一角。因為近 50% 的網路攻擊是從組織的數位供應鏈發起的，IONIX 讓資安團隊能透過攻擊面可見性、持續的漏洞評估和主動保護來保護其攻擊面的每個組件。

IONIX 威脅暴露雷達（Threat Exposure）使資安和 IT 團隊可以輕鬆辨識組織的真實攻擊面及數位供應鏈中的關鍵暴露並採取行動。


### 不間斷的攻擊面管理
自動調整覆蓋範圍以適應變化並監控風險。

### 減少攻擊面
有系統地降低關鍵風險並淘汰未使用或被忽視的資產。

### 子公司風險控管
透過自動歸因集中監督並實現在地化的攻擊面管理。

### 弱點管理
透過攻擊面發現、評估和優先排序的自動化來強化既有資安計畫。

### 數位供應鏈安全
保護組織免於數位供應鏈威脅。

### M&A 併購相關風險
管理併購過程中，從評估到整合所有階段的網路風險。

### 雲端營運安全
獲取跨公有雲平台的可見性並管理風險暴露。

### 攻擊面驗證
使用自動化測試來驗證風險暴露的情況，並確認零時差威脅的可利用性（exploitability）。

• **攻擊面發現**

**發現您真正的攻擊面**

完整了解組織在數位供應鏈所有暴露的資產和有風險的連結。


• **網路風險評估**

**跨資產和連接的風險暴露**

動態監控整個數位資產和連接的風險。


• **風險優先順序**

**優先考慮最重要的事情**

根據事件影響範圍（blast radius）、可利用性和威脅情資，聚焦在當前最需要解決的問題。


• **主動威脅預防**

**更快、更多的威脅修復**

透過跨團隊明確的行動項目與工作流程整合加速風險處理，並藉由 IONIX Active Protection 實現自動風險緩解。

Array

## APV Application Delivery Controller

# 應用交付控制器

APV 系列應用交付控制器是次世代 ADC，可優化雲端服務和企業應用程式的可用性、效能和安全性，同時大幅降低資料中心的維運成本與複雜度。

### 提供伺服器負載平衡

APV 系列應用交付控制器能確保雲端服務和企業應用程式的可用性達 99.999%。透過多種分流演算法讓企業伺服器的擴充更具彈性，並藉由健康檢查機制即時確認伺服器運作及效能狀況，適當分配流量或故障轉移，確保服務不中斷同時優化品質。APV 系列可在第 2、3、4 及 7 層為各種協議執行負載平衡（包括 WebSocket、WebSocket Secure）。

### 提供 SSL/TLS 加速與卸載的功能

APV 系列簡化 SSL 認證/金鑰管理，實現智能內容管理和路由功能。若選購硬體加速器可進一步提升連線速度與數量，將網頁解密後的資料傳送給網站伺服器，降低伺服器所需的加解密運算效能；或選擇將解密後的資料先提供給資安設備（如WAF）檢查分析後再傳送給伺服器，讓傳輸加密與資安兩者都兼顧。SSL 金鑰交換演算法提供 RSA 及 ECC 非對稱加密演算法，選購硬體加速器可讓系統提供更好的性能與容量。

現今多數網路流量都是 SSL 數據，而加密數據無法被部分資安設備檢查，例如 IDS/IPS、防火牆等，因而只能繞過這些資安設備。APV SSL 攔截(Intercept)可解密 SSL 流量，提供給資安設備檢查，然後再重新加密轉發給目的地端。

### 提供線路負載平衡(LLB)與全域伺服器負載平衡(GSLB)

LLB 和 GSLB 可確保廣域網路(WAN)及分散式站點、混合雲環境的維運正常與負載均衡。LLB 監控多個廣域網路和動態流量分配，以提供優質的用戶體驗為主要目的。GSLB 可將流量在地理位置分散的應用服務，根據距離、語言、容量、負載和反應時間在各站點之間智能分配服務，以實現最佳效能和可用性。

