CipherTech
TRUST&SECURITY

亞利安科技 — 值得信賴的資安好夥伴

亞利安科技CipherTech為國內外知名資安產品的專業代理商，代理產品橫跨網路安全、主機安全、資料安全，是提供企業資產與營運機密保護的全方位資安合作夥伴。

完整的產品線

成立於2007年，亞利安奠基於資料庫加密方案及硬體安全模組HSM，客戶群以金融業為主。加密產品是保護企業機敏資料的最後一道防線，企業在加密之前仍須建構防禦的安全防護。

亞利安觀察到政府與企業對於網路應用程式的漏洞補強一直缺乏良好的對策，數年前SQL injection攻擊手法導致許多網站發生大規模個資外洩問題，加上個資法頒布執行後，企業對於資料庫存取軌跡紀錄、特殊權限安控稽核管理，個資盤點等需求開始湧現。

因此亞利安陸續引進imperva網路應用程式防火牆、資料庫監控稽核暨安全防護系統、Array Networks網路功能虛擬化專屬平台等知名產品，協助企業進行防禦規劃。

隨著企業逐漸進行數位轉型，亞利安也認知到，要讓IT環境下的商務服務運作順暢，必須先了解網路與應用程式運作的狀況，因此代理智慧型管理介面的 Netscout 產品，可透過 Dependency Mapping 功能，找出每個伺服器彼此之間聯繫的邏輯關係，進行應用服務追蹤時，就能知道應用程式運作時會與哪些周邊伺服器聯繫，繼而有效的管理、分析效能。

近年來APT進階持續威脅亦成為政府、企業另一項難解的資安問題，為此，亞利安也透過Thales Vormetric 透明加密解決方案及Netscout AED智能威脅防護系統，由內而外從資料庫保護、封包解析到情資分析，提供完整而全面的保護。

扎實的技術背景

資訊安全是既廣且深的專業領域，尤其亞利安代理的產品線多元，技術團隊更需要十八般武藝兼備，才能駕馭產品，為客戶解決問題。亞利安特別重視人員培訓，公司逾五成的資源與能力投注在技術人員培訓上，無論是參與原廠教育訓練、認證，或是內部定期培訓課程，都務求全員能對產品有扎實的掌握度，隨時了解各項最新的資安訊息。同時，亞利安也與JrSys等國內資安業者進行技術合作，提供PKI應用、生物辨識、IoT物聯網等領域的資安解決方案，希望客戶帶來與時俱進的防護及服務。

專業的服務

由於深耕資安領域多年，亞利安十分了解什麼樣的企業環境與資安問題，需要哪一種解藥。企業要建構縱深防禦的資安架構，除了找到對的產品，更需要能夠量身訂製的規劃藍圖及完整的資安健檢，才能得到專業建議與服務。

亞利安熟悉金融、電信、政府、電子商務、教育、醫療等各產業需求，持續以深厚的技術、專業、快速反應的態度為客戶服務，是企業可以放心、信賴的資安夥伴。

目錄 CONTENT

02	Thales	支付專用硬體安全模組(HSM) payShield Manager Vormetric 資料保護解決方案 SafeNet Luna Network HSM
11	Imperva	網站應用程式防火牆(WAF) Incapsula雲端應用交付服務 Attack Analytics 雲端AI告警分析系統 資料庫稽核系統(DAM)/資料庫安控防火牆(DBF) CounterBreach 資料庫AI智能防護
21	Array Networks	APV 應用服務傳遞控制器 AVX 網路功能虛擬化專屬平台
23	Netscout	網路與應用程式服務保障管理平台 混合雲應用分析探測器 網路與應用效能管理系統 ATA 威脅分析管理系統 AED 智能威脅防護系統 網路流量管理
31	JrSys	PDF Sign 電子合約 Trusted IoT 金鑰管理系統(KMS) 特權帳號管理系統

CipherTech TRUST&SECURITY

THALES

Thales集團是專注於航太、國防、安全市場的電子設備領導廠商，與Gemalto合併後，全球在50個國家超過8萬名員工，而Thales集團旗下的 eSecurity 事業群所提供的資料保護與金鑰管理解決方案，已為各大企業擊80%的銀行交易提供防護，其中包含19家世界最大銀行。Thales資料保護解決方案能使遍及企業的資料都得到保護，包含使用中資料、移動中資料以及儲存中資料。

硬體安全模組(HSM) 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加密模組 (Hardware Security Module)
- 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2500 tps
- 提供高可用性及完善的金鑰管理機制
- 符合FIPS 140-2 Level 3 安全等級，提供硬體強化的防竄改環境、防外力破壞

特色

- 專為信用卡支付系統設計，包含發卡與支付作業。提供4種軟體授權方式，可依功能需求選擇，包括HSM 8000 base equivalent、Transaction Processing（交易處理）、Magnetic Stripe Issuers（磁條卡發卡）、EMV Issuers（EMV發卡）。
- 擁有最高可用性與高效能，是首部具有雙電源供應器的金融交易專用硬體加密器，可避免因單一元件故障而造成系統停擺的問題。同時能處理最高每秒2500筆交易量，滿足金融業瞬間大量交易需求。
- 可同時間支援不同應用程式，各程式均有專屬金鑰保護，滿足業務集中管理、遠端管理要求，降低維運成本。
- 與現有Thales payShield 9000 及 HSM 8000 設備相容，不需改變現有資安政策，可共用現有的LMK IC 晶片卡，以及現有的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：從讀卡機產生的密鑰，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。
- 保護終端卡模擬(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，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。

法規遵循

- 整機符合支付系統交易安全要求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硬體加密模組標準 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發卡機構安全稽核要求，包括美國運通卡、Discover、JCB、萬事達卡、銀聯以及Visa卡。
- payShield 10K 符合GlobalPlatform 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 專為信用卡支付系統設計包含發卡與支付作業

支付方式、載具的變化，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、儲值、虛擬帳號、電子錢包、QR Code等無卡片支付方式，收單的部分也有無線化、行動化的趨勢。第三方支付國內甚至有專法通過，第三方支付產業可預期蓬勃發展,國內外電商及銀行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定嚴格的交易機制，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、交易資料加解密等關鍵工作，HSM除了確保安全性之外，同時也可簡化作業流程，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
製發卡作業	NFC近場通訊
PCI DSS	HCE P2PE點對點加密
磁條卡交易	VISA/Master/JCB/ American Express銀聯卡
ATM 交易	
信用卡交易	
網路銀行	

技術規格

密碼演算法

- DES 和 Tripel-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)
- HMAC、MD5、SHA-1、SHA-2

物理安全性

- 防篡改和回應設計
- 一旦遭到任何篡改攻擊，機敏資料會立即清除
- 行動、電壓和溫度的警報觸發器

金融服務標準

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

邏輯安全性

- 本地主金鑰(LMK)選項-變體和金鑰塊
- 使用智慧卡對安全人員進行雙重身份驗證(2FA)
- 雙重控制權-實體鑰匙或智慧卡
- 預設情況下提供最高強度的安全設定
- 使用者控制記錄事件範圍的審計跟蹤

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、1000 和 2500 次調用(CPS)
- 透過payShield 遠端管理(VM)、payShield 監控(VM) 和 payShield 可信任管理裝置(TMD)實現遠端管理和監控選項
- 格式保留加密(FPE)選項
- 多個LMK選項-每個HSM最多20個分區

payShield Manager

全方位的HSM管理工具

- 使用一般瀏覽器介面
- Smart cards做存取認證、模擬實體鑰匙、保存LMK

使維運人員24小時都能存取HSMs

- 調整設定，更新韌體，licenses執行金鑰管理操作

主要優勢

- 簡單使用，集中、遠端管理HSM
- 不需耗費時間往返機房
- 強化的存取控制及稽核紀錄

payShield Monitor

全方位的HSM監控工具

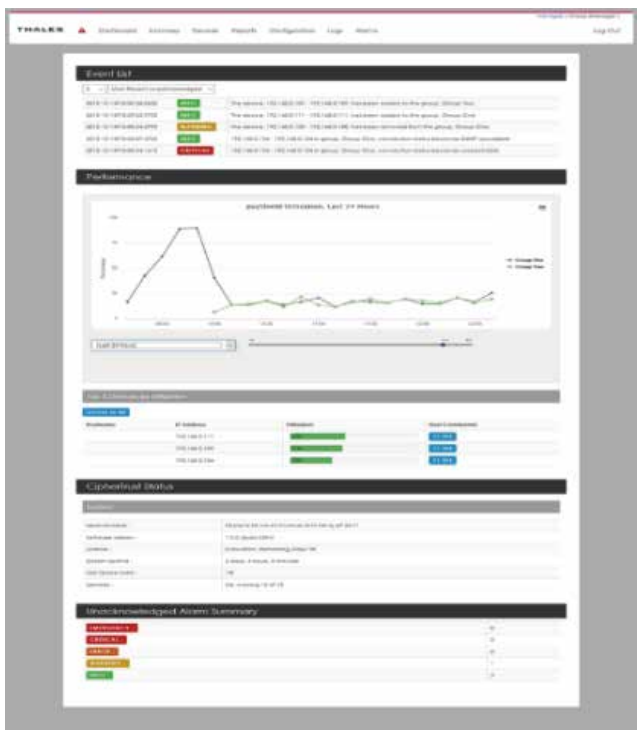
- 具備瀏覽器介面的VM虛擬機器

使維運人員24小時都能檢視HSM運作狀態

- 效能報告、設定變更、異常報警.....等

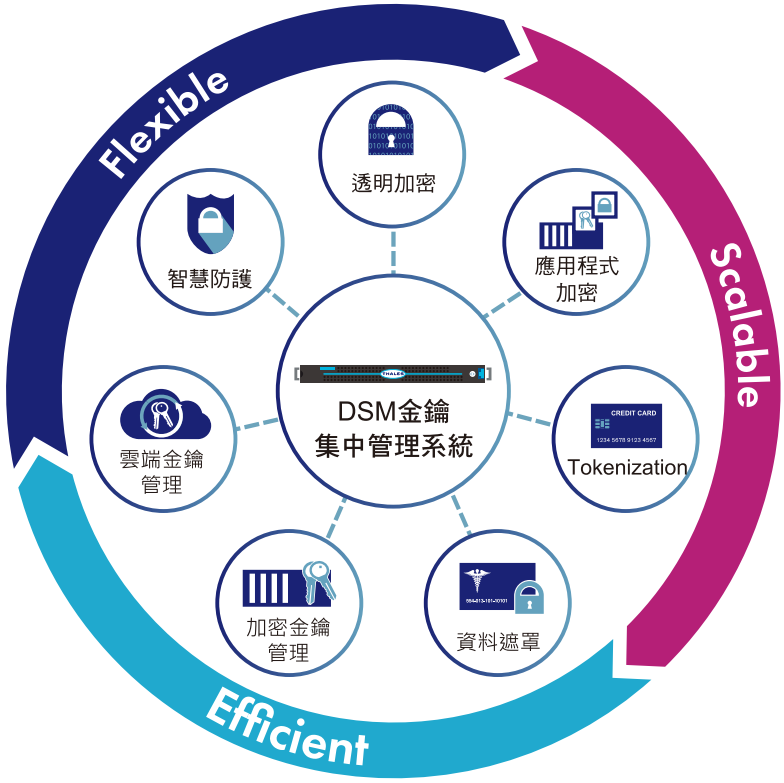
主要優勢

- 減少維運成本
- 優化HSM效能及使用率
- 加強應變能力



Vormetric 資料保護解決方案

Thales（與Vormetric合併）為企業的資料安全提供簡單、有效的管理解決方式。整體方案建構在一個可彈性擴充的架構下，擁有多種可個別佈署建置的資料保護及加密產品，同時提供高效、集中的金鑰管理機制。透過集中金鑰管理平台及彈性佈署模式，無論資料存放在雲端、虛擬或是傳統儲存架構，企業都可以橫跨資料庫、檔案、大數據環境，制定保護政策以符合法規要求。藉由這樣的整體方案，企業可以隨資料保護的法規要求，彈性擴張資料保護範圍，同時顯著降低滿足要求所需的成本。



DSM 金鑰集中管理系統

提供集中式金鑰管理，以及整體方案全產品線的資料保護政策管理功能。可選擇虛擬化版本或FIPS 140-2 認證的原廠硬體。具備 Web GUI介面、CLI介面外，亦提供API呼叫方式介接。運作架構支援Cluster容錯機制。支援管理第三方系統的金鑰，以及Log轉發到SIEM、log server。

