



你所不知道的 Fortinet

Q3 202108

Dave Peng (彭冠嘉)

Technical Consultant Taiwan



New Feature



全方位的資安

成功案例分享



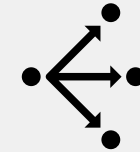
NP7 新晶片問世



Line, Teams 等通訊軟體整合



Gartner 領先的 SDWAN



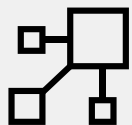
AI 防毒機制的導入



控管 Youtube 頻道



自動化腳本機制



原廠支援客製化 IPS, App



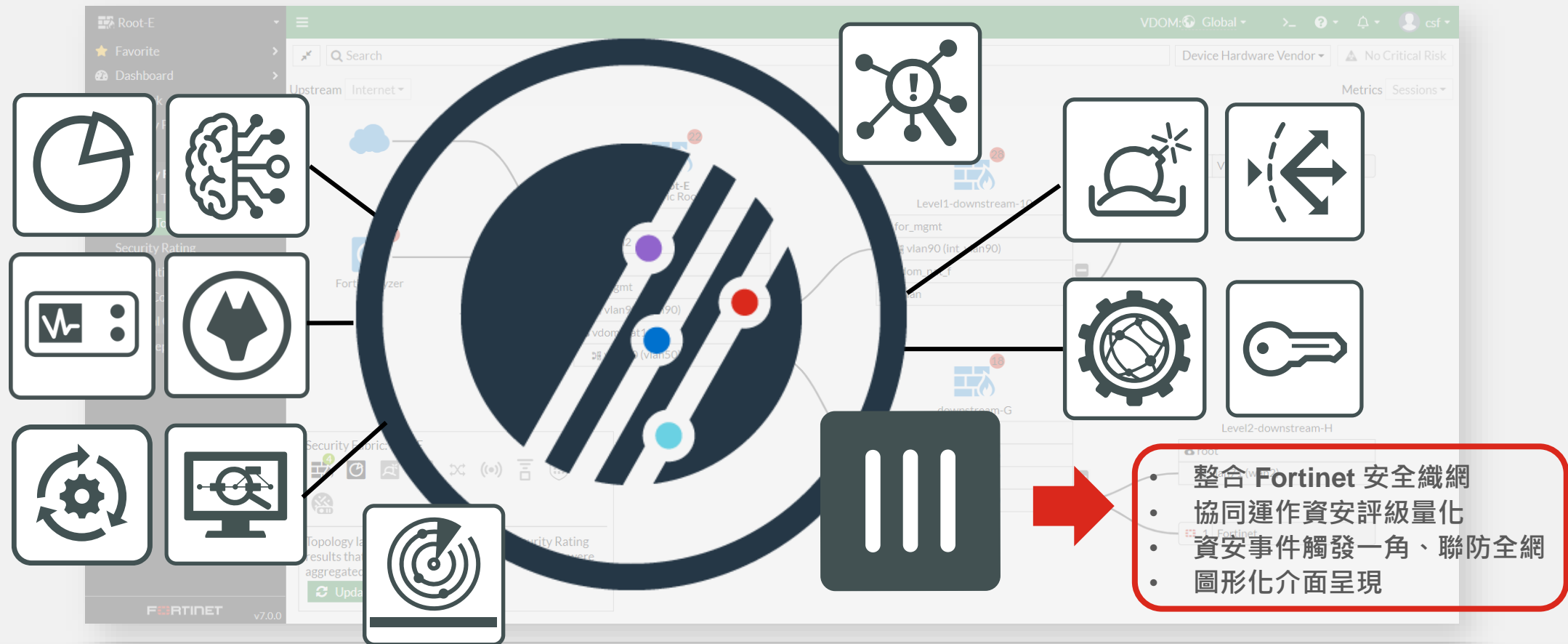
IoT / OT 辨識及防護



Fortinet 大家族齊聚一堂

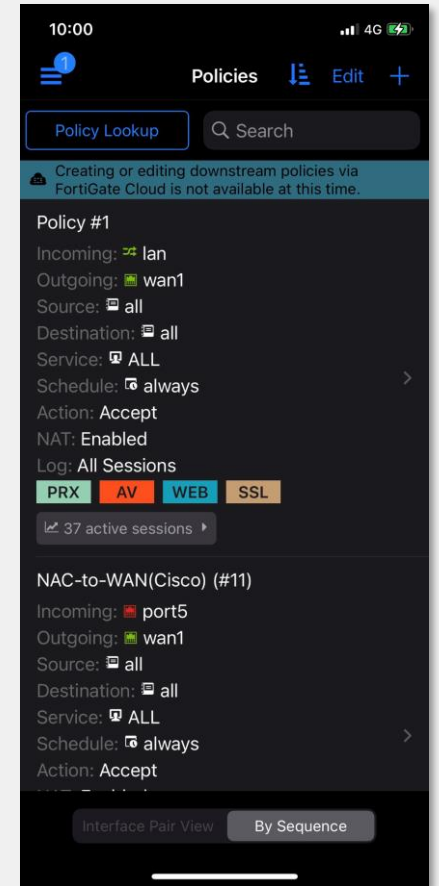
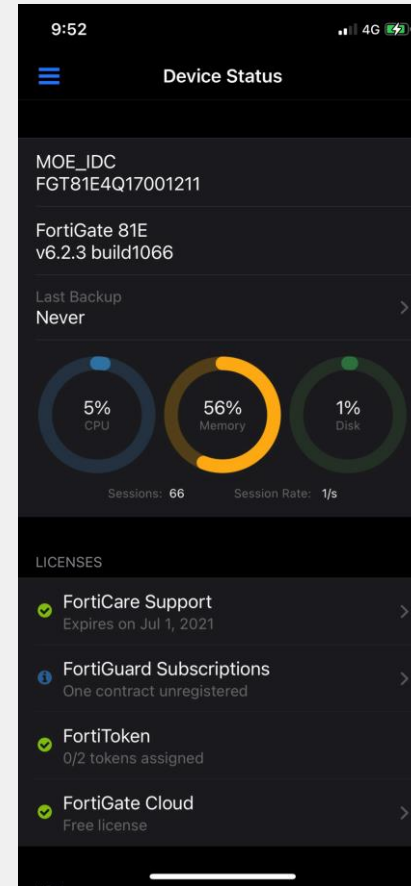
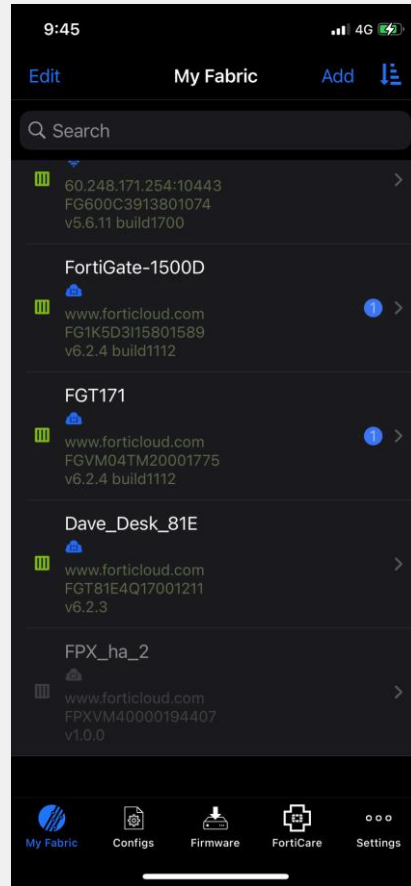
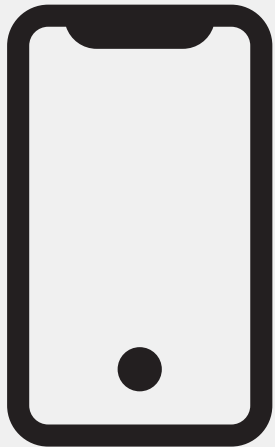
Score : 10 / 100

- Fortinet 的產品互相可以做到自動化及統一管理的功能



一機在手，希望無窮

Score : 20 / 100



你的專屬資安助理: Outbreak Alert

Score : 30 / 100

- FortiGuard 資安事件爆發警報將成為向客戶和合作夥伴傳達重要信息的機制。
- 當發生對網路安全產生重大影響並影響眾多組織的資安事件與攻擊時，即時更新 FortiGuard 爆發警報的鏈接
- 可以產出 HTML、PDF、XML 和 CSV 格式的報告

HAFNIUM, DearCry, and more

Targeting Exchange Servers with 0-day exploits

Issue	Impact	Targets
Microsoft has detected multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. (Device Security)	Threat actor use these vulnerabilities steal data and perform additional malicious actions that lead to further compromise. <u>DearCry</u> Ransomware is piggybacking on the original attack (Content Security)	HAFNIUM primary in the United States Industry sectors: infectious diseases, law firms, higher education institutions, defense policy think tanks Set 2 attacks like have a wider range

Background

On June 30 it was disclosed that the technical details and a proof-of-concept (PoC) exploit have been accidentally leaked for a currently unpatched vulnerability in Windows that allows remote code execution. Despite the need for authentication, the severity of the issue is critical as threat actors can use it to take over a Windows domain server to easily deploy malware across a company's network. The issue affects Windows Print Spooler and the researchers named it PrintNightmare.

Summary

This report displays the findings on attack attempts to exploit MS. Exchange vulnerabilities from Fortigate.

