



安全納入設計： CISO需要瞭解的原則、承諾與實踐方法

鄺偉基 Daniel Kwong
Fortinet 北亞區 市場總監兼首席資安長

Fortinet 是全球最大、最值得信賴的網路安全公司之一



創立時間：2000 年 10 月

創始人：謝青和謝華

總部：加利福尼亞州桑尼維爾市

Fortinet IPO (FTNT) 時間：2009 年 11 月

納入兩大指數：納斯達克 100 與標普 500

入選：2023 年道瓊永續發展全球與北美指數



全球用戶數量

83萬+

1,378

全球專利數量

2024 帳單收入

\$65.3億+

(截至 2024 年 12 月 31 日)

~\$32億+

自 2017 年以來，我們
一直致力於創新投資，
其中 85% 用於研發
(截至 2024 年 9 月 30 日)

市值

\$725億

(截至 2024 年 12 月 31 日)

證卷投資級評級

BBB+ Baa1



最值得信賴的 美國網路安全公司

Fortinet #7 在富比士最值得信賴的公司排名



#1 在企業網路與安全領域排名

Fortinet 守護 **80%** 《財富》世界 100 強企業和 **72%** 全球 2000 大企業安全

Fortinet 引領社會可持續發展，貢獻卓越力量

解決社會環境中面臨的網路安全風險



全球夥伴
關係和協作共贏



INTERPOL

CENTER FOR
CYBERSECURITY
POLICY AND LAW



減少對環境
的負面影響



承諾
淨零排放

到 2030 年
Fortinet 自有設施

88%
與行業標準 CPU
相比，功耗更低

到 2050 年
跨價值鏈



縮小網資訊安全
技能差距



承諾為
100 萬

人提供資訊安全專業培訓

到 **2026** 年



TECHVETS

WOMCY
LATAM Women in Cybersecurity

600+

培訓機構遍佈 98 個國家/地區

積極推動負責
任的商業實踐



100%

主要合作商已接受我們的合規性和道德
標準培訓

FORTINET

可信資源中心



CSA STAR



GDPR



HIPAA



ISMAP

ISO

ISO 27001

ISO

ISO 27001 SoA

ISO

ISO 9001



SOC 2



TISAX



VPAT



Fortinet 榮獲 天下永續公民獎 外商類組 前 15 大外商公司

全民資安教育・從小扎根

2024天下永續公民獎

天下雜誌
CommonWealth
Magazine

外商企業

2024 排名	2023 排名	公司名稱	平均 總分	企業 承諾	社會 參與	環境 永續
1	3	台灣艾司摩爾科技	8.675	8.67	8.68	8.68
2	10	台灣美光記憶體	8.450	8.26	8.55	8.54
3	5	台灣日立江森自控	8.338	8.27	8.47	8.28
4	11	英屬維京群島商太古可口可樂台灣分公司	8.321	8.26	8.26	8.44
5	2	台灣萊雅	8.250	8.03	8.54	8.18
6	8	滙豐(台灣)商業銀行	8.148	8.21	7.94	8.29
7	-	台灣資生堂	8.138	8.05	8.29	8.07
8	6	星展(台灣)商業銀行	8.136	8.06	8.20	8.14
9	12	巴拿馬商帝亞吉歐台灣分公司	7.999	8.05	7.88	8.07
10	-	花王(台灣)	7.988	7.82	8.04	8.10
11	13	宜家家居	7.942	7.91	7.79	8.13
12	-	德州儀器工業	7.939	8.05	7.96	7.81
13	-	台灣韋能能源	7.743	7.78	7.64	7.80
14	-	台灣阿斯特捷利康	7.619	7.79	7.61	7.46
15	-	 Fortinet Taiwan	7.502	7.41	7.55	7.55



我們用心耕耘・讓數位世界變得更好、更安全

2024天下永續公民獎

天下雜誌
Citizenship
Magazine

外商企業

2024 排名	2023 排名	公司名稱	平均 總分	企業 承諾	社會 參與	環境 永續
1	3	台灣艾司摩爾科技	8.675	8.67	8.68	8.68
2	10	台灣美光記憶體	8.450	8.26	8.55	8.54
3	5	台灣日立江森自控	8.338	8.27	8.47	8.28
4	11	英屬維京群島太古可口可樂台灣分公司	8.321	8.26	8.26	8.44
5	2	台灣萊雅	8.250	8.03	8.54	8.18
6	8	滙豐(台灣)商業銀行	8.148	8.21	7.94	8.29
7	-	台灣資生堂	8.138	8.05	8.29	8.07
8	6	星展(台灣)商業銀行	8.136	8.06	8.20	8.14
9	12	巴拿馬商帝亞吉歐台灣分公司	7.999	8.05	7.88	8.07
10	-	花王(台灣)	7.988	7.82	8.04	8.10
11	13	宜家家居	7.942	7.91	7.79	8.13
12	-	德州儀器工業	7.939	8.05	7.96	7.81
13	-	台灣韋能能源	7.743	7.78	7.64	7.80
14	-	台灣阿斯特捷利康	7.619	7.79	7.61	7.46
15	-	Fortinet Taiwan	7.502	7.41	7.55	7.55

