Secure OT Summit 2022

護航 OT/IT 融合 創新數位發展

OT IT 融合防護阻絕威脅之 Fortinet安全織網解決方案

徐嘉鴻 Loco Hsu

Fortinet 台灣區 OT 資安技術顧問

Agenda

01 **Ransomware Threat Landscape**

不斷演變的威脅和勒索軟件的興起

02 **Fortinet OT Security Fabric**

針對OT環境的深度防禦方法

03 **Use CASE**

使用案例

© Fortinet Inc. All Rights Reserved.

Secure OT Summit 2022
護航 OT/IT 融合 創新數位發展

Ransomware Threat Landscape

不斷演變的威脅和勒索軟件的興起

歷年來針對 OT 基礎設施的重大攻擊事件

這些風險真的存在

2010
- Stuxnet disrupts Iranian nuclear program

2013
- New York dam floodgates compromised

2014
- Hospital drug infusion pumps hacked
- Michigan traffic light hacked

2015
- German steel mill furnace destroyed

- Car transmission and brakes controlled

- Ukraine power grid knocked offline

2016
- MIRAI Botnet 145,00 IoT devices

2017
- Merck & Co. global production shutdown by ransomware ($1B loss)

- Maersk Shipping global shutdown by ransomeware ($250M loss)

2018
- Trisis/Triton: Malware designed to compromise Safety

2019
- Global Aluminum producer shutdown by ransomware

- ASCO parts shutdown by ransomware

2020
- Ekans Ransomware attack on Honda, Fresenius

- SolarWinds Orion

2021
- Attempted poisoning of Tampa H20 Supply

FORTINET

© Fortinet Inc. All Rights Reserved.

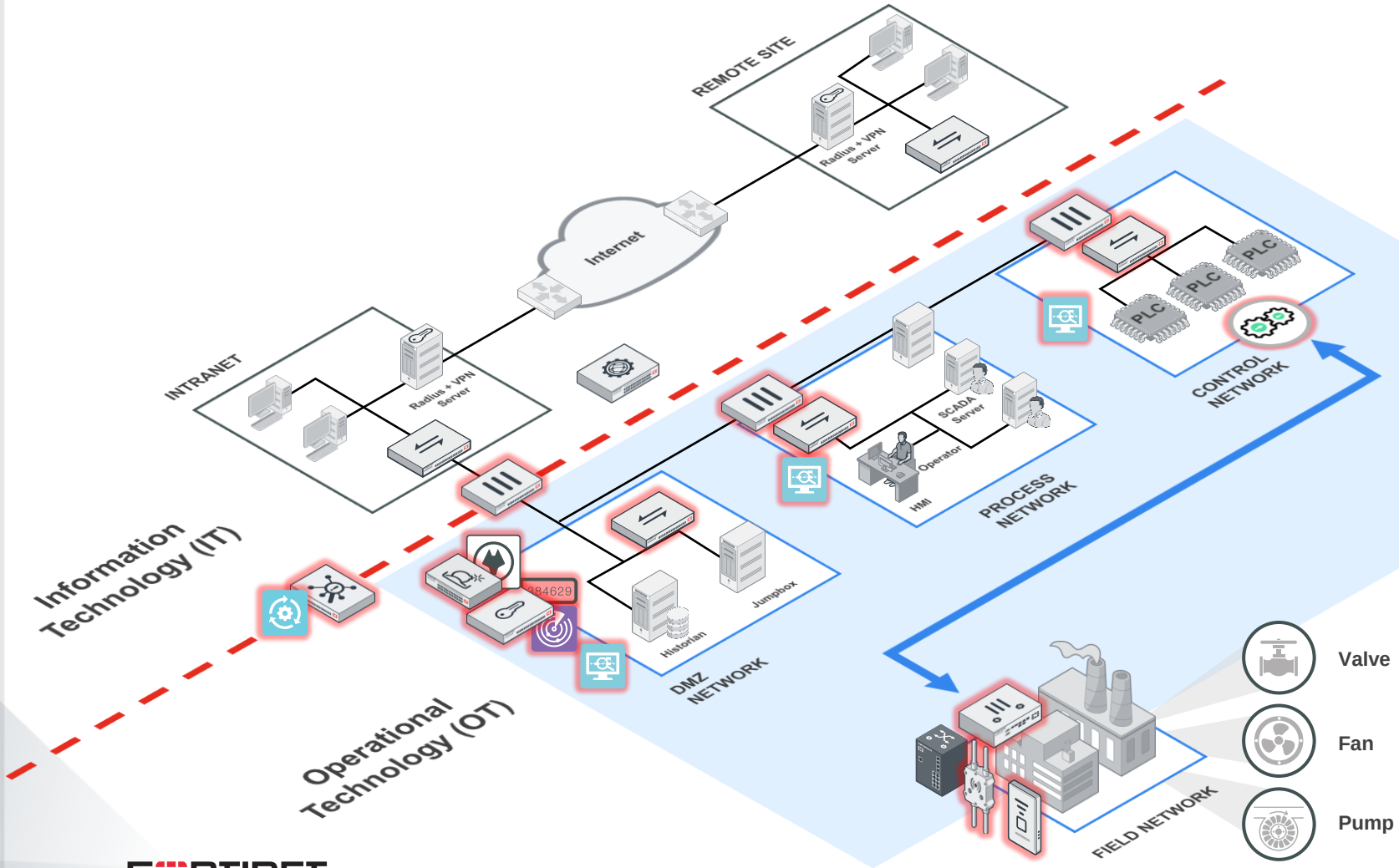
Secure OT Summit 2022

護航 OT/IT 融合 創新數位發展

Fortinet OT Security Fabric

針對OT環境的深度防禦方法

提供 OT 與 IT 整合安全的關鍵使用情境



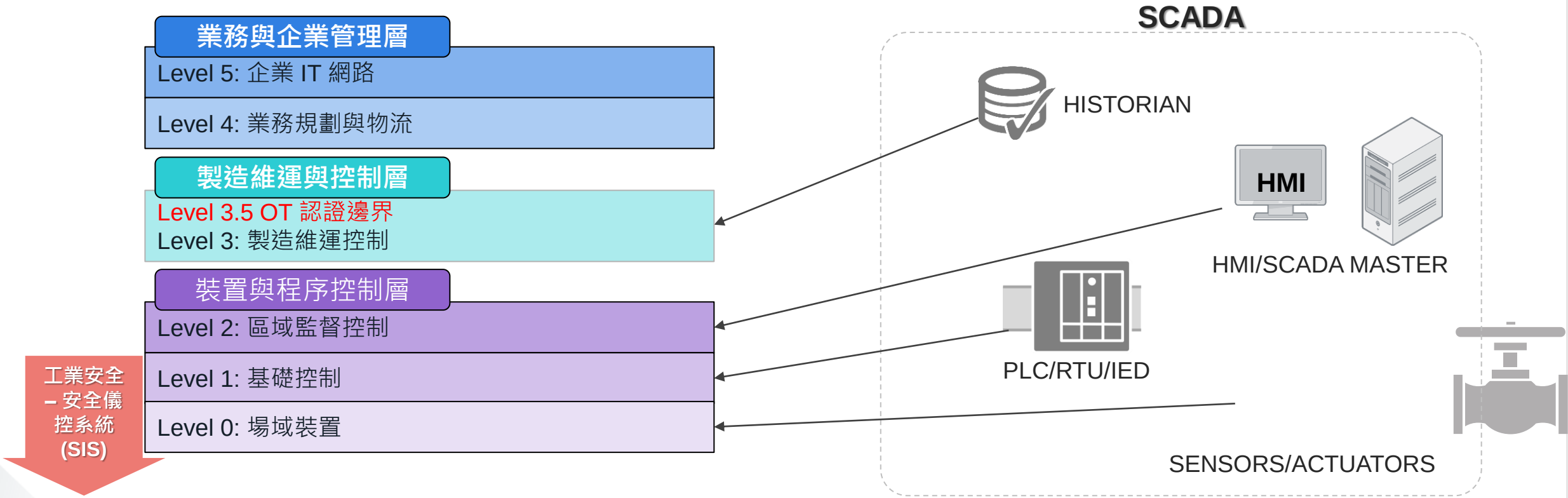
- 區域分隔與控管
- 安全的遠端連線
- 深度的 OT 可視性
- 角色導向存取控制
- 保護關鍵終端設備
- 集中式安全管理維運
- 進階持續性威脅防護

© Fortinet Inc. All Rights Reserved.

