
底盤系統 x 鈑金件
決戰汽零終點線
決勝11個彎道・讓你在生產賽道上領先達交
2023
7/12
第7彎：趨勢篇
15:00~15:30 線上直播 LIVE
你的二項疑慮，在導入機聯網前
Digiwin TV
看火影忍者 學資安!!
NEXT to YOU

Q: 封閉式網路環境就沒有資安問題了？ ✗

仍會有資料傳輸媒介，媒介仍會藏毒（ex.隨身碟）

Q: 機加工產業/OT場域遭駭客入侵機率很低？ ✗

1. 過去聯網場域少，故機率相對低，但現今OT+IT聯網趨於普遍。
2. 產業的交期壓力，成為駭客勒索、要求贖金的把柄。

Q: 備份做得完善，就能避免資安問題了？ ✗

1. 備份僅是讓資料復原，能讓產線恢復運作。但資料外流的問題已發生。
2. 要在病毒入侵、資安被竊取前，就提前阻止問題發生。

企業資通治理 技術面向

基礎資安防護/概念 → 資安策略:組織資安韌性

資安防護矩陣

NIST CSF 五大功能		事前		事中		事後
		Identify (識別)	Protect (保護)	Detect (偵測)	Respond (回應)	Recover (恢復)
五個保護對象	設備 Devices	弱點掃瞄 滲透測試 源碼檢測 威脅情資 資產識別 網路識別 身分驗證	終端/行動裝置防護 AV/HIPS/APT	漏洞修補管理 機房環境管控		資料備份 異地備份 異地備援
	應用 Applications		APP層防護 WAF/SPAM	端點偵測與回應 EDR		
	網路 Networks		網路微分割 NGFW/IDS/VPN	威脅情資/SOC		
	數據 Data	資訊盤點 數據分類	資料與雲端應用安全 Encryption/DLP	網路偵測與回應 NDR		
	使用者 Users	社交攻擊	通行進出管理/多因素認證 資安教育	資安事件管理SIEM		
				資安自動回應SOAR		
Degree of Dpendency 依賴程度		Technology 技術				People 人
		Process (處理)				

資安防護不是 0 或 1，而是0～100%的過程及完成性。企業應針對現況思考資安策略，現在做了哪些?

更多講師簡報
都在 就享知 DigiKnow

輸入邀請碼**16657**

再贈**50元超商購物金**喔!!!

