FORTINET

OT 資安不再若有似無

Degas Tsao / 曹仁賢 / Security Consultant

May 2024

FORTINET

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

防火牆放哪裡!!! 資安需求在哪裡???

Access Limited to Authorized Personnel

OT無所不在

製造業

能源及基礎設施

運輸業

© Fortinet Inc. All Rights Reserved.

工控安全藍圖

具有Fortinet安全之網的標準OT資安框架

Information Technology

Fortinet Security Fabric

Remote Access
- 3rd Party Access
- Remote Worker Access

VPN

Wide Area
- SD-WAN
- 3G/4G/5G Extension
- VPN

SD-WAN

Operational Technology

Operations & Control Zones

Management & Analytics
- Security Incident & Event Management, Orchestration & Automation

FortiSandbox

Advanced Threat Protection
- AI, Sandbox and Deception

FortiToken

FortiNAC

Authentication
- Identity & Access Management,
- Behavior Analytics

FortiDeceptor

Forticonnect

Internal Segmentation
- Next Gen Firewall
- Enterprise Protection

FortiGate

Zones of Control
- Zones and Conduits
- Micro Segmentation
- Physical & Virtual Segmentation

FortiSwitch

Control Area Zones

Application & Traffic Visibility
- Next Gen Firewall
- Industrial Threat Feed
- Application Control
- IPS

FortiGate

FortiGuard Industrial Security Service

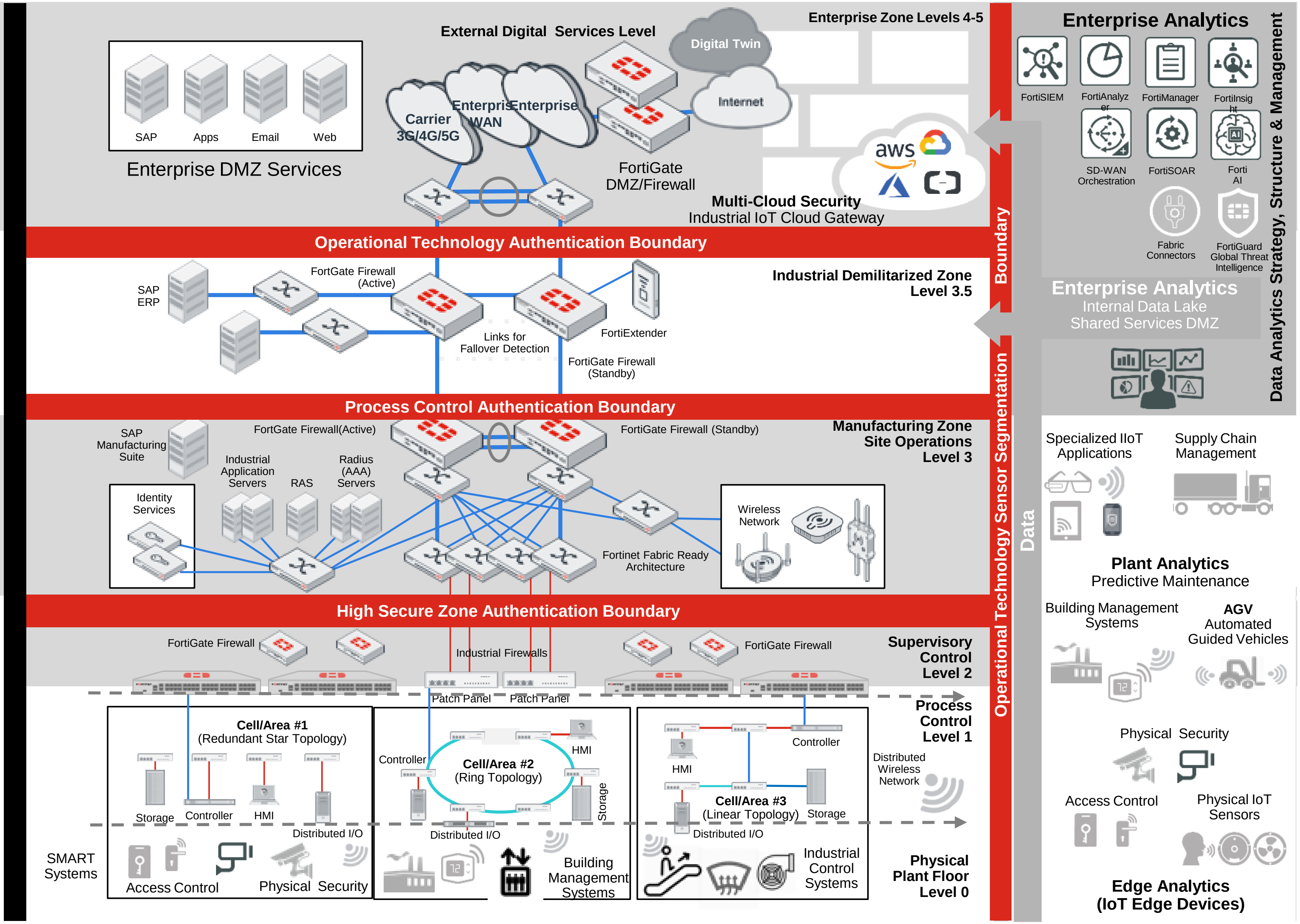
Zones of Control
- Zones and Conduits
- Micro Segmentation
- Physical & Virtual Segmentation

FortiNAC

Secure Access
- Industrial L2 Switching and WiFi
- Network Access Control

FortiEDR

Endpoint
- Advanced Endpoint Detection and Response



Enterprise Zone Levels 4-5
External Digital Services Level
Digital Twin
SAP
Apps
Email
Web
Enterprise DMZ Services
Carrier 3G/4G/5G
Enterprise WAN
Enterprise
Internet
FortiGate DMZ/Firewall
Multi-Cloud Security
Industrial IoT Cloud Gateway
Operational Technology Authentication Boundary
SAP ERP
FortGate Firewall (Active)
Links for Fallover Detection
FortiExtender
FortiGate Firewall (Standby)
Industrial Demilitarized Zone Level 3.5
Process Control Authentication Boundary
SAP Manufacturing Suite
FortGate Firewall(Active)
FortiGate Firewall (Standby)
Manufacturing Zone Site Operations Level 3
Industrial Application Servers
RAS
Radius (AAA) Servers
Identity Services
Wireless Network
Fortinet Fabric Ready Architecture
High Secure Zone Authentication Boundary
FortiGate Firewall
Industrial Firewalls
FortiGate Firewall
Supervisory Control Level 2
Patch Panel
Patch Panel
Process Control Level 1
Cell/Area #1 (Redundant Star Topology)
Storage
Controller
HMI
Distributed I/O
Controller
Cell/Area #2 (Ring Topology)
HMI
Storage
Distributed I/O
Controller
HMI
Cell/Area #3 (Linear Topology)
Storage
Distributed I/O
Distributed Wireless Network
SMART Systems
Access Control
Physical Security
Building Management Systems
Industrial Control Systems
Physical Plant Floor Level 0
Operational Technology Sensor Segmentation Boundary
Data
Enterprise Analytics
FortiSIEM
FortiAnalyzer
FortiManager
FortiInsight
SD-WAN Orchestration
FortiSOAR
Forti AI
Fabric Connectors
FortiGuard Global Threat Intelligence
Enterprise Analytics
Internal Data Lake
Shared Services DMZ
Data Analytics Strategy, Structure & Management
Specialized IIoT Applications
Supply Chain Management
Plant Analytics
Predictive Maintenance
Building Management Systems
AGV
Automated Guided Vehicles
Physical Security
Access Control
Physical IoT Sensors
Edge Analytics (IoT Edge Devices)