- 原廠硬體通過FIPS 140-2 Level 2以上認證
- 虛擬化版本通過FIPS 140-2 Level 1 認證
- 可管理10000個以上的agent
- 具備Web GUI、CLI、API介面
- 支援Cluster架構，提供高可用性
- 可制定加解密政策、存取政策
- 支援雙因素認證(two-factor authentication)登入
- 可支援Vormetric產品線的金鑰及政策管理，包含：
  - 應用程式加密
  - 檔案、資料庫透明加密
  - 資料遮罩
  - 資料符記化(Tokenization)
- 可支援第三方系統金鑰管理，包含：
  - IBM InfoSphere Guardium Data Encryption
  - Microsoft SQL TDE
  - Oracle TDE
  - 支援KMIP協定之加密設備
- 具備金鑰使用及存取稽核記錄
- 支援Syslog RFC5424, CEF, LEEF格式，可整合第三方SIEM

Vormetric 透明加密

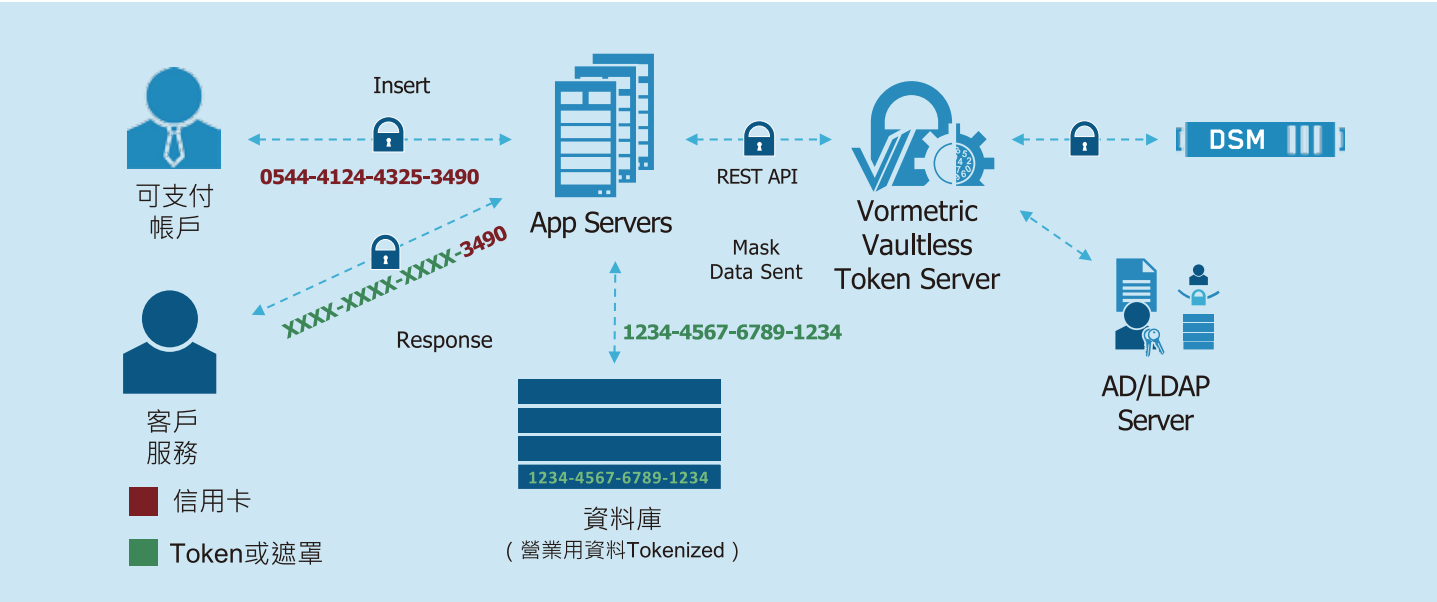
透過在檔案伺服器或資料庫伺服器上安裝代理程式，執行在DSM集中管理系統設定的各項加密政策、存取控制政策，並收集政策執行、觸發記錄，回送到DSM做統一保存及分析。在不需修改應用程式的情況下，達到資料保護目的，並符合法規、內稽內控要求。

- 支援實體、虛擬、雲端、大數據環境
- 作業系統支援
  - Windows: XP, Vista, 7, 8, Server 2008, 2012
  - Linux: RHEL, SuSE Linux Enterprise Server, Oracle Red Hat Compatible Kernel, Ubuntu
  - UNIX: IBM AIX, HP-UX, Solaris
- 資料庫支援
  - Oracle, DB2, SQL Server, MySQL, Sybase
- 大數據支援
  - NoSQL: Couchbase, DataStax, MongoDB
  - Hadoop: Cloudera, Hortonworks, IBM
  - SAP HANA
  - Teradata
- CPU加密優化支援
  - Intel and AMD AES-NI
  - SPARC encryption
  - IBM P8 cryptographic coprocessor
- Container支援
  - Docker
- 通過FIPS 140-2 Level 1認證
- 至少可根據使用者名稱、應用程序、檔案型態、時間，做為存取控制的條件
- 可限制有權限帳號，利用command方式讀取資料
- 免停機加密金鑰更新（Live Data Transformation）
  讓檔案及資料庫在使用中狀態也能進行加密及金鑰定期更新，不中斷使用者、應用程式與業務流程執行。

遮罩或符記化(Tokenization)

透過 RESTful APIs，搭配軟體式 token server，為現有應用程式提供簡單增加Tokenization及動態資料遮罩功能的方式。以獨立 Token server 產生隨機 token，將資料確實打亂，降低破解機率。而遮罩功能還可以設定資料還原權限，限制使用者可以完整還原或僅能部分還原資料。

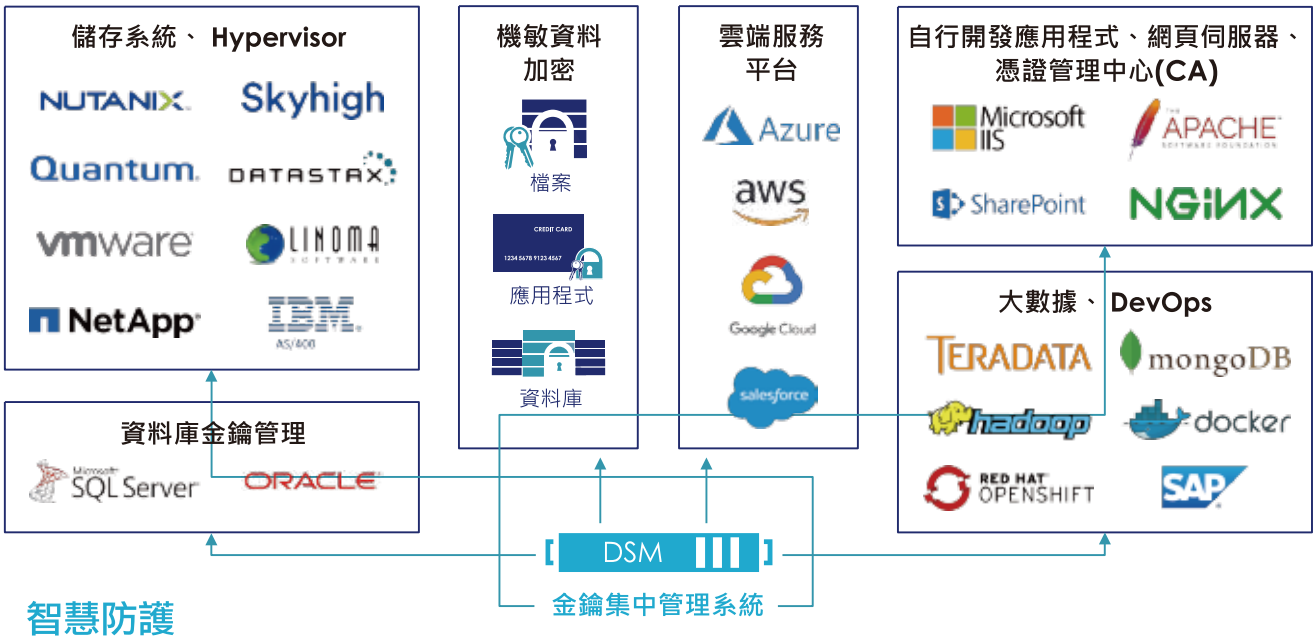
- 獨立VM版的Token server，提供GUI介面設定去識別政策及資料符記化。
- 提供REST API，使現有應用程式可與Token server介接。
- 政策可彈性設定將資料遮罩或符記化。
- 遮罩後的資料，可依據使用者權限，設定可完整還原或只能部分還原資料。



金鑰管理平台

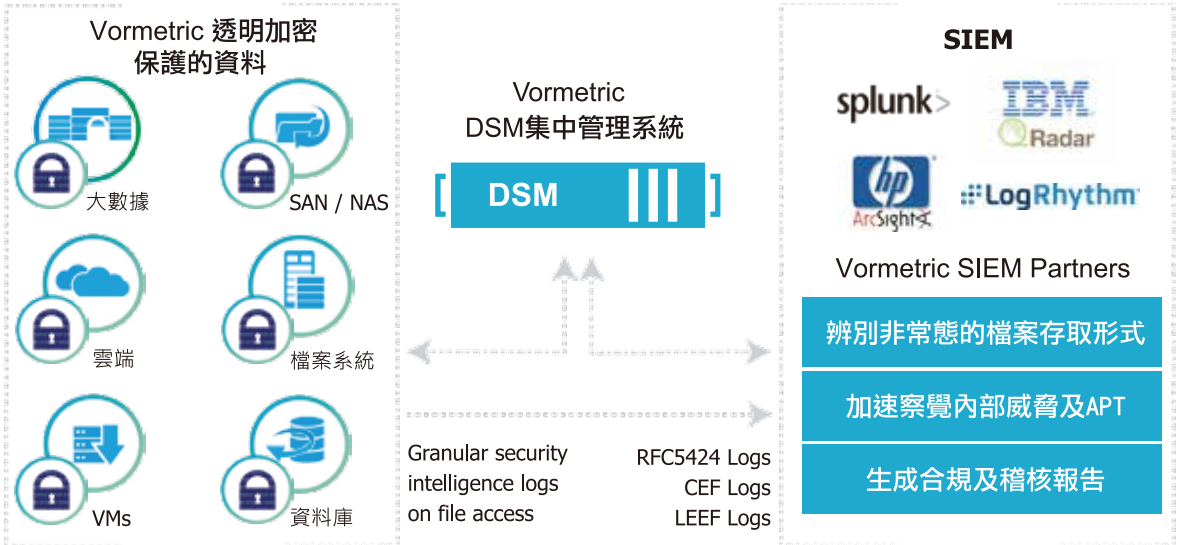
金鑰管理平台的用意，是讓企業能夠集中管理所有內部使用的加密金鑰。合併、集中管理金鑰，能夠透過統一的平台、操作介面，持續不斷的維護金鑰政策，同時減少訓練及維運成本。Vormetric金鑰管理平台可管理的範圍包括：

- 所有Vormetric產品
- 支援KMIP協定的加密產品
- 第三方具備加密功能的系統，如IBM InfoSphere Guardium Data Encryption, Microsoft SQL Server TDE, Oracle TDE



智慧防護

Vormetric　智慧防護提供細部事件紀錄，可整合至SIEM系統，快速產出法規、資安所需報表。這些紀錄產出由使用者、應用程式觸發的所有允許和拒絕的檔案存取稽核軌跡。發生在檔案系統的紀錄，可幫助減少未授權使用者嘗試竊取機敏資料的風險，讓管理者清楚知道不尋常的檔案存取行為，加快察覺內部資安威脅、駭客及APT攻擊並能立即反應。



Thales 滿足 PCI 主要合規項目

合規項目	PCI DSS	Thales 對應解決方案
保護持卡人資料	3.4, 3.5, 3.6	透明加密、應用程式加密、Tokenization、雲端資料防護、基於HSM的金鑰保護
資料傳輸加密	4.1	基於HSM的金鑰保護
限制對持卡人資料的存取	7.2	依據企業政策進行權限控管、使用者及設備身分認證、加密金鑰管理
識別、驗證對系統的存取	8.1, 8.3, 8.7	使用者及設備身分認證、依據企業政策進行權限控管、基於HSM的金鑰保護
追蹤對持卡人資料的存取	10.1, 10.2, 10.3	智慧防護、依據企業政策進行權限控管