↑第1步. 掃碼進入頁面

←第2步. 輸入邀請碼**16657**

←第3步. 完成基本資訊點選註冊

請幫溫溫完成KPI惹~

win your digivalue 贏在數位價值

鼎新企業運維

攜手Fortinet完整資安防護

鼎新電腦

企業運維

實現智能運營、助力數位轉型

傳統維護的難題

維護複雜

傳統資料中心維護種類繁多，從硬體風火水電，到軟體系統、資料庫、中介軟體等，人工運維的工作量繁雜，缺口多。

無統一管理

傳統資料中心維護的領域眾多，各個領域的運維工具煙沖式建設，無法實現統一管理，也無法統一操作。

新技術帶來挑戰

各類公有雲、私有雲、超融合等等解決方案的出現，給維護工程師帶來天翻地覆的變化。

服務滿意度低

服務因人而異，隨著系統及服務場景的複雜性日益增加，服務無法“一鍵直達”，導致服務交付滿意度低。

漏洞補不完

資安攻擊不間斷，缺乏數據支持，永遠不知道漏洞在哪裡，花很多冤枉錢仍然被勒索。

鼎新企業智能運維

統一入口的運維

打造承載各類場景SaaS工具的統一運維PaaS平臺，為企業運維的監管控提供統一入口，並具備平臺層的靈活擴展性。

建立數據運維

運維平臺集成數據，如服務工單數據、監控告警資料、企業漏洞，效能數據等，通過資料採擷不斷持續改善服務品質和運營水準。

打造IT服務體系

打造IT自助服務，線上支援及智慧客服，建立資料中心與用戶之間的連接通道。

完整的資安防護

主動偵測威脅、攻擊防護、防止加密及刪除，移除感染源，事情防範、事後保護一次完成。

價值效益

管控融合

統一運維入口，管控可視化

數據賦能

數據智能分析，實現運維創新

全方位監控

網路、伺服器、系統等完整監控，智能告警

資安守衛

守護企業不受資安威脅，漏洞一覽無遺

AGENDA

1 企業的資安威脅

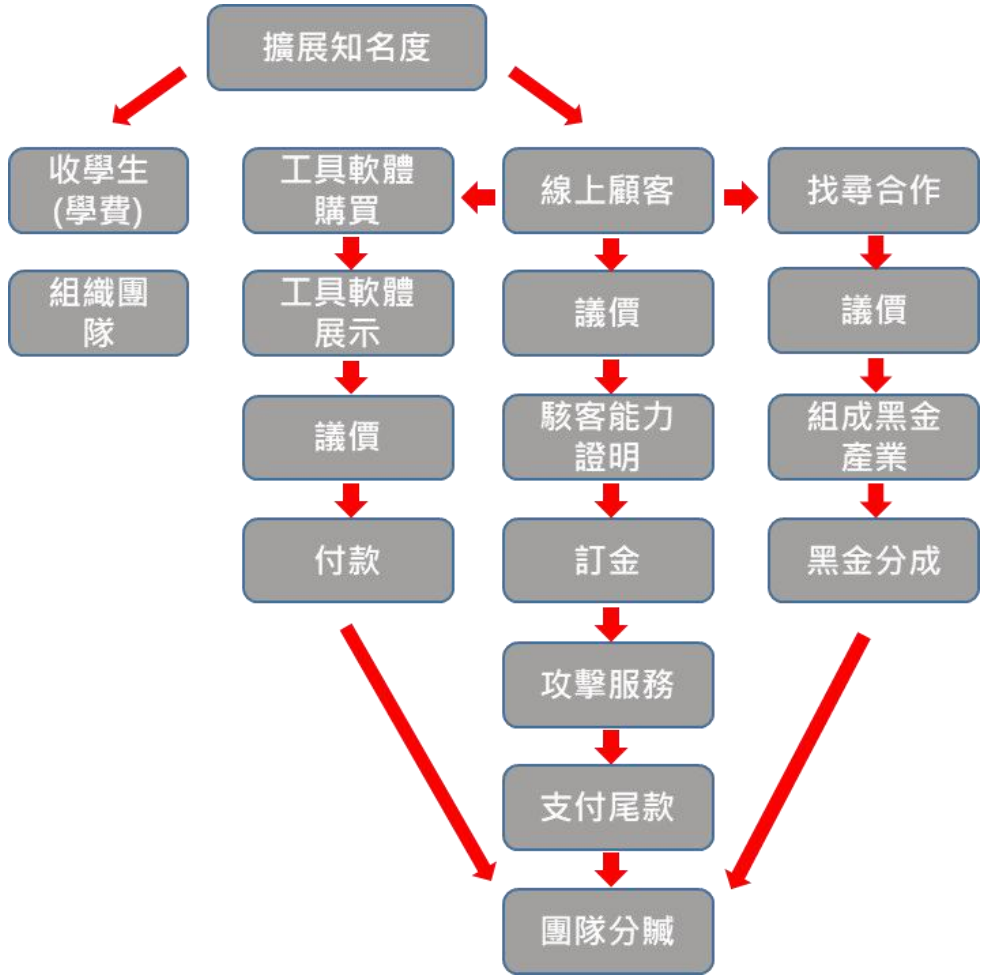
2 EDR對企業的幫助

3 資安運維服務

企業面臨的資安威脅

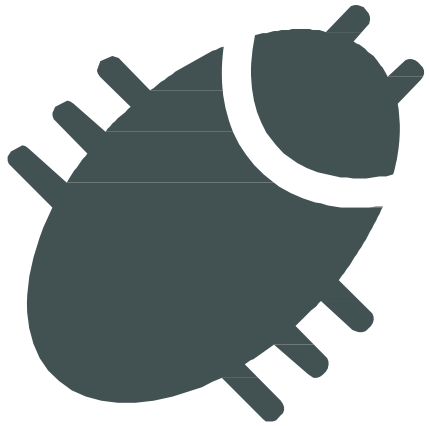
駭客型態的Change，企業化經營

- 低風險高獲利的商業模式成熟，取得技術、無可追蹤的金流
- 以前的孤狼式攻擊，演變至 跨國集團聯合作戰
- 高超的技巧演變至，人人皆可為駭客
- 開始具有家族，集團的概念

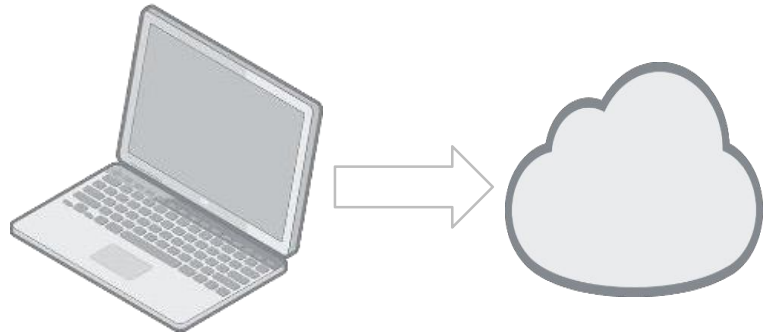


企業資安的挑戰

威脅層面
與日俱進



系統弱點
不斷暴露



雲端應用
規避檢測

層出不窮的資安事件

【臺灣史上最大資安事件】深度剖析台積產線中毒大當機始末

台積電晶圓廠之所以爆發大規模的病毒感染有兩個關鍵，其一是新機臺上線的SOP程序因為人為疏失出錯，導致早已藏匿病毒的機臺沒有被防毒軟體擋下。加上台積所有臺灣廠區的生產網路全部連結在一起，才會因為一臺機臺染上病毒，就造成北中南廠區大規模疫情的嚴重後果

文/ 王宏仁 | 2018-08-10 發表

讚 6.5 萬 按讚加入iThome粉絲團 讚 267 分享

宏碁遭駭客攻擊，勒索 5,000 萬美元

作者 侯 冠州 | 發布日期 2021 年 03 月 20 日 14:54 | 分類 網路、資訊安全、產業 分享 分享 Follow 讚 1,101 分享

遭勒索軟體綁架四天 Garmin三億贖身內幕

Hami書城 / 2020-08-24

國際知名GPS和穿戴裝置大廠Garmin，7月23日遭勒索軟體「綁架」，就連Garmin台灣分公司也受害，網路中斷4天，直到7月27日才陸續恢復。「最後付了1千萬美金（新台幣3億元）贖身！」知情人士透露。

事實上，台灣企近來已成國際駭客眼中的待宰羔羊，光是今年5月，就發生中油、台塑及半導體封測大廠「力成」遭勒索軟體入侵事件。多位資安專家慨歎，「企業不重視資料備份，遭攻擊後又怕傷形象，不敢報警，多付錢了事。」