最廣的資訊安全平台

50+ 緊密整合的產品線

Fortinet 網路安全平台可保護整個攻擊面，同時緊密整合到客戶目前和未來的基礎架構中

網路安全

Network Firewall
Wireless and Wired LAN
5G
OT Security
NAC

完整覆蓋的SASE

SD-WAN
SSE
Single-Vendor SASE
ZTNA
DEM
Cloud Firewall
WAF

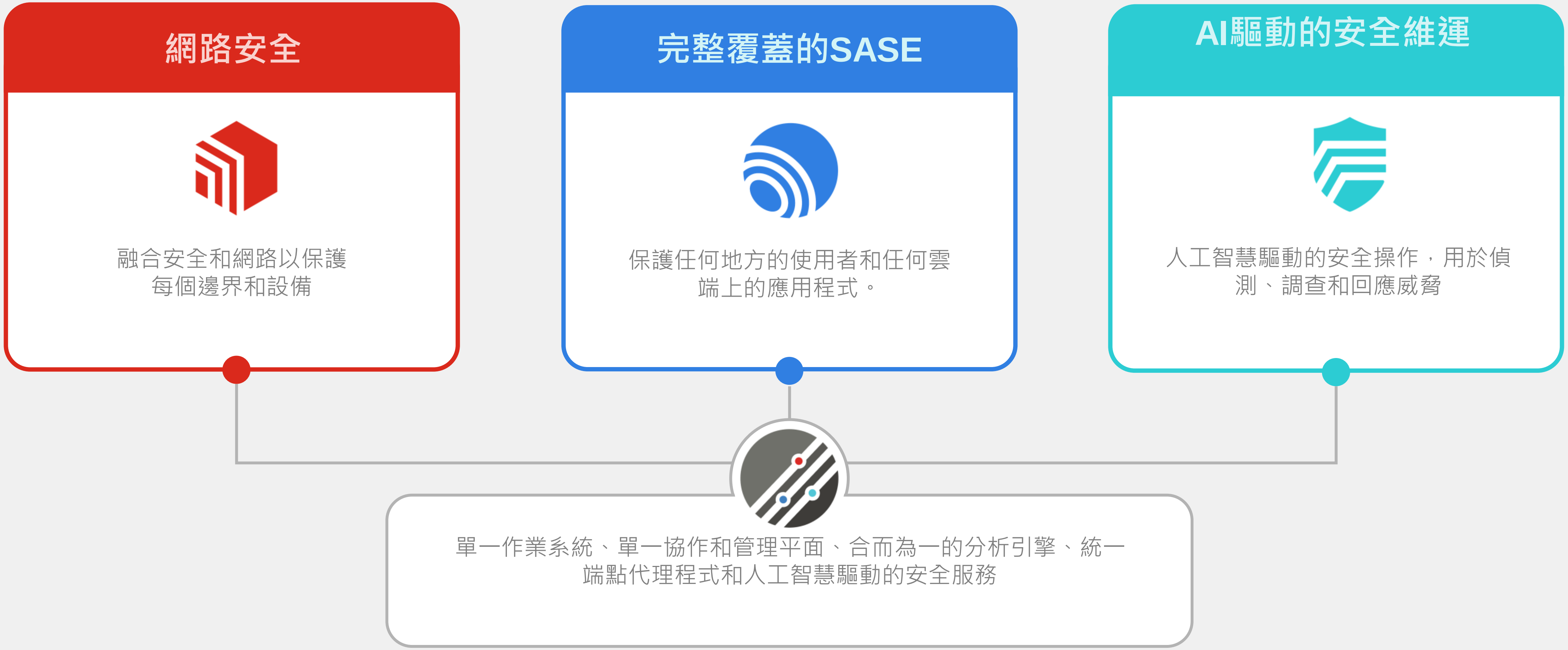
維運安全

SIEM
SOAR
EDR/XDR
NDR
Deception
Email Security

© Fortinet Inc. All Rights Reserved.

Fortinet 安全織網願景

資訊安全無所不在



網路安全

融合安全和網路以保護
每個邊界和設備

完整覆蓋的SASE

保護任何地方的使用者和任何雲
端上的應用程式。

AI驅動的安全維運

人工智慧驅動的安全操作，用於偵
測、調查和回應威脅

單一作業系統、單一協作和管理平面、合而為一的分析引擎、統一
端點代理程式和人工智慧驅動的安全服務

單一平台 –Fortinet安全織網

網路安全

覆蓋

所有邊緣、使用者和裝置的安全和網路融合

維運安全

統整

整合的安全營運平台可加快偵測和回應時間

完整覆蓋的 SASE

服務

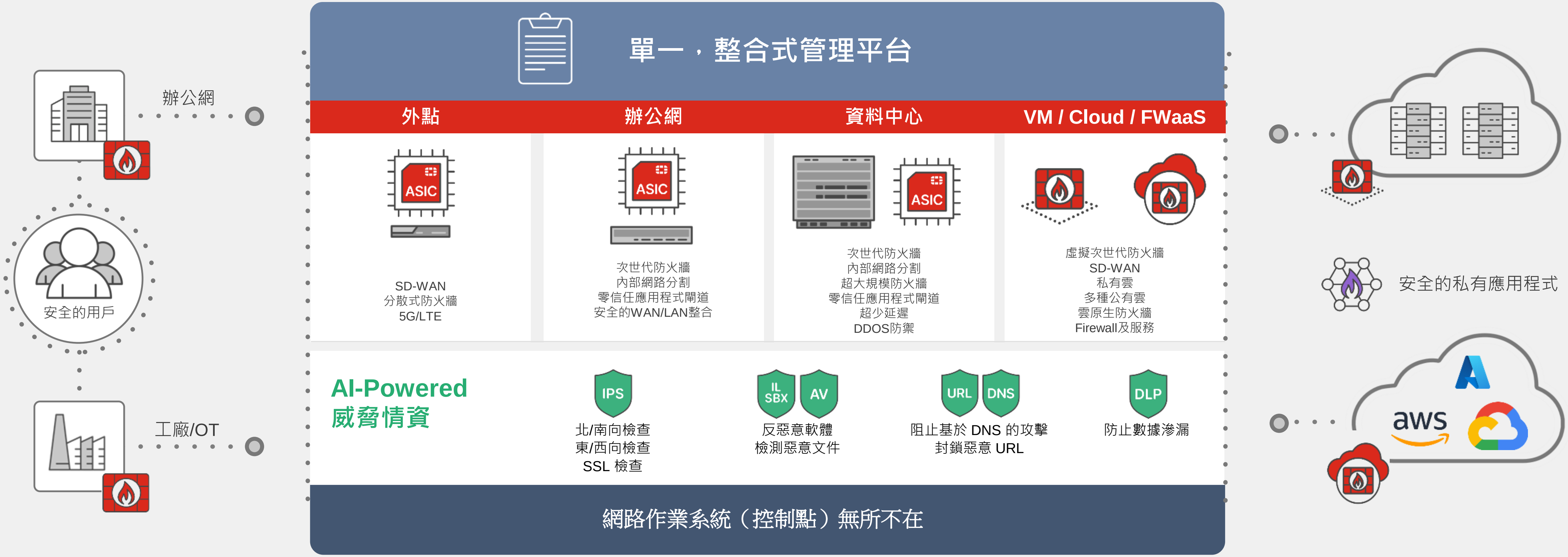
靈活使用安全服務，以確保存取安全並保護任何雲端上的網路、應用程式和數據

OS

- AI驅動技術
- FortiCloud
- FortiPoints
- FortiGuard Labs
- OT 資訊安全平台
- 生態系統

© Fortinet Inc. All Rights Reserved.