普渡工業控制階層模型

Purdue Model For Industrial Control Hierarchy

- 包含所有 OT 系統基本功能和組成的框架
- 區隔裝置和設備以增進 OT 網路資訊安全
- 基於 OT 環境的階層區隔定義

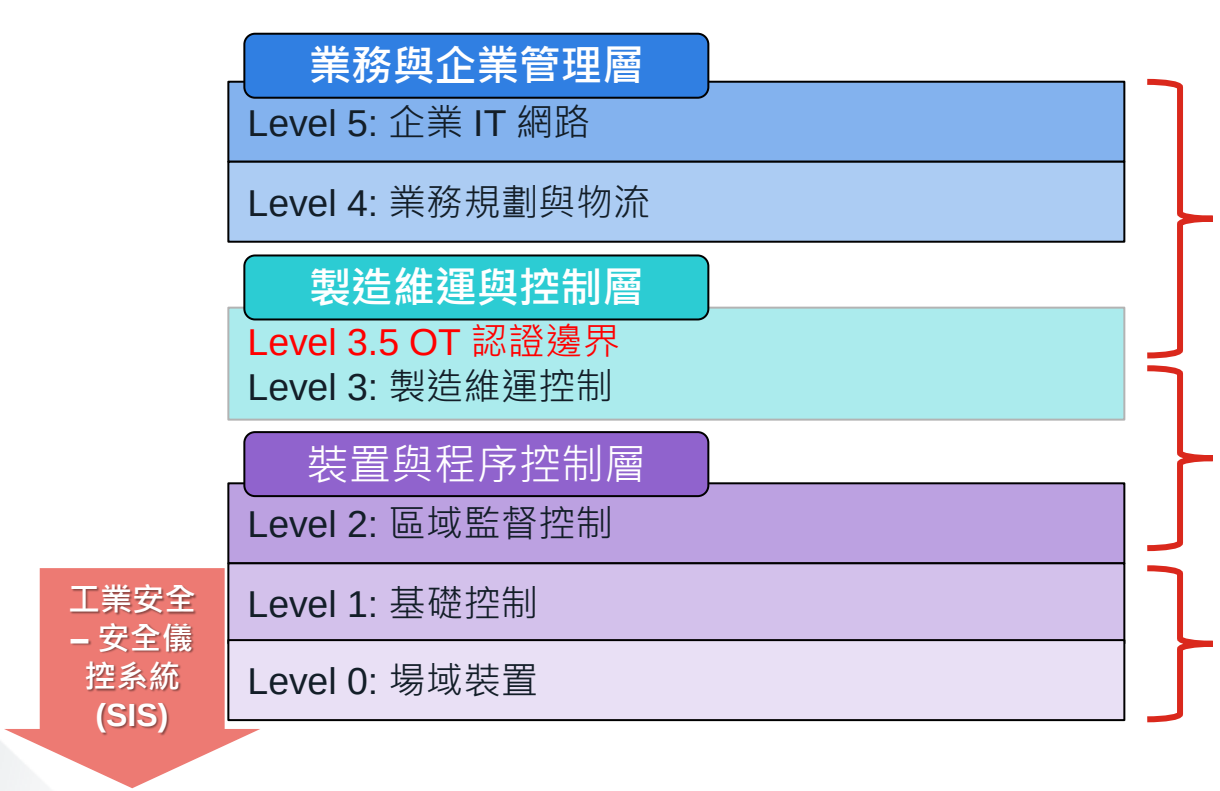


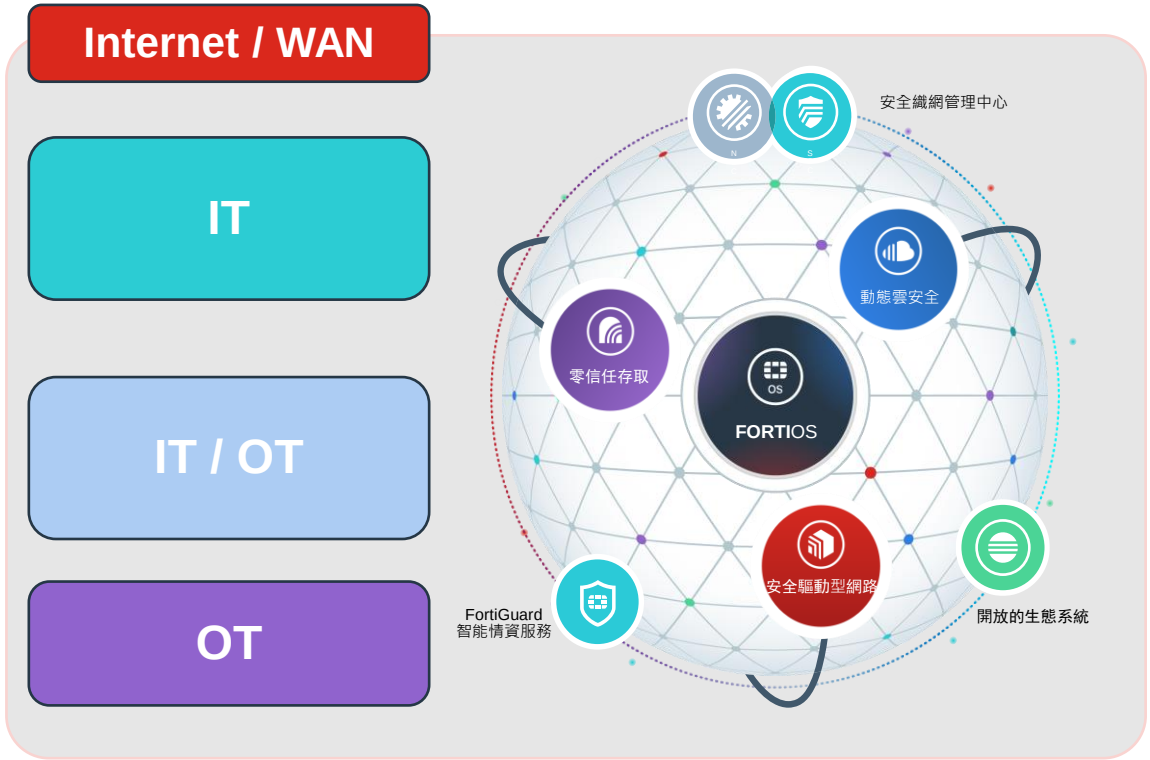
© Fortinet Inc. All Rights Reserved.

普渡工業控制階層模型

Purdue Model For Industrial Control Hierarchy

- 包含所有 OT 系統基本功能和組成的框架
- 區隔裝置和設備以增進 OT 網路資訊安全
- 基於 OT 環境的階層區隔定義



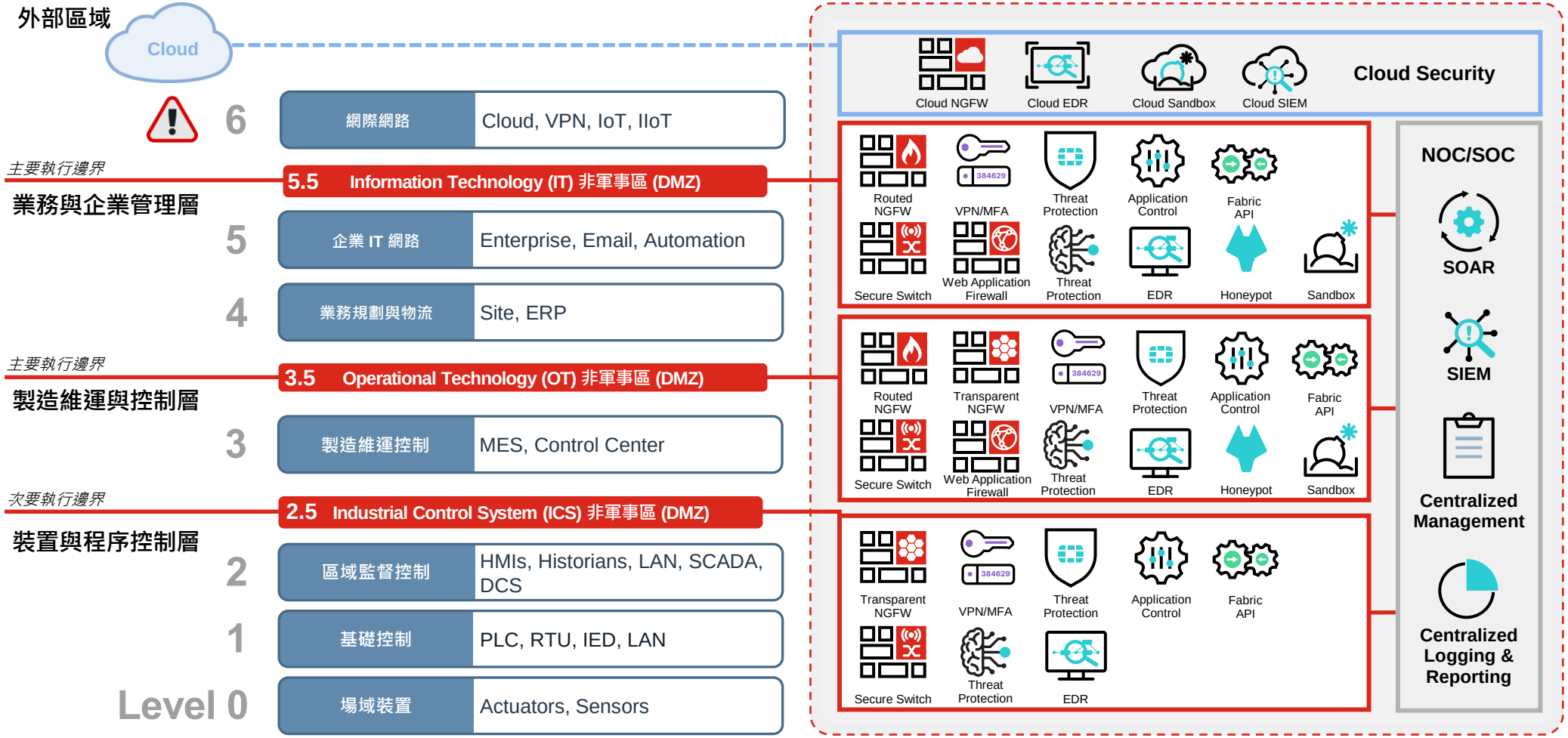


© Fortinet Inc. All Rights Reserved.

強化您的 OT 資安防護

部署 Fortinet 安全織網

- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防
- 網路營運中心/資安營運中心



DMZ: Demilitarized Zone, Security Conduit
EDR: Endpoint Detection & Response
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
Zones: Security Zones
MFA: Multi-factor Authentication
NGFW: Next-Generation Firewall
VPN: Virtual Private Network

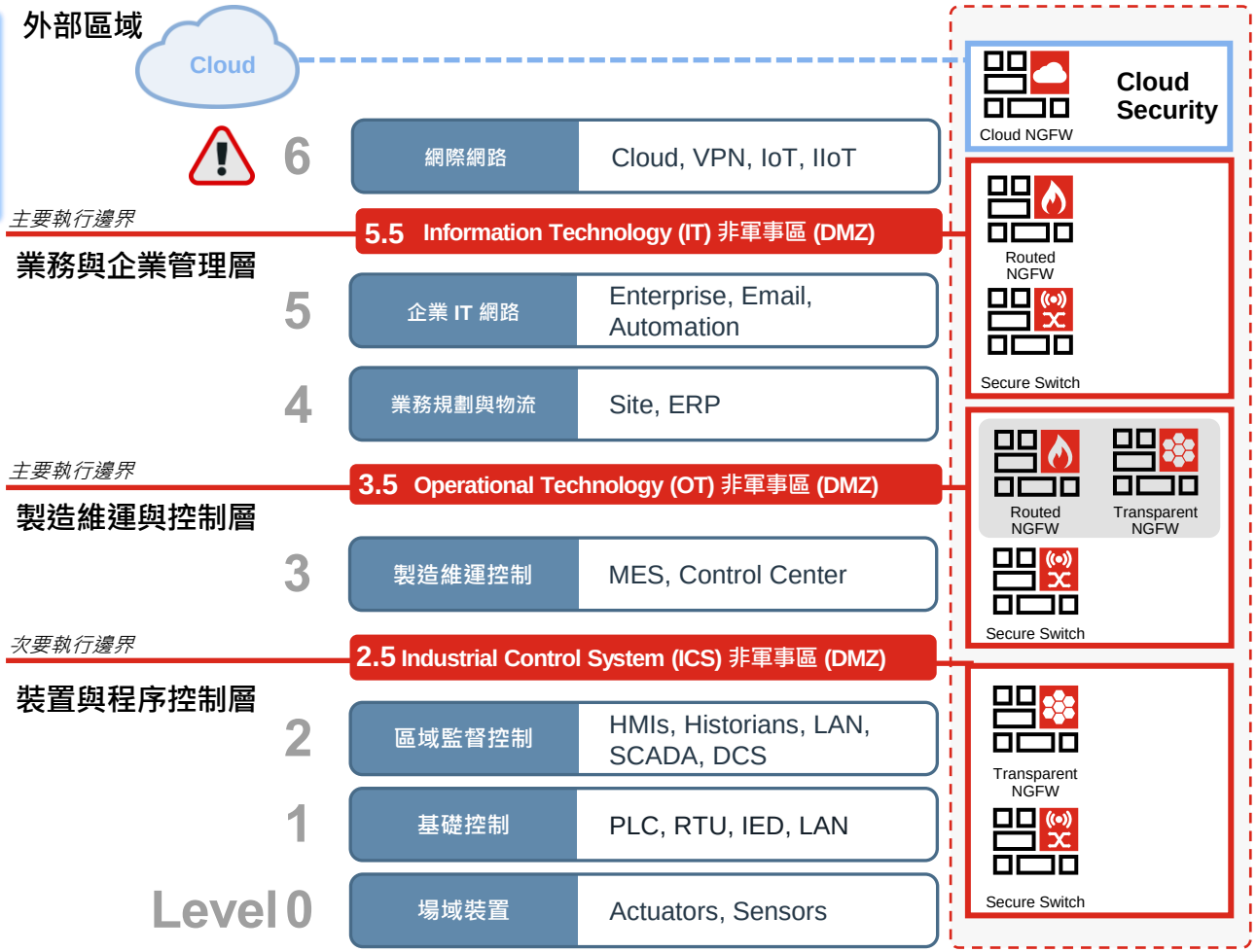
FORTINET

© Fortinet Inc. All Rights Reserved.