Thales 滿足 GDPR 主要合規項

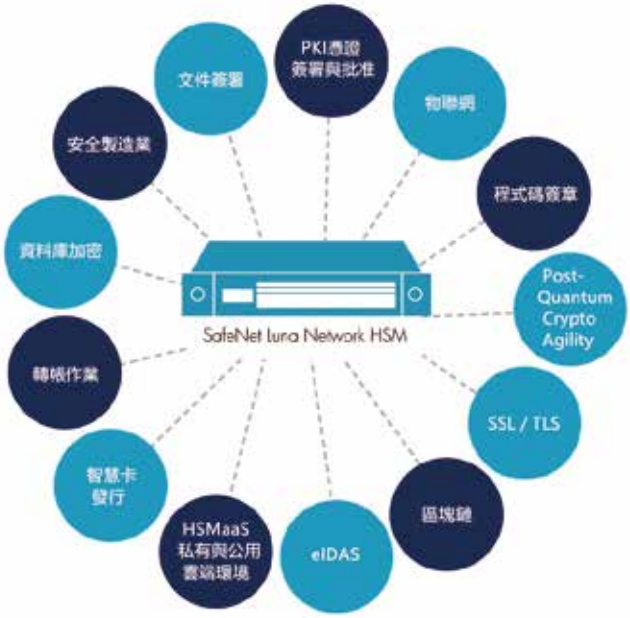
合規項目	GDPR 法規條例	Thales 對應解決方案
資料加密	Article 6, 25, 32	透明加密、應用程式加密、雲端金鑰管理、雲端資料防護
資安事件通報	Article 33, 34	透明加密、應用程式加密、雲端金鑰管理、雲端資料防護
資料存取控管	Article 5	依據企業政策進行權限控管、使用者及設備身分認證
資料存取稽核記錄	Article 5	智慧防護

SafeNet Luna Network HSM

- 超過每秒 20,000 ECC 和 10,000 RSA 作業的高效運行，符合您高效能的需求。
- 延遲時間更短，效能更高。

最高的安全性與合規規格

- 金鑰永保通過 FIPS 驗證*、防竄改硬體
- 符合 GDPR、eIDAS、HIPAA、PCI-DSS 等合規要求。
- 雲端現存標準
- MofN 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
- 以外部 Quantum RNG 植入的高品質金鑰



降低成本並節省時間

- 遠端管理 HSM - 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
- 多應用程式或租戶中分享 HSM，有效管理資源
- 彈性分割區規則，符合您的金鑰管理與合規需求
- 使用 SafeNet Luna Client 作為容器，攜帶更容易、效率更高、經常性開銷更低
- 功能模組
  - ° 延伸原生 HSM 功能
  - ° 於 HSM 安全規範中建立和部署自訂代碼

技術規格

支援作業系統

- Windows、Linux、Solaris、AIX
- 虛擬：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

加密

- 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、SM3 等
- Key Derivation：SP800-108 Counter Mode
- Key Wrapping：SP800-38F
- Digital Wallet Encryption：BIP32
- 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

實體規格

- 標準 1U 19 英吋機架式規格
- 尺寸：19” x 21” x 1.725”（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

供應機型

SafeNet Luna Network HSM 兩大系列各有 3 種不同機型供您選擇，符合您需求。

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：	企業效能：	最大效能：
RSA-2048：1,000 tps	RSA-2048：5,000 tps	RSA-2048：10,000 tps
ECC P256：2,000 tps	ECC P256：10,000 tps	ECC P256：22,000 tps
AES-GCM：2,000 tps	AES-GCM：10,000 tps	AES-GCM：17,000 tps

Luna S 系列：多因素（PED）驗證，較高安全性保障。

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：	企業效能：	最大效能：
RSA-2048：1,000 tps	RSA-2048：5,000 tps	RSA-2048：10,000 tps
ECC P256：2,000 tps	ECC P256：10,000 tps	ECC P256：22,000 tps
AES-GCM：2,000 tps	AES-GCM：10,000 tps	AES-GCM：17,000 tps

tps = 每秒事務處理量

imperva

Imperva
網路應用程式防火牆(WAF)

Imperva網路應用程式防火牆是唯一連續6年位於 Garther WAF Report 領導象限的廠商

Imperva 目前於全球超過70個國家有使用客戶，已有超過2600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、製造業等各個領域。於台灣也已有超過130家客戶使用，且使用客戶持續快速增加中。

特色

- 自動學習：自動且動態的白名單學習機制及政策調整，大幅減少維運人力及時間
- 佈建方式：用戶可彈性選擇Inline或sniffing方式，不需更動現有架構及程式，並具備集中控管機制
- 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：不需專業能力即可操作使用，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：權限控管功能，各司其職
- 更新機制：由原廠維護，每週更新報表範本、政策定義、黑名單...
- 整合弱點掃描：可匯入網頁弱點掃描report; 並提供資料庫弱點評估功能
- Threat Radar：結合第三方專業機構，即時防護最新攻擊事件
- 服務：原廠支援團隊分佈兩地，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級單位對網站應用程式防火牆的部署要求。
- Imperva網站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。

精確監控和保護Web應用程式

Imperva Web 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協定驗證

HTTP 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Web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(ACD)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Web蠕蟲獨特的特性組合來抵禦零時差的新蠕蟲攻擊。

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。

Web服務保護

Imperva 透過動態學習Web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Web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 Web 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能夠精細的檢測不可接受的行為，並防止惡意活動。

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。研究的結果就是提供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 Web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，同時還能延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。

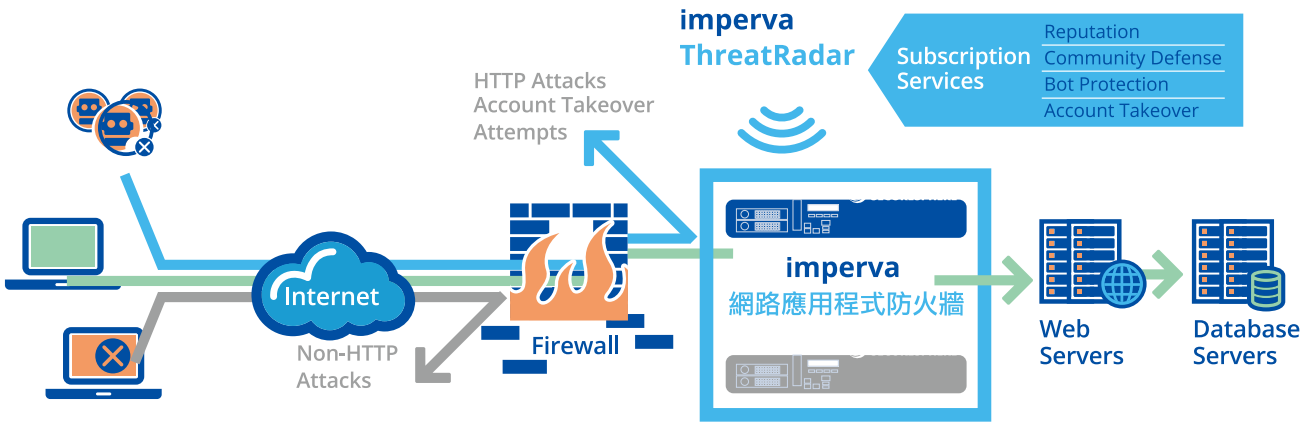
同等級產品最佳監控和報表功能

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報表。

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，包括領先的 SIEM 和日誌管理解決方案、基於角色進行身份驗證和用於弱點評估的Web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

Imperva Incapsula 雲端應用交付服務

安全是 Incapsula 的核心

目前，全球數以萬計的企業都用 Imperva Incapsula 來保護、加速他們的網站和網路應用程式-無論是中小型企業、電子商務網站，或是大型、高度安全導向的SaaS供應商和金融機構。

無論您是進行小規模的電子商務或是大型企業的IT營運，Imperva Incapsula 都能增進您的網站安全與效能。透過雲端服務的方式，Incapsula 減少硬體與應用程式管理的負擔，並提供超越傳統內部解決方案的有力工具。

Imperva Incapsula 提供符合企業需求的網站安全選項和效能服務

無論你需要的是網路應用程式防火牆，或是 DDoS 防護、CDN 或負載平衡解決方案，Incapsula 都能提供。這種全方位的應用交付解決方案能讓企業將不同服務和設備整合到單一企業級的雲端服務中，以簡化IT營運流程並降低成本。

Incapsula 是以雲端為基礎的應用交付服務，讓各種規模的線上業務都能享有企業級的網站安全、效能和可用性。Incapsula 提供最佳的網路應用程式防火牆、完整的 DDoS 防護、全球內容傳遞網路 CDN 和應用層負載平衡器，均可作為個別獨立服務或整合性解決方案。只需透過簡單的 DNS 變更即可啟用，不需安裝軟硬體、修改程式或其他複雜的整合。

基本方案	Enterprise 20	Enterprise 50	Enterprise 100
Cloud WAF / CDN	20 M	50 M	100 M
Site Domain	1 site	1 site	1 site
DDoS 防禦(選購)	Unlimit	Unlimit	Unlimit

除了以上基本選購方案，客戶還可依個別需求彈性調整雲端WAF流量和保護的Domain數量。

DDoS 流量清洗服務將依基本方案不同，而有不同選購價格。

DDoS 防護

自動緩解最大量和最智慧化的DDoS攻擊

全面防禦所有型態的DDoS攻擊

Incapsula 以遍佈全球的高容量網絡，保護企業網站免於各種DDoS威脅，包括網路層攻擊（如SYN 或 UDP Flood）和企圖消耗伺服器資源的應用層攻擊（如GET Flood）。Incapsula 服務可以檢測、緩解利用應用程式、網路伺服器和DNS伺服器漏洞所進行的進階攻擊和大型殭屍網路威脅。

企業級網路應用程式防火牆（WAF）

Incapsula 企業級、PCI 認證的 WAF 能保護您的網站或應用程式免於應用層的入侵攻擊。結合 Imperva 領先業界的 WAF 技術與經驗，Incapsula 以雲端為基礎的 WAF 能抵禦包含OWASP 十大威脅等各種網路攻擊及弱點，同時並能依企業組織的安全政策在 WAF 中設定客製化的安全規則。

透明緩解（Transparent Mitigation）

Incapsula 以低於0.01%的誤報率提供透明緩解服務，且不影響正常用戶使用，讓您享有真正的DDoS防護。即使遭遇長時間的攻擊，也不會造成業務中斷。

自動檢測、即時觸發與層級攻擊進階緩解

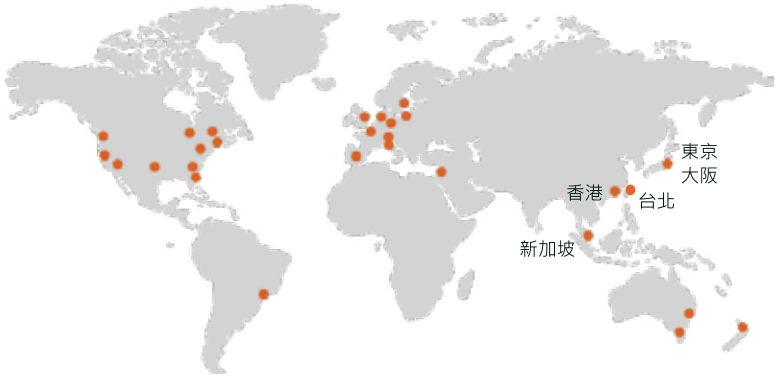
Incapsula 的來源識別技術（visitor identification technology）能區分網站正常來源（訪客、搜尋引擎等）和自動、惡意來源，並能區分人與Bot的流量、“好”與“壞”Bot的不同，辨別AJAX和API。