培育資安人才

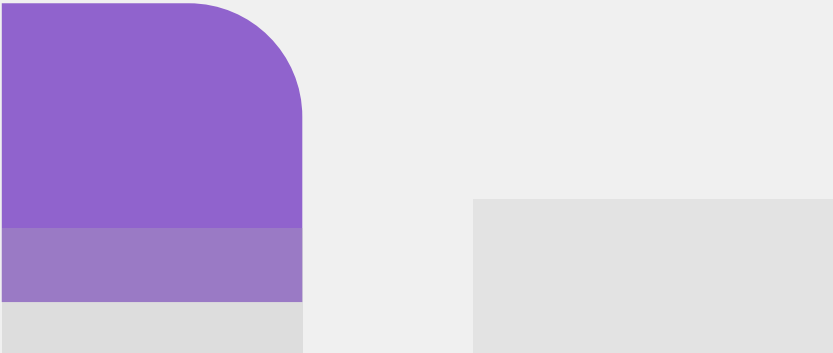
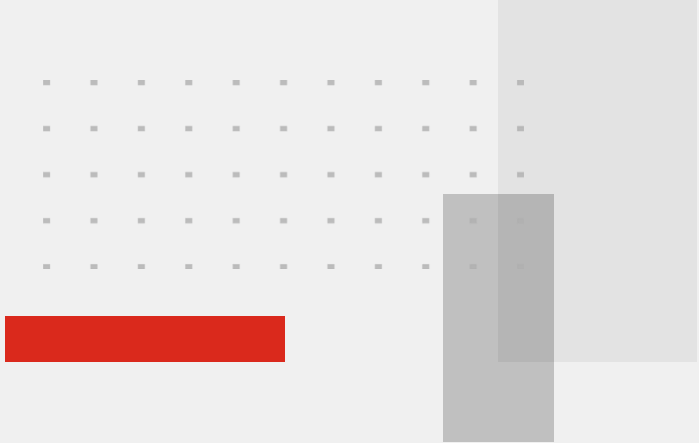
投入全民資安
教育

擴展技術研發

設立全球物流
中心

落實企業ESG

綠色供應鏈管
理



議程

1. 安全納入設計的重要性
2. 實施安全納入設計的核心要素
3. 安全納入設計承諾 – CISA
4. 行動建議與最佳實踐



安全納入設計的重要性

01



甚麼是安全納入設計？



When Volvo invented the three-point seat belt in 1959, they made the patent free for all competitors to use in order to save lives because it had more value as a free life-saving tool than something to profit from.

Volvo Car USA LLC (Volvo) on behalf of Volvo Car Group, has decided that a defect which relates to motor vehicle safety exists in certain model year 2007–2018 S60 Series, V60 Series, S80 Series, XC60, XC70 and V70 vehicles.

找出安全問題

The reason for Recall R10029:

Volvo Cars investigations have identified a problem regarding the front seat belt fastening, mounted on the outboard side of the front seat. The front seat belt fastening cable, may under certain circumstances, suffer from wear and fatigue if repeatedly bent over the seat cushion. This could cause damage to the cable, which could result in reduced or no seat belt restraint function.

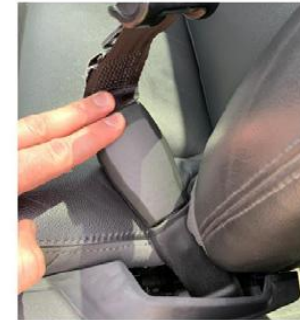
提供替代解決方法直至修復

Until your vehicle has been repaired, we recommend that the driver and passenger secure that the seat belt fastening is in a vertical position, aligned with the backrest (see pictures), so that it will not be bent over the seat cushion when entering the seat. This will reduce the risk of damage of the seat belt fastening.

