iSecurity

The Hub of Security Innovations

Stop more attacks

超前部署，拒敵於境外

數位資安系統 | 賴銘俊

前言

Information Security

資料的安全企業必須要有所作為，盡可能降低風險與損害—

風險來自於**外部的威脅**與**內部的洩漏**，而標的物就是**端點**，因此妥善的端點防護是資料保護的根本

How

針對**外部威脅**，無論是根據特徵、行為，有判斷就會有誤判/漏判！

No detection is good prevention

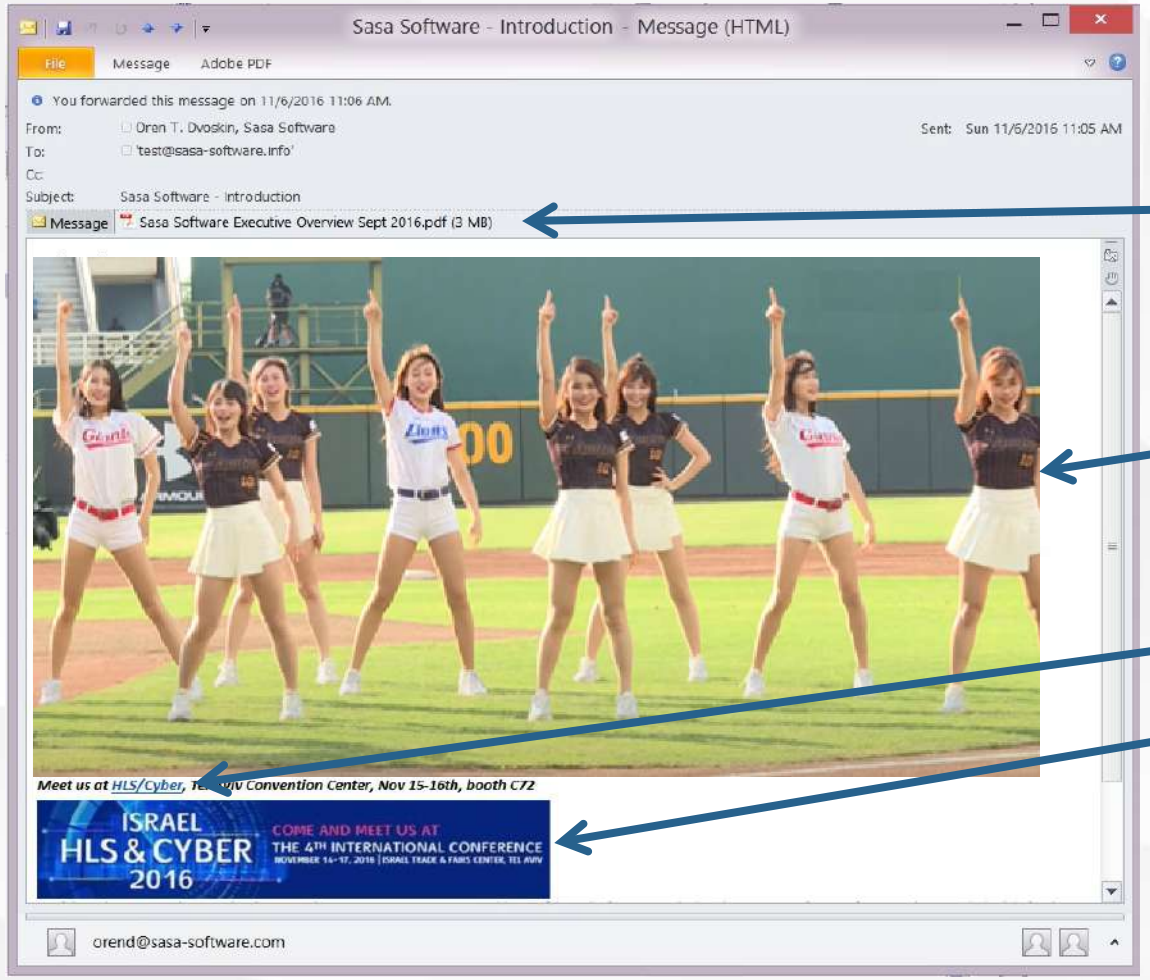
No detection is good prevention

外部威脅解決方案

iSecurity
The Hub of Security Innovations

郵件風險說明

- 外部威脅80%來自郵件，無法避免的威脅進入點
- 郵件內容之風險