BGP 路由基礎設施防護

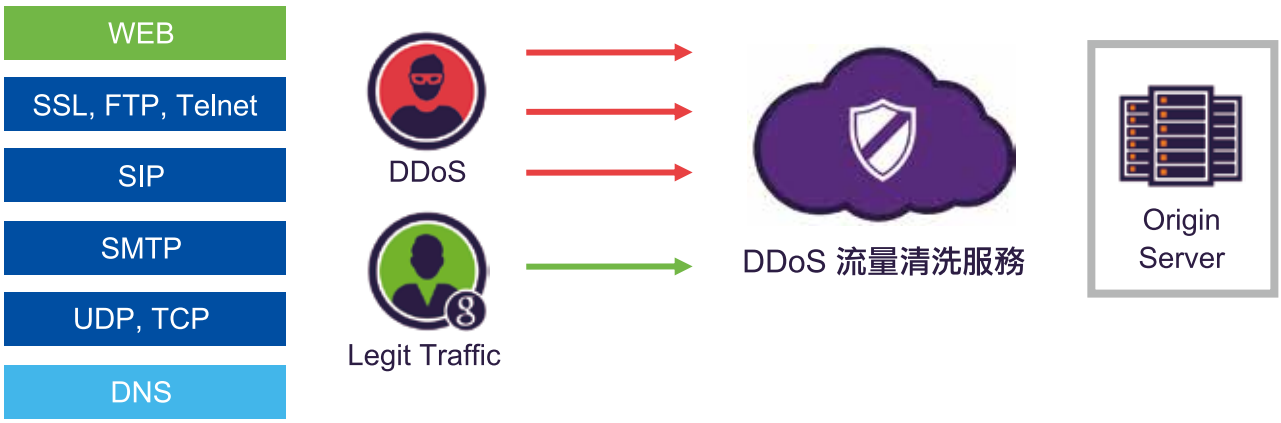
為保護整個 IP subnet 裡的關鍵基礎架構（如Web、電子郵件、FTP伺服器），Incapsula 提供基於BGP路由的DDoS客製化防護。遭受攻擊時，流量將透過具有BGP公告訊息的 Incapsula 清洗中心重新傳輸，完成檢查後，正常的流量便會透過GRE通道安全地傳到企業網路。

DDoS 和資安專家提供的全球支援

Incapsula經驗豐富的網路維運中心（NOC）工程師團隊會持續進行監控和DDoS緩解。這項服務包含主動安全事件管理與回應、不間斷的實時監控、策略調整、攻擊報告摘要和24x7的技術支援。



可保護的伺服器類型



imperva

Imperva Attack Analytics
雲端AI告警分析系統

在眾多告警事件裡找出真正的威脅

資安團隊現今所需面臨的挑戰包括：

- 資安系統每天都會發送數以萬計的告警。
- 單靠人力難以分析所有的告警事件。
- 無法在眾多告警事件中，即時辨別真正的威脅。
- 缺乏對所有應用程式攻擊提供單一、具整合性的分析介面。

由於持續發生資料外洩、複雜的威脅與超量的告警事件，資安分析變得越來越繁瑣、複雜。隨著企業逐步將應用程式移轉到雲端，無論是在內部、雲端、或是混合式環境，保護應用程式都變得越來越複雜。

IT 團隊需要適當的資訊與分析能力才能明確回應並解決資安事件。針對系統提供的大量資料，使用AI人工智慧及機器學習，是辨別即刻威脅的唯一方式。

Imperva Attack Analytics 雲端AI告警分析系統將成千上萬的告警事件相互串聯，並縮減至幾個簡要的說明。Attack Analytics 採用AI人工智慧及機器學習，讓應用程式的資安事件分析變得簡單，同時也讓 IT 團隊能針對真正的資安威脅採取快速且正確的因應措施。系統會將告警事件依屬性及嚴重程度分門別類，以便透過機器學習技術進行快速調查。強大的深入分析功能讓資安團隊能針對鎖定的攻擊事件進行重點分析。

Attack Analytics 是 Imperva 應用程式防護解決方案之一，整合 Imperva WAF 及 Incapsula 網路應用程式防火牆(WAF)所提供的告警事件訊息，系統從實體、虛擬和雲端部署設備中收集資料，並透過AI人工智慧加以分析，提供企業在應用程式防護上的所需的統一監控及統整分析。

Attack Analytics 將成千上萬的告警事件縮減至幾個簡要的說明。

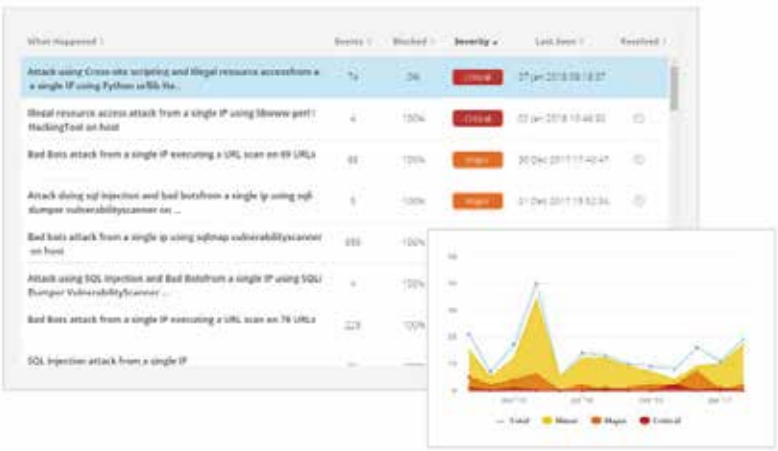
將資安告警去蕪存菁

提升營運效率

Attack Analytics 將大量 WAF 告警縮減至幾個簡要說明，藉此降低資安事件分析所需的時間。在事件處理量大幅降低的情況下，資安團隊的營運效益也因而獲得顯著提升

降低風險

Attack Analytics 將告警事件分類並排定優先順序，進而降低資安事件調查分析的複雜性。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。AI人工智慧的導入，能降低隱藏在大量告警事件下的威脅風險。



單一、具整合性的 WAF 告警分析介面

單一控管介面

當企業開始部署雲端資安項目以保護雲端應用程式及API，監控企業整體的資安事件也變得更加困難。Attack Analytics 提供單一介面，控管所有 Imperva 雲端及內部網路應用程式防火牆所產生的告警事件，進而提供完整可視性，協助企業控管內外部資安攻擊。

全球性的洞察分析

Attack Analytics 運用AI人工智慧，彙集在全球所蒐集到的事件資料，並加以分析、辨別各種攻擊型態。這些資訊在判斷駭客是採取常見攻擊或新的手法上，具有相當大的價值。Attack Analytics 所提供的彙整性智能分析將能幫助企業快速辨別各種攻擊。

適用雲端環境

Attack Analytics 是雲端防護解決方案，因此可一鍵部署，沒有規模限制，並能依企業需求設定告警事件的接收處理數量。

Imperva 應用程式防護解決方案

Imperva應用程式防護解決方案採用靈活的混合模式，將雲端服務結合虛擬、實體設備，進而提供應用程式防護和DDoS防禦。

Imperva提供可在企業內部或雲端部署的實體即虛擬設備；而Incapsula則提供各種雲端防護服務。

imperva

Imperva SecureSphere 資料庫稽核系統(DAM) 資料庫安控防火牆(DBF)

- 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

- 持續稽核與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記錄，包含：「何人、何時、何處和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以及SQL錯誤和資料庫登錄活動。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(DLC)命令、資料操作語言(DML)命令和SELECT。
- 防止篡改的稽核記錄：監控詳細的稽核資料，將其儲存在一個安全的外部硬體儲存設備中，可透過唯讀的方式來存取。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。未授權的更改、欺騙性活動以及資料庫攻擊可以在到達受保護系統之前就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：提供包括透通的網路監視、輕巧的Agent監視、自身稽核收集或混合模式。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，以滿足客戶特有的拓撲和需求。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. 使用內建和客製報表來衡量控制的有效性。
  12項 PCI-DSS 要求中總共有7項可由Imperva DAM來完成。
- Imperva 使企業能夠保持獨立稽核線索，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(SOX)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瞭解資料庫伺服器間的資料。基於資料庫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弱點評估和最佳做法，這有助於企業糾正和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(ADC)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(Dynamic-Profiling) 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(Dynamic-Profiling) 技術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錯誤和資料庫登陸活動。

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、協定層及SQL層的資料庫攻擊。透過詳細的行為更改稽核可以準確的針對欺騙性活動、資料庫修改以及攻擊進行告警 - 發送即時告警、分配後續任務以及確保變更的控制。

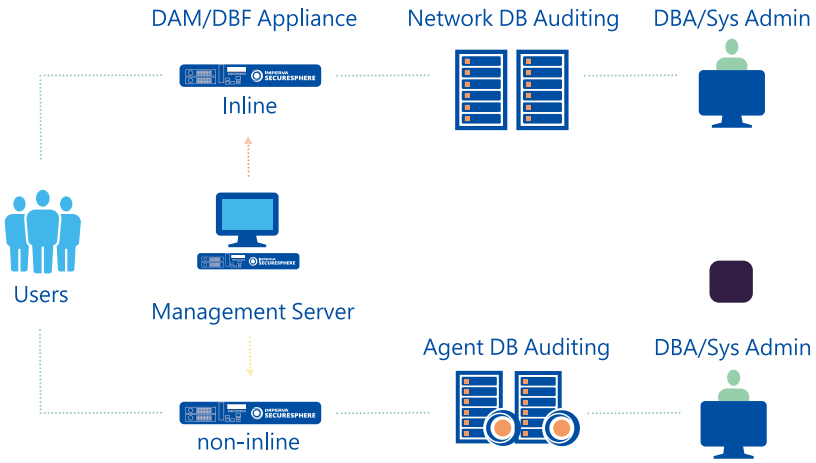
原始資料保存與回復

資料庫稽核軌跡原始資料(Raw Data)，可以加密、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、Monunt Ponint 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資訊，通過互動式稽核分析可以全面瞭解所稽核的活動，這可使不瞭解技術的資料庫稽核人員只需點幾下滑鼠即可從幾乎所有角度分析、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

靈活的部屬模式：網路、Agent、內建稽核或混合模式

Imperva 提供最簡易的部屬選項，包括透通的網路監視、輕巧的 Agent 監視、自身稽核收集或混合模式。這種非侵入性的體系結構使企業能夠以任意方式混合部屬，以滿足客戶特有的拓撲和需求。

Agent 代理程式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備的稽核功能，可以很容易地支援任何環境，從中小企業到大型企業，這是其他資料庫防火牆解決方按無法與之相比的。

Imperva 可部署在inline或non-inline網路監控環境，同時控管特權及應用程式使用者帳戶的資料庫行為

imperva

Imperva CounterBreach
資料庫AI智能防護

員工需要存取資訊資產才能執行工作，但惡意或出於無知而濫用權限的存取是難以發現且具高風險的。

GARTNER, BEST PRACTICES FOR MANAGING 'INSIDER' SECURITY THREATS, ANDREW WALLS, 17 JUNE, 2014

保護企業資料，免於內部威脅

對企業而言，最大的資安威脅其實是內部人員。出於工作需求，員工、外包廠商、顧問和供應商必須具備存取企業資料庫和共享檔案內機敏資料的權限。
然而，當內部人員濫用這些存取權限，或是內部人員被外部駭客利用時，就可能造成企業資料外洩。要能準確辨別並遏制內部威脅，需要對使用者行為深入分析，包括使用者存取的資料和存取的方式。

Imperva CounterBreach 資料庫AI智能防護

Imperva CounterBreach 能保護儲存在資料庫和共享檔案中的企業資料，避免被惡意、粗心大意和帳號被盜用的使用者竊取或濫用。透過動態學習使用者正常存取資料的模式，CounterBreach 能偵測不當的資料存取行為與相關使用者，藉此發現潛在的資料外洩事件，並主動向 IT 團隊進行危險行為告警。

找出不當的使用者存取行為

CounterBreach 透過機器學習及動態群體分析，自動找出異常的資料存取事件。這個過程可建立一般使用者存取資料庫和共享檔案的完整行為模式基準，進而檢測並設定異常活動的告警優先順序。
結合對使用者的專業分析和存取資料的方式，為企業提供找出資料外洩事件所需的資訊和準確性。透過 CounterBreach，資安團隊可以快速辨別惡意和正常的資料存取事件，並能立即依不同的風險行為採取有效的行動。

CounterBreach 主要特點

偵測關鍵資料的誤用

行為分析偵測到的事件將顯示在 CounterBreach 易於操作的儀表板上。CounterBreach 彙整最具風險的使用者、用戶端主機(Client host)和伺服器，以便IT人員能針對最嚴重的資料存取事件進行優先排序，並讓資安人員可以深入了解各個事件並查看相關細節資訊。