驚！日月光集團遭勒索病毒攻擊　一度關閉系統

更新時間： 2021/04/05 17:01

日月光控股、日月光半導體高雄楠梓加工廠區。資料照，楊喻斐攝

層出不窮的資安事件

04/27臺灣證券交易所宣布重大訊息處理程序有新的修訂，當上市公司發生重大資安事件時，需發布重大訊息對外揭露。

2018/08 台積電

遭病毒攻擊至少有5廠房受影響，
損失76億、報廢上萬片晶圓

2020/05 力成

IC封測元件大廠
部分伺服器受到勒索病毒攻擊

2020/05 中油

全台加油站的捷利卡
及中油PAY支付都已停擺

2020/05 台塑

部分伺服器遭到勒索病毒攻擊

2020/11 仁寶

遭到勒索軟體攻擊，
公司內部系統癱瘓

2021/03 宏碁ACER

財務表格、銀行結餘等機密資料。
勒索 5,000 萬美元

2021/04 日月光

部分伺服器受到勒索病毒攻擊

2021/04 廣達

加密勒索，代工的蘋果產品，
以及員工與客戶資料外流

2021/05 威剛科技

遭到勒索軟體攻擊，
公司內部伺服器停擺

造成企業損失

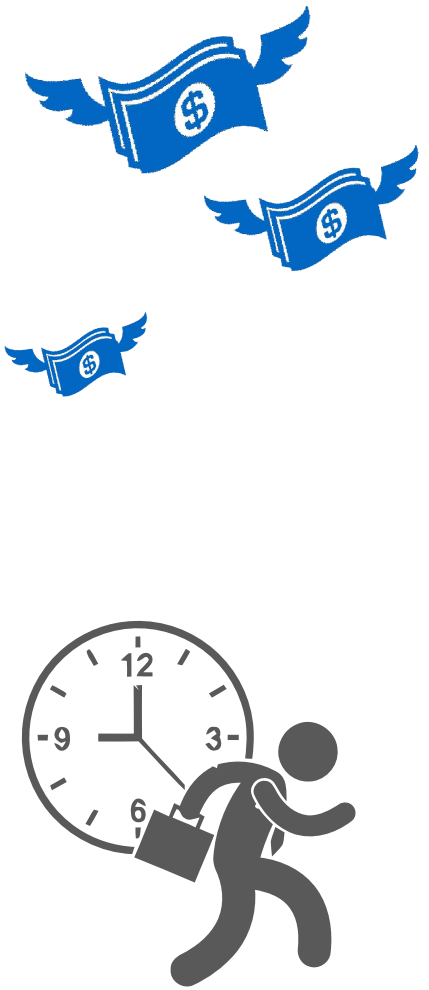
駭客攻擊手法

- 外部服務滲透攻擊
- 釣魚攻擊
- 社交攻擊
- 自帶裝置(有惡意程式的裝置)
- USB病毒
- IOT攻擊
- 內部網路攻擊
  (網路偵測、暴力破解)

企業資安事故

- 勒索加密
- 網路詐騙
- 挖礦病毒
- 資料竊取

事故衝擊



傳統防毒 & 鼎新資安EDR元件差異

傳統防毒跟鼎新資安元件有何不同?

傳統防毒 Endpoint Protection Platform:

是一種安全解決方案，可以將用於智能手機和PC等業務的設備定位為端點設備，
並防止端點設備受到端點威脅和惡意軟件的侵害。

企業運維資安EDR:

監視端點內部的安全性，在檢測到惡意軟件或異常行為時通知管理員，並隔離威脅性惡意軟體。
EDR具有掌握和分析惡意軟體和威脅侵入的感染路徑並防止二次災難。

防毒 跟 企業運維EDR 有何不同?

- EPP(防毒軟體)

事前防範(檔案型防護)

資安工具,惡意軟體的過濾

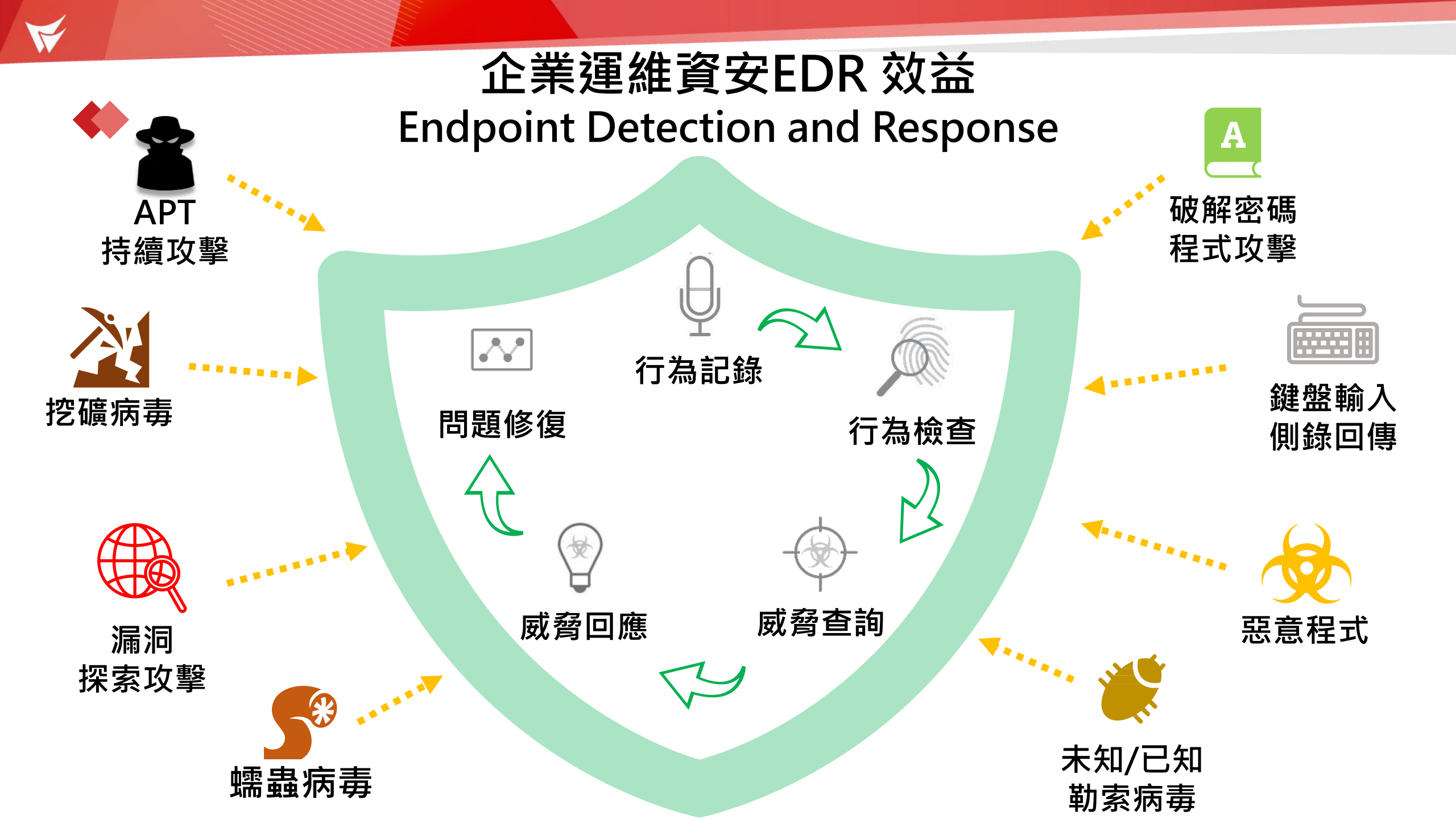
- EDR (偵測與回應)