次世代防火牆到完整覆蓋的混合式防火牆



辦公網

安全的用戶

工廠/OT

單一，整合式管理平台

外點	辦公網	資料中心	VM / Cloud / FWaaS
SD-WAN 分散式防火牆 5G/LTE	次世代防火牆 內部網路分割 零信任應用程式閘道 安全的WAN/LAN整合	次世代防火牆 內部網路分割 超大規模防火牆 零信任應用程式閘道 超少延遲 DDOS防禦	虛擬次世代防火牆 SD-WAN 私有雲 多種公有雲 雲原生防火牆 Firewall及服務

AI-Powered 威脅情資

IPS
北/南向檢查
東/西向檢查
SSL 檢查

IL SBX / AV
反惡意軟體
檢測惡意文件

URL / DNS
阻止基於 DNS 的攻擊
封鎖惡意 URL

DLP
防止數據滲漏

網路作業系統（控制點）無所不在

安全的私有應用程式

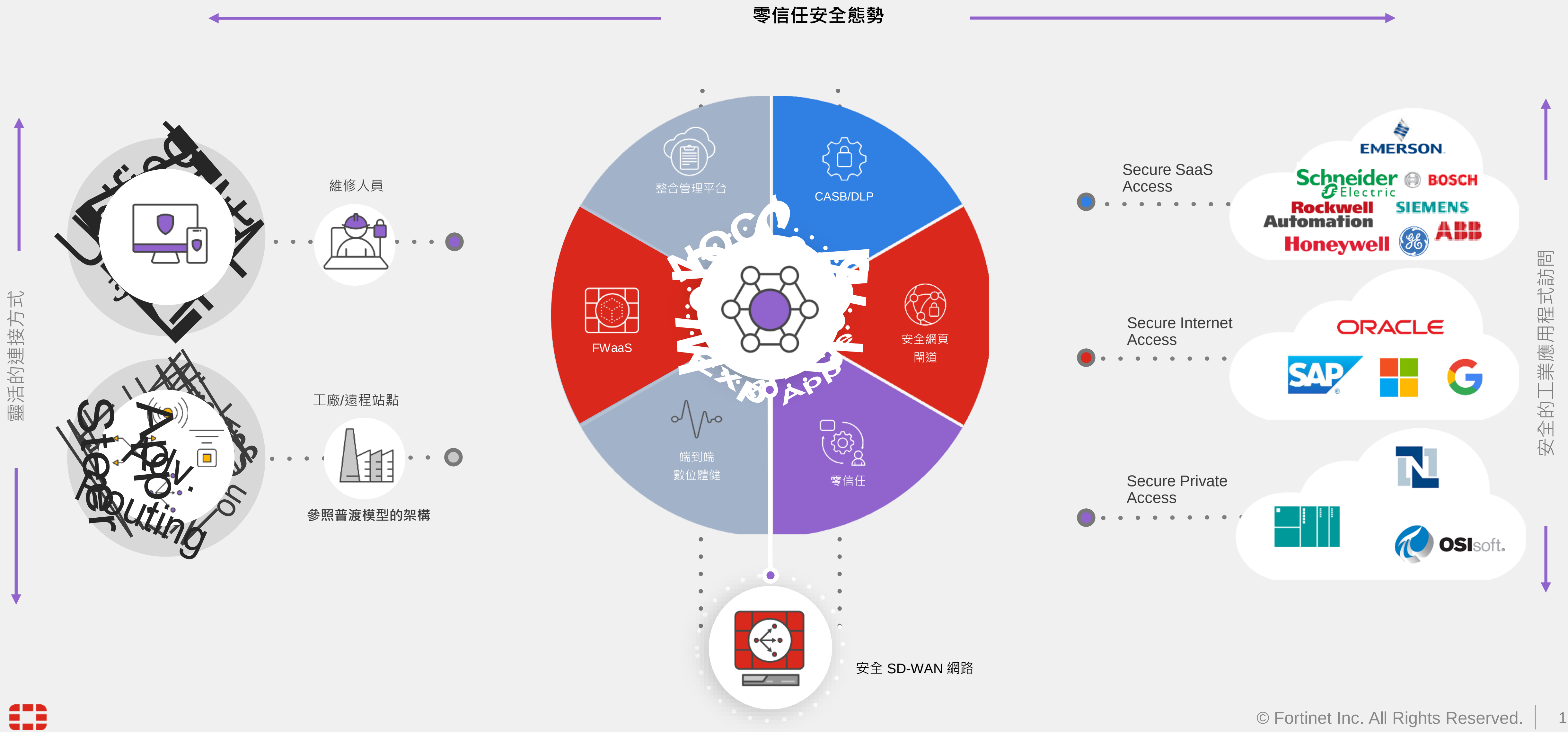
到 2026 年，超過 60% 的組織將部署不只一種類型的防火牆，這將促進混合覆蓋的防火牆採用。

Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hils, Tom Lintemuth, December 2022.

© Fortinet Inc. All Rights Reserved.