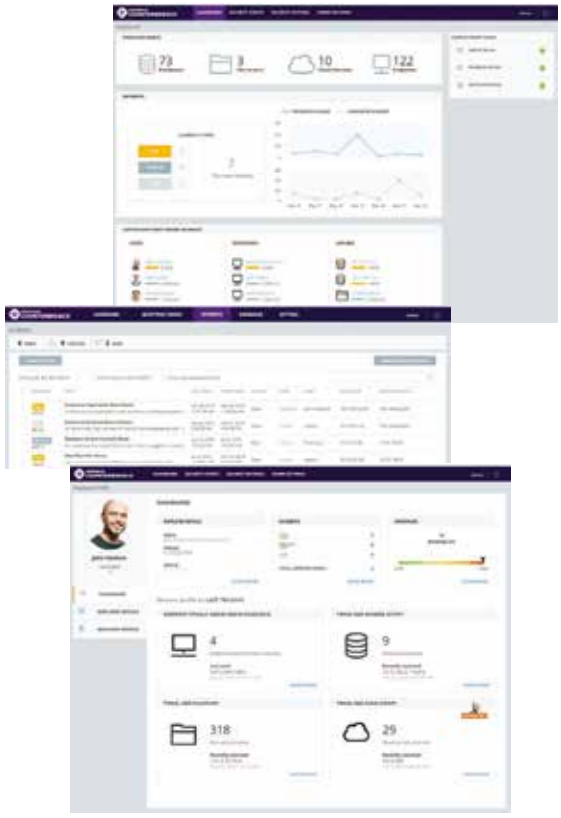
加快事件應變速度

資安團隊可以依嚴重程度、特定使用者、伺服器或用戶端主機作為過濾條件，有效調查不當的資料存取行為，藉此深入了解特定事件，查看相關使用者和被存取資料的細節資訊。而 SOC 人員可以接著關閉被授權或不能立即修復的事件或白名單行為。

簡化調查流程

資安團隊可以透過使用者儀表板分析特定使用者的資料存取行為，並以同一介面查看事件內容，藉此獲得整個組織內的使用者資料存取全貌。

同時資安團隊也可深入調查特定使用者的相關事件和異常行為，並與該使用者所處群體內的一般使用者行為基準進行對等比較。



- CounterBreach 儀表板匯集了所有企業資料內的威脅指標
- CounterBreach 事件分析介面將所有異常存取事件依嚴重性排序
- CounterBreach 使用者分析介面提供存取企業資料的使用者一覽表，並標示具風險的使用者行為

系統需求

CounterBreach 必備條件

CounterBreach 需結合下列 Imperva 稽核安控產品之一：資料庫稽核(DAM)、資料庫安控防火牆(DBF)。

CounterBreach 虛擬版本

CounterBreach易於部署為虛擬設備，且不會影響既有的系統運作。每個硬體主機(host)及虛擬系統(guest)所需的最小系統要求如下表所示。

	硬體主機(Host)		虛擬系統(Guest)				
	Hypervisor	Processor	CPU	Memory	Disk Space	Operating System	File System
CounterBreach Admin Server	Dual-core server Intel VTx or AMD-V	VMWare ESX/ESXi 5.X/6.X	2	4 GB	50 GB		
CounterBreach Analytics Server			4	16 GB	1 TB		

[1] CounterBreach 管理主機 (Admin Server) 用於行為分析 (Behavior Analytics)，Imperva 將在上述規格環境下，以軟體方式安裝在預先設定好的虛擬設備上。

支援平台

CounterBreach 資料庫AI智能防護	
Database Platforms	Oracle, Microsoft SQL Server, DB2 for LUW, Sybase ASE
File Systems	CIFS file storage systems, NAS devisces
File Operating Systems	Microsoft Windows Server
SIEM Integration	Splunk, ArcSight
Supported Syslog Formats	CEF, LEEF, Raw

APV Application Delivery Controller

應用服務傳遞控制器

APV 系列應用服務傳遞控制器，可使用於雲端服務與企業級的產品。在可用性，運行效能，以及安全性上，提供適合的解決方案，同時大幅降低資料中心的維運成本與複雜度。

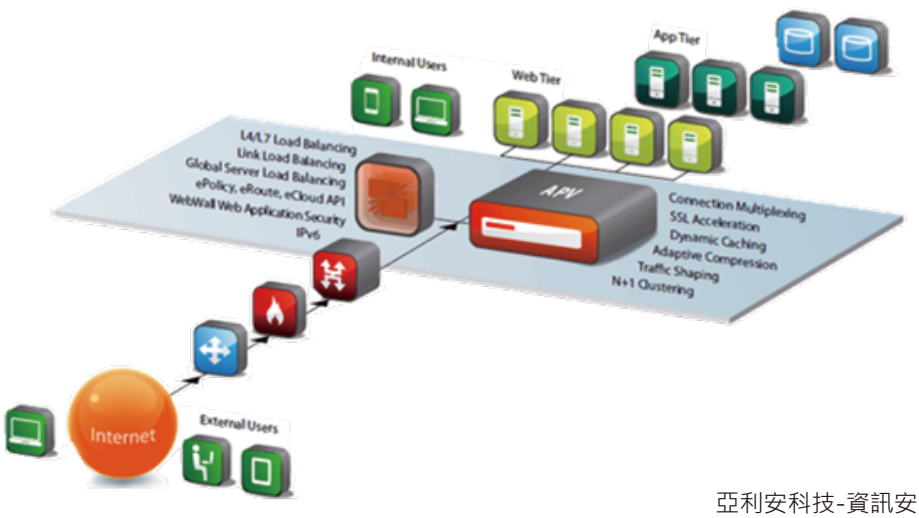
提供伺服器負載平衡；透過多種分流演算法讓企業伺服器的擴充更彈性。運行中檢查伺服器運行或效能狀況，適當分配流量或故障轉移，確保服務不中斷與優化品質。可選擇由第 2,3,4 及 7 層的協議(包括 WebSocket, WebSocket Secure)執行負載平衡。

提供 SSL/TLS 加速與卸載的功能；可選購硬體加速器提升更高的連線速度與數量，將網頁解密後的資料傳送給網站伺服器降低伺服器原先需要花費的加解密運算效能。或將解密後的資料先提供給資安設備(如:應用程式防火牆)檢查與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，選購硬體加速器讓系統提供更好的性能與容量。
SSL 攔截(SSL Intercept)；現今大部分網路流量是 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，從而繞過這些資安設備。APV 的 SSL攔截可解密 SSL 流量，提供給資安設備檢查。然後重新加密轉發給目的地端。

提供線路負載平衡與全域伺服器負載平衡(GSLB)；確保廣域網路(WAN)維運正常與負載均衡。線路負載平衡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。全域伺服器負載平衡在地理位置分散的應用服務，根據鄰近性，語言，容量，負載和反應時間在各站點之間智能分配服務，以實現最佳性能和可用性。

提供 DDoS 防護；APV 具有 L4 及 L7 的 DDoS 防護，如 SYN-Flood、tear drop、ping-of-death、Nimda、Smurf...等。APV 亦透過機器學習方式，檢測異常行為、設定的門檻值、存取控制、網路地址轉換急狀態封包檢測等，來防止攻擊及未經授權的訪問。

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。
提供 CLI 命令介面管理系統外，也提供網頁圖型化介面管理。也可透過 XML-RPC 或 RESTful API ，讓管理更簡單有效。
除了提供多種硬體型號方便採購的選擇，亦提供虛擬版軟體，安裝在您的環境或雲端中一樣是您最好的選擇。



AVX Network Functions Platform
網路功能虛擬化專屬平台

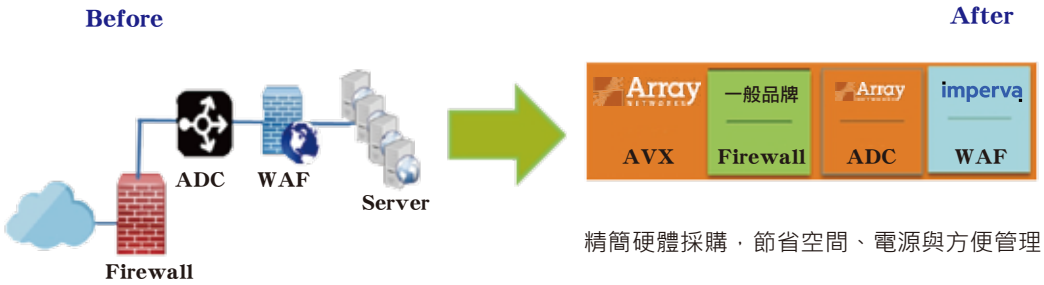
AVX 系列網路功能虛擬化專屬平台(NFP)是專門為服務供應商和企業客戶設計，方便於資料中心整合，但也適用在雲端或虛擬化的靈活性或專用虛擬設備的效能；AVX 擁有分配給每一個虛擬功能和設備(VNFs/VAs) 的專屬的 CPU、SSL 硬體加速、記憶體和網路介面資源的獨特能力，是目前市場上少數「能夠在共享的環境裡面提供虛擬網路功能和虛擬設備(VNFs/VAs) 效能保證」的解決方案。針對網路 I/O 密集型或 CPU 運算密集型處理的網路產品提供虛擬化的最佳平台選擇。

每一個虛擬設備都可配置專屬的 CPU、SSL 硬體加速、記憶體和網路介面資源；具有虛擬設備敏捷的配置需求，又具有專用的性能，消除虛擬化後共用資源的不穩定性。每一個虛擬設備完全獨立，可符合相關法規和高安全性環境的分離要求。透過不同型號，最多可達 32 個 專屬 VA；減少設備採購數量與使用空間，降低數據中心建置與管理成本。

-獨特的結合硬體與軟體架構，利用 SR-IOV、DPDK、NUMA boundary 及 CPU pinning 等優化技術來保證性能與擴充需求。
-提供多種 VA image 格式；如: raw、qcow2、vmdk、tgz(壓縮的 raw 或 qcow2)及 ani(Array 壓縮的 raw 或 qcow2) 等檔案格式。
-平台可以加購 自主開發的 ADC 或 SSL VPN 授權；既可以減少硬體的採購，也降低購買的成本。
-提供不同的硬體型號，方便選擇適合現在與未來擴充需求。
-網路介面提供 1Gb、10Gb 或 40Gb 做選擇或增購，滿足不同介面或埠數的需求。
-提供 CLI 命令介面管理系統外，也提供網頁圖型化介面管理。也可透過 RESTful API ，讓管理更簡單有效。

提供不同的硬體型號與網路介面增購選擇

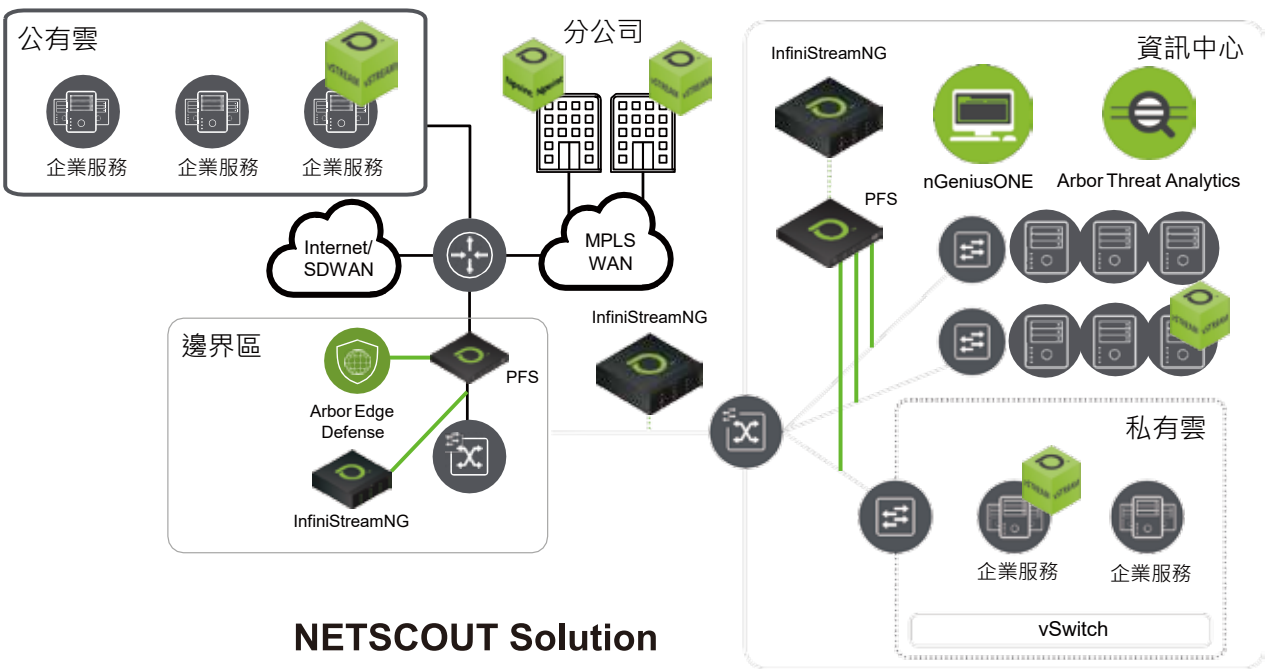
提供自有的虛擬設備授權，亦可安裝其他品牌或開放平台所提供的虛擬化設備



精簡硬體採購，節省空間、電源與方便管理

NETSCOUT

NETSCOUT 為應用程式與網路效能管理解決方案的市場領導者，能讓企業與服務供應商確保客戶的使用體驗與品質。
NETSCOUT 科技能使組織有效率的管理重要服務以及主動找出突發的效能問題，並快速找到導致企業營運中斷或造成使用者負面衝擊的資訊。
NETSCOUT 將原先收集的資訊進一步提供在資訊安全的分析，讓資訊管理更加完備。



NETSCOUT 如何幫助客戶控制應用程序性能?