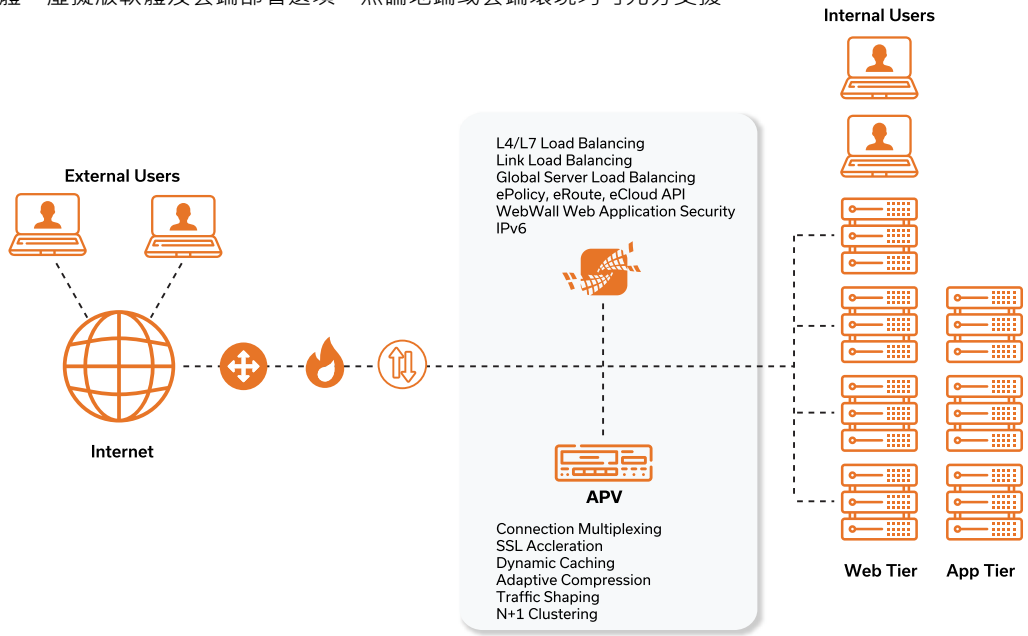
### 提供 DDoS 防護

結合 Array 網路應用程式防護功能套件 WebWall®，APV 系列產品可具備 L4 及 L7 的 DDoS 防護，如 SYN-Flood、tear drop、ping-of-death、Nimda、Smurf 等惡意攻擊，亦能透過機器學習檢測異常行為。此外，APV 設備還能透過設定的門檻值(threshold)、存取控制、網路地址轉換及狀態封包檢測等功能，防止攻擊及未經授權的存取訪問。

### 提供 IPv4 與 IPv6 地址

符合現在需求與未來考量。內建 64 位元的 SpeedCore® 專利引擎技術及專屬作業系統(Array OS)，達到優異的多核多工運算架構，以及自主開發的 SSL 協議技術，不需擔心開放技術 OpenSSL 的漏洞或效能問題。

除了提供 CLI 命令介面管理系統外，也提供 Web 圖型化介面，並可透過 XML-RPC 或 RESTful API 讓管理更簡單有效率。具備硬體、虛擬版軟體及雲端部署選項，無論地端或雲端環境均可充分支援。



Array

AG Secure Access Gateways

# SSL VPN 遠端存取平台

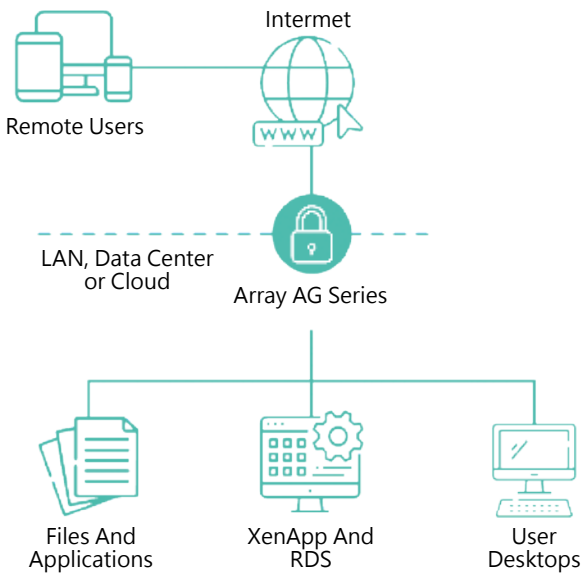
Array SSL VPN Gateway 讓來自各種遠端及移動設備安全存取各類應用、桌面、共享文件、網路和網站。AG 系列設備可部署在網路邊界或關鍵業務資源之前，提供員工、訪客、合作夥伴和其他相關群體安全的遠端存取。SSL VPN 是簡化用戶體驗同時減少潛在攻擊的理想選擇。

AG 系列提供完整的安全存取功能，包括 TLS 加密連線、設備驗證、端點和伺服器端的安全、進階 AAA 和細部政策管理。AG 系列提供硬體及虛擬版本，亦可在公有雲上使用（包括 AWS、Azure 和 Google Cloud），非常適合需要遠端存取各類應用的企業，以及需要靈活遠端存取以滿足廣泛客戶需求的雲端服務供應商。
Array SSL VPN 提供一流的安全遠端存取，滿足企業或組織單位對可擴展性、可靠性、靈活性和安全性的要求。