提供OT資產擁有者的完整覆蓋SASE

IT-OT 安全邊界之上的一致安全態勢



零信任安全態勢

靈活的連接方式

維修人員

工廠/遠程站點

參照普渡模型的架構

整合管理平台

CASB/DLP

FWaaS

安全網頁閘道

端到端數位體健

零信任

安全 SD-WAN 網路

Secure SaaS Access

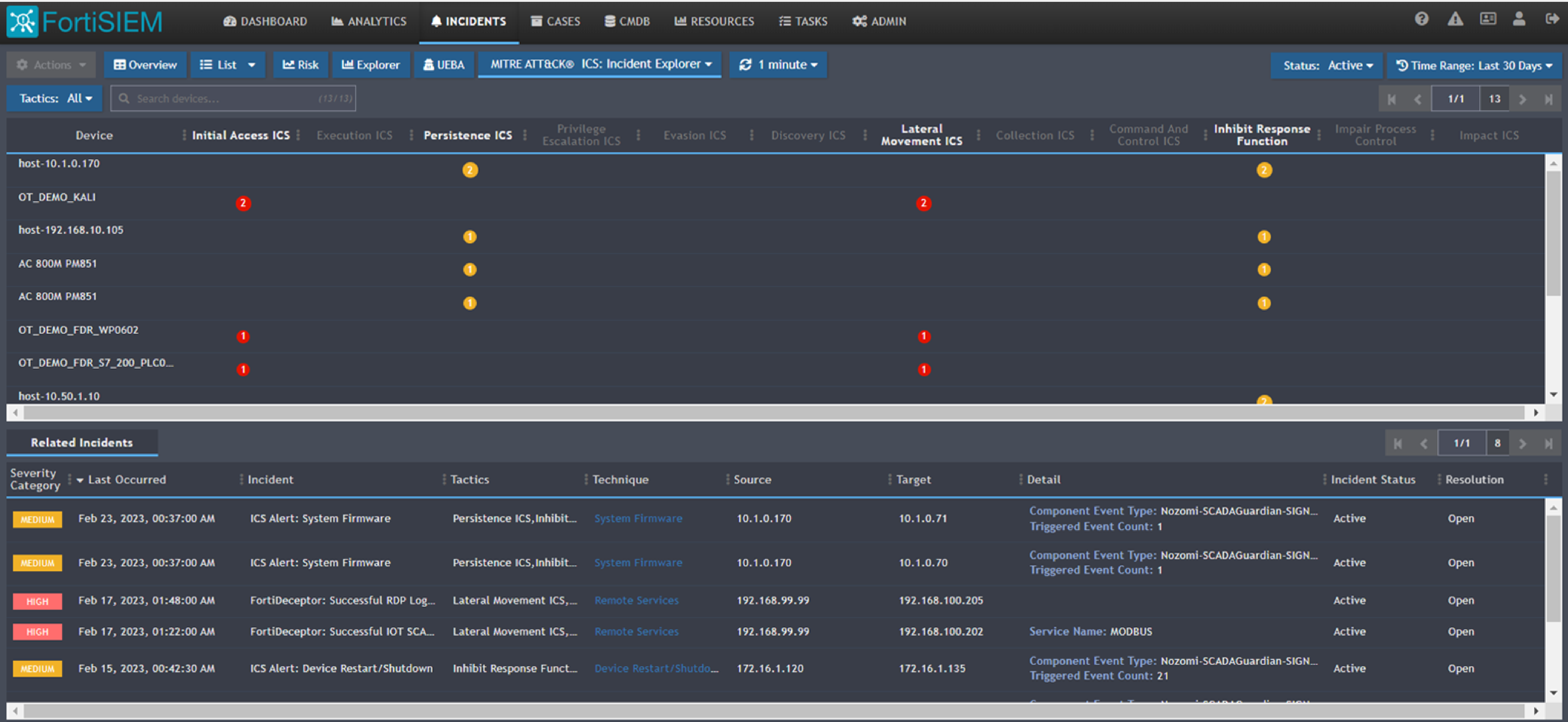
Secure Internet Access

Secure Private Access

安全的工業應用程式訪問

MITRE ATT&CK (OT)資安對抗策略、手段告警圖

觸發告警主機在資安攻擊鏈所處的狀態 – ICS/OT

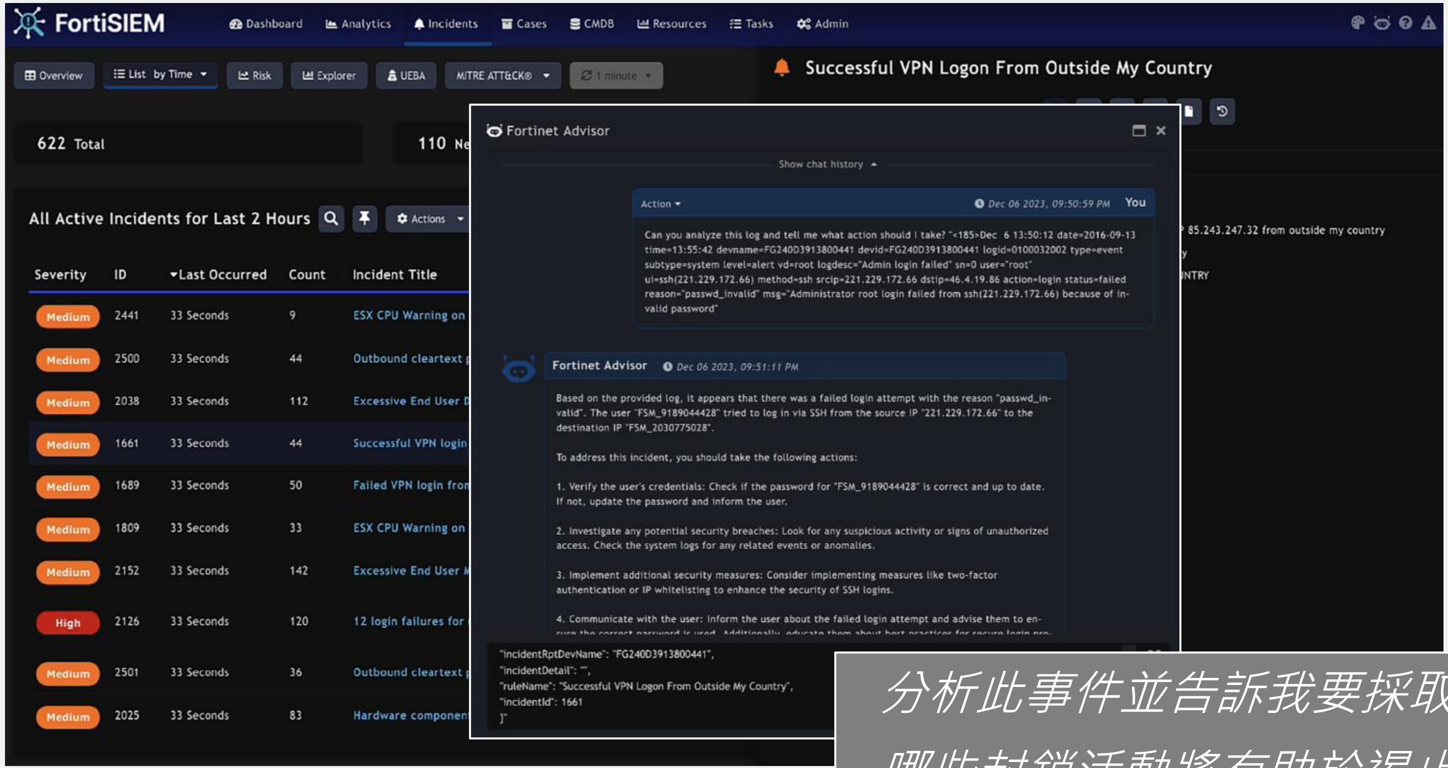


Device	Initial Access ICS	Execution ICS	Persistence ICS	Privilege Escalation ICS	Evasion ICS	Discovery ICS	Lateral Movement ICS	Collection ICS	Command And Control ICS	Inhibit Response Function	Impair Process Control	Impact ICS
host-10.1.0.170			2							2		
OT_DEMO_KALI	2						2					
host-192.168.10.105			1							1		
AC 800M PM851			1							1		
AC 800M PM851			1							1		
OT_DEMO_FDR_WP0602	1						1					
OT_DEMO_FDR_S7_200_PLC0...	1						1					
host-10.50.1.10										2		