This table shows detections by FortiGate IPS:

FortiGate IPS Detection

#	Device	Source	Destination	Attack	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	172.16.68.21	111.206.21.075	HTTP.Unknown.Tunnelling	3	2021-04-13 18:12:50	2021-04-13 20:44:44
2	Van_Office_FW1_Master	172.18.34.35	74.125.124.94	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
3	Van_Office_FW1_Master	172.16.197.102	10.50.0.0	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
4	Van_Office_FW1_Master	172.16.171.64	172.18.22.48	MS.Exchange.Server.UM.Core.Remote.Co de.Execution	3	2021-04-13 18:12:50	2021-04-13 20:44:44
5	FGT91E4Q16000534	172.16.68.21	111.206.21.075	HTTP.Unknown.Tunnelling	1	2021-04-13 18:15:19	2021-04-13 18:15:19
6	FGT91E4Q16000534	172.16.171.64	172.18.22.48	MS.Exchange.Server.UM.Core.Remote.Co de.Execution	1	2021-04-13 18:15:19	2021-04-13 18:15:19
7	FGT91E4Q16000534	172.18.34.35	74.125.124.94	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19
8	FGT91E4Q16000534	172.16.197.102	10.50.0.0	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19

This table shows detections by FortiGate AV:

FortiGate AV Detection

#	Device	Source	Destination	Virus	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	HTML/Agent.A121tr	1	2021-04-13 20:44:55	2021-04-13 20:44:55
2	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	ASP/WebShell.cltr	1	2021-04-13 20:44:55	2021-04-13 20:44:55