**可用性**
L3 VPN
L4 RDP
L7 Web
SSL/TLS 加密

**防護**
LDAP, SAML, OAuth
MFA, SSO, IDaaS
HW ID, Client Certs

**效能**
Per User
Per Resource
Per Virtual Portal




## 領先的SSL VPN功能

**不受設備限制，無論是控管設備或 BYOD**
Windows、Mac、Linux、Chromebook、iOS、Android 等。Desktop Direct 功能可確保個人設備的使用安全。

**設備認證和訪客安全檢查**
對設備認證、硬體唯一識別碼和客戶端安全策略執行身份驗證檢查。

**用戶身份認證、MFA 和 SSO 單一登入**
選擇 LDAP、SAML、OIDC 或基於雲的多因子驗證、IDaaS 和 SSO 單一登入。

**彈性的 SSL VPN 存取方式**
提供網路層存取、RDP、客戶端伺服器和來自單一入口網站的應用層存取。

**針對資源的存取政策**
對基於身份的 URL、APP 應用、檔案和網路存取的用戶政策進行編碼，並提供完整的日誌和統計資訊。

**可客制化的虛擬 Portal**
最多可達 256 個 Portal，並可根據安全性和多個社群的可用性偏好進行客制化。

**因應業務持續性的臨時授權**
臨時用戶授權可依業務需求提供，且成本比標準用戶授權更便宜。

**支援實體、虛擬和雲端部署**
可用作實體、虛擬設備或 AWS 和 GCP 上的雲端原生實例。

PacketX

# GRISM 網路能見度平台

## 打造 ZERO LEAKAGE 網路防禦機制

### 流量監控之完整性

A. 實體 vs 虛擬 / 明碼 vs 加密
所有流量收容匯聚
B. 解析萃取網路 Metadata

### 安全分析功能負荷降載

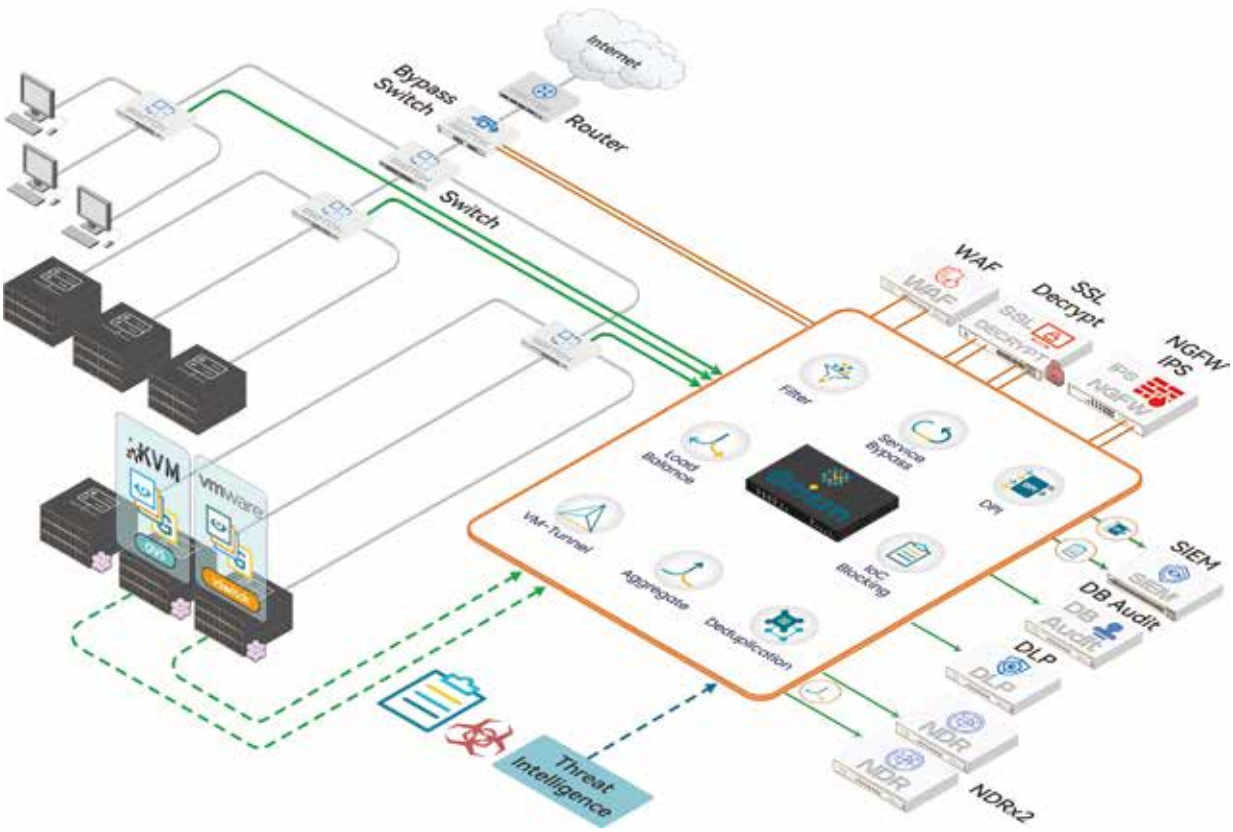
排除重複封包或低風險連線再精準遞送至多種且多台網路安全設備

### 情資驅動型防禦

匯入巨量威脅情資執行偵測
IoC Type：IP/Domain/URL/RegEx/Snort

## 能見度是網路安全的基石

為滿足網路管理和資訊安全需求，企業面對調整網路架構以部署流量分析設備（包含網路安全設備）的挑戰，此舉常導致網路延遲增加、可靠性降低和管理複雜度增加。在企業導入 GRISM 後，網路能明確地區隔為生產平面 (production plane) 與監控平面 (monitoring plane)，降低兩者的依存性，使其能夠獨立運維，從而解決上述問題。GRISM 作為監控平面之樞紐，能匯聚、複製、過濾及分配流量至分析設備，確保各分析設備僅能獲得必要之數據資料。再藉由持續更新的 IoC 清單，GRISM 還可有效阻斷使用加密通訊的惡意中繼站 (C2) 或釣魚網站，提升網路安全防護。



## 產品功能


**Netflow**
從封包流中擷取網路 Metadata

**Service Bypass**
可利用封包特徵辨識低風險流量，省略安全設備檢查

**Deduplication**
排除 L3 以上的重複封包