The seat belt lower fixing buckle rests in a position that is past the bolster of the seat

During entry, this "buckle" is permitted to fold over the lower cushion repeatedly

This can be avoided by placing the seatbelt as above before entry and exit



Seatbelt folded over onto the bottom of the seat

安全納入設計的目標是永續性

安全納入設計誘因 – 資訊安全環境及支出趨勢

全球資安支出增長



- 預計今年年底(2024)，全球資訊安全將達2150億美元，較2023年增長14%，凸顯安全需求緊迫。

威脅和揭露



- 跟蹤趨勢趨勢，把握未來方向，確保安全性揭露原則與時俱進，有效應對新興威脅

投資回報分析



- 企業需審視資安投資回報，理解高支出背後的長期效益與風險規避價值。

供應商數量激增



- 全球超過3,000家資訊安全供應商湧現，市場競爭激烈，推動創新與服務多樣化。

安全納入設計作為企業競爭優勢

減少後續修補工作



- 從產品和服務的初期設計階段就考慮安全性，能顯著降低後期修復成本，提升效率。

建立客戶信任



- 通過展示對安全的重視，企業能夠贏得客戶信任，增強品牌形象，促進業務增長。

安全承諾透明度



- 安全納入設計使企業在競爭中脫穎而出，吸引注重隱私和安全透明度的消費者，擴大市場份額。

實施安全納入設計的核心要素

02



融入產品與服務開發全過程

設計階段整合安全

從構思到實現，安全考量貫穿始終，確保產品天生具備防護能力。

持續集成安全測試

開發流程中自動化安全檢查，及時發現並修復潛在威脅，保障軟體品質。

安全需求驅動設計

基於風險評估定義安全需求，指導設計決策，構建更穩固的系統架構。

增強透明度，揭露風險與客戶信任

01

透明風險溝通

主動向客戶揭露潛在安全風險，建立基於信任的關係。

02

主動漏洞揭露

及時公佈已知漏洞，展現公司對資安的重視與責任感。

03

客戶參與機制

邀請客戶參與資安回饋，共同提升產品安全性。

04

信任建立策略

通過定期資安審計報告，增強客戶對產品安全的信心。

SEC Charges Four Companies With Misleading Cyber Disclosures

One company, Unisys Corp., also charged with controls violations

FOR IMMEDIATE RELEASE | 2024-174

Washington D.C., Oct. 22, 2024 — The Securities and Exchange Commission today charged four current and former public companies – Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd, and Mimecast Limited – with making materially misleading disclosures regarding cybersecurity risks and intrusions. The SEC also charged Unisys with disclosure controls and procedures violations. The companies agreed to pay the following civil penalties to settle the SEC's charges:

- Unisys will pay a \$4 million civil penalty;
- Avaya. will pay a \$1 million civil penalty;
- Check Point will pay a \$995,000 civil penalty; and
- Mimecast will pay a \$990,000 civil penalty.