事後保護(行為型防護)

記錄使用者的行為軌跡,偵測與回應異常行為

防毒軟體功能		EDR偵測與回應防護
防毒引擎 (AV)/Hash比對/情資分享		行為模型建立
端點防火牆		惡意軟體遏制功能
應用程式控管 (伺服器)		使用者行為軌跡記錄，提供日後稽核
網頁過濾		弱點漏洞防禦
通訊埠與設備控管		系統回復機制
弱點與補釘管理		

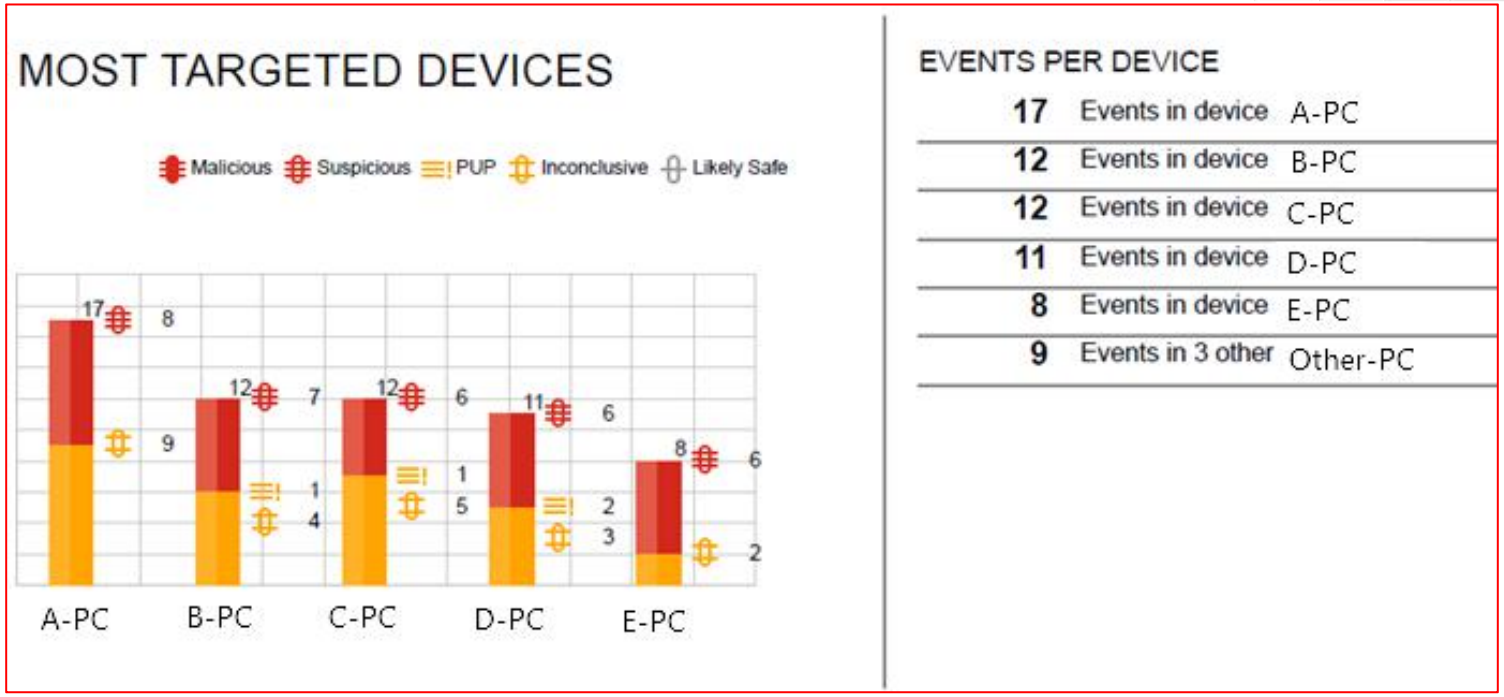
企業運維資安EDR 效益
Endpoint Detection and Response