**Sophisticated Filter**
L2-L7 Session-Based 或 Packet-Based 封包過濾

**Load Balance**
可用 HA 配置執行 In-line 或 Out-of-Band 負載平衡。

**Aggregate**
可從多個來源或介面收集流量並進行封包預處理 (Pre-Processing)

**Massive Blocking**
透過大量情資匯入進行 Session 偵測及阻斷

**Tunnel Delivery**
支援跨站 (Cross-Site) 或監控 VM2VM 的 Traffic Span Tunnel

**Packet Slicing**
移除封包特定區域 (Section) 進行裁切

## 硬體規格

| | GRISM G8 | GRISM G8-BP2 | GRISM GBP2 | GRISM T12s-BP2 | GRISM T12s | GRISM T20 |
|---|---|---|---|---|---|---|
| 網路介面 | 1GbE RJ-45*8 | 1GbE RJ-45*8 | 1GbE RJ-45*8 | 10G/1G SFP+*12 | 10G/1G SFP+*12 | 10G/1G SFP+*20 |
| 硬體 Bypass | 1 pair GbE | 2 pair GbE | 2 pair GbE | 2 pair 10GbE | / | / |
| 流量轉發或複製 | 8Gbps | 8Gbps | 8Gbps | 40Gbps | 40Gbps | 200Gbps |
| 1:1 Netflow | Yes | Yes | / | Yes | Yes | Yes |
| Session 負載平衡 | Yes | Yes | / | Yes | Yes | Yes |
| 威脅指標容量 | 1M | 1M | / | 3M | 3M | 10M |

| | GRISM F4T4 | GRISM F2T12 | GRISM AT4G24 | GRISM AH6T48 | GRISM AH8T48 | GRISM AH32 |
|---|---|---|---|---|---|---|
| 網路介面 | 40G QSFP+*4<br>10G/1G SFP+*4 | 40G QSFP+*2<br>10G/1G SFP+*12 | 1GbE RJ-45*8 | 10G/1G SFP+*12 | 10G/1G SFP+*12 | 10G/1G SFP+*20 |
| 硬體 Bypass | / | / | / | / | / | / |
| 流量轉發或複製 | 200Gbps | 200Gbps | 42Gbps | 1.08Tbps | 2Tbps | 3.2Tbps |
| 1:1 Netflow | Yes | Yes | / | / | / | / |
| Session 負載平衡 | Yes | Yes | Yes | Yes | Yes | Yes |
| 威脅指標容量 | 10M | 10M | / | / | / | / |