Related Incidents

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail	Incident Status	Resolution
MEDIUM	Feb 23, 2023, 00:37:00 AM	ICS Alert: System Firmware	Persistence ICS,Inhibit...	System Firmware	10.1.0.170	10.1.0.71	Component Event Type: Nozomi-SCADAGuardian-SIGN... Triggered Event Count: 1	Active	Open
MEDIUM	Feb 23, 2023, 00:37:00 AM	ICS Alert: System Firmware	Persistence ICS,Inhibit...	System Firmware	10.1.0.170	10.1.0.70	Component Event Type: Nozomi-SCADAGuardian-SIGN... Triggered Event Count: 1	Active	Open
HIGH	Feb 17, 2023, 01:48:00 AM	FortiDeceptor: Successful RDP Log...	Lateral Movement ICS,...	Remote Services	192.168.99.99	192.168.100.205		Active	Open
HIGH	Feb 17, 2023, 01:22:00 AM	FortiDeceptor: Successful IOT SCA...	Lateral Movement ICS,...	Remote Services	192.168.99.99	192.168.100.202	Service Name: MODBUS	Active	Open
MEDIUM	Feb 15, 2023, 00:42:30 AM	ICS Alert: Device Restart/Shutdown	Inhibit Response Funct...	Device Restart/Shutdo...	172.16.1.120	172.16.1.135	Component Event Type: Nozomi-SCADAGuardian-SIGN... Triggered Event Count: 21	Active	Open

FortiAI – FortiSIEM 關鍵應用案例



Severity	ID	Last Occurred	Count	Incident Title
Medium	2441	33 Seconds	9	ESX CPU Warning on
Medium	2500	33 Seconds	44	Outbound cleartext
Medium	2038	33 Seconds	112	Excessive End User
Medium	1661	33 Seconds	44	Successful VPN login
Medium	1689	33 Seconds	50	Failed VPN login from
Medium	1809	33 Seconds	33	ESX CPU Warning on
Medium	2152	33 Seconds	142	Excessive End User
High	2126	33 Seconds	120	12 login failures for
Medium	2501	33 Seconds	36	Outbound cleartext
Medium	2025	33 Seconds	83	Hardware component

You Dec 06 2023, 09:50:59 PM

Can you analyze this log and tell me what action should I take? "<185>Dec 6 13:50:12 date=2016-09-13 time=13:55:42 devname=FG240D3913800441 devid=FG240D3913800441 logid=0100032002 type=event subtype=system level=alert vd=root logdesc="Admin login failed" sn=0 user="root" ui=ssh(221.229.172.66) method=ssh srcip=221.229.172.66 dstip=46.4.19.86 action=login status=failed reason="passwd_invalid" msg="Administrator root login failed from ssh(221.229.172.66) because of invalid password"

Fortinet Advisor Dec 06 2023, 09:51:11 PM

Based on the provided log, it appears that there was a failed login attempt with the reason "passwd_invalid". The user "FSM_9189044428" tried to log in via SSH from the source IP "221.229.172.66" to the destination IP "FSM_2030775028".

To address this incident, you should take the following actions:

1. Verify the user's credentials: Check if the password for "FSM_9189044428" is correct and up to date. If not, update the password and inform the user.

2. Investigate any potential security breaches: Look for any suspicious activity or signs of unauthorized access. Check the system logs for any related events or anomalies.

3. Implement additional security measures: Consider implementing measures like two-factor authentication or IP whitelisting to enhance the security of SSH logins.

4. Communicate with the user: Inform the user about the failed login attempt and advise them to ensure the correct password is used. Additionally, educate them about best practices for secure login pro-

```
"incidentRptDevName": "FG240D3913800441",
"incidentDetail": "",
"ruleName": "Successful VPN Logon From Outside My Country",
"incidentId": 1661
]"
```

解釋日誌和事件、提供建議操作、使用自然語言建立豐富的查詢和報告等等...

分析此事件並告訴我要採取什麼行動

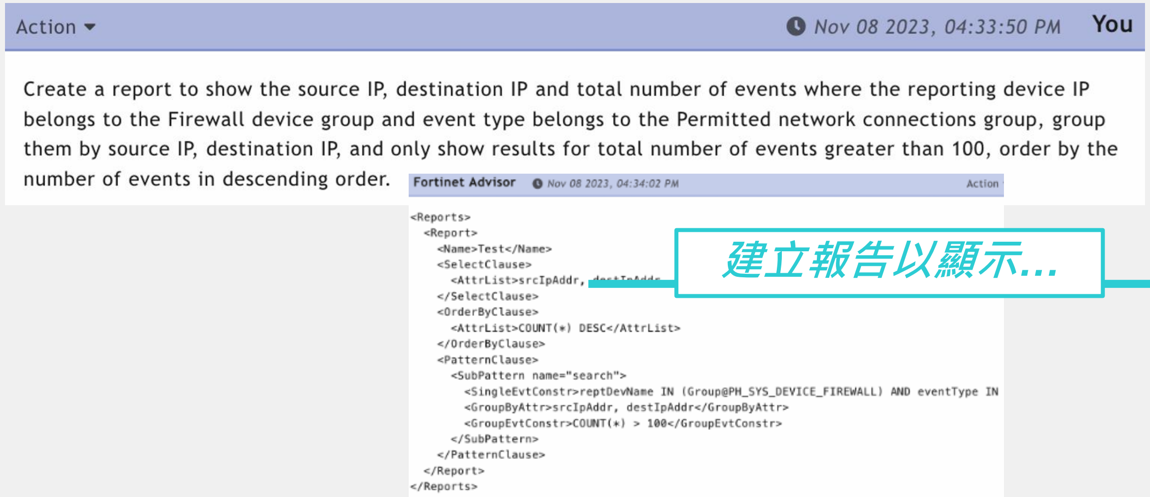
哪些封鎖活動將有助於遏止此事件？

建立過去 30 天內每個關鍵事件的事件報告

取得我的環境中最新的已知漏洞

FortiAI for FortiSIEM

自然語言和選單驅動的互動可協助事件管理等



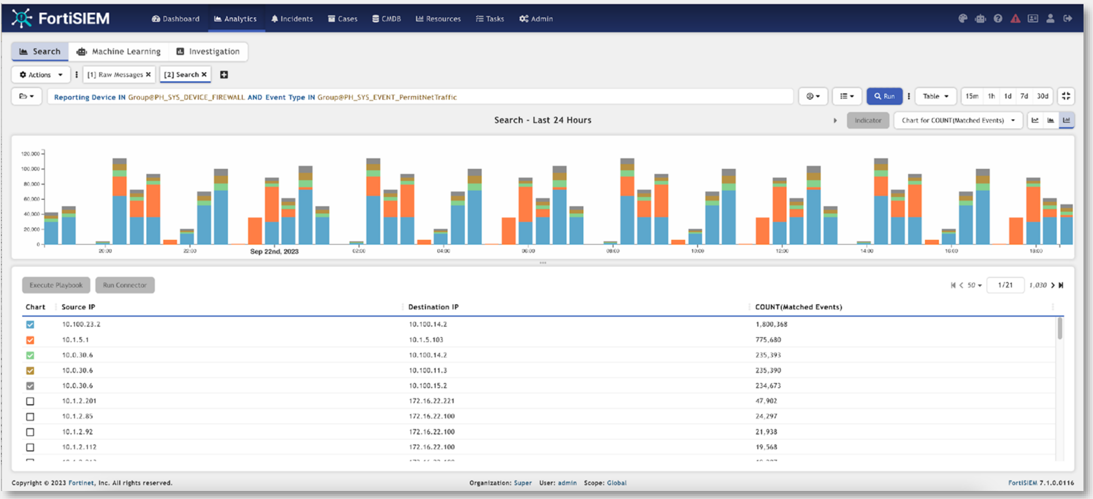
Nov 08 2023, 04:33:50 PM **You**

Create a report to show the source IP, destination IP and total number of events where the reporting device IP belongs to the Firewall device group and event type belongs to the Permitted network connections group, group them by source IP, destination IP, and only show results for total number of events greater than 100, order by the number of events in descending order.