控制應用程序性能並更快地解決服務交付問題變得前所未有的重要。
為了實現這一點，取決於對IT基礎架構中所有位置的持續監視。 NETSCOUT通過數據中心轉換解決方案實現了這一目標。
一些主要好處包括：

- 以更快的速度和敏捷性開發新的和重構的現有應用程序。
- 通過改善網絡和服務的可用性，可靠性和響應性來提高最終用戶和客戶的生產力。
- NetOps，SecOps和其他IT團隊之間更好的協作，減少了MTTR（平均修復時間）並進行了根本原因分析。

nGeniusONE 網路與應用程式服務保障管理平台

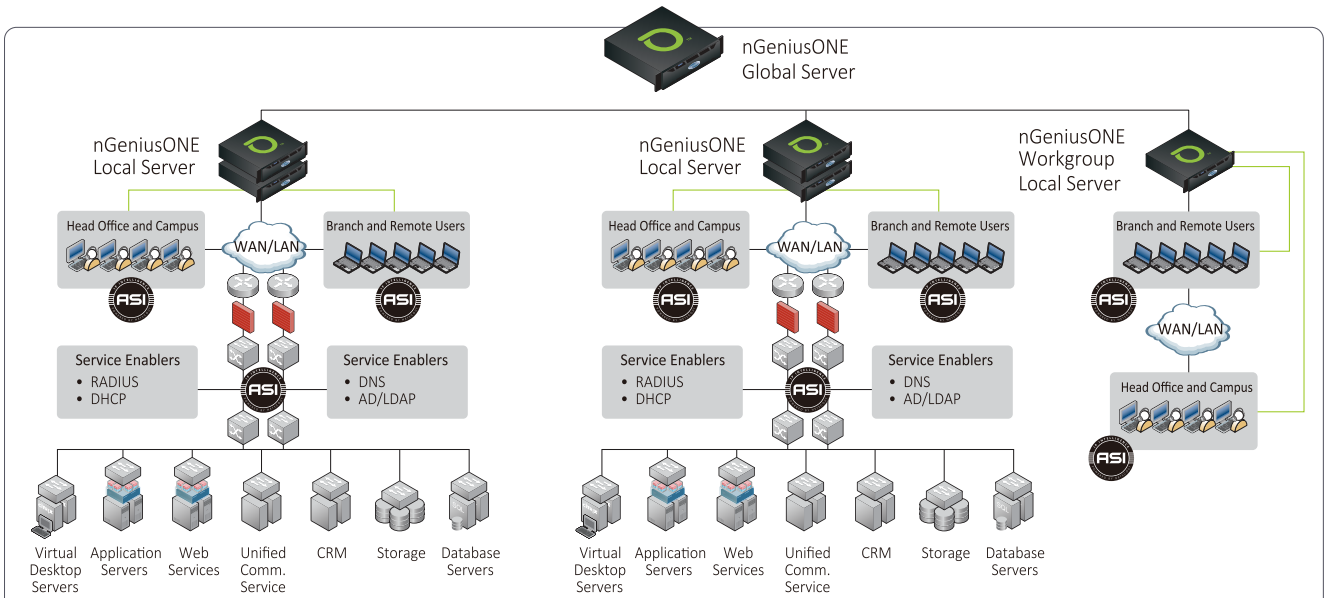
- 集中管理應用與網路效能解決方案，圖形化介面，操作簡單。
- 所有功能都透過瀏覽器來操作，可以達到任何時間、任何地點的監控需求。
- 支持包括 NetFlow/sFlow/NetStream/cFlow、SNMP MIBII、RMON II 等多種網路管理數據，以及網路數據封包截取。
- 獲得對網路流量的可讀性，包括聯網的應用系統、網路上任何伺服器、路由器、和交換器的流量信息、以及各內網和廣域網路的物理和邏輯通道的流量情況。
- 直覺式分析服務效能，由儀表板、服務和流量監視器、會話分析到封包分析。
- 獲得導致流量異常的原因，例如哪個協議、哪個IP用戶、哪個對話。
- 監控應用與伺服器的服務基準，能夠主動預警問題的徵兆提醒用戶注意。
- 威脅分析提供對可能的流量和應用程序 DDoS 的可見性攻擊。
- 直觀的即時圖表與封包解碼，可自動產生歷史流量報告，迅速解決問題的同時又能定時獲得報告。
- 可隨時產生報表，並列印、e-mail 發送和儲存監控結果，且報告可長期儲存。
- 集中管理架構，且管理設備種類眾多，可充分協助網路管理員作預防性網路效能管理。

特色

nGeniusONE 為 Top-Down 工作流程，透過高可視化儀表板呈現所有服務及網路與應用程式元件，提供即時、全面且一目了然的檢視，儀表板也能提供告警或經智慧分析的早期預警，讓網管部門主動預先維護服務的可用性與效能。

透過 Adaptive Session Intelligence 的深度封包解析技術，可解析出應用程式與網路的關鍵性能指標值(KxI)，如應用程式效能、新增及常用用戶數統計、應用請求及應用錯誤代碼統計。網路性能KxI如服務交付延遲統計、鏈路利用率與流量細節、QoS級別、應用服務使用率等。並可將網路 / 應用程式流量轉換成易於檢視的圖形統計介面，以便於IT/NT部門迅速處理突發的效能問題。

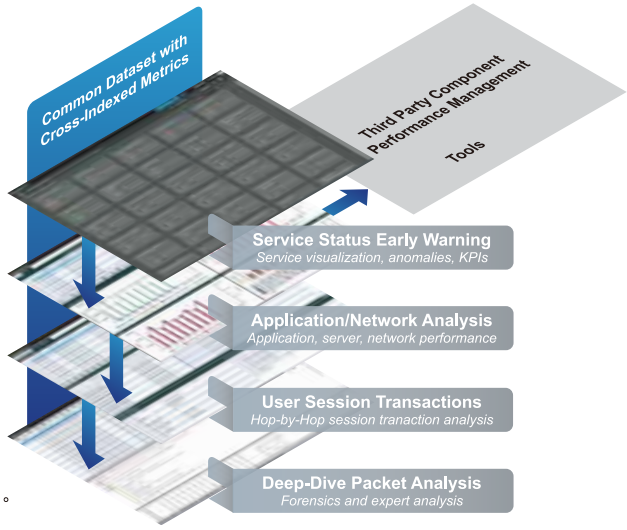
nGeniusONE 具備豐富的應用程式識別能力，包括市面一線的套裝應用程式、Web- based 及客製化應用程式，提供超過 2,000 種標準解碼協定識別能力，可預先定義每種服務的階層架構，包括伺服器 IP、應用程式、資料庫、DNS、認證機制等相關元素，都能被關聯串起。管理者可透過逐層鑽取，找出影響效能的問題。以服務為焦點的報表功能，能提供排程利用各種範本報表產出自己需要的報表，如服務效能分析等，或隨需求直接將 nGeniusONE Service Dashboard、Service Monitors或 Traffic Monitor 資訊轉成報表以供檢視。



Scalability of nGeniusONE Service Assurance platform

快速分類解決複雜的問題

結合 NETSCOUT 專利 ASI 技術 (Adaptive Service Intelligence)，nGeniusONE 平台提供整體性的服務性能可視圖形介面，支援複雜的多層、多供應商、多機房業務、數據應用服務及影音通信。精心設計的工作流程方便查找問題，減少平均修復時間。nGeniusONE 針對服務所設計的工作流程可實現上下切換、跨越多層的分析。



- **服務儀表板**
  提供網路狀態、告警和智能預警、應用程式和網路服務效能分析，讓 IT 人員可以專注於問題的分類查找。
- **數據封包分析**
  開啟數據封包分析，針對協議進行分析與證據資料收集。
- **內置報告模組**
  多種報表範本，可依需求每天、每周和每月自動產出報表。
- **服務監視**
  整體分析關鍵服務伺服器，提供圖形及數字統計資料。
  如延遲回應、連線故障、流量分析及錯誤代碼等，以確定影響服務性能問題的根本原因。
- **服務依賴關係**
  可自動分析網路資料，將當前的服務、應用環境和客戶端的關係以圖形化階層顯示。
- **會話分析**
  提供會話層分析回應圖，點對點的應用程序以有效識別具體問題。
- **威脅分析**
  分析收集資料中具有巨量攻擊、狀態耗盡攻擊及應用層攻擊的流量，提供統計分析數據。

系統架構

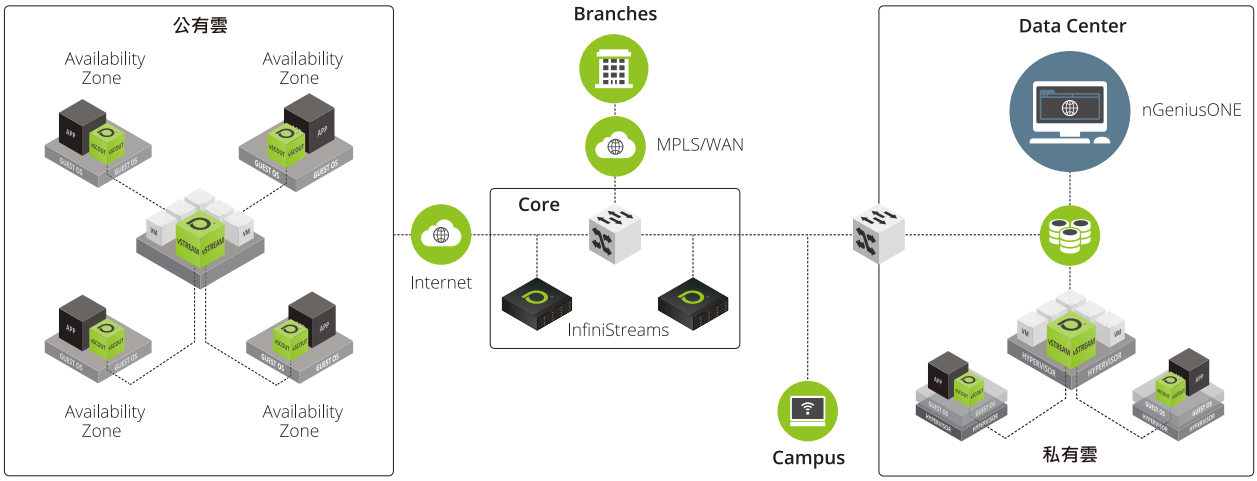
1. PFS 智慧監測交換機
   PFS交換機是接收原始資料流、預處理和智慧分發的設備。主要優化監測架構、拓展監測點，具備網路接入、多網路聚合、資料多路複製、智慧過濾和埠標籤等作用。
2. Infinistream 分析探測器
   Infinistream設備即時接收並儲存原始網路封包，提供網路流量和應用效能統計分析功能，而應用、VoIP 和網路效能等統計資料都會發送到 nGenius ONE伺服器，並在nGeniusONE伺服器集中儲存、展開和分析。
3. nGeniusONE 管理伺服器
   nGeniusONE 是核心管理系統，收集 Infinistream 或vASI虛擬探測器接收到的資訊及網路流量資訊。nGeniusONE 也可經由Flow collector收集、分析網路設備的Netflow資訊，提供整合性與相互關聯的網路效能管理分析。

nGeniusONE提供各種服務角度的儀表板視窗，由使用者自定義服務單元觀察，透過整合的服務儀表板視窗，實現從上到下的業務性能監控。從檢測網路/應用KPI參數到會話分析、數據封包解析，並提供服務單元組成的拓樸結構和視窗。

nGeniusONE解決方案為軟體結合的產品，其核心功能包括OSI網路管理五大功能中的三大功能-性能、故障、安全，含括OSI網路七層的全方面分析。結合多年累積的技術，能夠識別網路超過1000種協定，以直觀易懂的圖形和表格來監測網路運行過程中的各種異常徵兆和故障，即時發出示警並提供專業建議以快速解決問題，在網路和應用問題上可進行深入徹底的故障診斷。

vSTREAM 混合雲應用分析探測器

適用於數據中心和混合雲環境，提供應用服務效能和網路服務保障的可見性。



企業組織以往依賴傳統數據中心的功能，在導入多種雲服務後，便能更快速、有效地組建企業的服務。但是，這些關鍵應用程式運行在雲端新架構上，卻也增加了問題發生時的複雜性和風險：