TOPPAN

TOPPAN IDGATE

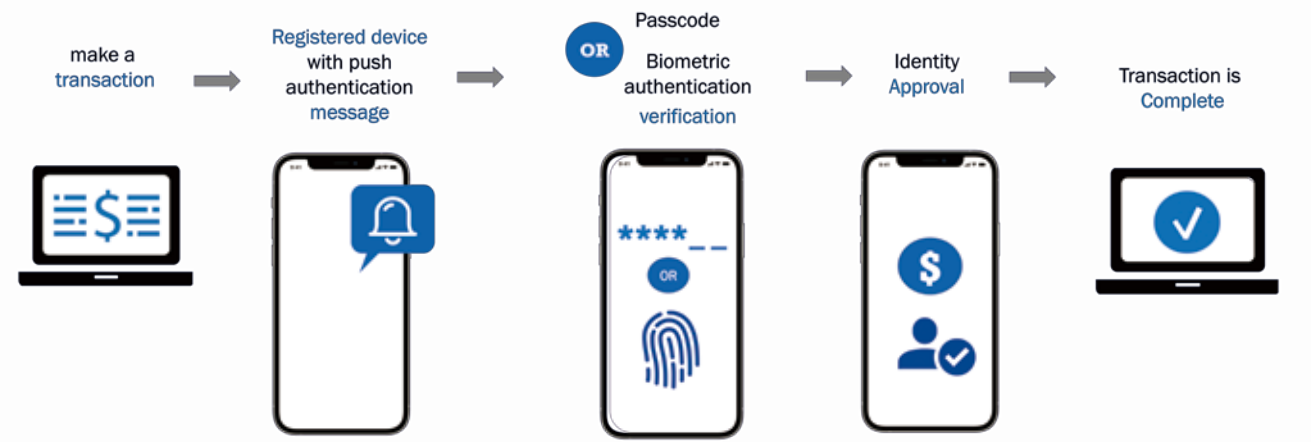
# 全方位身分驗證解決方案

## 時刻保障您的數位身分安全

TOPPAN IDGATE 提供備受讚譽的身分驗證解決方案，應用於金融機構、商業組織及政府單位，確保其數據不被竄改偽造。多年專注在數位金融身分驗證方案的開發經驗，我們針對每項數據安全需求，提供最符合客戶需求及合規性的身分驗證解決方案，保障全球各地用戶的數位身分安全。

TOPPAN IDGATE 解決方案以使用者角度出發，用戶不需要記住任何帳戶名稱或複雜的密碼，即可使用具備高度安全性的驗證流程，並提供可靠的防護，防止線上帳密竊取。從 AI 人臉辨識技術、Soft Token、MFA 多因子驗證方案到裝置重新綁定 ( Rebinding)，我們採用最先進的技術，提供完整數位身分生命週期方案，滿足各項法規標準，保護數位時代下個人身分免於被偽冒的風險。


## iDenKey：行動裝置綁定




## 以 iDenKey 進行設備綁定

iDenKey 使用設備綁定技術，用戶只需使用行動裝置即可下載APP綁定設備。透過 TOPPAN IDGATE 的 3+1 層保護技術，搭配專利的行動推播技術，提供可根據風險等級設計的身分驗證方案，並將行動裝置轉換為高安全強度的認證設備，達到銀行端的雙重保護，使交易流程更加安全、順暢。

iDenKey 在多個動態身份驗證層中使用了非對稱加密技術，並結合了 MFA 多因子身份驗證和動態身份驗證密碼。除了傳統的帳戶密碼外，多種保護措施更能防止數據洩漏，增強 Soft Token 安全，為用戶提供最佳存取安全。

## 基於風險的零信任身份認證方案

在金融業眾多服務中，不同服務需面臨不同的風險。TOPPAN IDGATE 提供了基於風險評估的身份認證方案，可以依據金融服務定義的風險層級要求用戶進行不同的認證模式，TOPPAN IDGATE 解決方案提供彈性化的系統設計，省去反覆修改系統所需花費的成本，在任何情境下達到靈活管理，為用戶提供最佳認證和安全防護的體驗。