- AV、Sandbox、EDR無法有效保護企業的安全



Headers

Attachments

Links

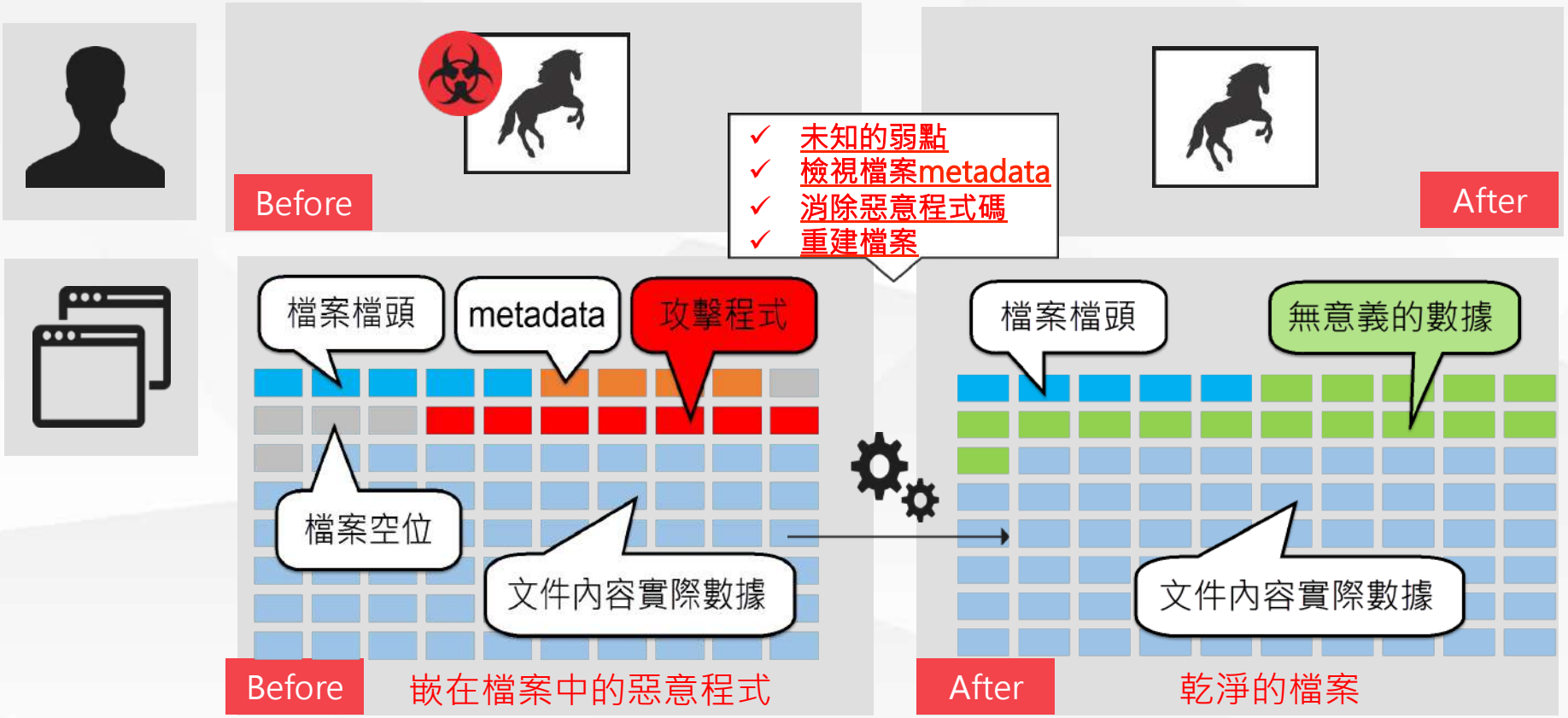
Embedded Elements

Email Body / HTML

iSecurity
The Hub of Security Innovations

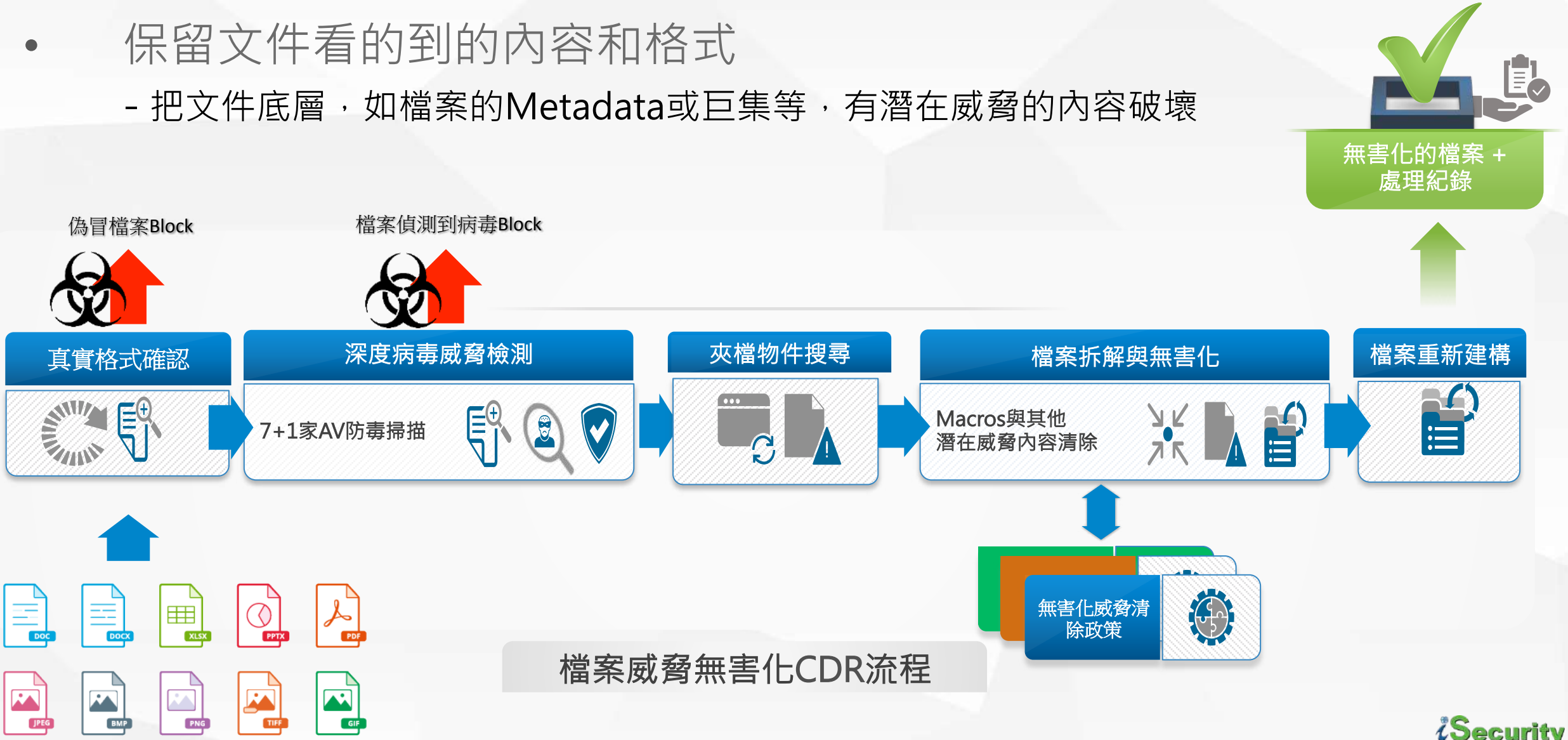
郵件風險解決方案—SASA

- CDR概念(Content disarm and reconstruction)
- 正常郵件不受影響



郵件風險解決方案—SASA

- 保留文件看的到的內容和格式
  - 把文件底層，如檔案的Metadata或巨集等，有潛在威脅的內容破壞

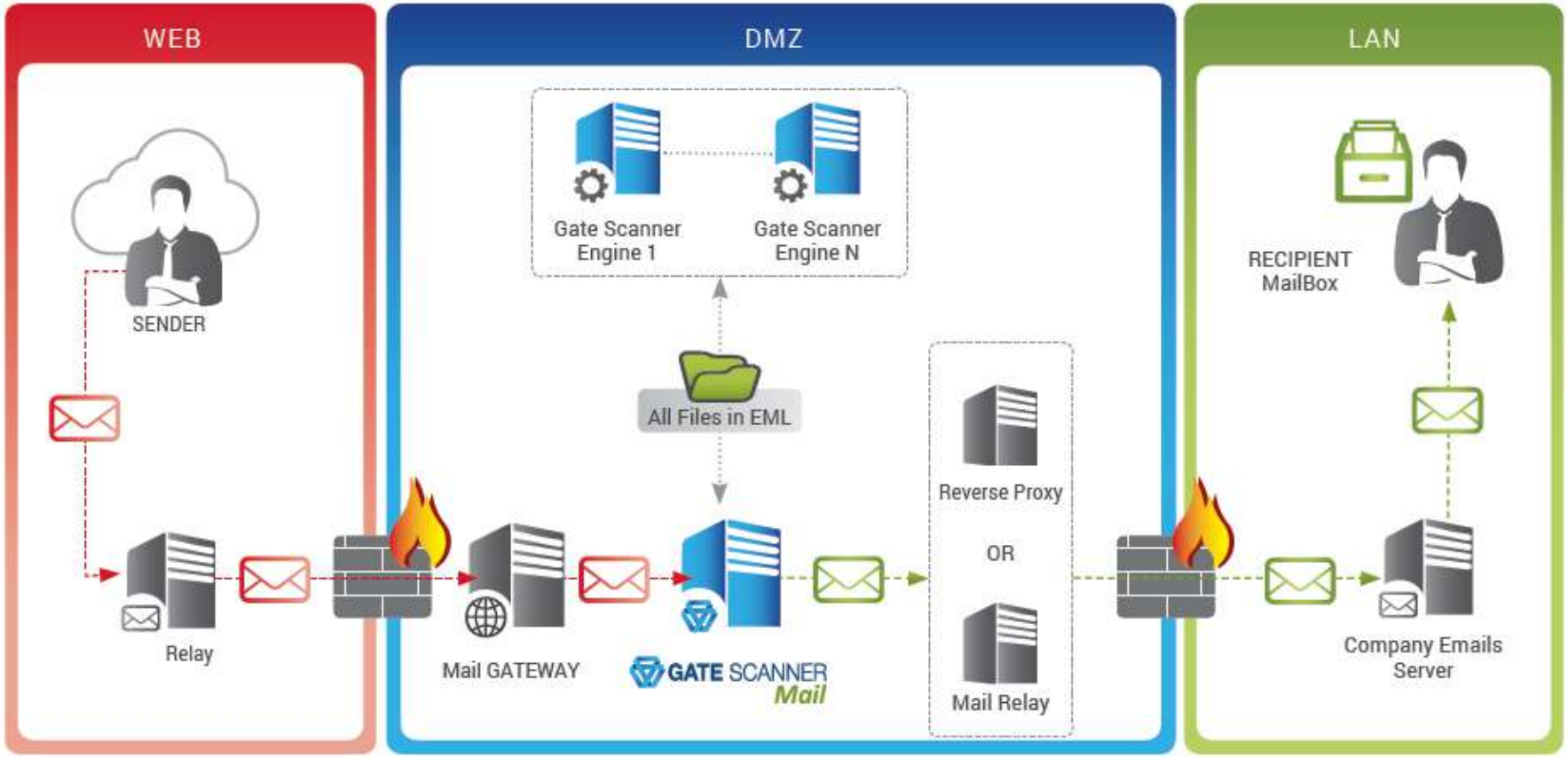


檔案威脅無害化CDR流程

iSecurity