Fortinet 鐵三角

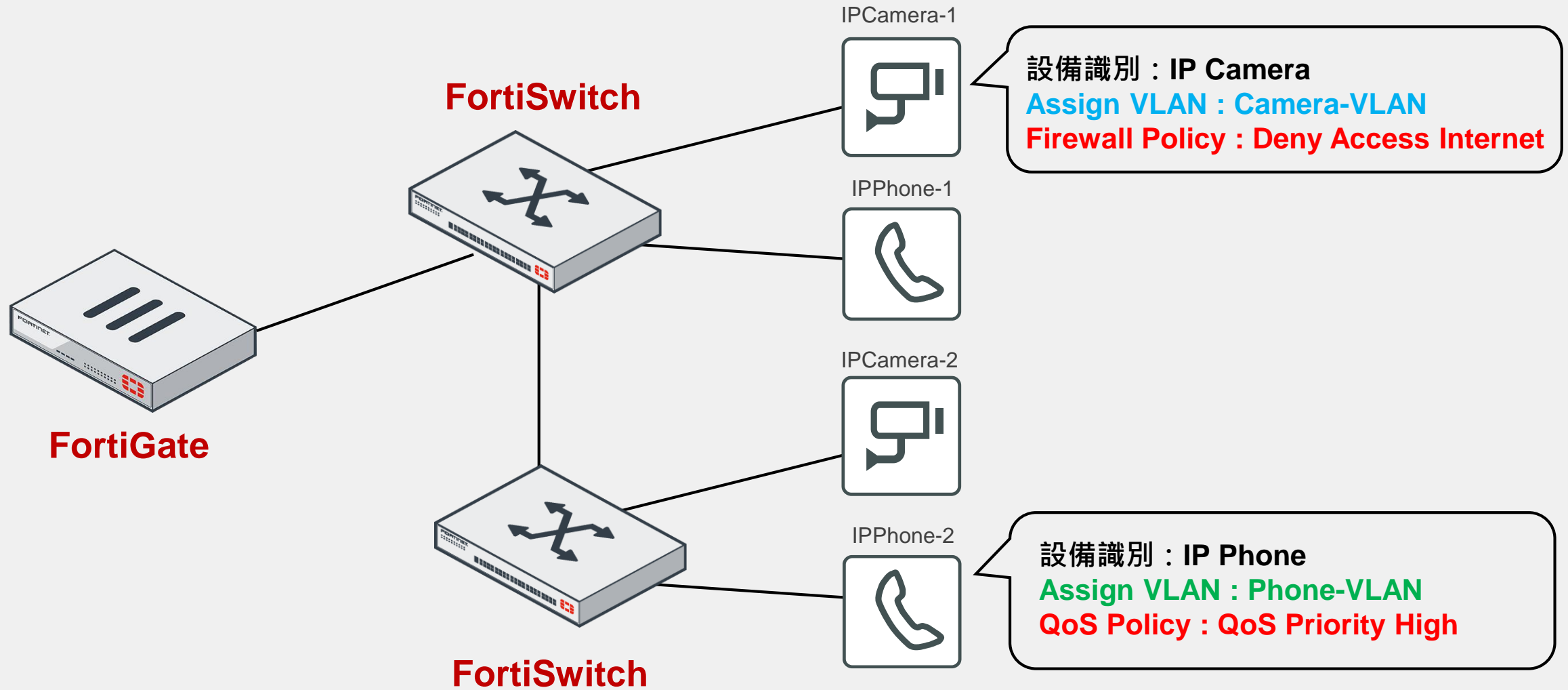
Score : 40 / 100

The screenshot displays the Fortinet FortiGate management console interface. At the top, there is a navigation bar with a search field, buttons for 'Access Device', 'No Access Device', and 'Device Traffic', and a status indicator for '7 Compromised Hosts'. Below this, a network topology diagram shows a host 'FG1KSD3115804861' connected to a high-availability pair of FortiGate devices: 'Demo-ISFW-PRI' and 'Demo-ISFW-BKP'. The main content area shows a host profile for IP address '10.88.23.9'. The profile includes fields for Device, Server, MAC Address, Interface, OS, Topology, Sessions, Bytes (Sent/Received), and Threat Score. A red triangle is drawn over the host profile, with five red hexagons containing the text: 'Anti-Virus', 'Web Filtering', 'IPS', 'Botnet', and 'Application Control'. A red arrow points downwards from the 'Web Filtering' hexagon. On the right side, there is a 'Sort By' dropdown set to 'Bytes (Sent/Received)' and a vertical list of three circular charts representing traffic for 'ACCESS-ENG', 'ACCESS-FIN', and 'ACCESS-SALES'. The bottom of the console shows a network diagram with a device labeled 'EM11C2V14007001'.



資安導向的網路環境 – NAC

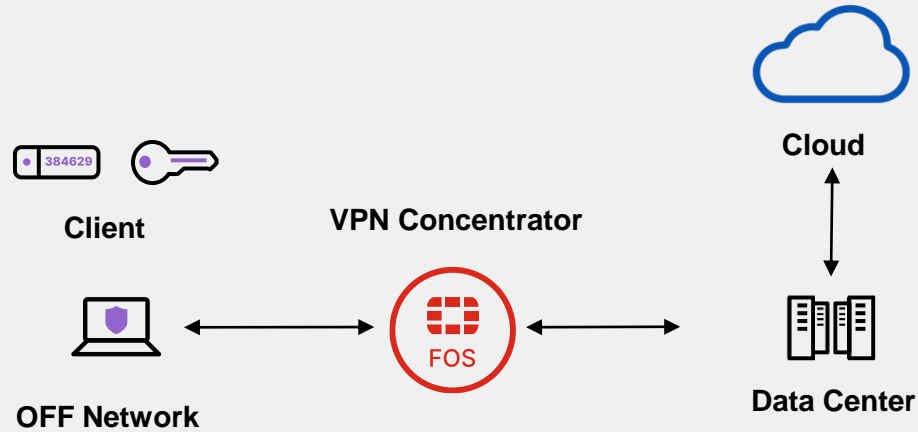
Score : 40 / 100



VPN



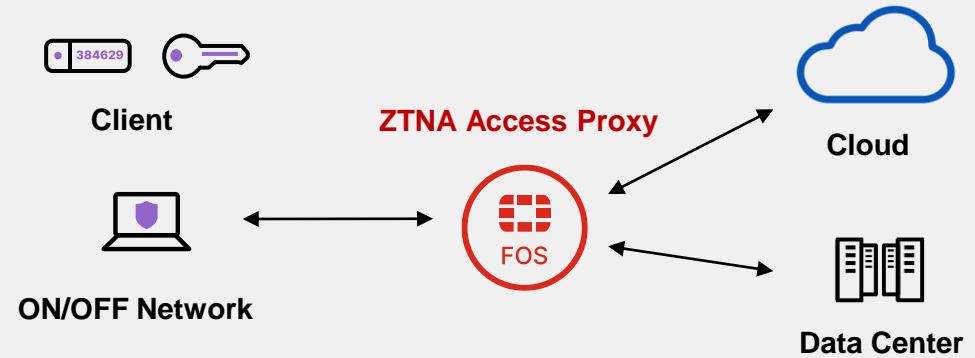
ZTNA Score : 50 / 100



登入時一次性的檢查

基於網段的存取

傳統的防火牆控制策略



持續性的資安狀態檢核

針對指定應用服務提供存取

使用者狀態上下文規則控制策略



Fortinet ZTNA 優勢

Score : 50 / 100

資安完整覆蓋 vs. 其他 ZTNA 解決方案

利用既有已投資的公司資產(次世代防火牆)

- 大多數的 ZTNA 解決方案是 SASE 服務商其中一項資安功能選項，伴隨著昂貴的訂閱費用
- 透過 FGT 可更快速的存取本地資料中心內的服務與資源
- 可運用 Fortinet SD-WAN, SD-Branch, Security Fabric 整合方案

專注於安全提升的 (“Secure ZTNA”)

- 延展 FGT 防護至企業提供服務的任何地方
- 存取流量穿越業界領導品牌 FortiGate 資安防護技術
- 提供 FortiGuard Labs services

資安完整覆蓋

- 只需啟用 FortiGate 和 FortiClient 中的 ZTNA 功能即可！
- 輕鬆的從 VPN Access 數位轉型至 ZTNA



Line 告警



Fortigate

自動阻擋惡意連線



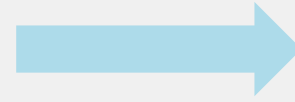
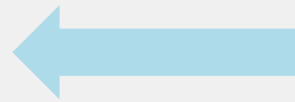
SOC 資料集中