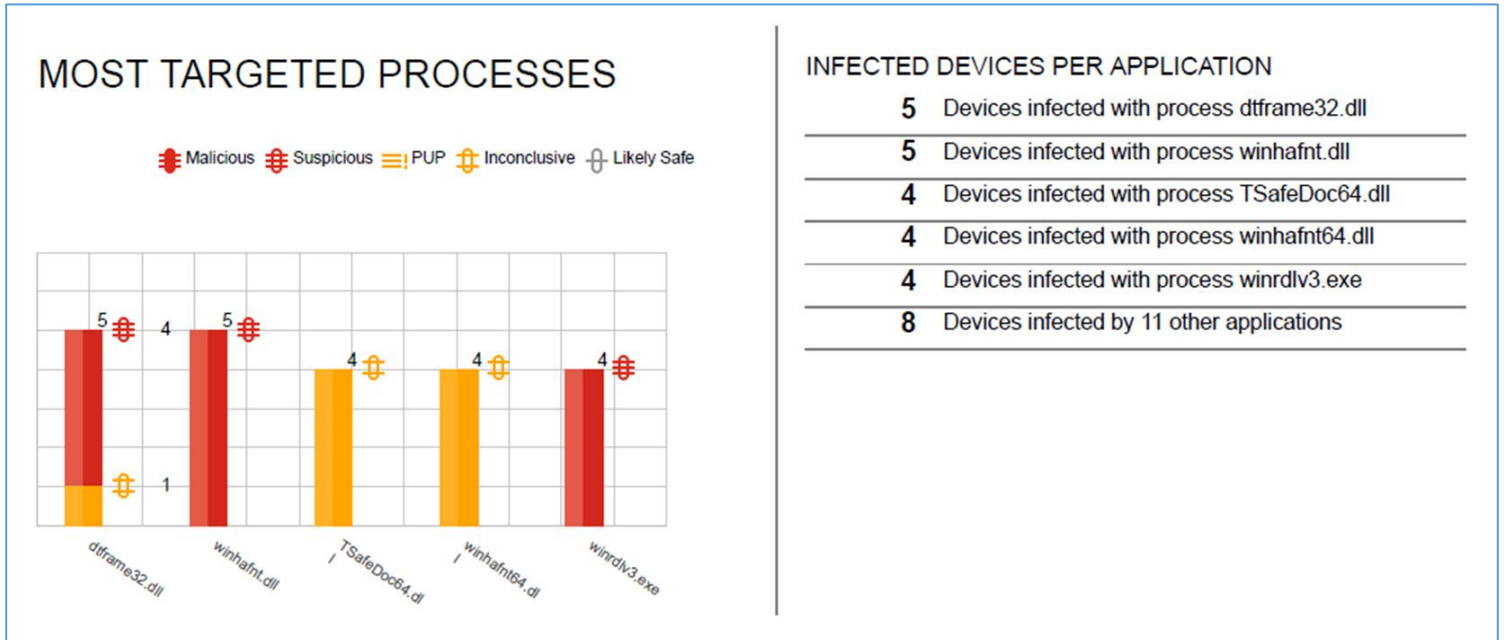


資安運維服務

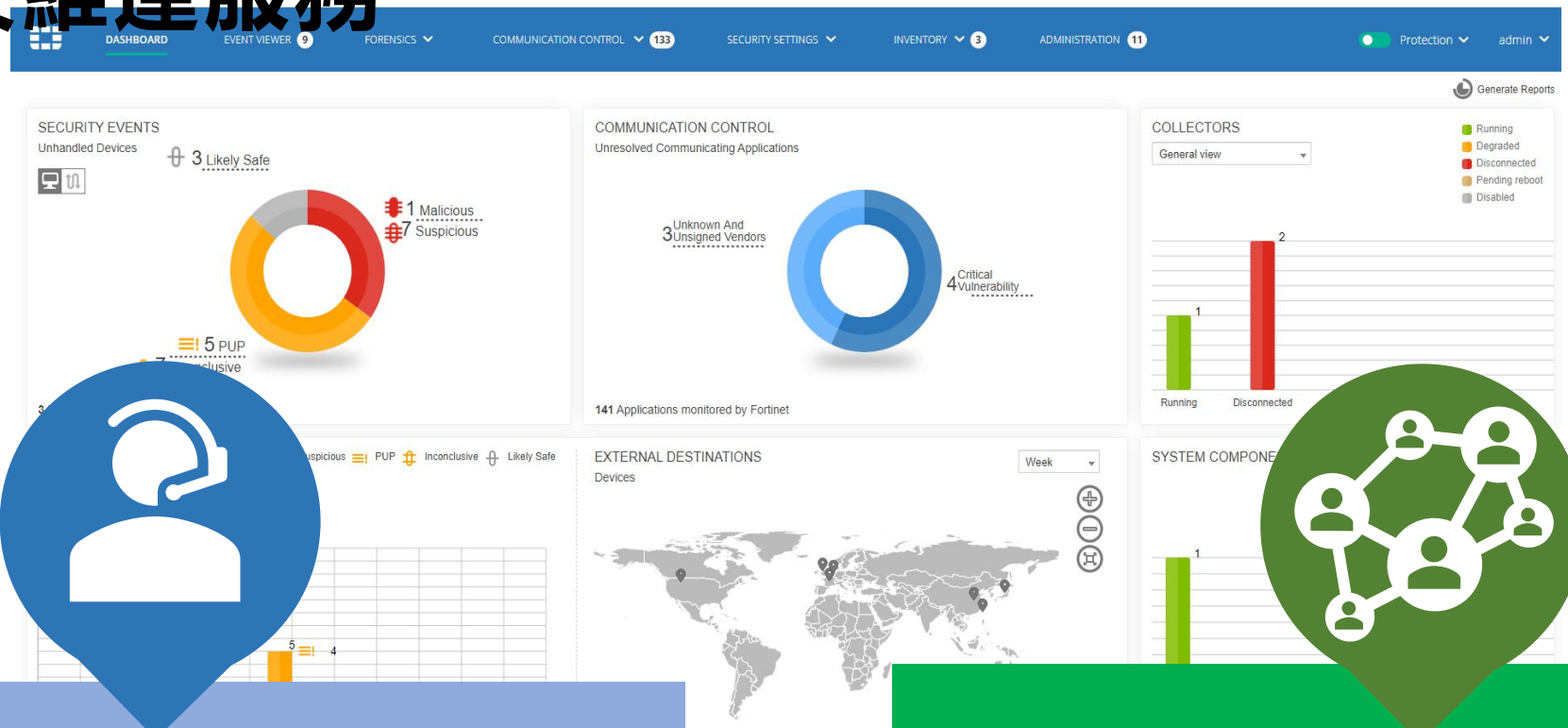
定期維護

- 提供的高風險性端點裝置
- 異常阻檔及攻擊防護記錄