- **架構的複雜性**
  混合型雲和基礎設施服務（IaaS）在服務時帶來一些挑戰，提供適合於企業的不同平台及公共雲和跨多個供應商技術和地點的解決方案。
- **不同的分析工具導致混亂**
  效能管理和整個解決方案採用不同工具分析容易造成混亂，且耗費更多的分析時間。
- **可見性約束**
  基於數據封包能見度變得越來越重要，能提供適當的解決方案成為更具挑戰性。 屬於企業資料中心的數據、公眾和混合雲環境如何因應環境的限制而能達到一樣的需求。
  因應現今更靈活的環境變化，持續提供應用服務效能的可見性。NETSCOUT 以專利 Adaptive Service Intelligence™（ASI）技術開發的 vSTREAM 來符合現今運用於私人、公眾及混合雲的環境需求。

vSTREAM-EMB

vSTREAM-EMB 為監控虛擬或物理網路提供了直接以軟體方式安裝於伺服器中：

- 運行於客戶作業系統中的執行程式。
- 可部署在 AWS Linux，Windows Server，RHEL/CentOS/Ubuntu 等系統中。
- 與應用程式一起常駐於虛擬機或容器，監控應用程式和服務。

vSTREAM-STL/vSTREAM-NSX

vSTREAM 為私有雲和公有雲提供如同 InfiniStream NG 的可見性分析，提供 ASI 流量分析技術的完整虛擬機。

- 私有雲：安裝為一個虛擬機，支持 VMware 和 Ubuntu/KVM 環境。
- 公共雲：作為 Amazon Web Services 和 Microsoft Azure 中進行部署。

nGeniusPULSE 主動式網路效能管理系統

使用在 Web, SaaS 應用程式和 VoIP 服務, 提供主動式測試和監控可用性及效能的管理。

- 主動式測試和監控 web, VoIP 或一般應用的可用性
- 可定時或手動即時測試
- 測試 HTTP/HTTPS Web 應用可用性和效能
- 測試 VoIP 服務可用性和通話品質
- 可使用 IP ping 或 TCP ping 測試可用性和效能
- 可客制化 Script 測試應用程序
- 方便部署在各種 OS 平台做為測試節點
- 除軟體測試節點程式，亦提供硬體式測試元件
- 收集伺服器與網路元件的 syslog、分析事件
- 收集網路元件的 SNMP 效能資訊
- 透過伺服器的 SNMP 或 WinRM 收集主機效能
- 提供 appliance 管理主機，亦可部署在虛擬服務器上
- 可結合 nGeniusONE，讓效能管理更全面

產品簡介

nGeniusPULSE 是一種可高度擴展、“主動式”的監測及效能解決方案。7 x 24 小時隨時主動測試，自動和定時模擬真實用戶操作。提供測試結果至管理系統上，以便主動發現效能品質或系統中斷告警原因。

nGeniusPULSE 測試節點稱為“nPoint”，可放在任何網路運作設備上自動或手動測試，並發送結果至nGenius-PULSE管理服務器。管理服務器具備易於使用的配置和管理功能，儀表板介面直觀，可監控伺服器、網路介面、路由器和交換機，向下分析各節點測試結果或各應用程式經由節點測試的細部效能訊息與告警。同時能查看統計訊息，如CPU利用率、記憶體、硬碟使用情況、I / O和接收的 syslog 訊息等。

nGeniusPULSE 能精確定位影響業務服務及其用戶基礎架構問題的確切訊息，配合 nGeniusONE 的深入查找，可以很容易地查明問題位置，並分配適當的資源來解決問題。

nPoint 部署提供從任何地方監視的靈活性

nPoint 有硬體和軟體兩個部署選項，以用戶所在位置進行主動測試。每個 nPoint 從其部署的位置測試，可更貼近真實狀況。組織也能依監測要求和環境決定採用軟體或硬體 nPoint。

硬體式 nPoint 是一種可以簡單安裝的微型設備，提供PoE介面（以太網供電），方便擺放在任何地方，並能從該位置執行 7x24 自動監控。常用於分支機構、倉庫、單個樓層、伺服器機櫃或其他遠端位置。nPoint 可在部署用戶沒有存取權限下載到筆記型電腦或服務器的狀態下，執行效能測試服務。

軟體式 nPoint 是一個小型的代理程式（約12MB），可下載到 Windows 或 Linux 機器。透過電子郵件發送給用戶安裝後(或由管理系統下載)，即可由中央管理系統手動測試或設定自動測試方式，執行自動監控作業。

URL 監測

nGeniusPULSE 可以監控任何 URL 效能及可用性，設定 URL 網址後 (亦支援登入程序) 便可指定測試結果 (例如指定 HTTP 回復 200 OK)、測試頻率及告警基準值。

nGeniusPULSE 可針對 HTTP/HTTPS 衡量應用程式的效能，包括 DNS、網路、服務器、客戶端、SSL 及應用程式時延分布，並統計服務的平均回應時間。

ATA Arbor Threat Analytics 威脅分析管理系統

提供企業的網絡威脅和風險調查解決方案，可幫助減少網絡威脅對業務的影響。

產品簡介

NETSCOUT 透過可擴充的封包檢測技術開發出來的 InfiniStreamNG 硬體式設備或安裝於虛擬系統的 vSTRREAM，對數據封包進行連續，實時的監控。借助 ASI 專利技術，可以檢測到威脅，並將其數據封包和會話層證據詳細取證分析，以完成安全事件分類和調查。

ATA 具有迅速有效地檢測，調查，驗證和回應威脅的能力，可作為威脅事件的預警系統。並具有豐富的數據分析資源，可減少網路威脅潛伏在企業的時間，從而減少危害公司資源和聲譽的風險。

Arbor Threat Analytics 提供企業級的網路監測和可視化，發現可能造成或導致網路和應用服務中斷的安全威脅、異常和合規性問題，其中包括：

- 內部的威脅造成流量或應用層的狀態耗盡和/或其他進一步的攻擊構成的威脅可以做為調查的一部分。
- 錯誤使用（或不安全使用）標準網路協議，例如 DNS 不當查詢，URL，外部IP錯誤或使用檔案傳輸協議（例如 SMB，CIFS 和 NFS）的攻擊。
- 使用較差或較弱的密碼（例如SSL / TLS或IPSEC）和/或憑證到期有關的問題。
- 異常行為、可疑活動和網絡上發生的應用層攻擊。

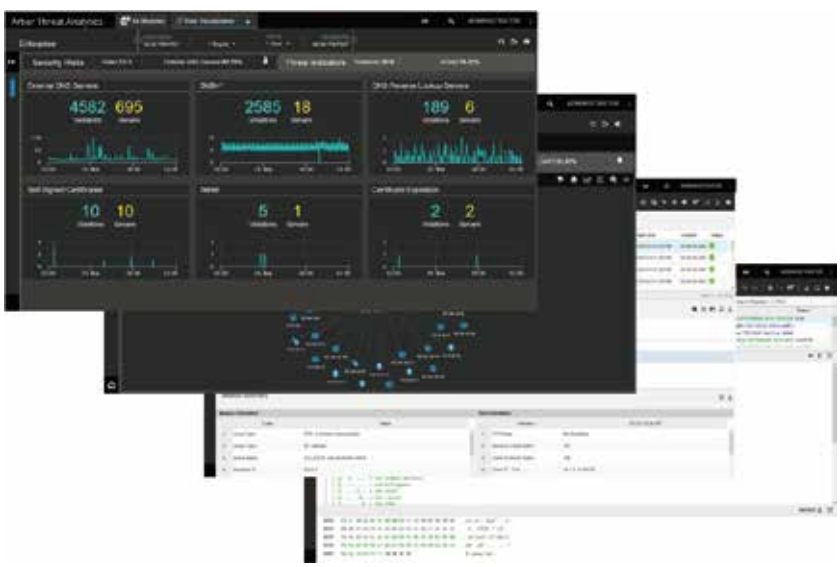
所以 ATA 提供以下關鍵分析與功能:

風險可視化 – 提供可視化儀表板，以及有關高風險威脅的詳細信息，包括協議和憑證安全性風險，可由此畫面透過分析會話和數據封包分析及取證證據。

網路調查 – 從“風險可視化”可向下分析網路中的活動，可查看系統效能及排除故障。

主機調查 – 以數據和圖形化提供，可以理解主機之間的拓普圖資訊。可以對懷疑有安全問題的特定主機，進一步深入了解會話和數據封包證據。

整合 SIEM – 與現有的 SecOps 工作流程整合，這些工作流程使用 SIEM 工具實現單一管理方法。 查看 Splunk 或選擇第三方安全工具檢查並蒐索發送到系統日誌上的 SIEM 事件。



風險可視化>>主機調查>>會話分析>>封包證據，透過簡易的操作即可完成事件調查。

AED Arbor Edge Defense 智能威脅防護系統

專為網路應用威脅與 DDoS 攻擊的第一道，也是最後一道防線。

產品簡介

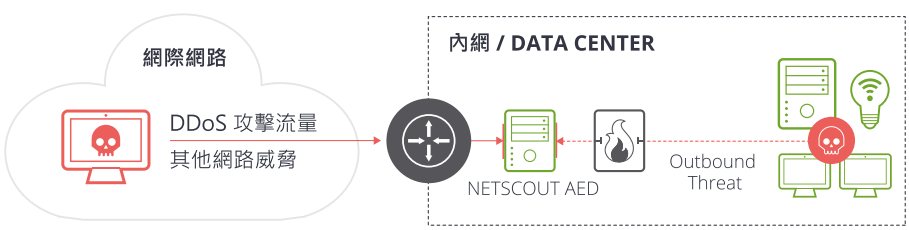
無論是新形態的 DDoS 攻擊，勒索軟體，利用網絡釣魚方式試圖破壞 BYOD 和物聯網設備，企業不斷面臨來自各種先進網路威脅。為了解決這些不斷演變的威脅，加班、將資安防護堆疊得越來越大、越來越複雜。但不幸的是仍然失敗了，數據洩露和停機時間的事件還是時有發生。

安全團隊需要最好的網路安全解決方案，可以檢測並阻擋所有網路威脅的類型 - 對內威脅和對外惡意通訊。同樣重要的是，這些解決方案還必須能夠整合到企業組織的現有安全架構中以降低成本、複雜性和風險。

NETSCOUT AED（Arbor Edge Defense）就是這樣一個解決方案。 AED 在網路邊界（即路由器和防火牆之間）的獨特位置上，其無狀態數據封包處理引擎以及從 NETSCOUT ATLAS 收到自動更新的威脅情資。使其能夠自動檢測和阻擋對內的威脅和來自內部被入侵主機的對外通訊，即是企業網路的第一道也是最後一道防線。

主要特點

- **第一道防線**
  NETSCOUT AED 部署在網路邊界，使用無狀態封包處理引擎技術並配備數百萬個入侵指標，可檢測並阻止對內通訊的網路威脅，從而減輕狀態式設備（如次世代防火牆）的壓力。
- **最後一道防線**
  NETSCOUT AED 可以檢測並阻止對已知不良 IP 地址，網域，URL，地理位置的對外通訊;幫助阻止組織中惡意軟體的對外連線，以避免資訊洩露及惡意軟體進一步擴散。
- **整合威脅情資**
  NETSCOUT AED 可接收 NETSCOUT ATLAS 的全球威脅情資，即時更新入侵指標。
- **最佳的 DDoS 保護**
  NETSCOUT AED 可以自動檢測和阻擋對內應用層，TCP 狀態耗盡和高達 40 Gbps的 DDoS 攻擊。 如果發生更大的 DDoS 攻擊，Cloud Signaling 會自動將流量導到 Arbor Cloud 或 MSSP 的雲端緩解中心。
- **具有客制化開發**
  NETSCOUT AED 支援 RESTful API 開發客制化管理介面，及支持 STIX / TAXII 可以自訂匯入自定威脅情資強化威脅攔截能力。
- **SDN/NFV 整合**
  NETSCOUT AED 可以與 OpenStack，Heat，Tacker，Ansible，Nokia Cloudband，Cisco NSO 以及其他 ONAP 或 ETSI NFV 管理和協作技術整合。
- **支持虛擬和混合雲環境**
  提供實體設備的解決方案外，vAED 是 NETSCOUT AED 設備的虛擬版本。可以在您的私人虛擬伺服器中運行，也提供像 Amazon Web Services 這樣雲環境的保護。