網路分割與微分割

部署 FortiGate、FortiSwitch 與 FortiAP

- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防
- 網路營運中心/資安營運中心



OT 相關的特定功能

- 多樣化的設備型式：
  - 工業等級型式: 防火牆、網路交換器、無線基地台
  - 一般商用機型
  - 虛擬主機型式
- 可透過 FortiManager 統一管理
- 可與業界領先 OT 合作夥伴與廠商整合
- 支援 DIN 掛軌設計，直流電供應器
- 支援透通模式部署及故障旁路 (bypass)
- 業界唯一工業等級具備 *Secure* SD-WAN 功能新世代防火牆
- 可整合網路存取控制解決方案 (NAC)

© Fortinet Inc. All Rights Reserved.

DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*

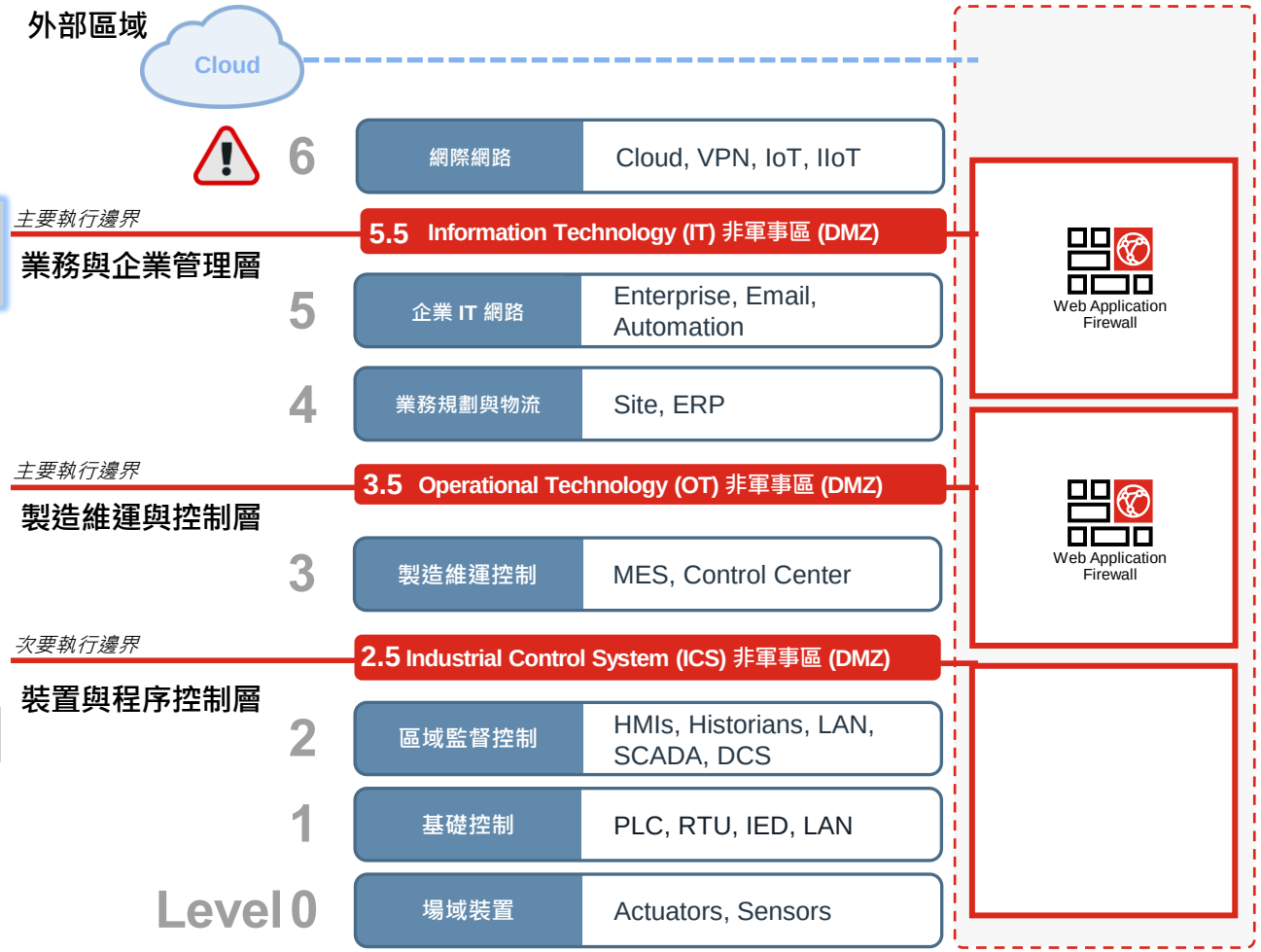
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

網頁服務安全

部署 FortiWeb

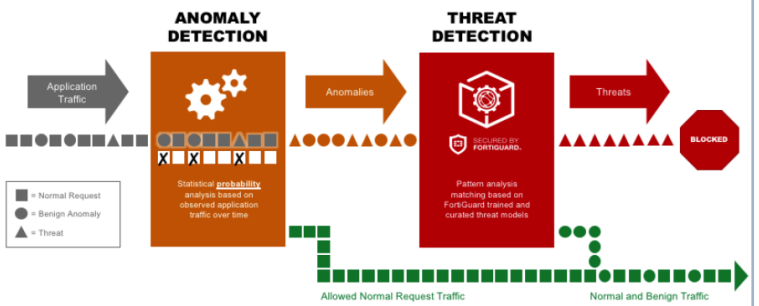
- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防

網路營運中心/資安營運中心



OT 相關的特定功能

- 當今人機介面 (HMI) 與歷程資料伺服器 (HISTORIAN) 多數使用 HTTP 協定
- 保障網頁應用服務與 API 資訊安全
- 透過機器學習 (ML) 偵測異常行為
  - 大幅簡化設定並增進防護效能
- 殭屍病毒網路緩解措施
- 識別並阻擋惡意網路流量
- 可整合第三方掃描機制
- **支援實體機與虛擬機部署型式**



© Fortinet Inc. All Rights Reserved.

DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*

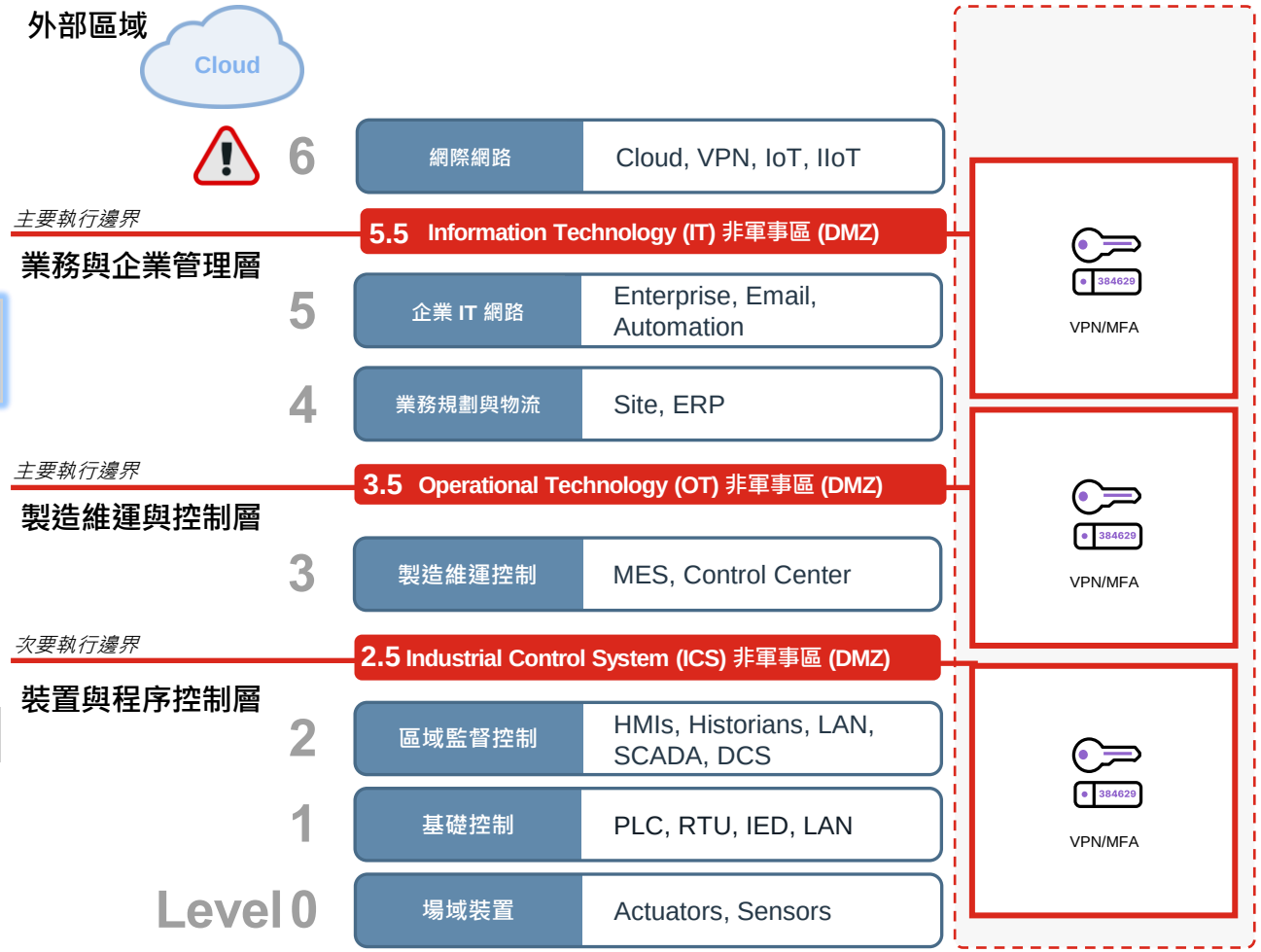
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