The Hub of Security Innovations

SASA特點

- ✓ Gate Scanner® CDR依據RFC2822國際標準拆解完整.eml 檔案
- ✓ 過濾電子郵件並拆解內文,表頭與附檔
- ✓ SASA特點：
  - 以色列國家級驗證與採用
  - 支援200+檔案格式
  - 維持檔案可用性
  - 多重壓縮與加密檔案
  - KIOSK，FTP/SFTP/SMB 及Network segment等

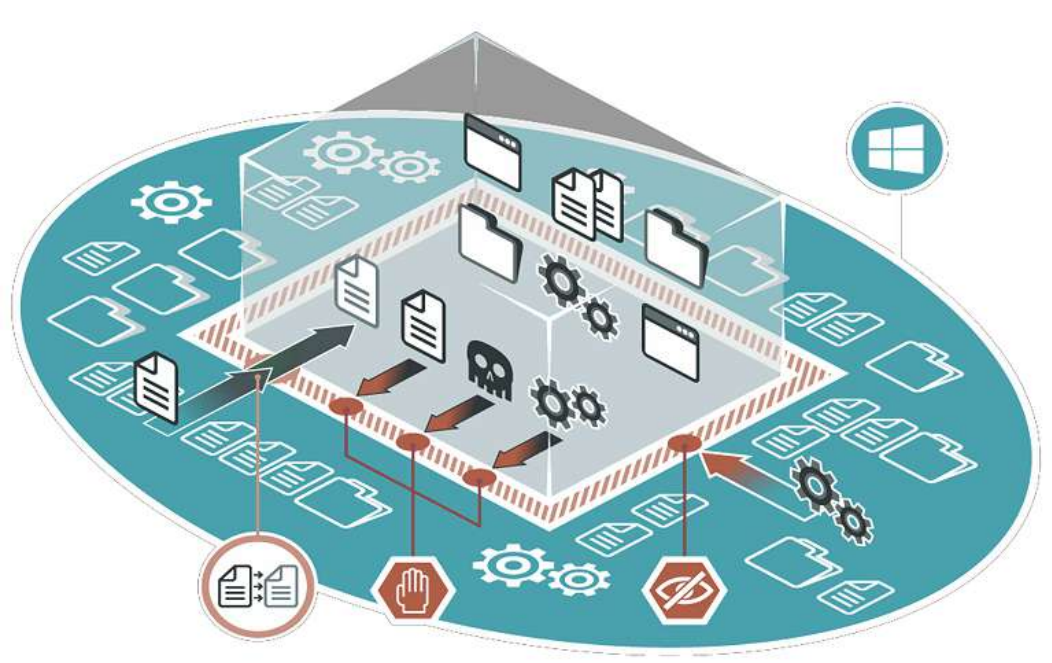


參考效能：20 GB /hour per GateScanner Engine
Note – Depending on the quantity of Gate Scanner engines and Gate Scanner type.
Tests done on virtual server 2008R2;, 8GB, Intel Xeon E5640 @ 2.659GHz