Fortinet Advisor Nov 08 2023, 04:34:02 PM

```
<Reports>
  <Report>
    <Name>Test</Name>
    <SelectClause>
      <AttrList>srcIpAddr, destIpAddr
    </SelectClause>
    <OrderByClause>
      <AttrList>COUNT(*) DESC</AttrList>
    </OrderByClause>
    <PatternClause>
      <SubPattern name="search">
        <SingleEvtConstr>reptDevName IN (Group@PH_SYS_DEVICE_FIREWALL) AND eventType IN
        <GroupByAttr>srcIpAddr, destIpAddr</GroupByAttr>
        <GroupEvtConstr>COUNT(*) > 100</GroupEvtConstr>
      </SubPattern>
    </PatternClause>
  </Report>
</Reports>
```

建立報告以顯示...

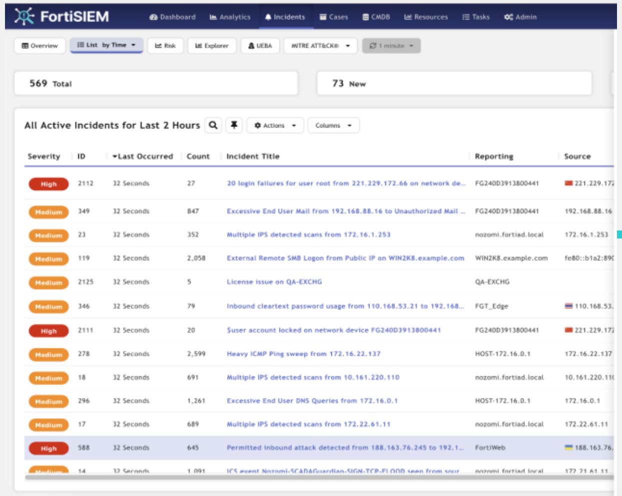


Reporting Device IN Group@PH_SYS_DEVICE_FIREWALL AND Event Type IN Group@PH_SYS_EVENT_PermitNetTraffic

Search - Last 24 Hours

Chart	Source IP	Destination IP	COUNT(Matched Events)
☑	10.100.23.2	10.100.14.2	1,800,368
☑	10.1.5.1	10.1.5.103	775,680
☑	10.0.30.6	10.100.14.2	235,393
☑	10.0.30.6	10.100.11.3	235,390
☑	10.0.30.6	10.100.15.2	234,673
☐	10.1.2.201	172.16.22.221	47,902
☐	10.1.2.85	172.16.22.100	24,297
☐	10.1.2.92	172.16.22.100	21,938
☐	10.1.2.112	172.16.22.100	19,568

Copyright © 2023 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 7.1.0.0116



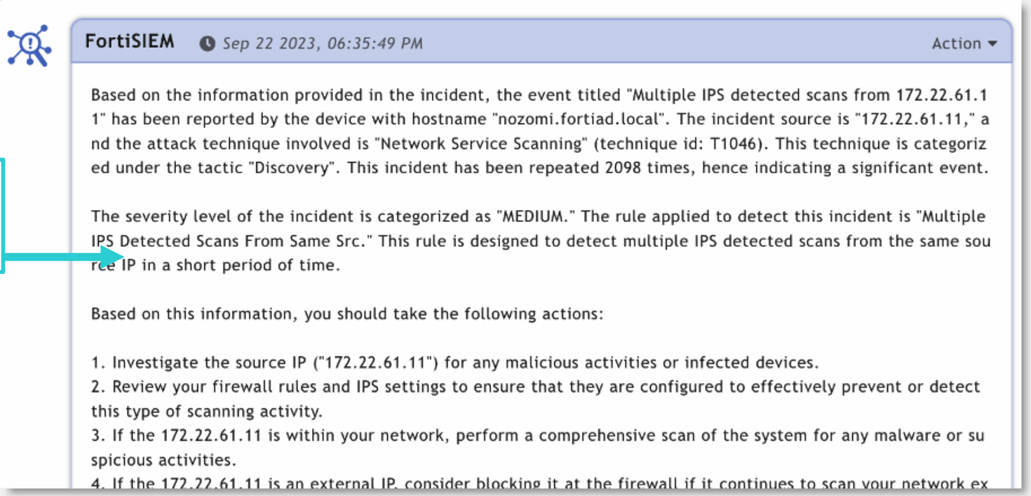
569 Total

73 New

All Active Incidents for Last 2 Hours

Severity	ID	Last Occurred	Count	Incident Title	Reporting	Source
High	2112	32 Seconds	27	20 login failures for user root from 221.229.172.66 on network de...	FG240D3913800441	221.229.172
Medium	349	32 Seconds	847	Excessive End User Mail from 192.168.88.16 to Unauthorized Mail ...	FG240D3913800441	192.168.88.16
Medium	23	32 Seconds	352	Multiple IPS detected scans from 172.16.1.253	nozomi.fortiad.local	172.16.1.253
Medium	119	32 Seconds	2,058	External Remote SMB Logon from Public IP on WIN2K8.example.com	WIN2K8.example.com	fe80::b1a2:89
Medium	2125	32 Seconds	5	License issue on QA-EXCHG	QA-EXCHG	
Medium	346	32 Seconds	79	Inbound cleartext password usage from 110.168.53.21 to 192.168...	FGT_Edge	110.168.53.
High	2111	32 Seconds	20	$user account locked on network device FG240D3913800441	FG240D3913800441	221.229.172
Medium	278	32 Seconds	2,599	Heavy ICMP Ping sweep from 172.16.22.137	HOST-172.16.0.1	172.16.22.137
Medium	18	32 Seconds	691	Multiple IPS detected scans from 10.161.220.110	nozomi.fortiad.local	10.161.220.11
Medium	296	32 Seconds	1,261	Excessive End User DNS Queries from 172.16.0.1	HOST-172.16.0.1	172.16.0.1
Medium	17	32 Seconds	689	Multiple IPS detected scans from 172.22.61.11	nozomi.fortiad.local	172.22.61.11
High	588	32 Seconds	645	Permitted inbound attack detected from 188.163.76.245 to 192.1...	FortiWeb	188.163.76.
Medium	14	32 Seconds	1,091	ICS event Nozomi-SCADAGuardian-SIGN-TCP-FLOOD seen from sour	nozomi.fortiad.local	172.21.61.11

分析事件並提出行動建議



FortiSIEM Sep 22 2023, 06:35:49 PM

Based on the information provided in the incident, the event titled "Multiple IPS detected scans from 172.22.61.11" has been reported by the device with hostname "nozomi.fortiad.local". The incident source is "172.22.61.11," and the attack technique involved is "Network Service Scanning" (technique id: T1046). This technique is categorized under the tactic "Discovery". This incident has been repeated 2098 times, hence indicating a significant event.

The severity level of the incident is categorized as "MEDIUM." The rule applied to detect this incident is "Multiple IPS Detected Scans From Same Src." This rule is designed to detect multiple IPS detected scans from the same source IP in a short period of time.