安全遠端存取

部署 FortiAuthenticator、FortiClient 與 FortiToken

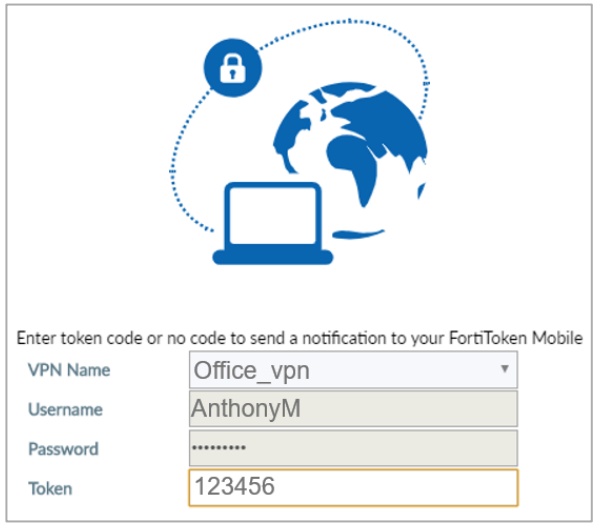
- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防

網路營運中心/資安營運中心



OT 相關的特定功能

- FortiClient 具備 VPN 用戶端功能並支援雙因子認證機制
- FortiAuthenticator 作為使用者認證伺服器，支援雙因子認證，包括 PKI、 OTP
  - 提供使用者本地資料庫或整合第三方目錄伺服器，如 LDAP
- FortiToken 提供 OTP 能力
  - 型式可為硬體式或軟體 (行動裝置)
  - 提供使用者自行註冊設置能力



© Fortinet Inc. All Rights Reserved.

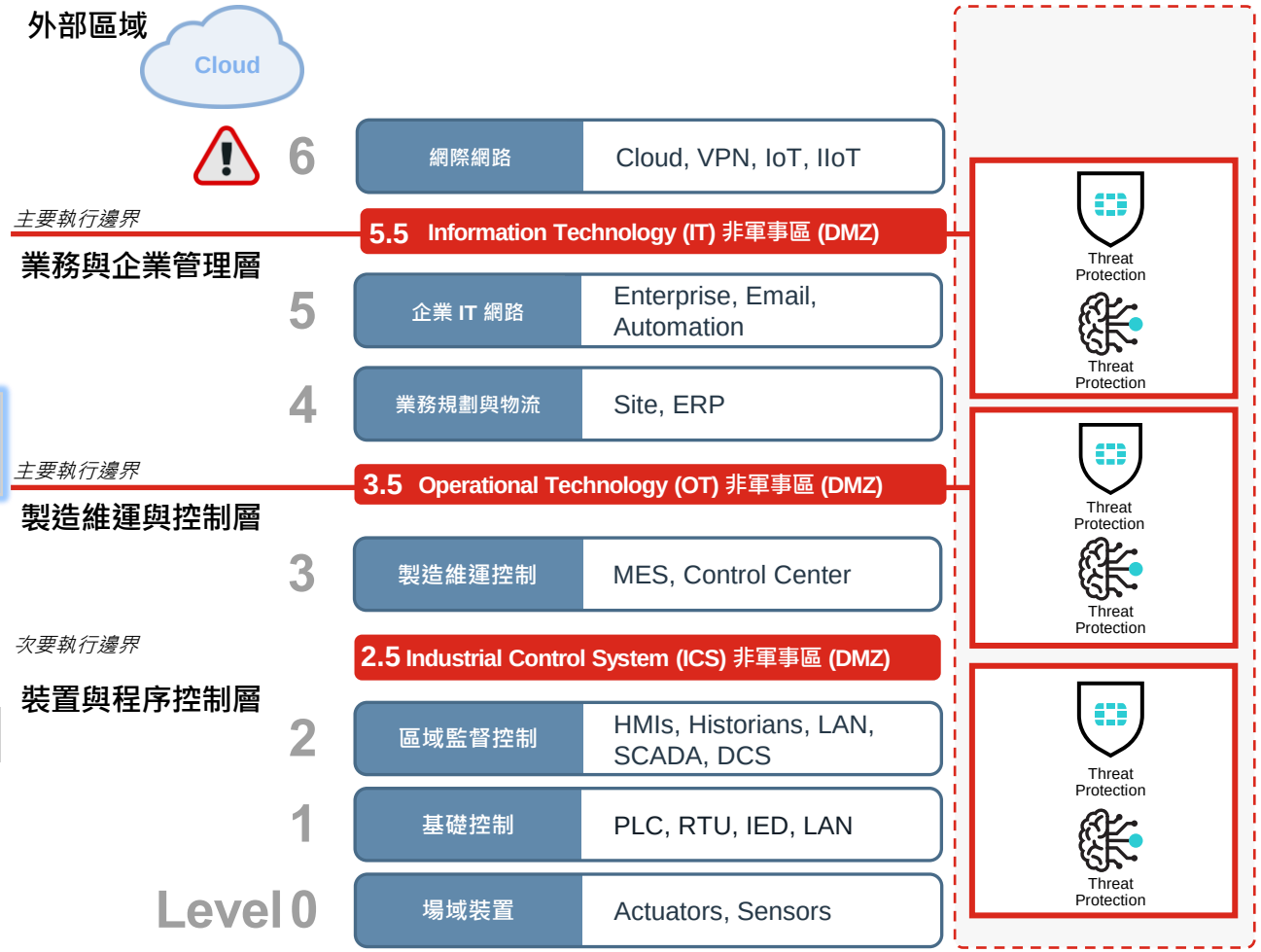
DMZ: Demilitarized Zone, Security Conduit　　Zones: Security Zones

NGFW: Next-Generation Firewall　　VPN: Virtual Private Network

資安威脅防護與 AI

部署 FortiAI、FortiGate OT IPS 與 AV 功能

- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- **資安威脅防護**
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防
- 網路營運中心/資安營運中心



OT 相關的特定功能

- 快速偵測已知的惡意程式與入侵攻擊
- FortiGate 檢測到惡意流量時可選擇僅監看記錄或立即阻擋
- 400+ OT IPS 特徵碼資料庫 (總資料庫 13,300+ 筆)
- FortiAI 為新一代惡意程式偵測工具，經由神經網路的自主學習，針對已知或未知的惡意程式，提供次秒級的偵測效率
- FortiGuard Labs 開發並維護相關的資安威脅情資與特徵碼資料庫

為 OT 提供入侵防護 / 虛擬補丁

- 7 Technologies / Schneider Electric
- ABB
- Advantech
- Broadwin
- CitectSCADA
- CoDeSys
- Cogent
- DATAC
- Eaton
- GE
- Iconics
- InduSoft
- IntelliCom
- GE
- Iconics
- InduSoft
- IntelliCom
- Measuresoft
- Microsys
- MOXA
- PcVue
- Progea
- QNX
- RealFlex
- Rockwell Automation
- RSLogix
- Siemens
- Sunway
- TeeChart
- VxWorks
- WellinTech
- Yokogawa
- …

FORTINET

© Fortinet Inc. All Rights Reserved.

DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*

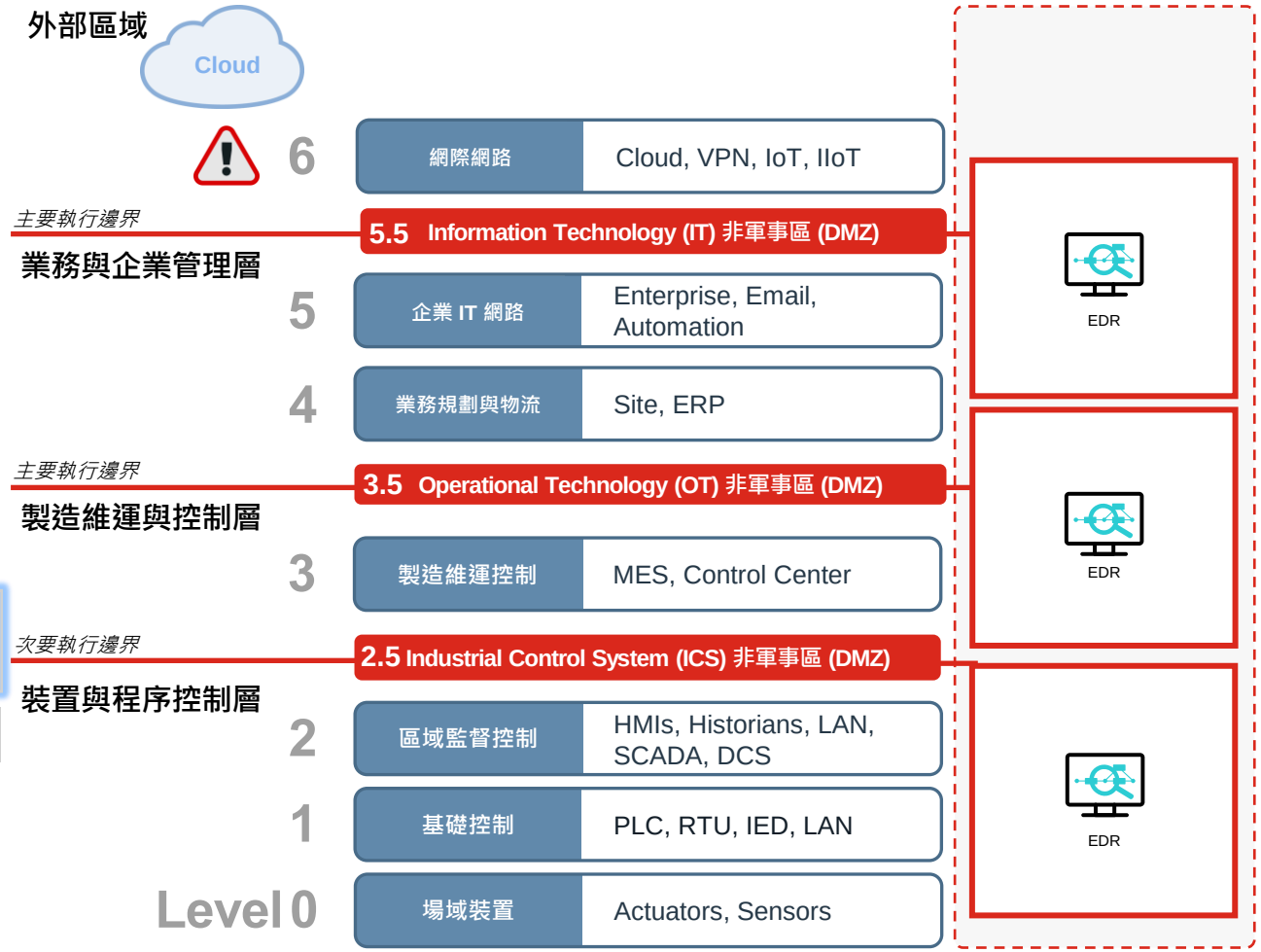
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