iSecurity

Web風險解決方案—BUFFERZONE

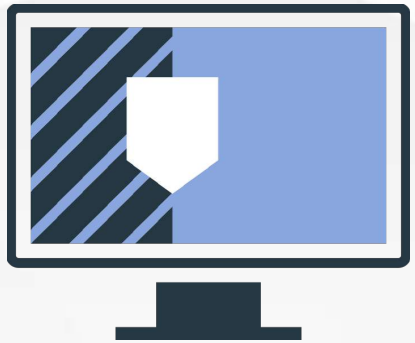
- 上網風險始終存在
- Proxy做法—永無止盡的維護黑名單但總是有遺漏，公司外呢？
- BUFFERZONE隔離區是最簡單有效的方法



核心技術

應用程序在隔離容器執行，並在容器的邊界採用上下文的存取控制， 防止子程序延伸的攻擊，以保護主機免受容器中運行的代碼和數據的攻擊。

利用端點主機上的少量的系統資源，提供透明與徹底的應用程式保護。
容器內的所有的程式在執行階段，都只被賦予最小的執行權限。



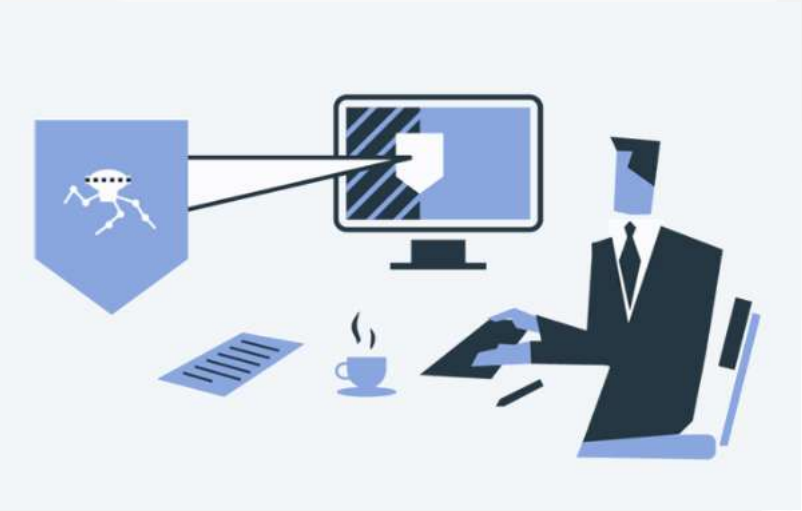
iSecurity
The Hub of Security Innovations

BUFFERZONE無憂無慮的上網體驗

- 支援主流的瀏覽器：Chrome、Edge、Firefox等。
- 不需要特徵碼更新/網站黑名單，防範所有上網威脅
- 下載的檔案都在隔離區中開啟，達到最全面的防護
- 使用者不需改變上網習慣-ActiveX/自動同步都還在
- 瀏覽器上的擴充元件與網頁認證均不受影響，

如網銀及網路ATM讀卡機轉帳/報稅，滑鼠右鍵都可運作

- 不傳送畫面不佔用網路頻寬



—為應用程序提供虛擬容器，以隔離進程和潛在威脅，保護系統

iSecurity
The Hub of Security Innovations

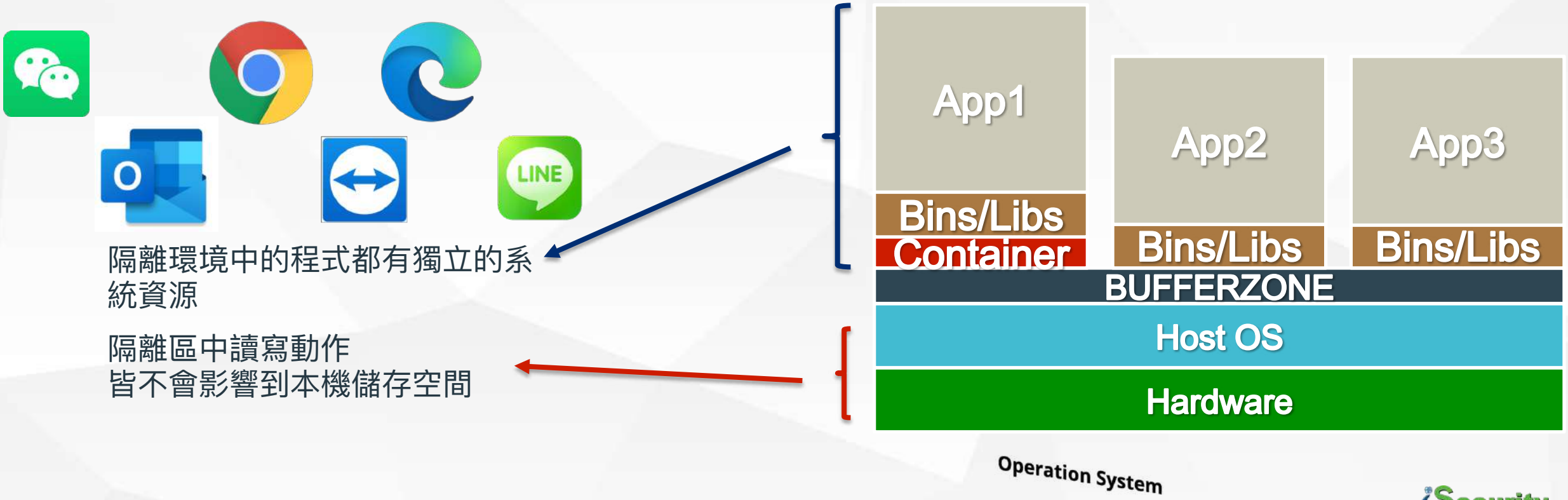
BUFFERZONE怎麼做？

- 除了上網之外，還能做更多...