- 主動追蹤路徑並向客戶提出告警





資安維運服務



月維護

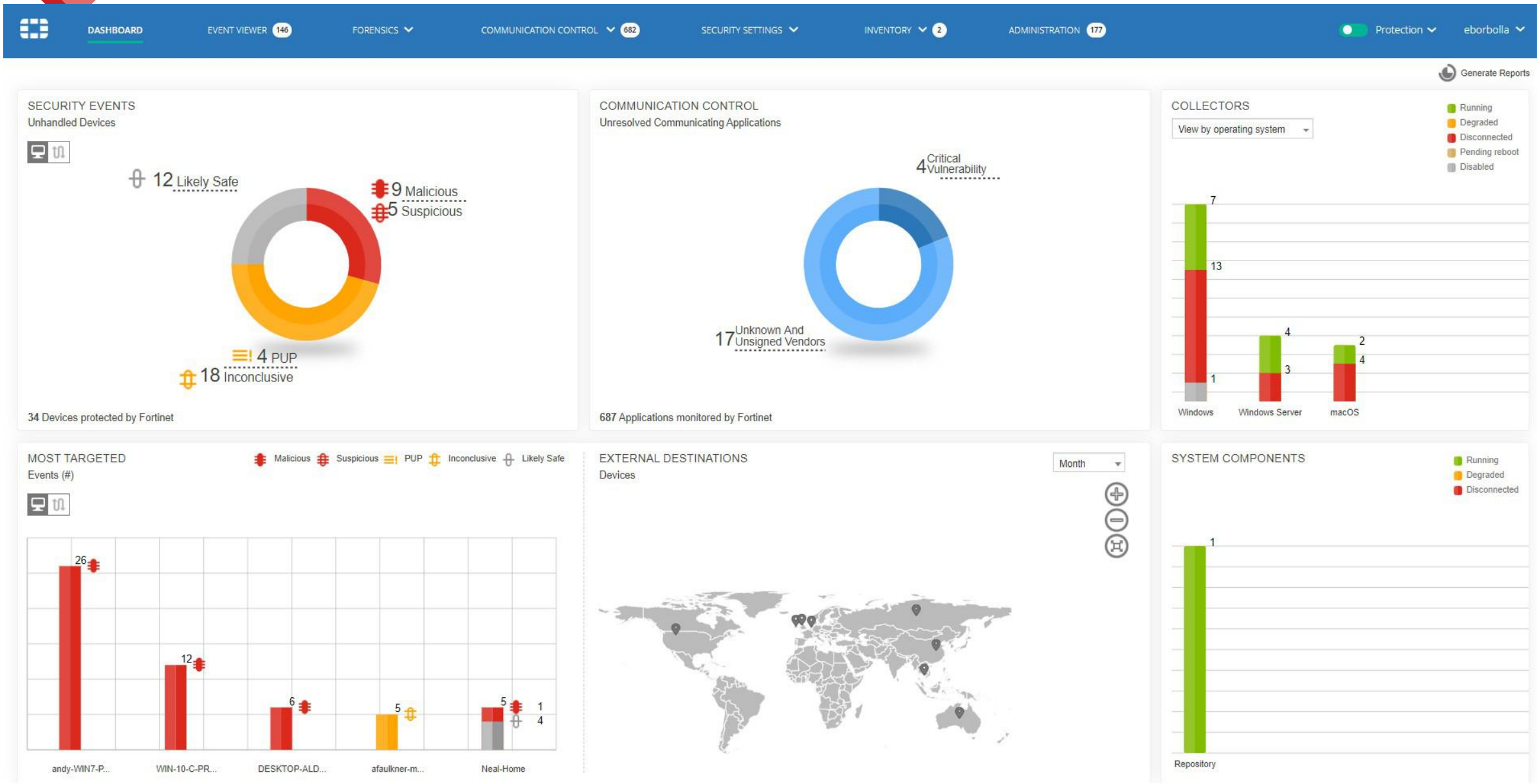
鼎新運維部
定期進行連線檢視防護記錄，
有異常阻檔及攻擊防護事件，
主動追蹤路徑並向客戶提出告警