內建 250 萬筆惡意 IP

可整合外部情資



FortiSIEM



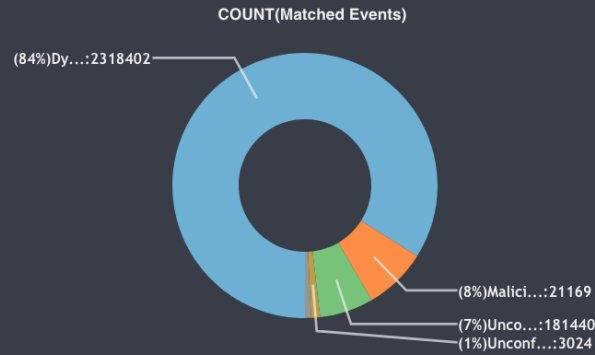
Aruba

自動隔離惡意使用者



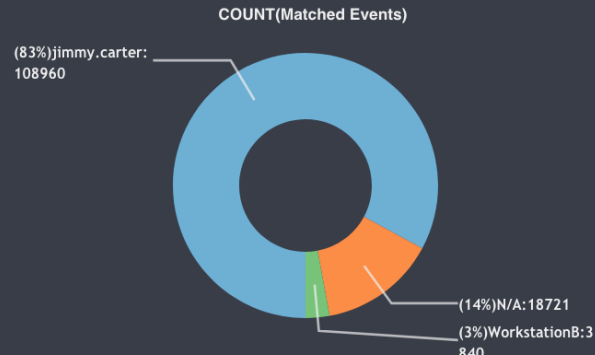
FortiEDR Top EDR Rules

Last 1 week@19:16

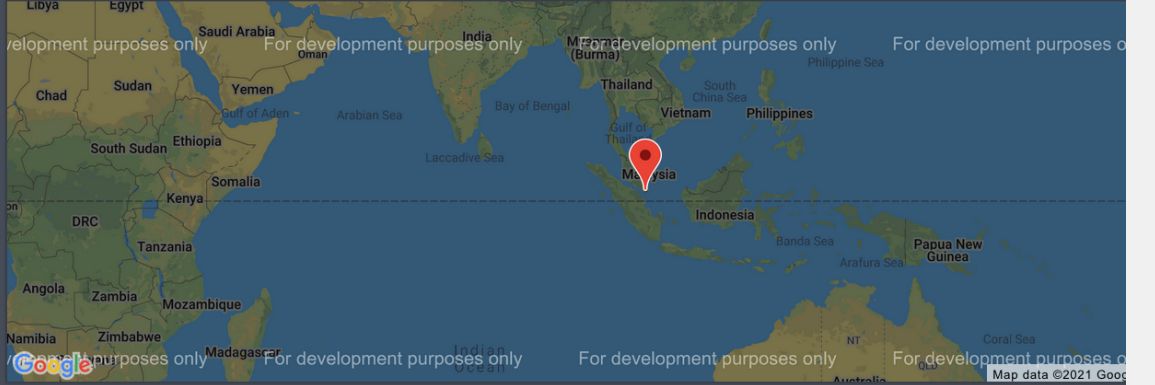


FortiEDR Top Users with Security Events

Last 8 hours@19:15



FortiEDR Top External Destinations



FortiEDR Security Events by Rule Name

Last 8 hours@19:15

Event Name	Firewall Action	Rule Name	COUNT(Matched Events)
FortiEDR blocked malicious file	Blocked (Simulation)	Malicious File Detected	8160
FortiEDR blocked suspicious file	Blocked	Dynamic Code - Malicious Runtime	2880
FortiEDR-Security-FortiEDR-Syslog-message-FortiEDR...	FortiEDR Syslog message		1920
FortiEDR blocked malicious file	Blocked (Simulation)	Unconfirmed Executable - Execution	1440
FortiEDR-Security-PUP-Blocked	Blocked (Simulation)	Malicious File Detected	1440
FortiEDR blocked suspicious file	Blocked	Suspicious Application - Connection	960
FortiEDR blocked inconclusive file	Blocked (Simulation)	Malicious File Detected	480

FortiEDR Security Events

Event Receive Time	Reporting IP	Event Name	Raw Event Log
Jan 25 2021, 05:03:26 PM	35.246.165.37	FortiEDR blocked malicious ...	<133>1 2020-10-22T10:50:39.000Z fortinetdem
Jan 25 2021, 05:03:26 PM	35.246.165.37	FortiEDR blocked inconclusi...	<133>1 2020-10-22T11:12:44.000Z fortinetdem
Jan 25 2021, 05:03:25 PM	35.246.165.37	FortiEDR blocked suspicious...	<133>1 2020-10-22T10:58:22.000Z fortinetdem
Jan 25 2021, 05:03:25 PM	35.246.165.37	FortiEDR blocked malicious ...	<133>1 2020-10-22T10:50:02.000Z fortinetdem
Jan 25 2021, 05:03:25 PM	35.246.165.37	FortiEDR blocked suspicious...	<133>1 2020-10-22T10:58:20.000Z fortinetdem
Jan 25 2021, 05:03:25 PM	35.246.165.37	FortiEDR blocked inconclusi...	<133>1 2020-10-22T10:54:26.000Z fortinetdem
Jan 25 2021, 05:03:25 PM	35.246.165.37	FortiEDR blocked inconclusi...	<133>1 2020-10-22T10:13:45.000Z fortinetdem