iSecurity
The Hub of Security Innovations

BUFFERZONE的可用性

- 限制的應用程式(LINE、WeChat等)一律在隔離區內開啟使用
- 可依員工作業環境客製化隔離的應用程式



隔離環境中的程式都有獨立的系統資源

隔離區中讀寫動作
皆不會影響到本機儲存空間

內部洩漏及其他風險…

iSecurity
The Hub of Security Innovations

內外兼顧的守護者—Digital Guardian

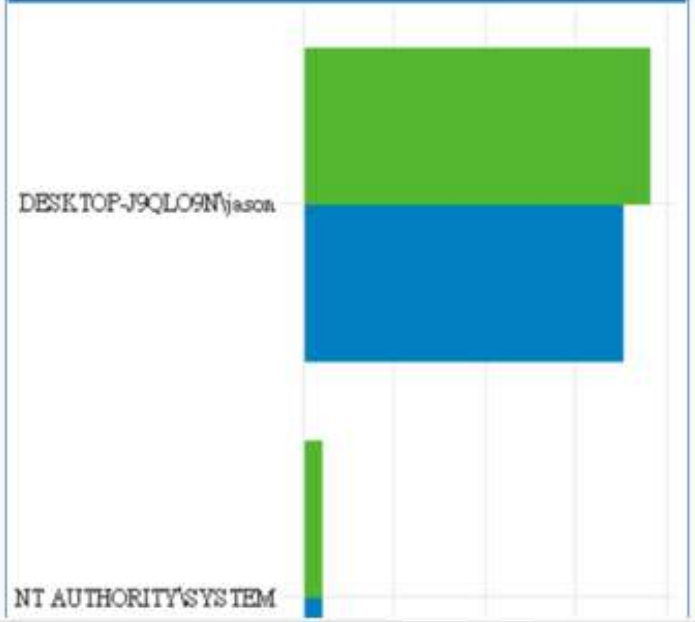
iSecurity
The Hub of Security Innovations

Custom report

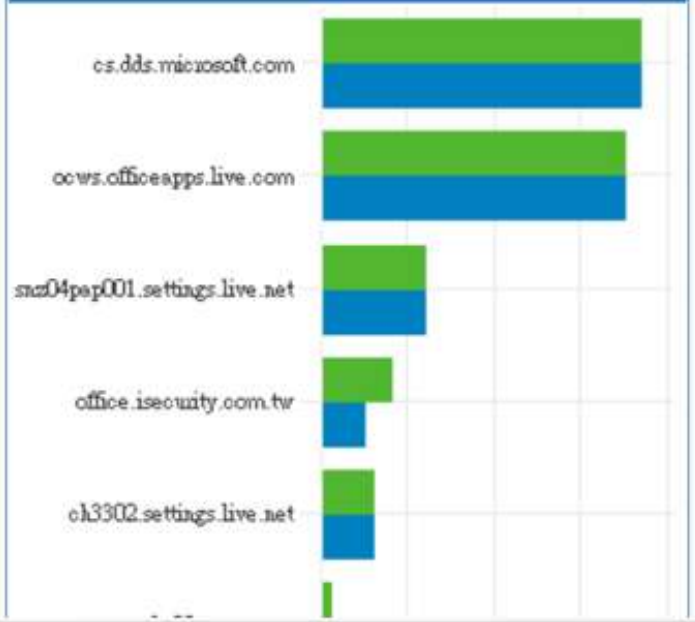
Dashboard – network upload egress (v2)