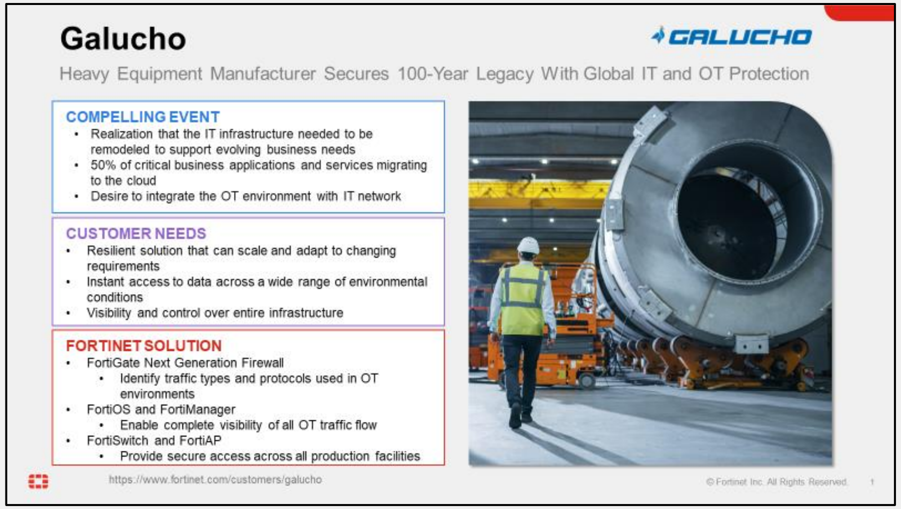
Based on this information, you should take the following actions:

1. Investigate the source IP ("172.22.61.11") for any malicious activities or infected devices.
2. Review your firewall rules and IPS settings to ensure that they are configured to effectively prevent or detect this type of scanning activity.
3. If the 172.22.61.11 is within your network, perform a comprehensive scan of the system for any malware or suspicious activities.
4. If the 172.22.61.11 is an external IP, consider blocking it at the firewall if it continues to scan your network ex

© Fortinet Inc. All Rights Reserved.

客戶和產業共享價值

- 近20年在OT領域
- 超過52,000個客戶
- 依行業建置的方案
- 全球，在地，雲端
- 產業別
  - 製造業
  - 能源/基礎建設
  - 石化/瓦斯
  - 水力/廢水
  - 運輸
  - 醫療
  - 智慧建築



Galucho

GALUCHO

Heavy Equipment Manufacturer Secures 100-Year Legacy With Global IT and OT Protection

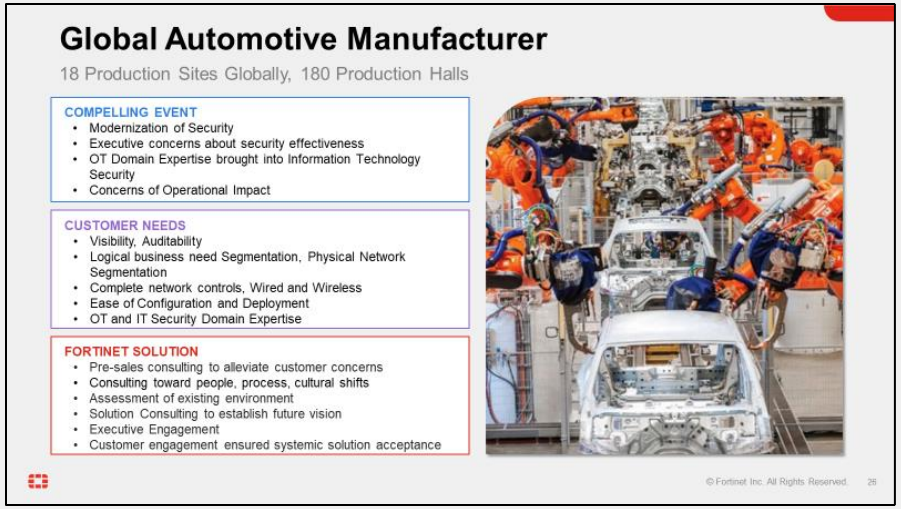
COMPELLING EVENT
- Realization that the IT infrastructure needed to be remodeled to support evolving business needs
- 50% of critical business applications and services migrating to the cloud
- Desire to integrate the OT environment with IT network

CUSTOMER NEEDS
- Resilient solution that can scale and adapt to changing requirements
- Instant access to data across a wide range of environmental conditions
- Visibility and control over entire infrastructure

FORTINET SOLUTION
- FortiGate Next Generation Firewall
  - Identify traffic types and protocols used in OT environments
- FortiOS and FortiManager
  - Enable complete visibility of all OT traffic flow
- FortiSwitch and FortiAP
  - Provide secure access across all production facilities

https://www.fortinet.com/customers/galucho

© Fortinet Inc. All Rights Reserved. 1



Global Automotive Manufacturer

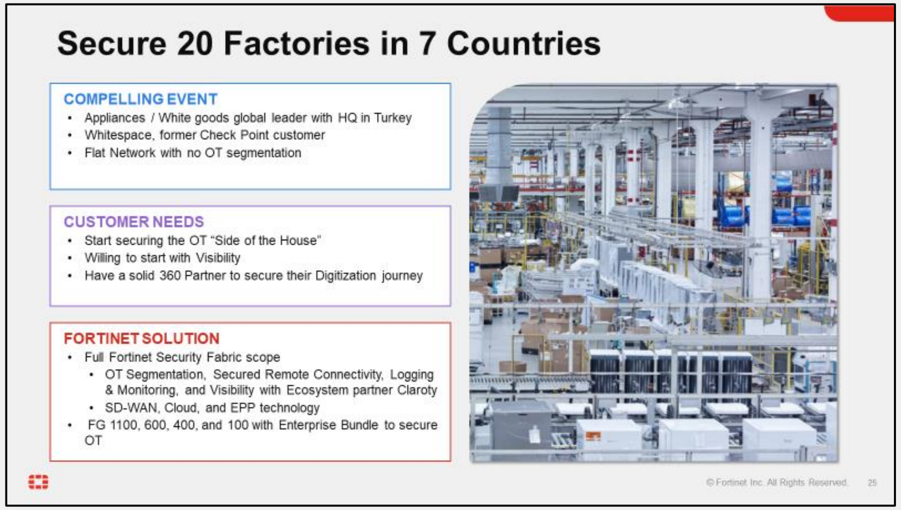
18 Production Sites Globally, 180 Production Halls

COMPELLING EVENT
- Modernization of Security
- Executive concerns about security effectiveness
- OT Domain Expertise brought into Information Technology Security
- Concerns of Operational Impact

CUSTOMER NEEDS
- Visibility, Auditability
- Logical business need Segmentation, Physical Network Segmentation
- Complete network controls, Wired and Wireless
- Ease of Configuration and Deployment
- OT and IT Security Domain Expertise

FORTINET SOLUTION
- Pre-sales consulting to alleviate customer concerns
- Consulting toward people, process, cultural shifts
- Assessment of existing environment
- Solution Consulting to establish future vision
- Executive Engagement
- Customer engagement ensured systemic solution acceptance