FortiEDR Malicious Files by Workstation

Last 8 hours@19:15

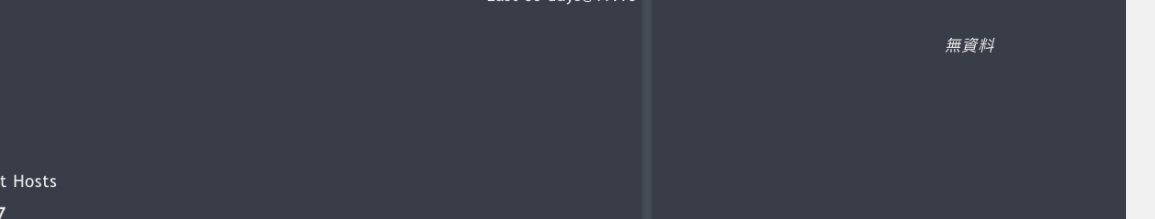
Source IP	File Name	COUNT(Matched Events)
192.168.1.155		110400
10.1.1.8		15360
192.168.1.69		3840
192.168.1.246		

Workstation Count



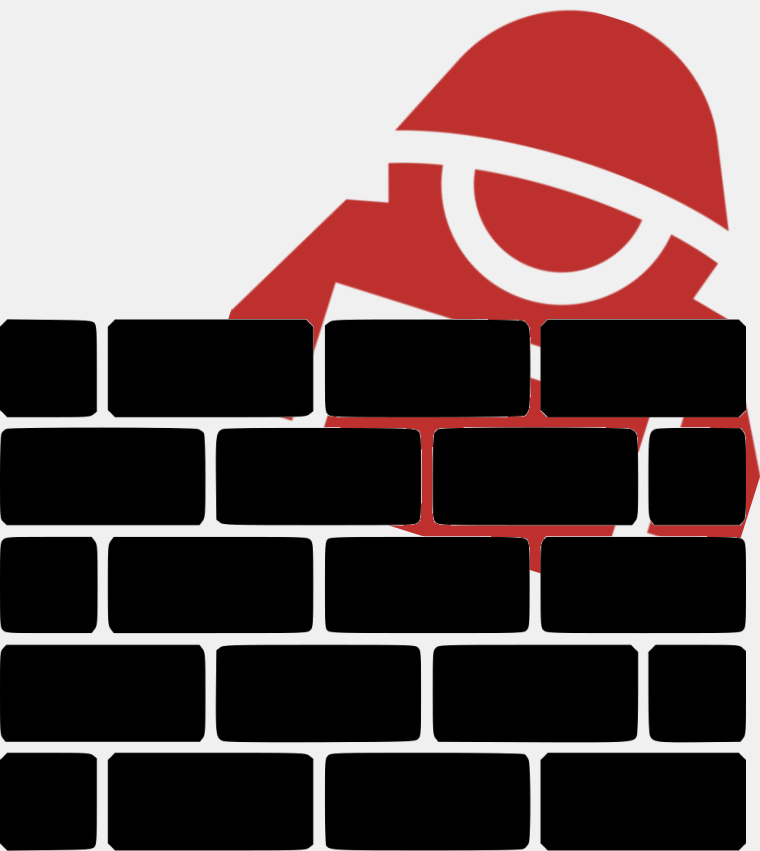
FortiEDR Most Targeted Application

Last 60 days@19:16

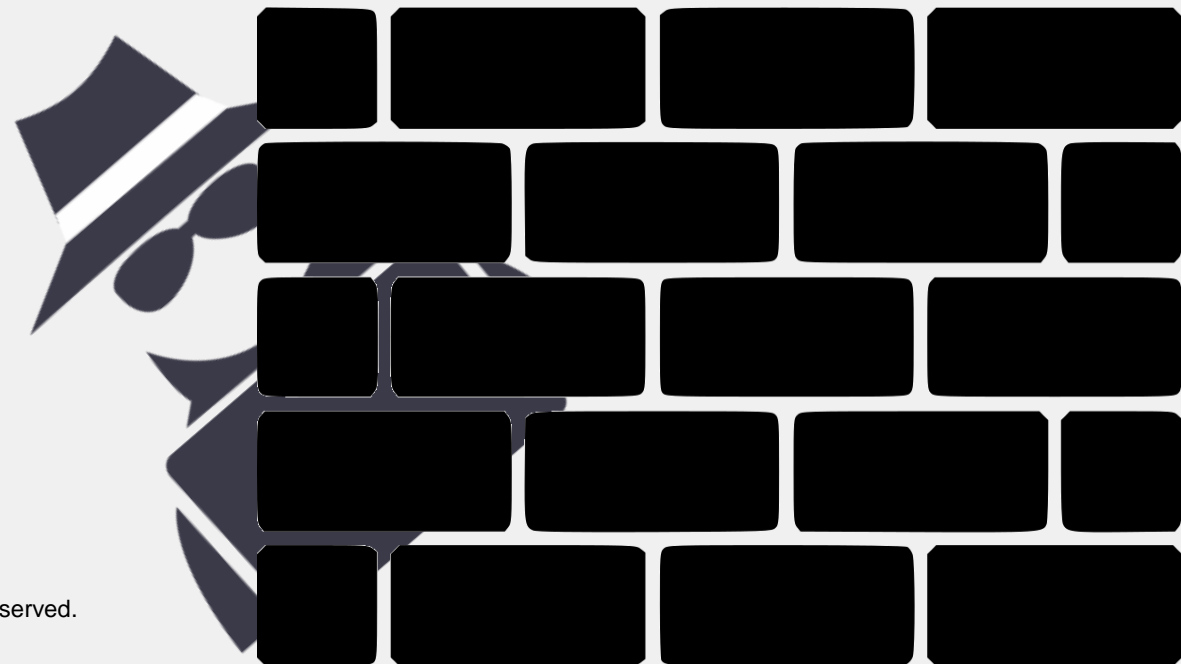


傳統資安 Mind

Score : 70 / 100



防禦不可能做到 100%

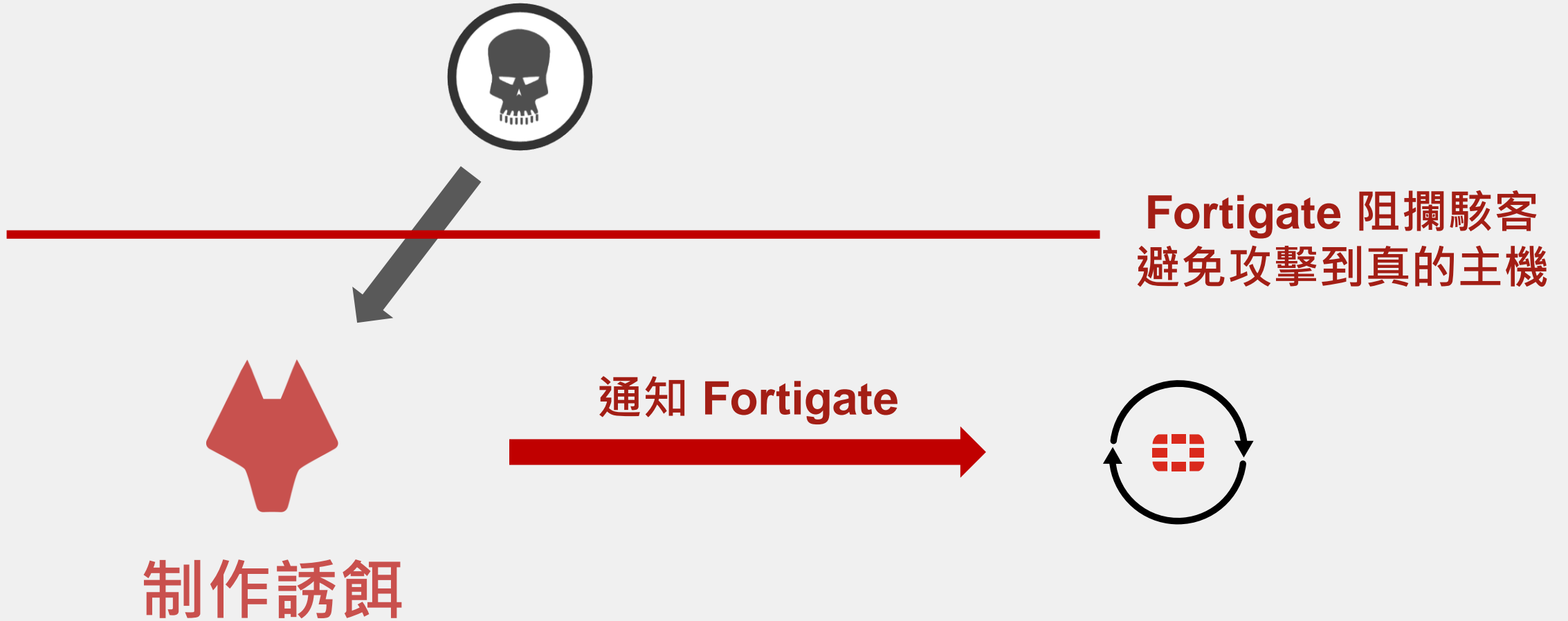


以駭客來思考的 Mind

Score : 70 / 100



駭客開始攻擊假主機



Why FortiDeceptor

Score : 70 / 100



新世代解決方案：
利用部署誘餌，即時引出內部及外部的侵入者
並且聯動第一時間做防護。



IPS – 入侵偵測



AV – 惡意軟件偵測