AED 在網路邊界上的獨特位置 + 無狀態封包處理引擎 + ATLAS 全球威脅情資 = 進階網路威脅的第一道和最後一道防線。

Packet Flow Switch & TAPs 網路流量管理

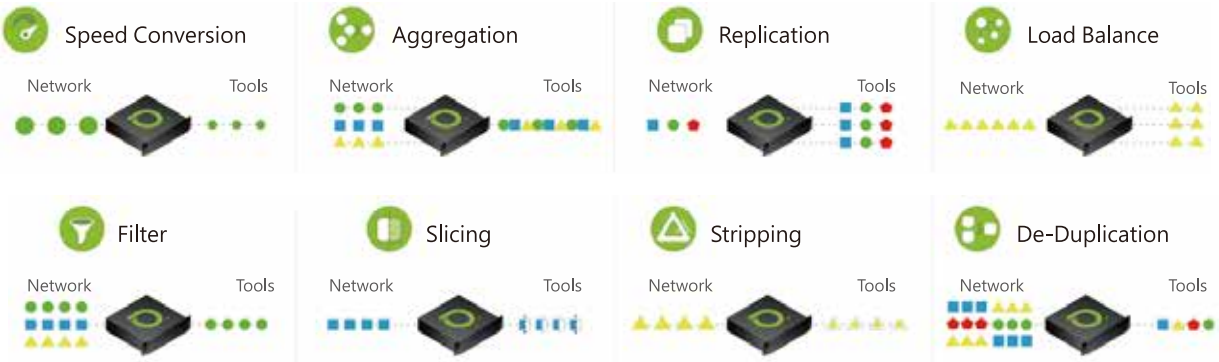
滿足經濟、高效且完整的數據封包可見性應用需求，簡化監控體系結構並降低資訊流量應用安全風險。

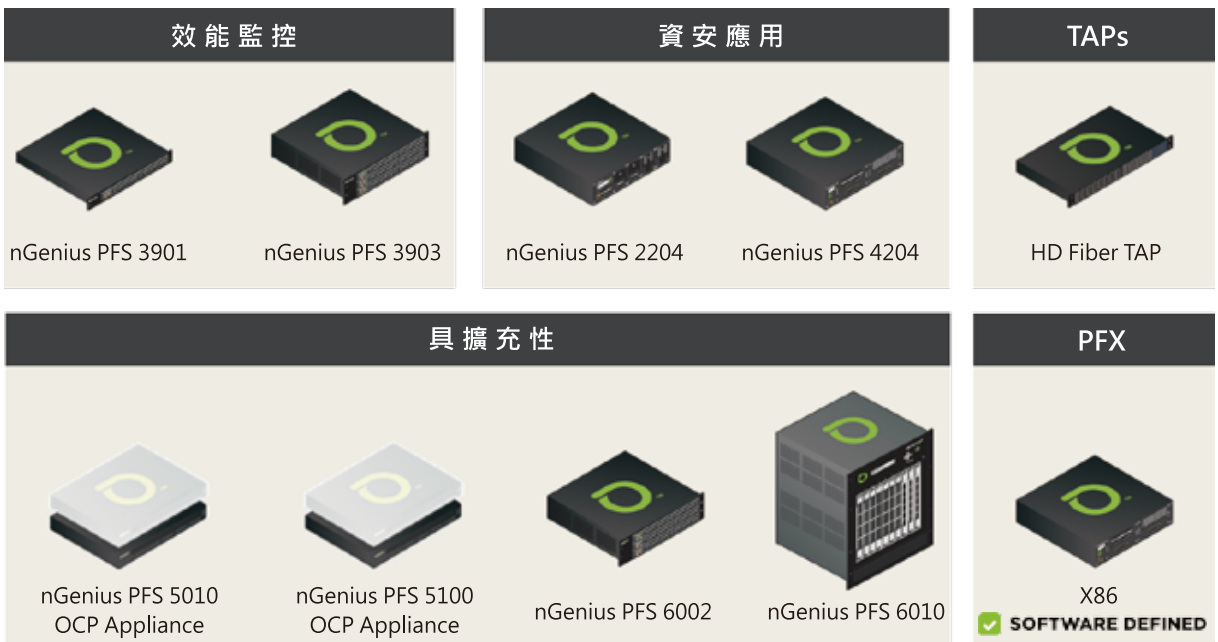
產品簡介

隨著網路應用的普及，無論是效能監控、網路安全分析或資料側錄，NetScout PFS 及 TAPs 都能讓 IT 人員對整個網路的流量進行複製、過濾、聚合、拆分或管理。透過 nGenius PFS 管理平台，NetScout 簡化了流量獲取與分配的程序，滿足效能管理、服務交付管理與安全管理等各種網路流量分析需求。

主要特點

- 可動態配置需要的連接及多元組合
- 可彈性擴展的模組化架構提供設備和預算運用的便利性
- 易於使用的管理平台讓維護更加簡便
- 提供管理系統，可集中管理所有 PFS 設備





PFS 5000 是符合 OCP 建議的設備，提供流量的複製、過濾、聚合及負載平衡，且流量可導到其他控制器做進一步處理。NetScout 亦提供控制器解決方案 PFX，可處理 PFS 5000 或其他品牌設備導引過來的流量。

Jrsys
捷而思股份有限公司

PDFSign 電子合約

PDF Sign 讓您可以隨時隨地，安全快速地登入系統，進行文件上傳或簽署。替您省去郵寄和紙本文件的成本、縮短作業流程時間、減少文件遺失風險，並符合中華民國電子簽章法，更可進一步提供您整合貴公司的流程。

支援通用型HSM 加強簽章憑證的安全防護，完美保護貴公司的電子文件。

產品特色

- **使用全球標準PDF電子簽章**
  - 支援多種國際通用的 PDF Reader
- **支援各種裝置**
  - PC
  - iPhone
  - Android
- **支援多簽章格式及憑證**
  - 電子簽章/時間戳記
  - 手寫/圖檔 簽名
  - 可整合生物辯識
- **具可驗證性**
  - 結合捷而思 PKI QR Code 專利技術，可透過電腦或手機驗證PDF檔或印出的紙本文件之真實性
- **有效保存稽核軌跡**
  - 所有上傳、簽核、通知發送，皆保存在系統紀錄中，且提供查詢機制
- **具RESTful API及SDK**
  - 可支援客製需求
  - 可支援整合現行系統流程

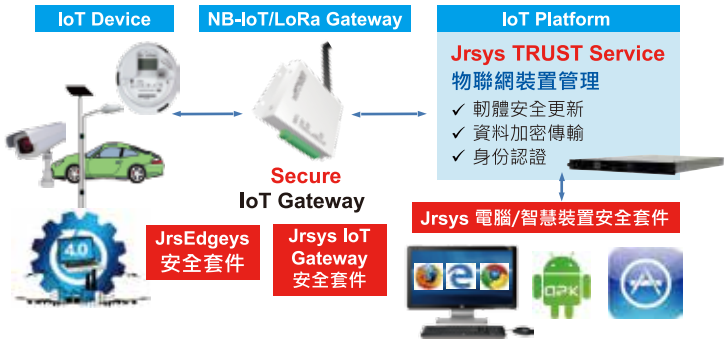
Trusted IoT

Jrsys Trusted IoT 具備輕量、高速、省電及高安全的特性，在不影響設備的使用狀況下，保護您的 IoT 環境，免於成為駭客手中殭屍網路。

Trusted IoT 資安管理平台提供安全白名單管控，可全面管理設備、firmware 、使用人員，同時加密傳輸資料，避免資料遭竊取、竄改、盜用，讓您的資料，只給對的人、對的設備，並在對的服務上流通及使用。

產品特色

- **支援各式 protocol**
  - LoRa, SigFox, NB-IoT (LPWAN)
  - Bluetooth, ZigBee, Wi-Fi
- **支援全應用**
  - 設備 ←→ 雲端主機
  - 設備 ←→ 地端主機
  - 個人 ←→ 主機
- **支援公用 / 私有憑證**
  - 設備效能允可下，可支援客戶自有憑證
  - 可協助建立客戶自有CA
- **有效保存稽核軌跡**
  - 所有設定、簽驗、發送紀錄，皆保存在系統紀錄中，且提供查詢機制
- **具RESTful API及SDK**
  - 可支援客製需求
- **支援 nCipher HSM**
  - 符合FIPS 140-2高安全等級，有效保護貴公司的金鑰安全
  - 1500 tps 的高效能，充分滿足物聯網設備的傳輸需求



Jrsys
捷而思股份有限公司

金鑰管理系統(KMS)

金鑰管理系統用於生成、分發及管理裝置和應用程式金鑰的一種整合服務。
串接HSM來進行金鑰管理，並可針對特殊情境，提供客製化系統開發，運用於軟/韌體更新，裝置/載具金鑰生成。讓使用者能更簡便的控管不同裝置的金鑰，並可針對某個金鑰或裝置管理。分層式權限設計，讓系統更安全，達到高防護。

產品特色

- **基本金鑰管理功能**
  - -生成/管理/刪除金鑰
  - -支援HSM硬體加解密模組
  - -支援對稱式/非對稱式金鑰演算法
  - -可整合外部CA

- **客製化加解密/簽章服務**
  - -End-Entity 金鑰、憑證生成
  - -特定格式的資料加解密
  - -資料數位簽章

- **多元應用相關案例**
  - -IoT韌體簽章
  - -電子文件簽屬系統
  - -文件加解密系統
  - -外僑卡製卡系統
  - -時戳服務
  - -OTP server

- **權限式控制管理**
  - -區分金鑰管理者、金鑰使用者、系統管理者
  - -特定格式的資料加解密
  - -針對特定角色開放功能操作/使用

特權帳號管理系統

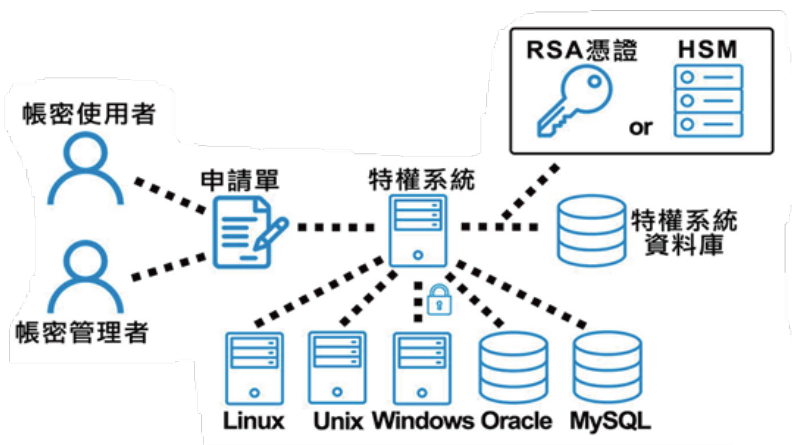
內部擁有多台主機及眾多帳號，耗費人力及時間進行控管，此系統針對主機特權帳號盤點及密碼管理提供自動申借及自動回收服務的跨平台系統，提供多因子多重認證及可搭配HSM進行二次加密，協助企業降低對特殊權限帳號濫用造成的風險，簡化作業流程，有效控管組織內部主機及重要服務系統存取，以期達到資訊治理、法規遵循及積極服務的目的。

產品特色

- **基本功能介紹**
  - -自動申借/自動回收帳號及密碼
  - -具有時效性限制
  - -可搭配HSM進行二次加密

- **系統登入驗證方式**
  - -個人登入憑證驗證
  - -AD帳號驗證
  - -操作環境驗證
  - -可配合單一簽入及整合OTP二次驗證

- **密碼申借核准方式**
  - -可搭配政策一層或多層核准模式
  - -電子郵件附件加密寄送
  - -遠端連線使用，到期自動回收帳號密碼

- **稽核日誌紀錄**
  - -紀錄帳號申請/存取/異動/回收/異常
  - -可查詢或匯出紀錄
  - -自動變更失敗時，系統會主動通知管理者

- **支援平台及連線方式**
  - -OS：Windows/Unix/Linux/Mac
  - -DB：MSSQL/MySQL/Oracle
  - -連線方式：SSH/RDPHTTP/HTTPS /TCP-IP/Telnet