零信任網路架構的概念就是對任何資料存取皆永不信任且必須驗證的原則；因此，每一次的網路行為，都需要進行驗證，確認數位身分後，才可以進行下一步的網路功能。

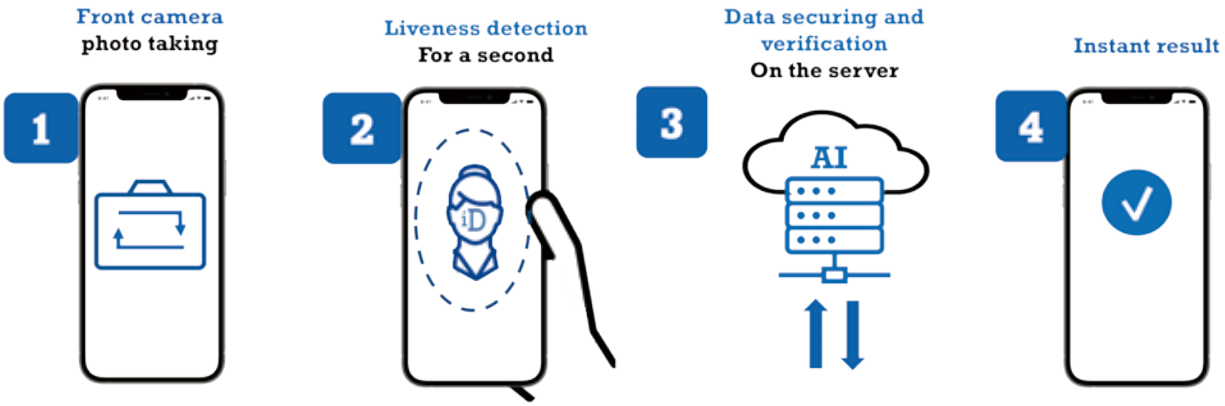
iDenKey 身分驗證零信任方案，以 FIDO2 鑑別伺服器為主機系統，搭配多因子驗證機制，提供依照風險等級為基礎的驗證服務，為零信任網路架構下最佳的身分驗證解決方案。透過符合 FIDO2 標準的 USB Key，為身分驗證的第一道防護；同時支援手機作業系統 Android 及 iOS，可以透過 FIDO2 USB Key 及手機 APP 進行身分鑑別，提升身分驗證行動效率。

- **金融安全等級方案**
  國內超過七成銀行所採用的數位身分驗證為技術核心，提供政府零信任機制金融等級的安全防護。
- **通過 FIDO 認證**
  IDGATE 驗證方案通過 FIDO2 及 FIDO UAF 認證，並擁有實際的導入經驗。
- **高穩定性**
  IDGATE 驗證核心累積超過千萬使用人次，部署之系統每月活躍使用者超過百萬人次，系統穩定度高，獲得金融產業高度肯定。
- **以風險為基礎的零信任驗證機制**
  可因應法規和銀行政策要求，針對不同業務和場域定義其風險等級，並依根據這些風險等級調整不同的身份認證機制設計。
- **榮獲 2024 Globee Cybersecurity Award 銀牌獎（在 Authentication 認證方案領域獲此殊榮）**

## iDenFace：生物辨識及線上開戶解決方案

### AI 人臉辨識系統

iDenFace 人臉辨識技術，利用靜默活體偵測，以 AI 模型進行圖像處理與特徵值比對，可分辨真假人臉數據，如螢幕翻拍、靜態圖像及仿真矽膠面具，可提供線上開戶流程人證辨識及換機裝置重新綁定，加強身分驗證安全。iDenFace 可在極短時間內完成高精度的人臉辨識，無論客戶使用哪種行動裝置，都能進行兼具精準度、安全性與效率的臉部辨識比對，且具備系統高相容性，可廣泛用於各項需要高規格認證的服務。




### 人證比對

TOPPAN IDGATE 的人證比對技術，榮獲 NIST FRVT 1:1 評測全台第一的殊榮，以操作直覺的拍攝方式，進行證件頭像與用戶影像的相符性檢查。iDenFace 透過色彩校正確保照片來源品質，並利用靜默活體偵測與 AI 模型進行特徵值比對，確保使用者與身分證上的人像為同一人，並為擷取資料進行加密，增加 eKYC 線上開戶流程的安全性。

# PoExtract
# SOOP-CLM集中式日誌管理平台

## Service-Oriented Operation Portal - Centralized Log Management

SOOP-CLM 是一個高性價比的企業級集中化日誌管理解決方案，由於它吃到飽授權特色，可以集中收容多樣性的日誌來源與不同的日誌格式，並進一步分析、關聯、儲存及視覺化日誌資料。不但一次滿足政府法令及稽核等需求，也是企業面對資訊安全與大數據時代的堅強後盾，更可以結合其他第三方解決方案，節省整體擁有成本，增加企業競爭力。