NTU EGRESS - TREND

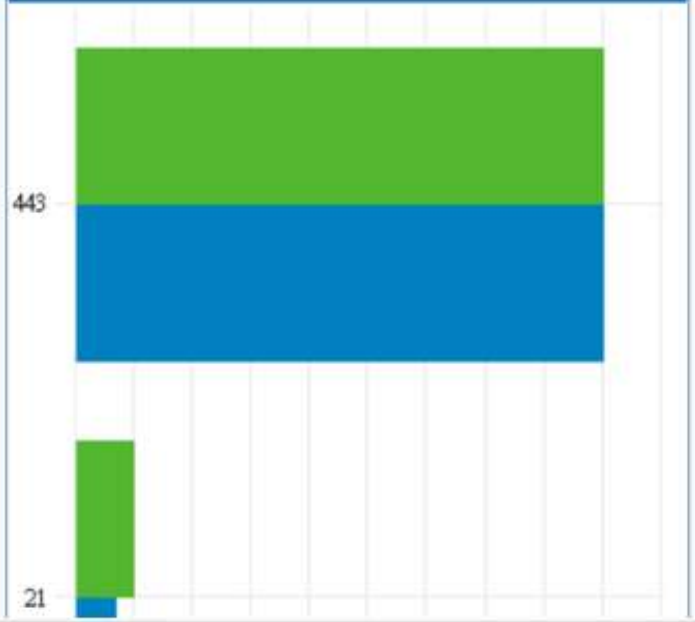
NTU EGRESS - TOP USERS



NTU EGRESS - TOP HOSTS

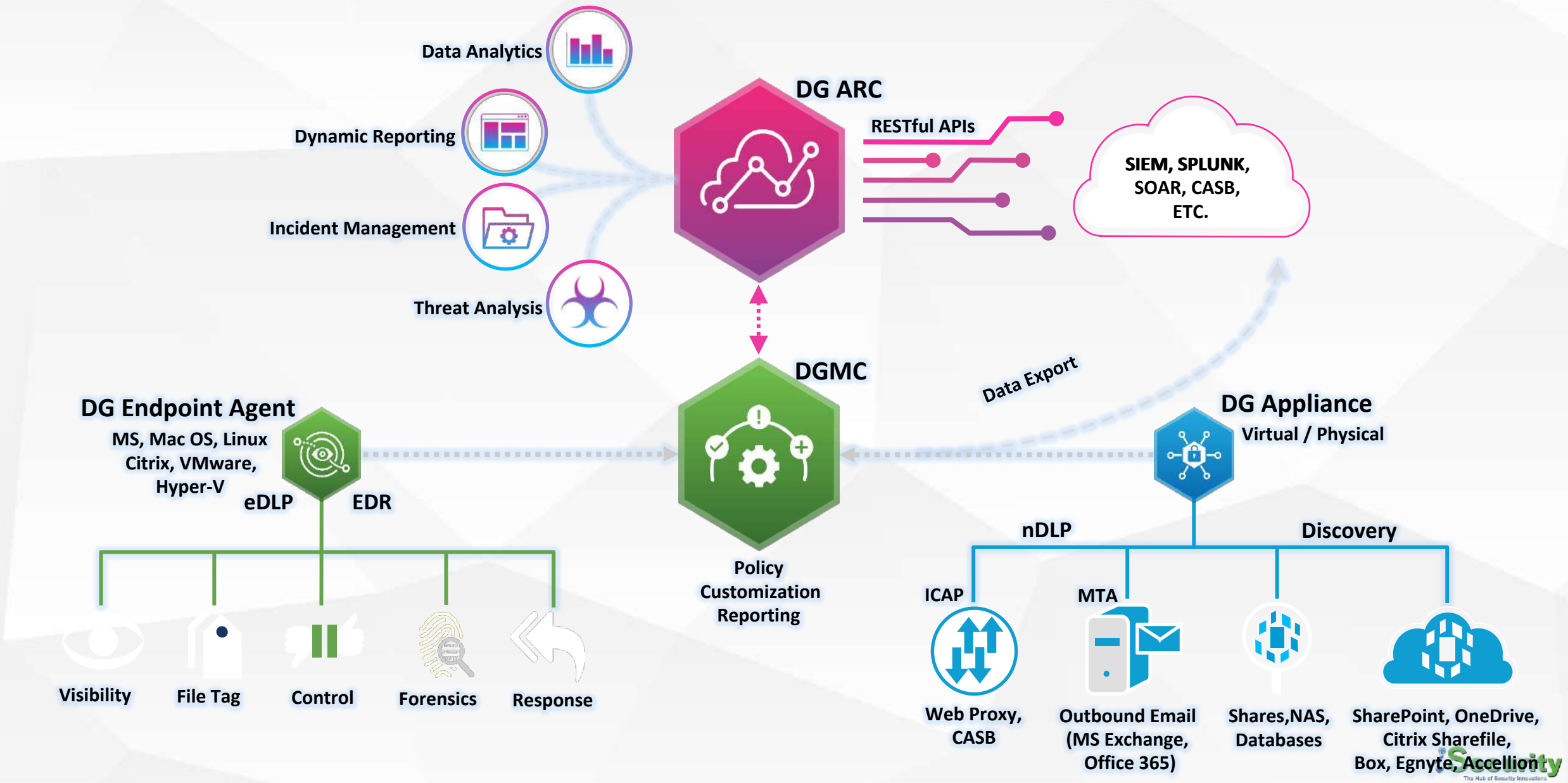


NTU EGRESS - TOP PORTS



iSecurity

Digital Guardian架構圖



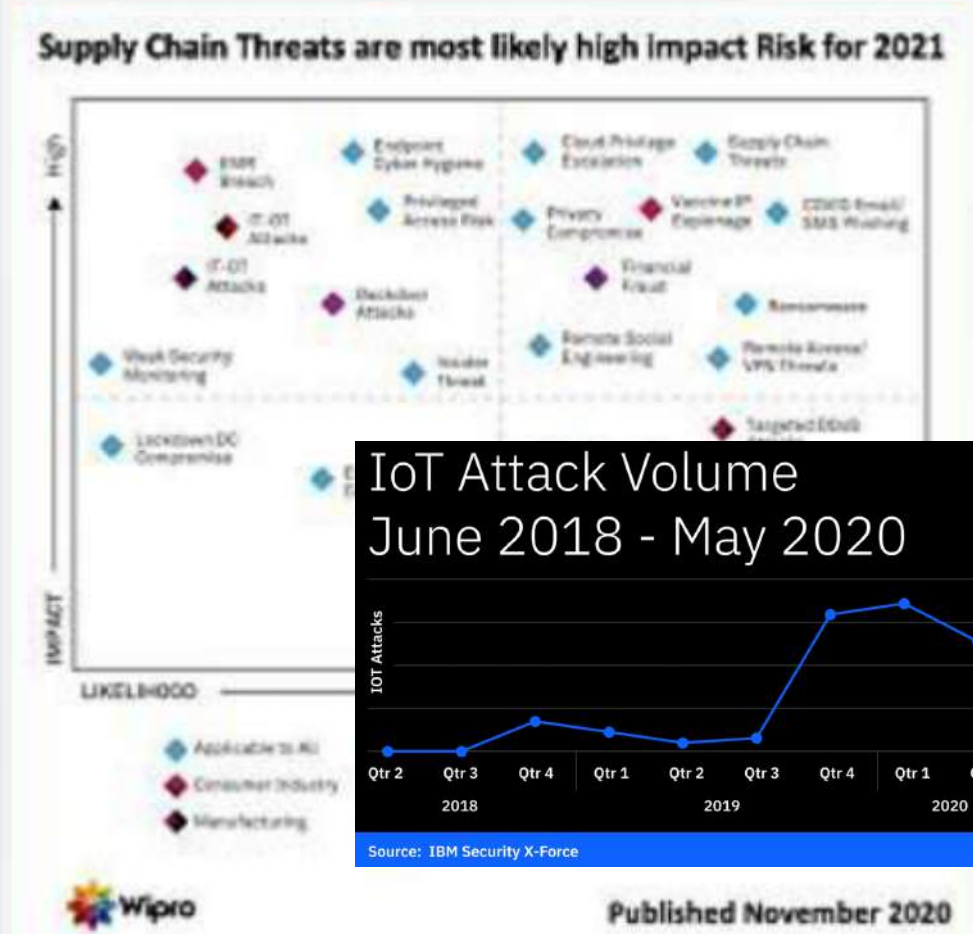
端點最佳方案

iSecurity
The Hub of Security Innovations

One more thing...