終端安全防護

部署 FortiEDR

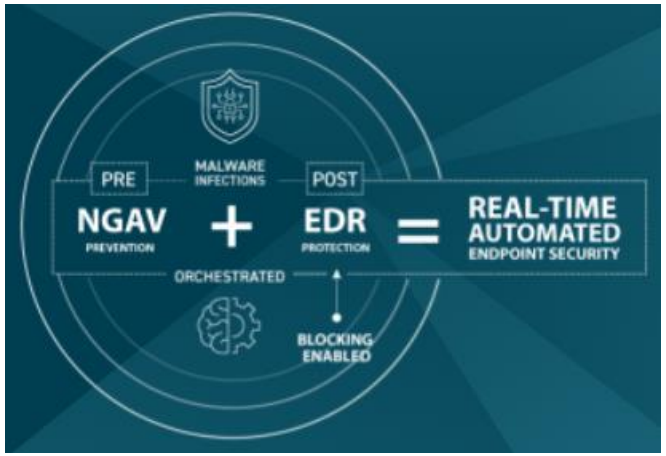
- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- **終端安全防護**
- 蜜罐偵測聯防
- 沙箱偵測聯防

網路營運中心/資安營運中心



OT 相關的特定功能

- 兼容舊版的作業系統，一直支援到 Windows XP Service Pack 3
- 支援地端部署 (air-gap) 或雲端部署模式.
- 極其輕量化的終端代理程式，不會造成老舊作業系統運作負擔.
- 在在不中斷正常服務的情況下對可疑行為發出告警
- 可允許 / 阻擋應用程式通訊行為
- 無關通訊協定的異常行為偵測能力
- 可阻擋未允許授權的 USB 裝置.
- 控管應用程式可執行的動作
- 針對環境內的OT設備提供探勘能力



© Fortinet Inc. All Rights Reserved.

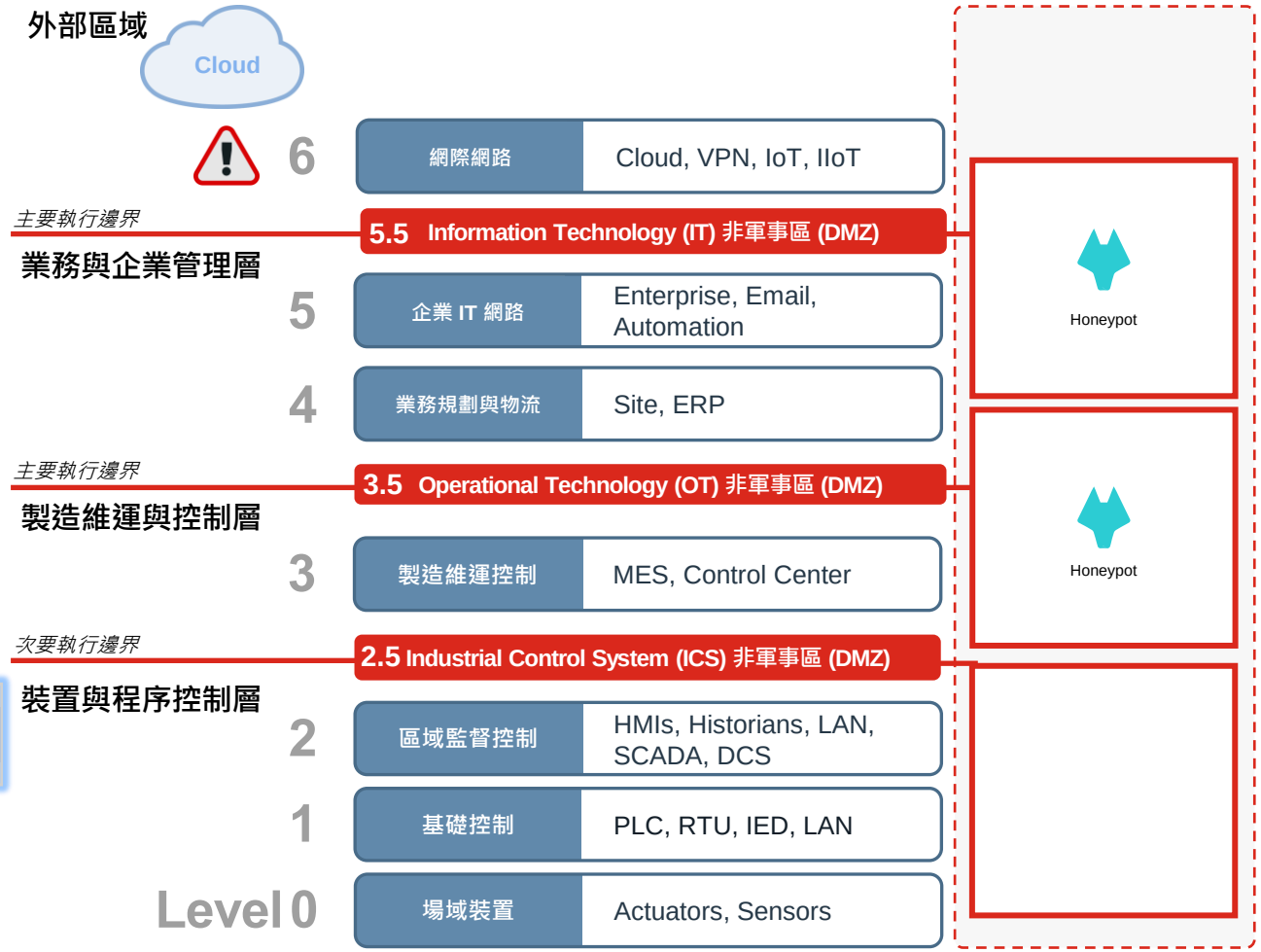
DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*

NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

進階欺敵技術偵測聯防

部署 FortiDeceptor

- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防
- 網路營運中心/資安營運中心



OT 相關的特定功能

- 能夠為 OT/IT 網路模擬 Jumpboxes 和 VPN 服務等伺服器
- 能夠模擬 SCADA 和 ICS 通訊協定
- 能夠在 ICS 網路中模擬人機介面 (HMI)、可程式邏輯控制器 (PLC)
- 可與 FortiSIEM 新世代 SIEM 平台整合
- 配置簡單，可彈性部署於各網段
- 可與 Fortinet 安全織網聯防

誘餌支持的通訊協定

- MODBUS
- S7COMM
- BACNET
- IPMI
- TRICONEX
- GUARDIAN-AST
- IEC104
- HTTPS
- FTP
- TFTP
- SNMP

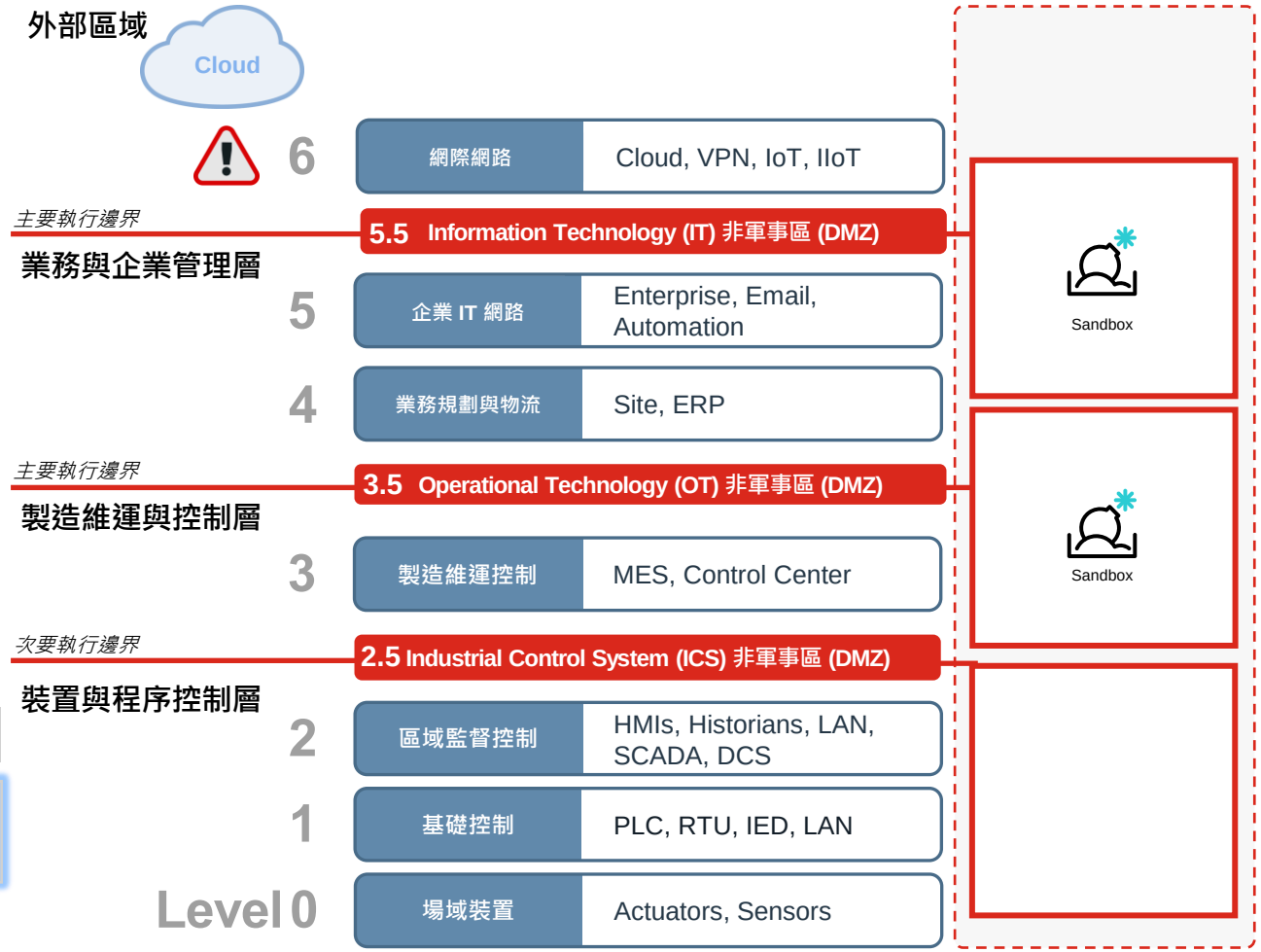
© Fortinet Inc. All Rights Reserved.

DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*
NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

沙箱偵測聯防

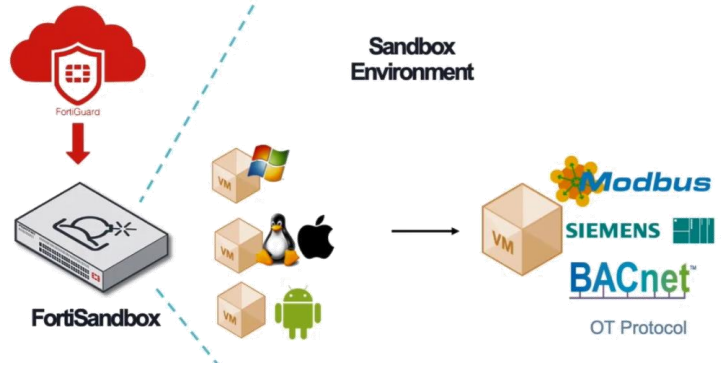
部署 FortiSandbox

- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防
- 網路營運中心/資安營運中心



OT 相關的特定功能

- 在部署軟體至工程工作站 (EWS) 之前，掃描軟體是否內藏惡意內容
- 能夠在 Windows、Linux 和特定於 OT 模擬器虛擬機中引爆對象藉以偵測威脅
- 能夠掃描有效負載以查看它們是否使用了 ICS 相關通訊協定，例如 Modbus、Siemens S7、BACNet 等
- 可掃描 OT惡意程式與已知漏洞
- 可對未知的檔案產生入侵指標
- 可偵測新的未知惡意程式
- 可與 Fortinet 安全織網聯防



© Fortinet Inc. All Rights Reserved.

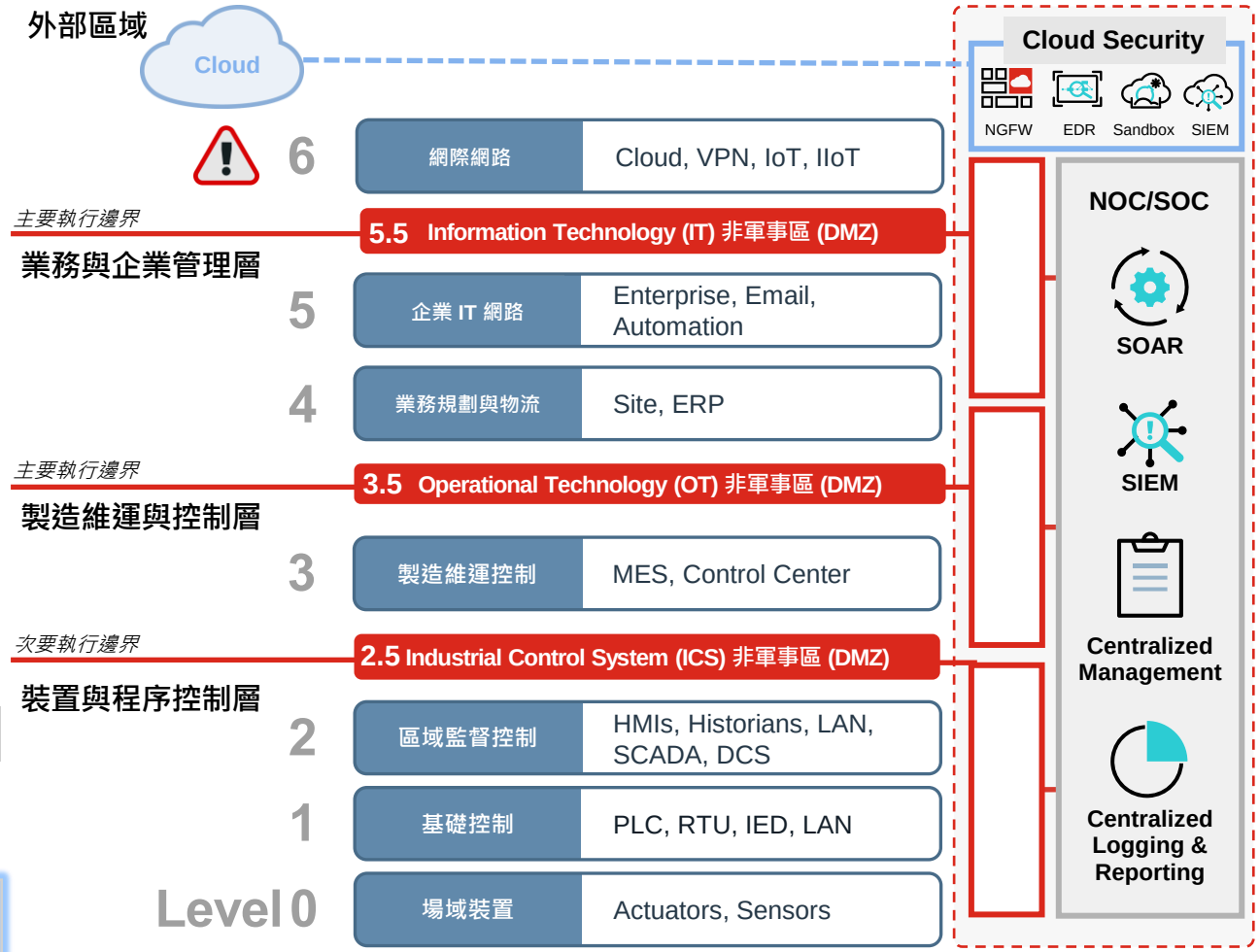
DMZ: Demilitarized Zone, Security Conduit　　Zones: Security Zones

NGFW: Next-Generation Firewall　　VPN: Virtual Private Network

網路營運中心/資安營運中心

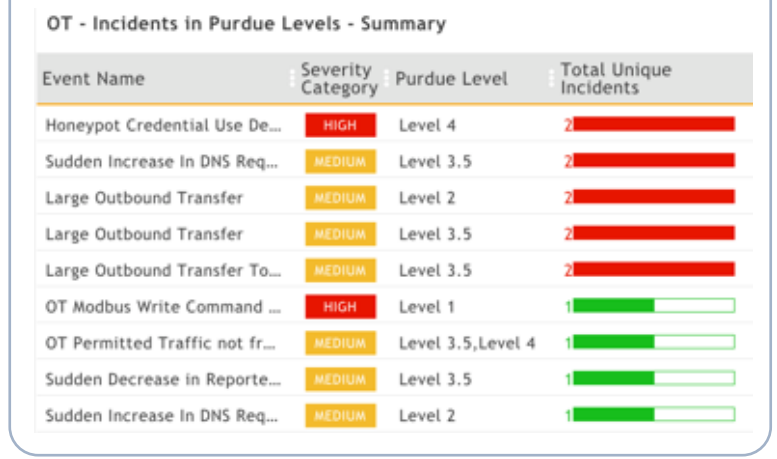
部署 FortiManager、FortiSIEM 與 FortiAnalyzer

- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防
- 網路營運中心/資安營運中心



OT 相關的特定功能

- FortiManager 可集中管理 FortiGates、FortiSwitches 與 FortiAPs
- 提供軟體、特徵碼資料庫更新與授權管理，不須連線網際網路
- FortiAnalyzer 可為 Fortinet 設備提供監看與報表功能
- FortiSIEM 提供跨品牌設備日誌收集與監管告警能力。支援地端、雲端或混合式部署模式，可與 OT 可視性相關廠商整合並聯防資安與網路設備



OT - Incidents in Purdue Levels - Summary

Event Name	Severity Category	Purdue Level	Total Unique Incidents
Honeypot Credential Use De...	HIGH	Level 4	2
Sudden Increase In DNS Req...	MEDIUM	Level 3.5	2
Large Outbound Transfer	MEDIUM	Level 2	2
Large Outbound Transfer	MEDIUM	Level 3.5	2
Large Outbound Transfer To...	MEDIUM	Level 3.5	2
OT Modbus Write Command ...	HIGH	Level 1	1
OT Permitted Traffic not fr...	MEDIUM	Level 3.5,Level 4	1
Sudden Decrease in Reporte...	MEDIUM	Level 3.5	1
Sudden Increase In DNS Req...	MEDIUM	Level 2	1

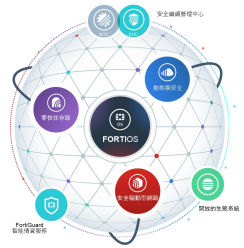
© Fortinet Inc. All Rights Reserved.

DMZ: Demilitarized Zone, Security Conduit *Zones: Security Zones*

NGFW: Next-Generation Firewall *VPN: Virtual Private Network*

強化您的 OT 資安防護

部署 Fortinet 安全織網



Fortinet Security Fabric

- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防
- 網路營運中心/資安營運中心

外部區域

Cloud

6	網際網路	Cloud, VPN, IoT, IIoT

主要執行邊界

5.5 Information Technology (IT) 非軍事區 (DMZ)

業務與企業管理層

5	企業 IT 網路	Enterprise, Email, Automation
4	業務規劃與物流	Site, ERP

主要執行邊界

3.5 Operational Technology (OT) 非軍事區 (DMZ)

製造維運與控制層

3	製造維運控制	MES, Control Center

次要執行邊界

2.5 Industrial Control System (ICS) 非軍事區 (DMZ)

裝置與程序控制層

2	區域監督控制	HMIs, Historians, LAN, SCADA, DCS
1	基礎控制	PLC, RTU, IED, LAN
Level 0	場域裝置	Actuators, Sensors

Cloud Security

Cloud NGFW, Cloud EDR, Cloud Sandbox, Cloud SIEM

Routed NGFW, VPN/MFA, Threat Protection, Application Control, Fabric API, Secure Switch, Web Application Firewall, Threat Protection, EDR, Honeypot, Sandbox

Routed NGFW, Transparent NGFW, VPN/MFA, Threat Protection, Application Control, Fabric API, Secure Switch, Web Application Firewall, Threat Protection, EDR, Honeypot, Sandbox

Transparent NGFW, VPN/MFA, Threat Protection, Application Control, Fabric API, Secure Switch, Threat Protection, EDR

NOC/SOC

- SOAR
- SIEM
- Centralized Management
- Centralized Logging & Reporting

DMZ: Demilitarized Zone, Security Conduit
EDR: Endpoint Detection & Response
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
Zones: Security Zones
MFA: Multi-factor Authentication
NGFW: Next-Generation Firewall
VPN: Virtual Private Network