© Fortinet Inc. All Rights Reserved. 26



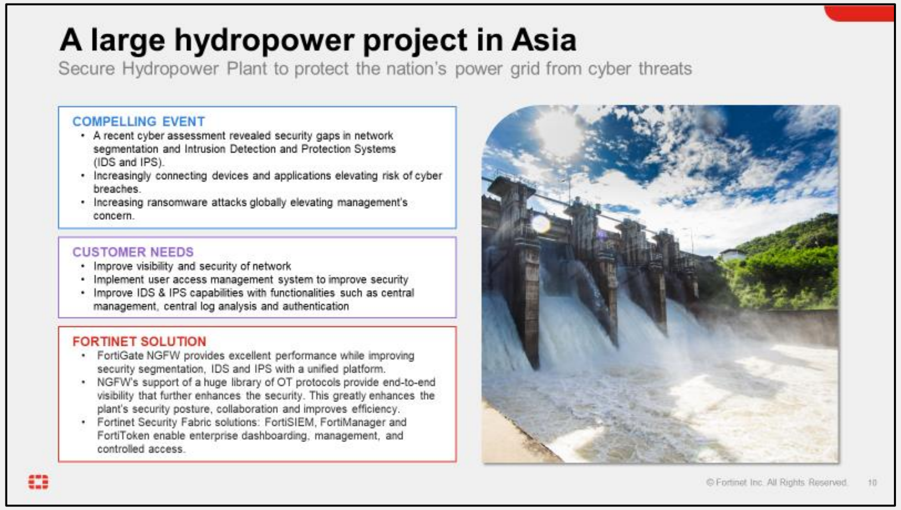
Secure 20 Factories in 7 Countries

COMPELLING EVENT
- Appliances / White goods global leader with HQ in Turkey
- Whitespace, former Check Point customer
- Flat Network with no OT segmentation

CUSTOMER NEEDS
- Start securing the OT "Side of the House"
- Willing to start with Visibility
- Have a solid 360 Partner to secure their Digitization journey

FORTINET SOLUTION
- Full Fortinet Security Fabric scope
  - OT Segmentation, Secured Remote Connectivity, Logging & Monitoring, and Visibility with Ecosystem partner Claroty
  - SD-WAN, Cloud, and EPP technology
- FG 1100, 600, 400, and 100 with Enterprise Bundle to secure OT

© Fortinet Inc. All Rights Reserved. 25



A large hydropower project in Asia

Secure Hydropower Plant to protect the nation's power grid from cyber threats

COMPELLING EVENT
- A recent cyber assessment revealed security gaps in network segmentation and Intrusion Detection and Protection Systems (IDS and IPS).
- Increasingly connecting devices and applications elevating risk of cyber breaches.
- Increasing ransomware attacks globally elevating management's concern.

CUSTOMER NEEDS
- Improve visibility and security of network
- Implement user access management system to improve security
- Improve IDS & IPS capabilities with functionalities such as central management, central log analysis and authentication

FORTINET SOLUTION
- FortiGate NGFW provides excellent performance while improving security segmentation, IDS and IPS with a unified platform.
- NGFW's support of a huge library of OT protocols provide end-to-end visibility that further enhances the security. This greatly enhances the plant's security posture, collaboration and improves efficiency.
- Fortinet Security Fabric solutions: FortiSIEM, FortiManager and FortiToken enable enterprise dashboarding, management, and controlled access.

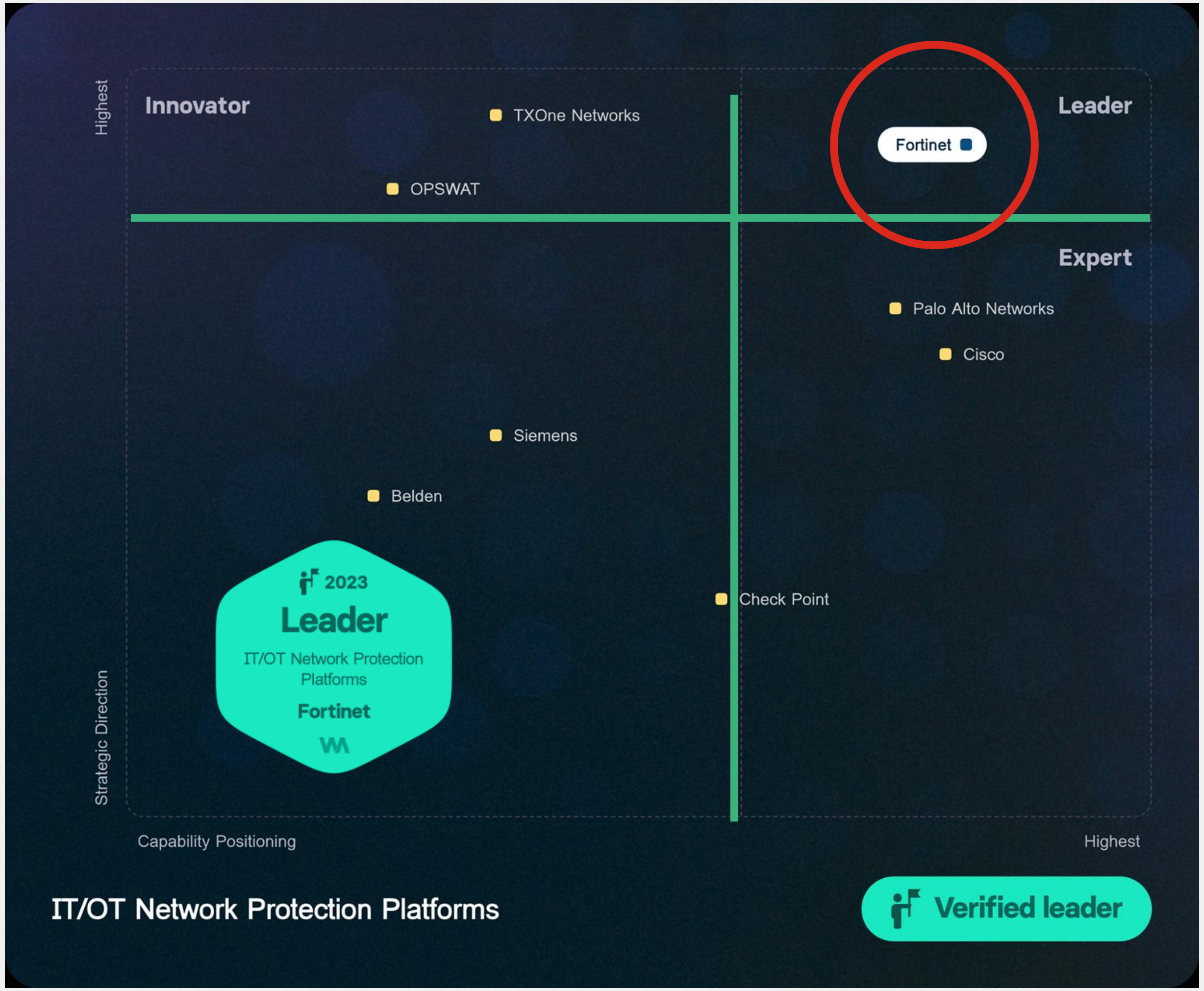
© Fortinet Inc. All Rights Reserved. 10

Fortinet 是 IT/OT 安全平台導航領域2023年的唯一領導者

Fortinet OT 安全平台連續兩年被評為 **Navigator Leader**

“Fortinet is a leading IT and OT cybersecurity solutions provider to the industrial and critical infrastructure sectors, with a high customer base and strong coverage of all industrial verticals.”

Westlands Advisory, Industrial Cybersecurity Outlook 2023-2030



FORTINET®