IOT設備的風險

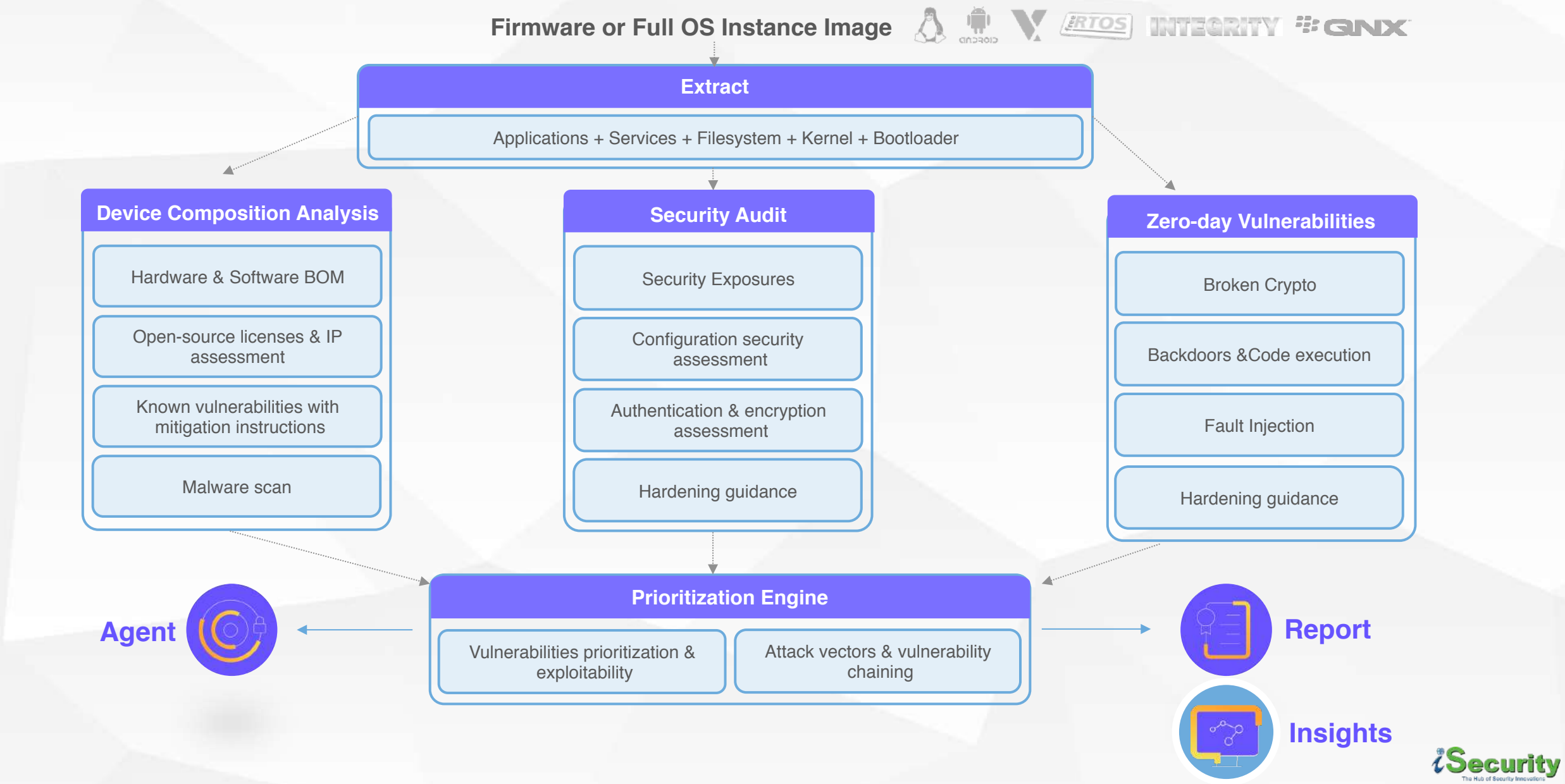
- 端點保護好了之後？
- IOT攻擊事件層出不窮



VDOO can Help

- 企業：每採購一套IT產品，就是為企業引進一個潛在的威脅，擴大了企業的被攻擊面(Attack Surface)
- 廠商：每賣出一套產品，帶給公司的不僅僅是有形的營收數字，更是一份無形的風險責任
- **盤點與掃描**
- VDOO-Vision: Automated Security Platform for IoT & Embedded Systems
  - ■設備資安健檢的最佳幫手
  - ■以最簡便最快速的方式將設備的資安弱點盡收眼底
  - ■涵蓋Sensors, Alarms, Access Point, Base Stations, Smart TV, Set-Top Boxes, Surveillance Cameras, Printers, Robots, Kiosks, Smart UPS, NAS ,……

VDOO's flow


Firmware or Full OS Instance Image
Extract
Applications + Services + Filesystem + Kernel + Bootloader
Device Composition Analysis
Hardware & Software BOM
Open-source licenses & IP assessment
Known vulnerabilities with mitigation instructions
Malware scan
Security Audit
Security Exposures
Configuration security assessment
Authentication & encryption assessment
Hardening guidance
Zero-day Vulnerabilities
Broken Crypto
Backdoors &Code execution
Fault Injection
Hardening guidance
Prioritization Engine
Vulnerabilities prioritization & exploitability
Attack vectors & vulnerability chaining
Agent
Report
Insights
iSecurity

VDOO's analysis results

Infotainment

info_0.1.tar.gz

VH

Threat Level

Compare Mode

- Report Overview
- Highlighted Issues
- Components
- All Security Issues
  - Exposures
  - CVEs
  - Potential Zero-Days
- Requirements
- Additional Info

Generate ERA

What is ERA?

... > Potential Zero-Days 3 Code Zero-Days / 0 Code Weaknesses

+ Files to scan

Search for...

Code Zero-Days 3 | Code Weaknesses 0 | Scanned

TO FIX 3 Items

Code Zero-Day ID	Description	File Path
VU-20-0149	Insufficient input validation resulting in shell command injection	/acme/lib/libac
VU-20-0150	Heap buffer overflow caused by copying a variable-sized buffer into a fixed-size...	/acme/lib/libac
VU-20-0151	Stack buffer overflow caused by copying a variable-sized buffer into a fixed-size...	/acme/lib/libac

MARKED DONE 0 Items

DEFERRED 0 Items

FALSE POSITIVE 0 Items

TO FIX

Insufficient input validation resulting in shell command injection

VU-20-0149

Impact High

Breakdown

Confidence Medium | Exploitability High | Severity High

CWE

CWE-78 : Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Attack Vector

Physical

Findings | Code | Risk Breakdown

What was found?