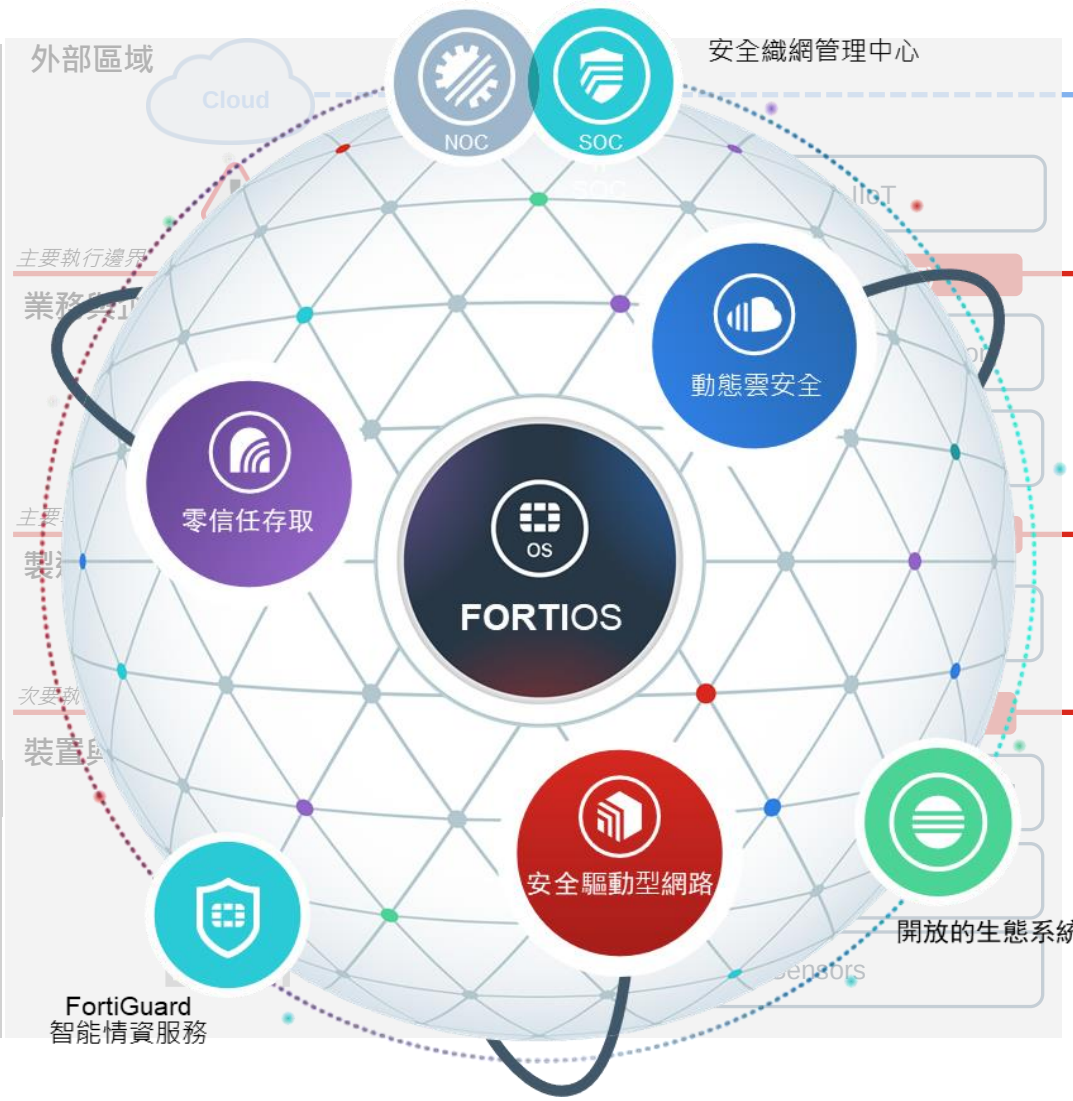
FORTINET

© Fortinet Inc. All Rights Reserved.

強化您的 OT 資安防護

部署 Fortinet 安全織網

- 網路分割
- 網路微分割
- 網頁服務安全
- 安全遠端存取
- 資安威脅防護
- 應用程式控管
- 終端安全防護
- 蜜罐偵測聯防
- 沙箱偵測聯防
- 網路營運中心/資安營運中心



Fortinet Security Fabric

Cloud Security
Cloud NGFW · Cloud EDR · Cloud Sandbox · Cloud SIEM

Routed NGFW · VPN/MFA · Threat Protection · Application Control · Fabric API
Secure Switch · Web Application Firewall · Threat Protection · EDR · Honeypot · Sandbox

Routed NGFW · Transparent NGFW · VPN/MFA · Threat Protection · Application Control · Fabric API
Secure Switch · Web Application Firewall · Threat Protection · EDR · Honeypot · Sandbox

Transparent NGFW · VPN/MFA · Threat Protection · Application Control · Fabric API
Secure Switch · Threat Protection · EDR

NOC/SOC
- SOAR
- SIEM
- Centralized Management
- Centralized Logging & Reporting

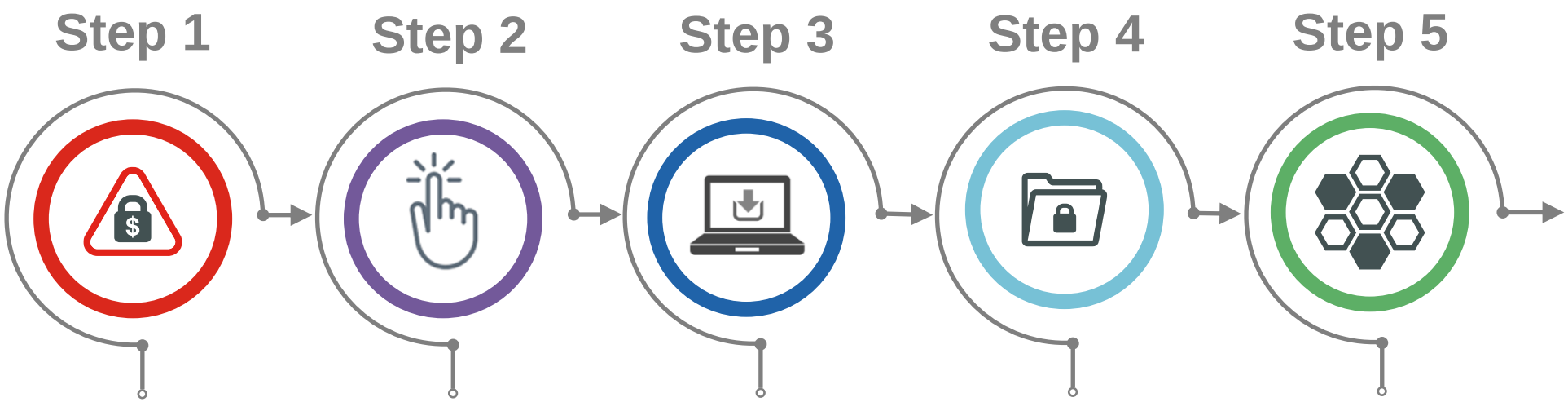
DMZ: Demilitarized Zone, Security Conduit
EDR: Endpoint Detection & Response
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
Zones: Security Zones
MFA: Multi-factor Authentication
NGFW: Next-Generation Firewall
VPN: Virtual Private Network

© Fortinet Inc. All Rights Reserved.

Use Case

防禦情境範例

How Ransomware Works? How can we prevent it?