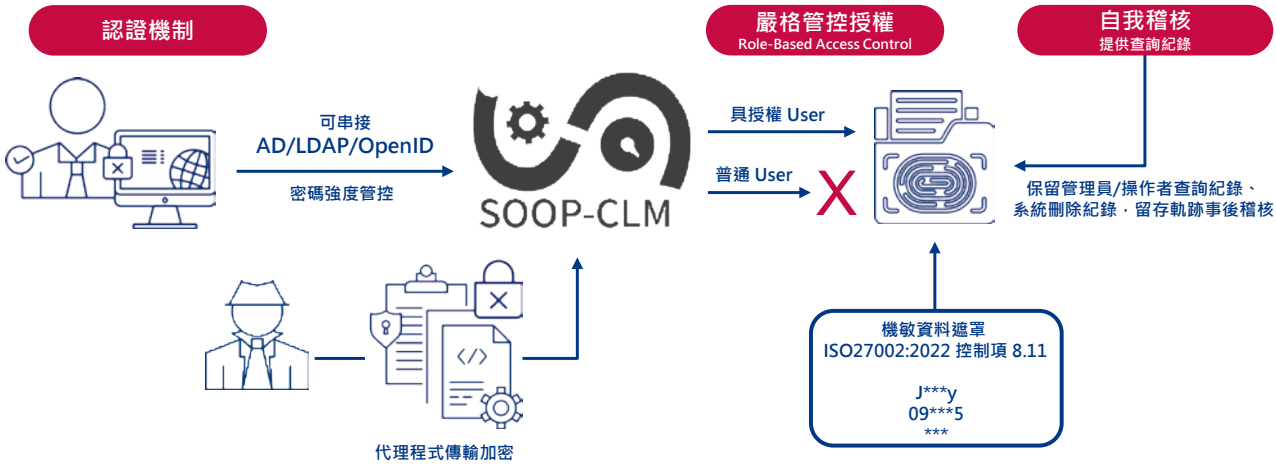
| 資通安全責任等級 | 保存範圍 | 保存項目 |
|---|---|---|
| A | 機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。 | 1. 作業系統日誌（OS event）<br>2. 網站日誌（web log）<br>3. 應用程式日誌（AP log）<br>4. 登入日誌（logon log） |
| B | 機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄 | |
| C | 機關應保存全部核心資通系統最近六個月之日誌紀錄。 | |

### 強大的集中收容能力，便於高效率查找及降低資料流失風險

可集中收容眾多裝置上不同格式的日誌資料，透過內建的多樣解析模組分析關聯所收容的各種日誌資料；提供關鍵字查詢並視覺化相關資訊，平均百萬資料秒級回應； 若結合 Data Queue 模組，作為蓄洪池之用，避免突發大量流量衝擊下，資料遺失風險；亦可將長期歷史資料壓縮儲存或整合 Hadoop 作為資料倉儲之用。

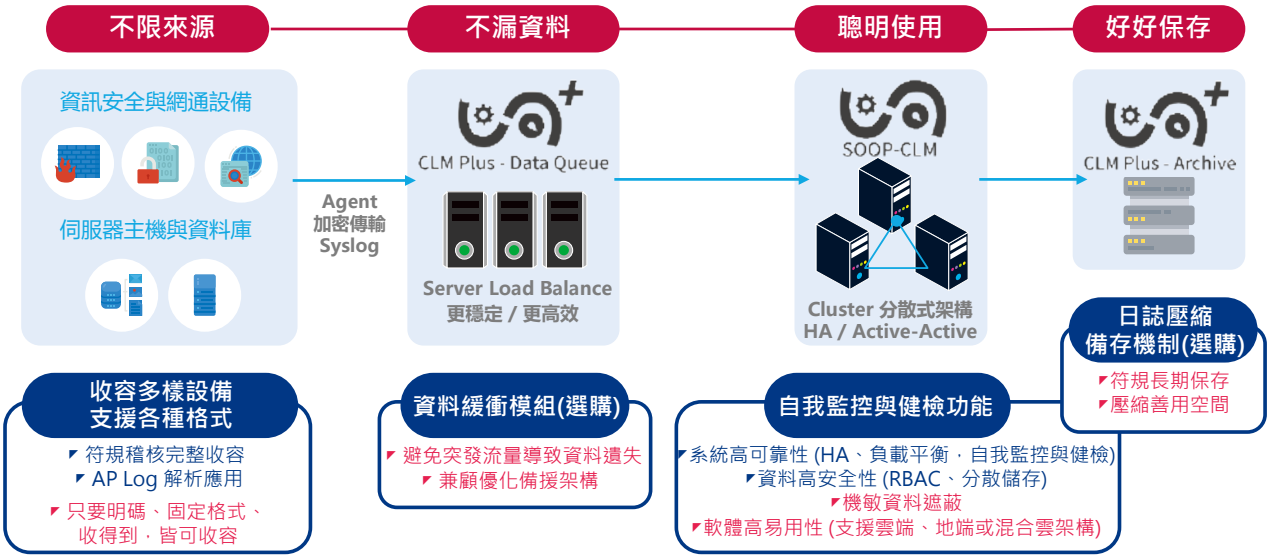

### 功能完整的日誌管理解決方案，易於操作上手及符合稽核管理要求

支援 AD/LDAP 及 OIDC 認證方式，具備密碼管控機制，嚴格的 Role-based 存取控管權限，內建Document Level Security 以符合 ISO-27001 要求，保護日誌資料且具不可竄改性，並可留存歷史資料以符合 ISO 27001 與 PCI DSS 等日誌稽核項目，達到法規遵循及企業稽核標準；提供簡易人機操作介面，可於 Web UI 上設定告警、報表排程和日誌解析規則等日誌管理功能，降低學習曲線；內建多樣視覺化模組，或運用時間過濾功能和拖拉式自定義儀表板功能，快速滿足不同視覺化需求。