異常處理

EDR異常攔截程式及網路行為

可電話報修鼎新客服部進行異常排除

資安維運服務

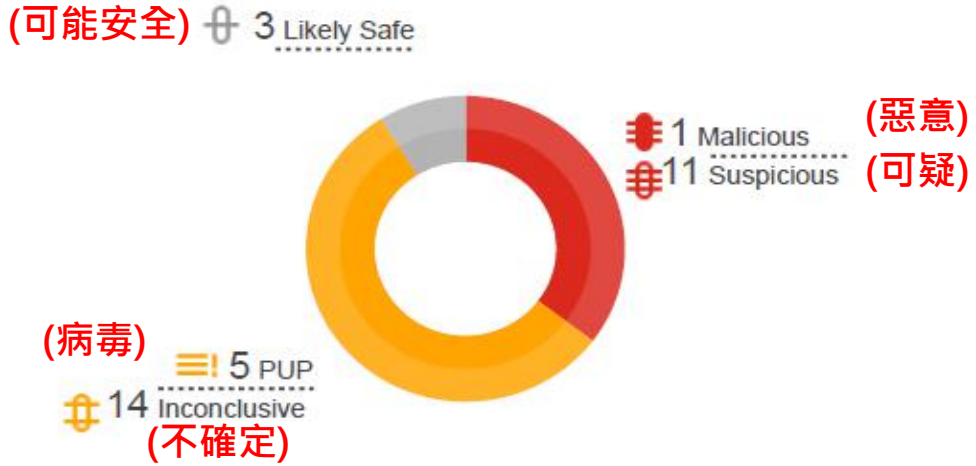

DASHBOARD
EVENT VIEWER 146
FORENSICS
COMMUNICATION CONTROL 682
SECURITY SETTINGS
INVENTORY 2
ADMINISTRATION 177
Protection
eborbolla
Generate Reports
SECURITY EVENTS
Unhandled Devices
12 Likely Safe
9 Malicious
5 Suspicious
4 PUP
18 Inconclusive
34 Devices protected by Fortinet
COMMUNICATION CONTROL
Unresolved Communicating Applications
4 Critical Vulnerability
17 Unknown And Unsigned Vendors
687 Applications monitored by Fortinet
COLLECTORS
View by operating system
Running
Degraded
Disconnected
Pending reboot
Disabled
7
13
1
4
3
2
4
Windows
Windows Server
macOS
MOST TARGETED
Events (#)
Malicious
Suspicious
PUP
Inconclusive
Likely Safe
26
12
6
5
5
1
4
andy-WIN7-P...
WIN-10-C-PR...
DESKTOP-ALD...
afaulkner-m...
Neal-Home
EXTERNAL DESTINATIONS
Devices
Month
SYSTEM COMPONENTS
Running
Degraded
Disconnected
1
Repository

資安維運服務

EXECUTIVE SUMMARY

Dec. 2020, 12 - Jan. 2021, 11

EVENTS STATISTICS



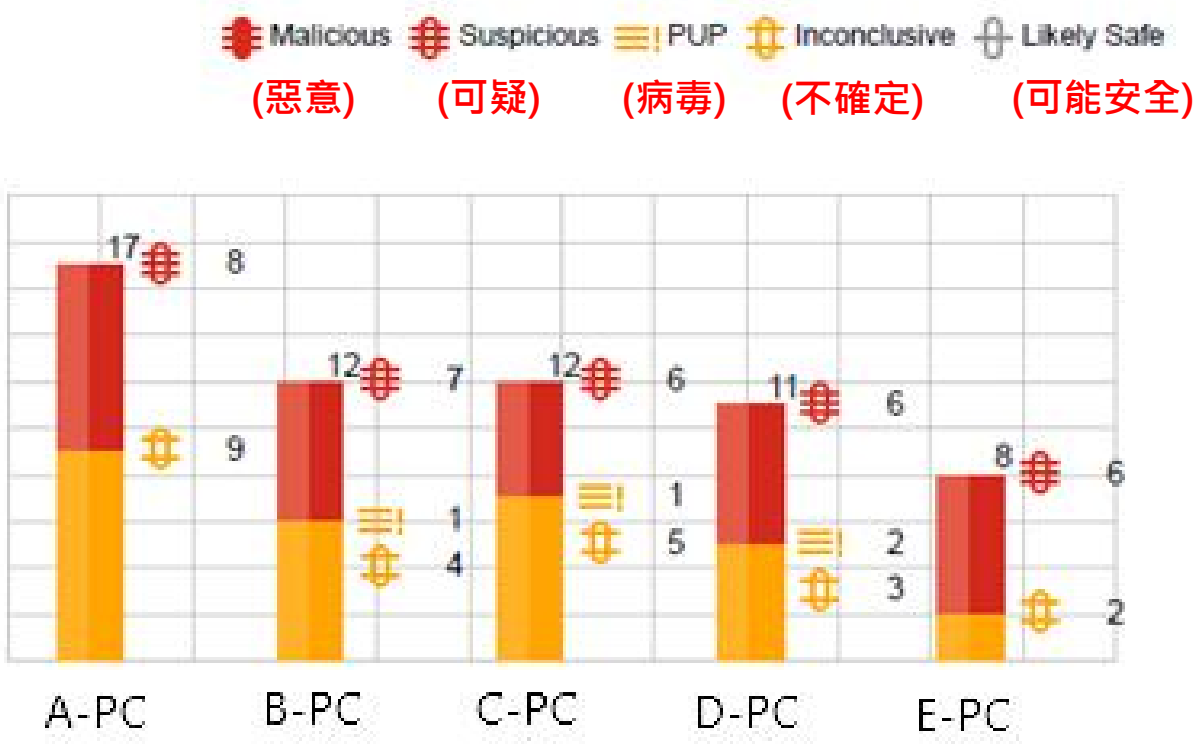
(總體安全報告)

34	OVERALL SECURITY EVENTS GENERATED
1	Malicious(惡意)
11	Suspicious (可疑)
5	PUP(病毒)
14	Inconclusive(不確定)
3	Likely Safe (可能安全)