WF – 網頁瀏覽偵測



ARAE – 自動尋找弱點



RTT – 即時找尋駭客蹤跡

FortiEDR, 勒索不再怕

Score : 80 / 100



路徑關聯



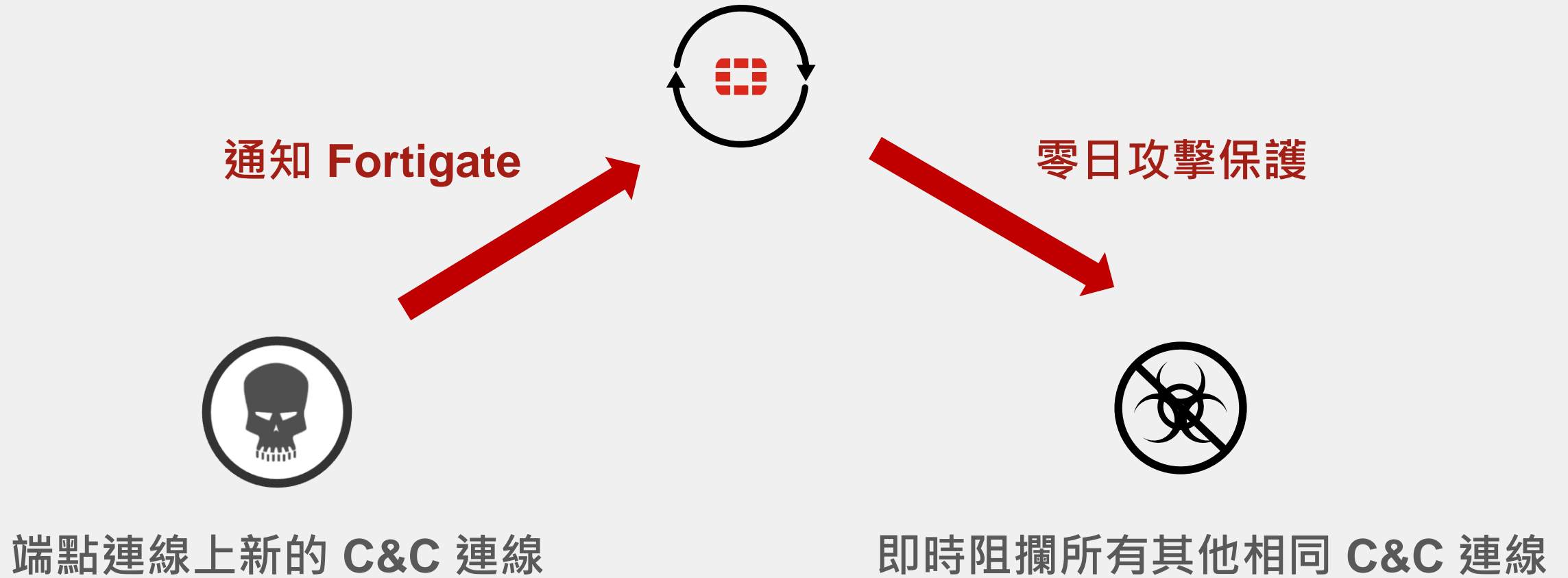
行為分析



扼殺勒索

整合 Fortigate, 全面性防禦

Score : 80 / 100



FortiGuard Security Services

SOC & NOC

- Content Security
- Web Security
- Advanced SOC/NOC

User Security

- User Security
- Device Security
- Bundled Security

Fabric Management Center - SOC

Endpoint

- FortiEDR
- FortiXDR

Breach

- FortiSandbox
- FortiDeceptor
- FortiAI

Incident Response

- FortiAnalyzer
- FortiSIEM
- FortiSOAR
- FortiGuard MDR Service

Fabric Management Center - NOC

- FortiManager
- FortiCloud
- FortiMonitor

Open Ecosystem

- Connector
- Fabric API
- DevOps
- Extended Fabric Ecosystem

Zero Trust Access

- FortiClient
- FortiNAC
- FortiVoice
- FortiToken
- FortiAuthenticator
- FortiCamera

Security-Driven Networking

LAN Edge

- FortiAP
- FortiSwitch

WAN Edge

- FortiGate SD-WAN
- FortiExtender

DC Edge

- FortiGate
- FortiProxy

Cloud Edge

- FortiSASE
- FortiSolator

Adaptive Cloud Security

Network

- FortiGate VM
- Multi-cloud SD-WAN
- FortiDDos

Platform

- FortiCASB
- FortiCWP
- Cloud Security Posture Management

Applications

- FortiWeb
- FortiMail
- FortiADC
- FortiGSLB



Security Mind

Score : 100 / 100



With Fortinet



FORTINET®