## 穩定可靠的分散式架構設計，有效降低維護負擔，避免單點失效風險

去中心化架構的分散式運作叢集設計(Active-Active)，內建 Load Balance 機制，支援雲端、地端或混合雲架構，輕鬆達到簡易擴充，高可用度的目標；透過 SOOP-CLM 的自我監控及健檢功能，維運人員可輕易的掌握系統平台當前狀態，當系統平台運作遭遇瓶頸時，可協助迅速排除異常，大幅降低管理難度；內建防呆機制，可阻擋一般性不當之人為操作或管理疏忽。

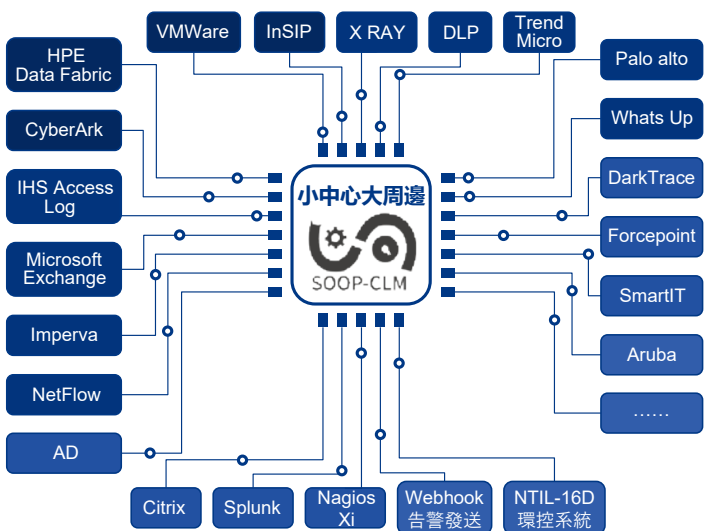



## 智能告警機制，提供真實的趨勢分析及反映真實狀況

SOOP-CLM 內建的動態閾值透過先進的演算法，自動依據過去的歷史數據，為不同時段定義更貼近現實的閾值，協助判斷是否發生異常，有效提升網路與資安告警的精準度，降低發送 False Alarm 的機率，協助用戶第一時間察覺異常，同時加速排除作業，提升系統可靠度，進一步推升使用者滿意度，達到早期告警、快速定位、高效維運的目標，如此一來，即可快速、精準定位異常範圍，有效減少排除異常時間，降低管理成本，提升維運效率。

## 小中心大周邊設計理念，整合其他第三方解決方案，擴大投資效益

提供多種 API，方便用戶整合或開發各種面向的第三方應用服務；在 IT 維運環境中，整合多種監控工具數據視覺化呈現，作為 NOC 之用；串接大數據平台，挖掘其中商業價值，擴大投資效益；整合 AIOps 工具，搭配 RPA 等機器人流程自動化工具，進行主動修復及預測分析等應用，讓 IT 管理更智慧化，加速企業數位轉型；結合 SOC 等資安軟硬體產品，不但可作為資安聯防一員，並可留下數位軌跡，以利數位鑑識查找，輔助資安政策制定。SOOP-CLM 的高整合性能發揮各產品的最大效益，節省整體擁有成本，增加企業競爭力。是企業在面對資安風險和 AI 時代的最佳選擇。




## 高性價比的計價方式，輕鬆擁有無後顧之憂

免費支援新設備的日誌解析處理，不必煩惱往後日誌平台維護支出增加；授權不限流量/EPS/容量/CPU/Memory/日誌來源設備數/日誌量/操作使用者數量，透過擴充硬體資源或節點方式，彈性部署節省使用成本；不斷推陳出新的日誌應用及插件，將投資效益發揮到最大；內建多樣化應用服務，大幅縮減客製化開發的時程及負擔；基於開源具備高自由度及在地支援，有效減少未來轉換成本和使用風險；國外官方維護及本地多方弱掃，雙重保障確實降低資安疑慮；客戶橫跨政府/金融/電信，產品經多方檢驗，品質成熟穩定有保障。