Delivery

FortiMail
FortiSandbox
FortiEDR
FortiClient
FortiGate

User clicks and attack begins

FortiClient
FortiEDR
FortiGate
FortiSandbox

Sensitive Data

FortiClient
FortiEDR

Command & Control and data Encryption

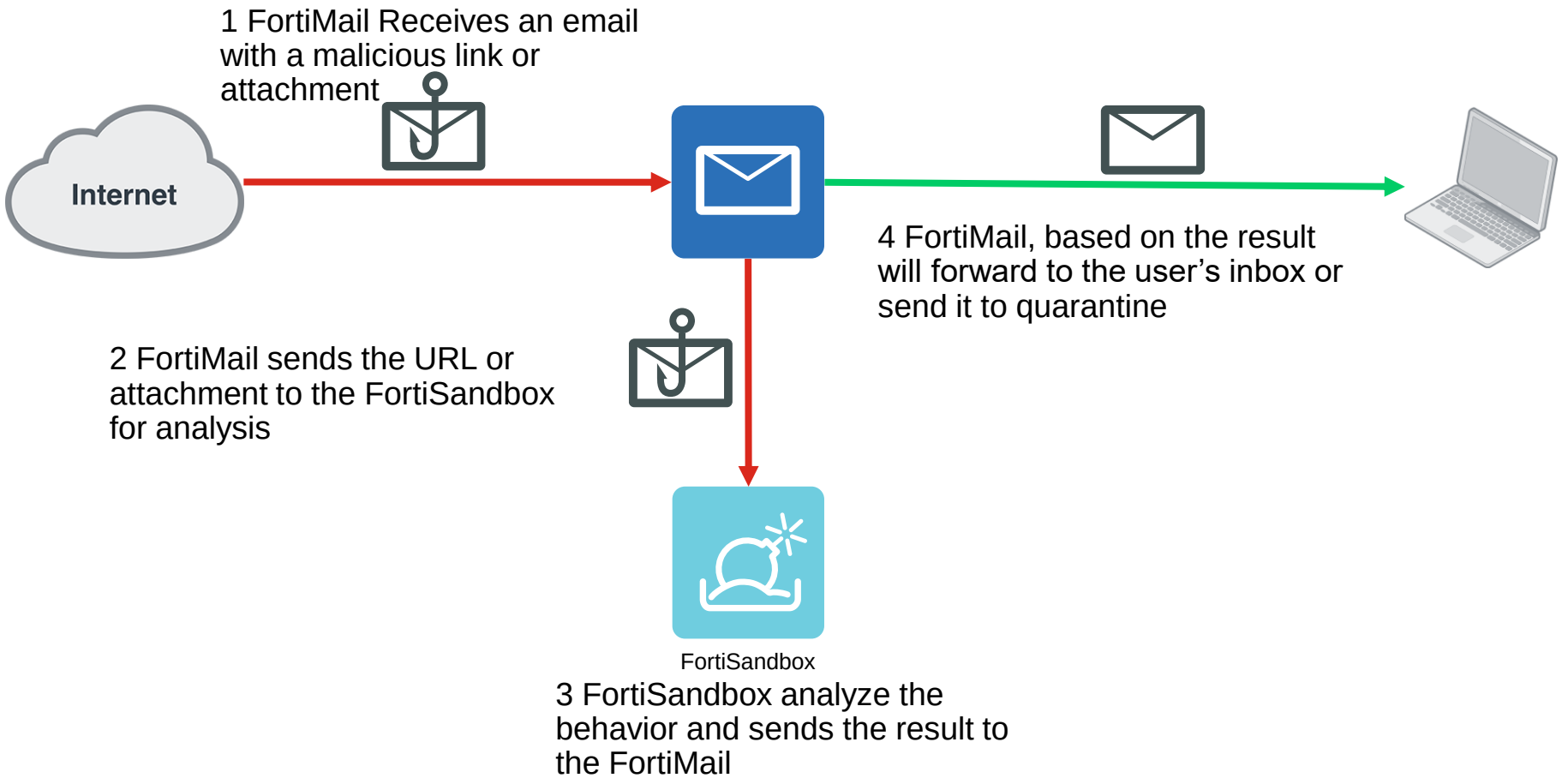
FortiClient
FortiEDR
FortiGate

Lateral Movement

FortiClient
FortiEDR
FortiSandbox

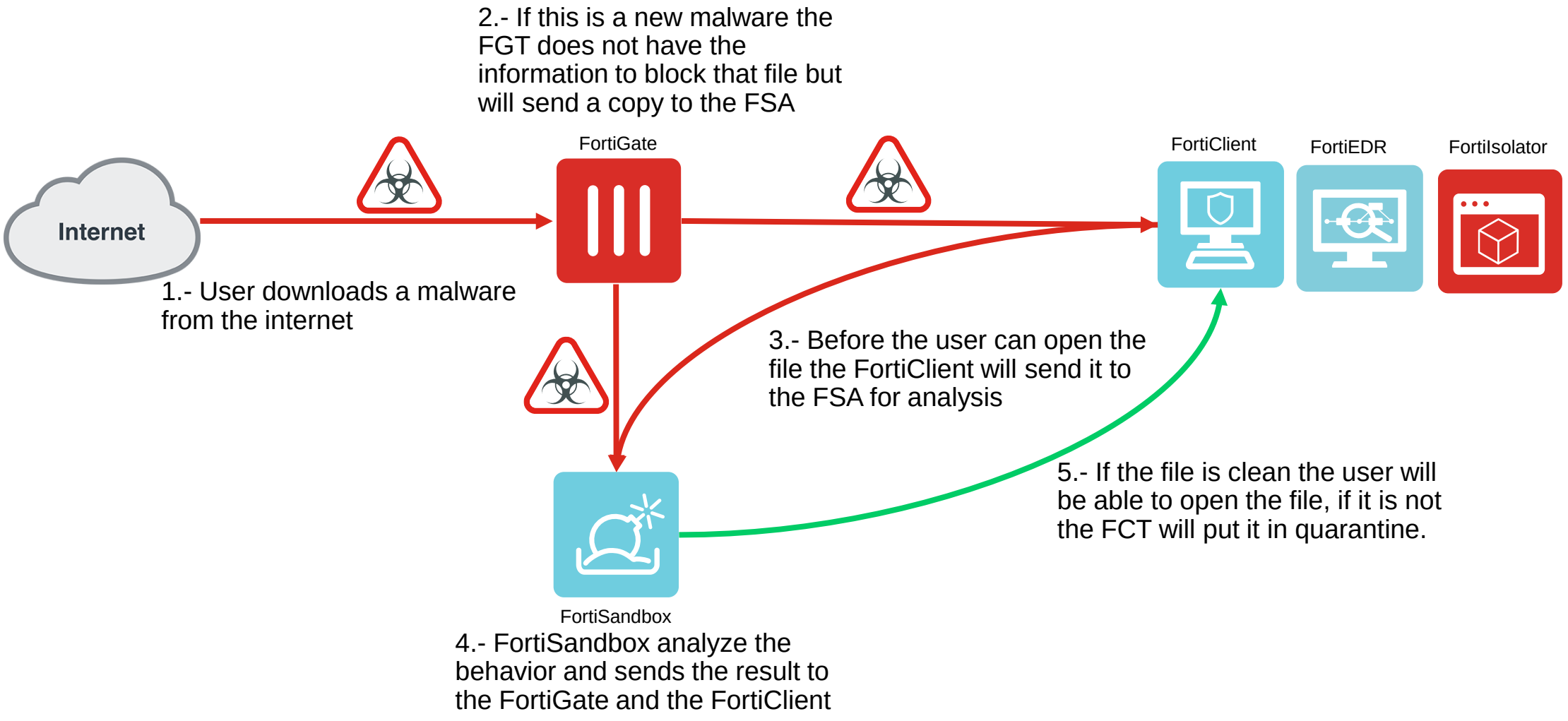
© Fortinet Inc. All Rights Reserved.

Use Case: Email Protection



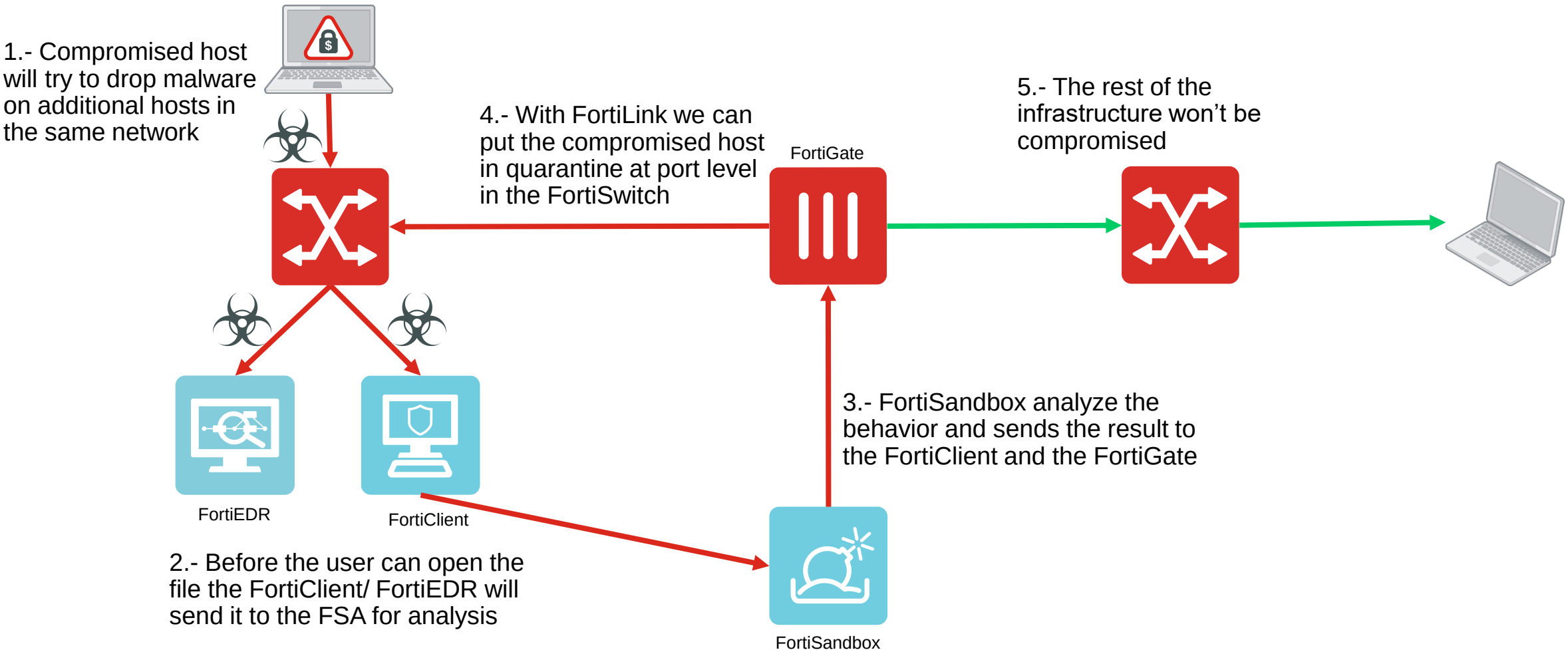
© Fortinet Inc. All Rights Reserved.

Use Case: Web Browsing



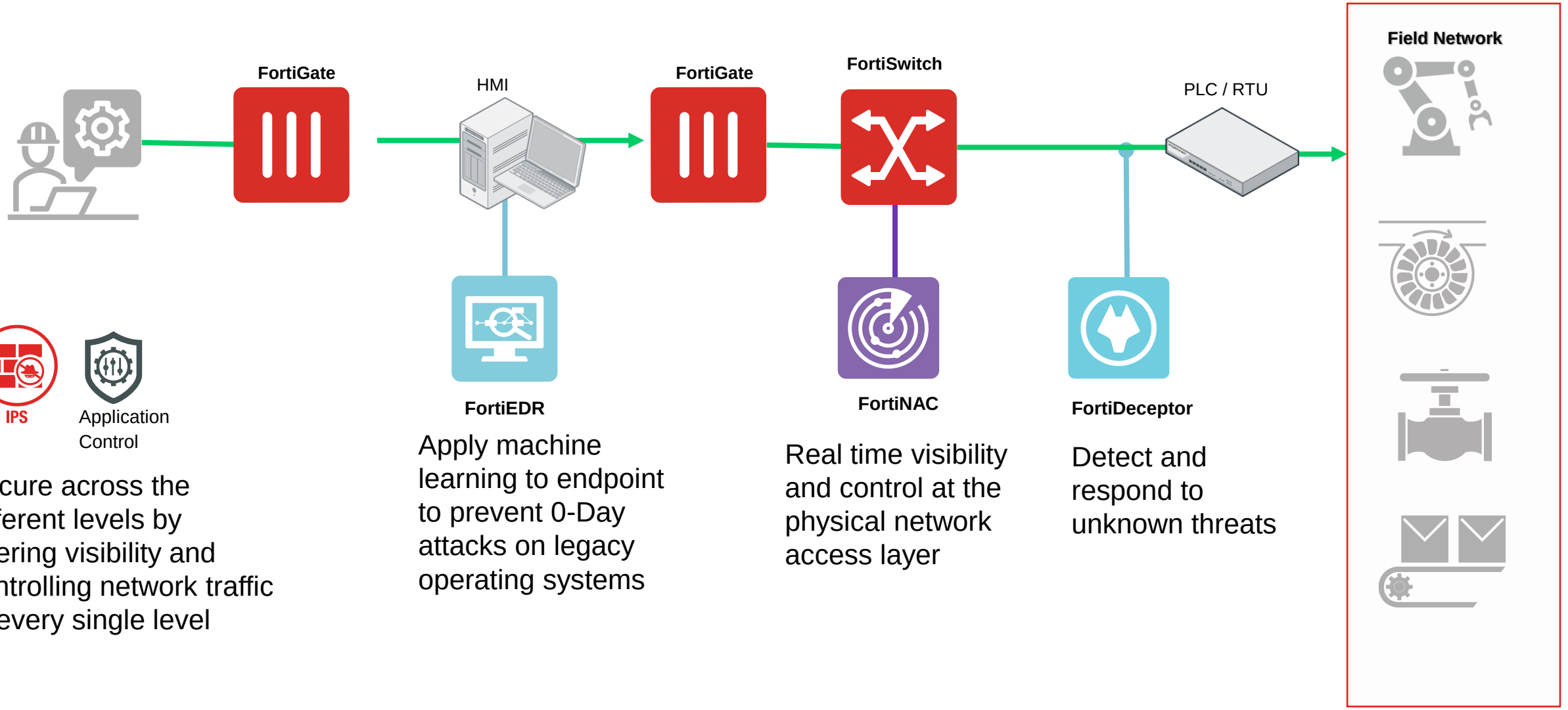
© Fortinet Inc. All Rights Reserved.

Use Case: Lateral movement



© Fortinet Inc. All Rights Reserved.

Ransomware Protection for OT Environments



IPS

Application Control

Secure across the different levels by offering visibility and controlling network traffic at every single level

Apply machine learning to endpoint to prevent 0-Day attacks on legacy operating systems

Real time visibility and control at the physical network access layer

Detect and respond to unknown threats

© Fortinet Inc. All Rights Reserved.

FORTINET®

Secure OT Summit 2022

護航 OT/IT 融合 創新數位發展