The potentially vulnerable code adds unsanitized external inputs to an internal buffer that is later executed by the operating system shell.

This can lead to command injection, resulting in malicious code execution.

Where was the vulnerability found?

What should I do?

Which scanner found it?

VDOO六大方針—IoT device的超級處方簽

Key Features

- 一目了然的IoT設備和內嵌式系統的風險及安全報告。
- 開源軟體的使用清單和相關license合法性檢查。
- 掌握所有設備既有的相關CVE漏洞。
- 提供依照CVE漏洞的風險\關鍵程度規劃的修補計畫。
- 針對個別漏洞和弱點提供修補手冊。
- 合規性和相關資安標準即時比對。

Key Benefits

- 提供設備上所有軟體和硬體的BOM表
- 簡單使用，韌體一鍵上傳無須複雜設定及操作
- 小時內即可完成分析，快速掌握IoT設備健康狀況
- 提供有效率的漏洞修補計畫
- 可對應合規性相關法規需求修補相關漏洞，加快產品符合法規的效率
- 可用於發現300多種特定於IoT設備的Zero-Day漏洞

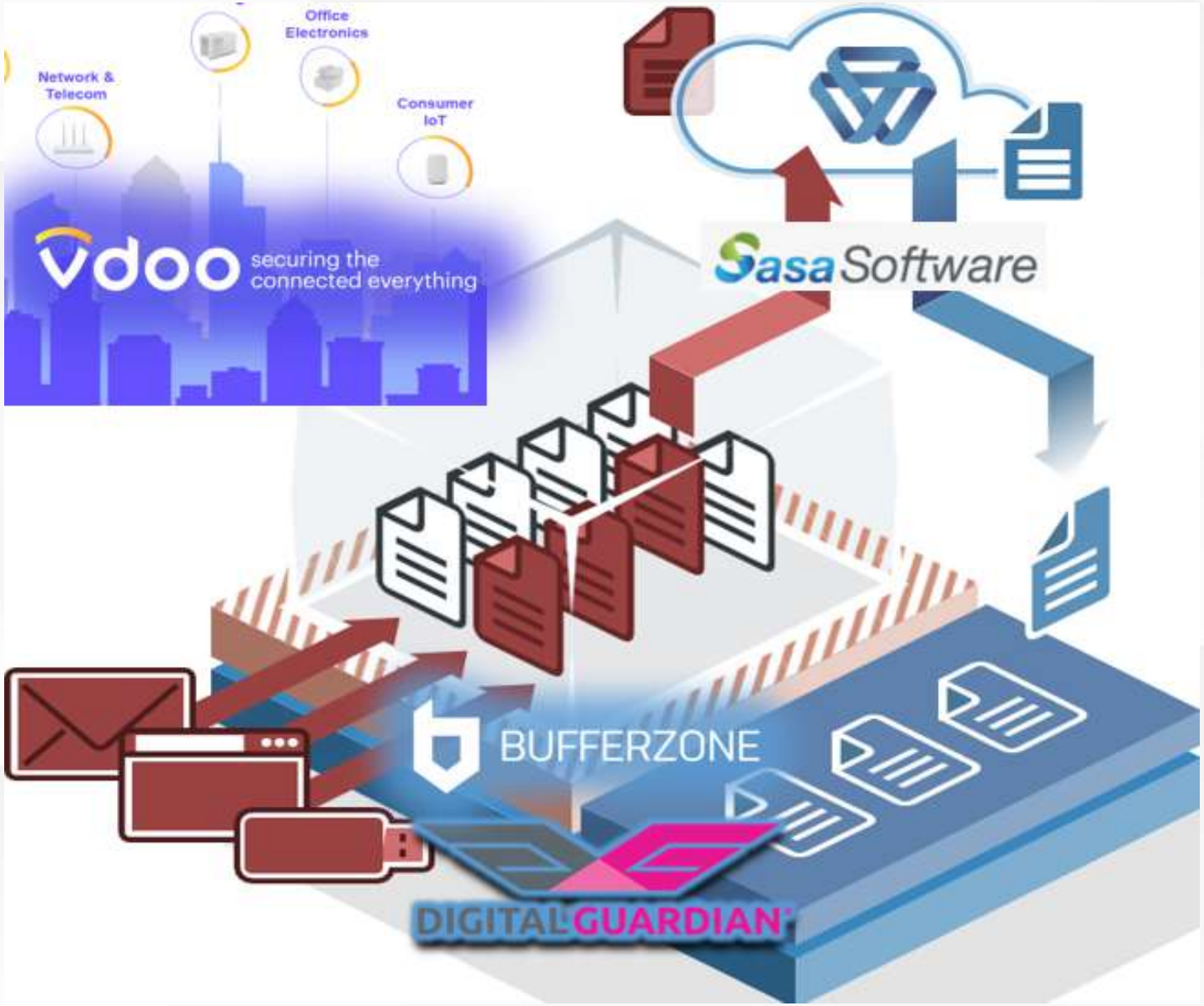
企業為何需要Vdoo?

能夠以最簡便最快速的方式為企業內既有或計劃採購的IT/OT設備執行資安健檢,
確保設備不會成為潛在的企業威脅

廠商為何需要Vdoo?

能夠以最簡便最快速的方式確保自家生產或銷售的IT/OT設備足以符合企業的
資安需求, 不會成為公司在銷售完成後的風險負擔

超前部署—Stop more attacks完整方案

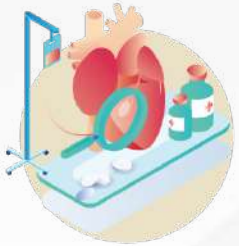


iSecurity
The Hub of Security Innovations

Cyber Resilience

強化企業資安體質
為未知威脅做好準備

1 Stop More Attacks
超前部署，拒敵於境外



2&3 Find & Fix breaches faster
次世代資安維運中心

4 Reduce breach impact
阻絕擴散降低損害

iSecurity
The Hub of Security Innovations

歡迎聯絡，謝謝！

02-7702 1088

iSecurity
The Hub of Security Innovations