21	**Exfiltration** prevention policies triggered events (61.76%)	(防止滲透攻擊政策觸發)
10	**Ransomware** prevention policies triggered events (29.41%)	(勒索加密攻擊政策觸發)
3	**Execution** prevention policies triggered events (8.82%)	(執行程式前政策觸發)

資安維運服務

MOST TARGETED DEVICES



EVENTS PER DEVICE

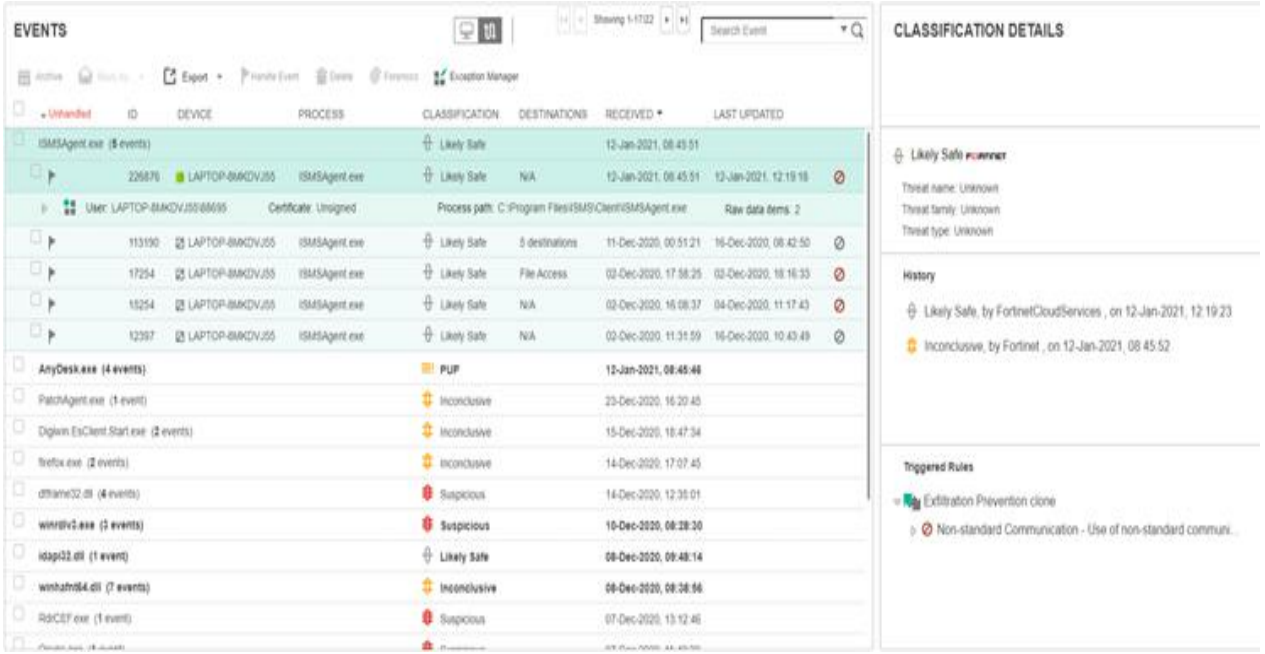
17	Events in device	A-PC
12	Events in device	B-PC
12	Events in device	C-PC
11	Events in device	D-PC
8	Events in device	E-PC
9	Events in 3 other	Other-PC

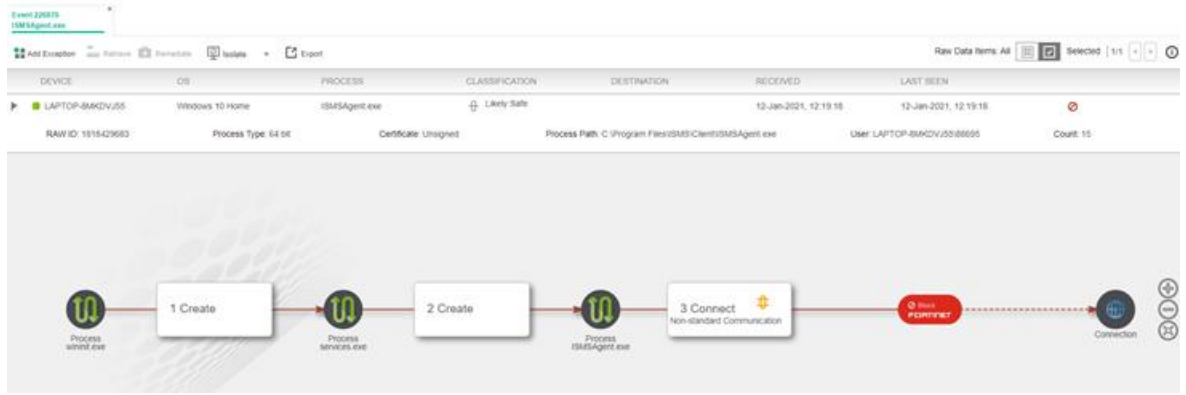
資安維運服務

資安維運防護，會設定異常程式阻檔，

當有異常攔截程式及網路威脅行為，

可電話報修 鼎新線上客服部:**0809-081668** 進行異常排除。





廣泛的支援系統應用

系統別	系統版本
Windows	Windows XP SP2 / SP3,7，8.x 和10.x， Windows Server 2003 R2、2008R1、2008 R2、2012、2012 R2，2016、2019
Mac	macOS Yosemite（10.10），ElCapitan（10.11），Sierra（10.12）， HighSierra（10.13），Mojave（10.14），Catalina（10.15）
VDI	VmwareHorizo ns 6 和 Citrix XenDesktop / XenApp
Linux	RedHat Entprise Linux 6.8、6.9，6.10 7.x CentOS 6.8、6.9、6.10、7.x Ubuntu 16.04、18.04