減少漏洞，強化防禦

實踐穩健設計



- 通過嚴謹的設計流程，從源頭減少潛在漏洞，確保系統穩固可靠

持續安全審計



- 定期進行安全審查，及時發現並修復新出現的威脅，增強系統防護能力。

最小許可權原則



- 限制系統元件存取權限，僅提供執行特定任務所需的最低許可權，降低風險暴露面。

加密與資料保護



- 採用增強式加密技術保護敏感資訊，確保資料在傳輸和存儲過程中的安全性和隱私

安全納入設計承諾-CISA

03



安全納入設計：提升多因素認證採用率



01

MFA成長趨勢

CISA展示MFA使用率顯著增長，強調安全身份驗證的重要性。

02

預設啟用MFA

在產品中預設啟用MFA，簡化用戶體驗，提升帳戶安全性。

03

用戶信任建立

通過MFA的普及，增強使用者對產品安全性的信心，促進長期忠誠度。

CISA 安全納入設計：漏洞報告與修補政策

01

記憶體安全(Memory Safe) 路線圖 跨產品線補丁統計

發佈針對不同類別的(MSL)漏洞修復計畫，明確時間表與優先順序，確保透明度與及時回應。

02

分享補丁採用的統計資料，證明對安全更新的重視與執行效率，增強客戶信心。

03

更新揭露政策

定期更新漏洞揭露與日誌保留政策，遵循最佳行業實踐，保障資訊處理的合規性。



Lacework FortiCNAPP 守護軟件開發安全納入設計

守護代碼安全到雲安全的統一防護平臺



部署

- 開發過程中的掃描碼和 API
- 解決安全性漏洞、惡意軟體和配置錯誤等問題
- 通過攻擊路徑分析明確風險優先順序

代碼安全

SCA

軟體元件
分析

SAST

靜態應用程式安全
測試

IaC

基礎設施即代碼
安全性

運行

- 評估雲基礎設施配置
- 評估身份及其存取權限
- 防止部署不合規的應用程式

雲配置

V A

漏洞評估

CSPM

安全態勢
管理

CIEM

雲基礎設施許可權管
理

代碼

- 持續監控風險暴露和敏感性資料
- 即時檢測異常行為和活躍威脅
- 即時掌控正在運行的進程或程式並映射網路連接

運行保護

CWP

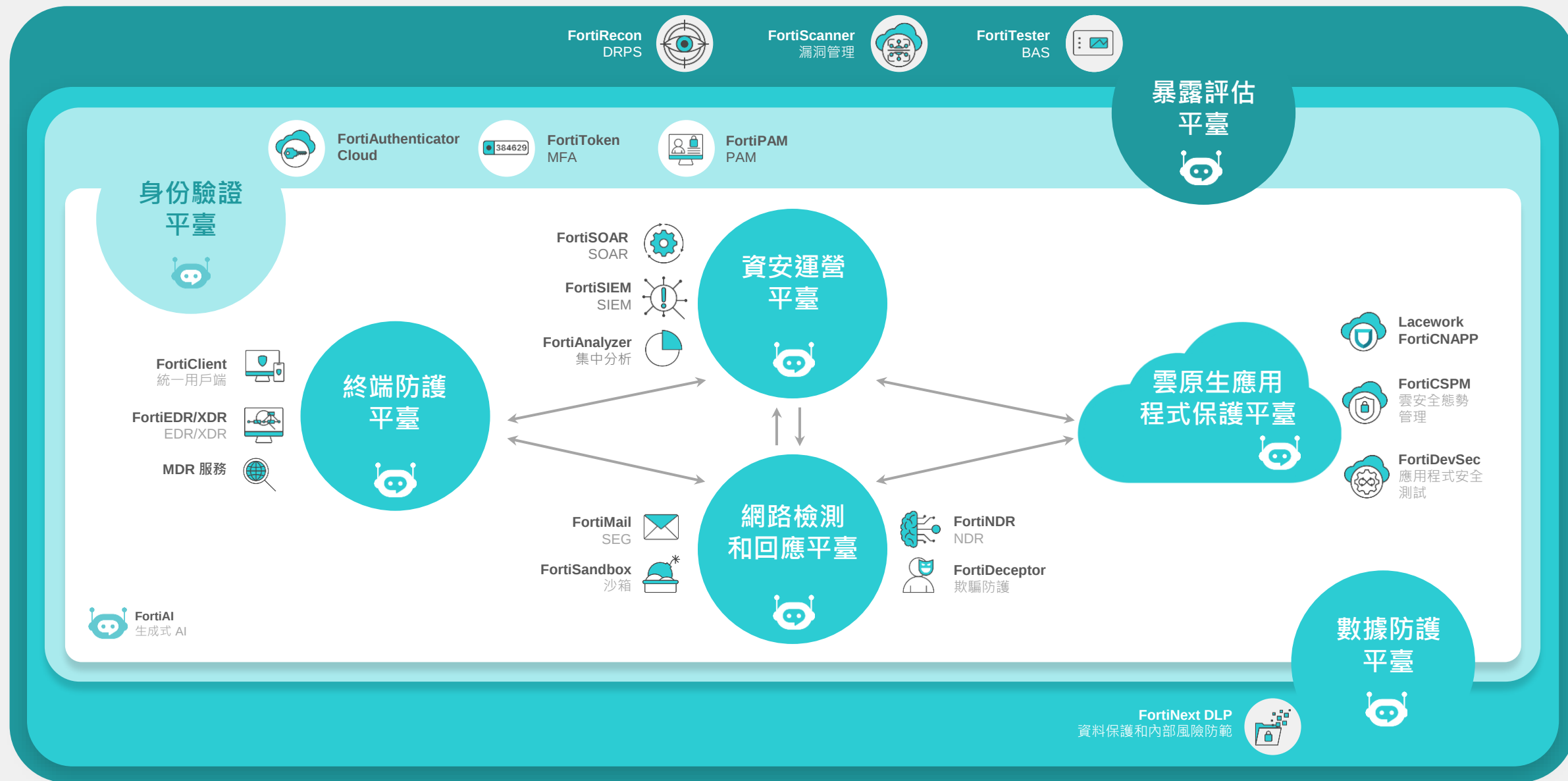
雲工作負載保護

CDR

雲檢測與
回應



AI 驅動的資安運營助力安全納入設計



行動建議與最佳實踐

04



構建安全納入設計文化培訓計畫



全員參與的安全納入意識

創建一個跨部門溝通與協作的平臺，確保資訊流暢，促進團隊間知識共用與問題解決。



定期安全納入培訓

提供持續的教育和培訓，使員工掌握最新的安全威脅和防護措施。



實戰演練與模擬攻擊

通過類比網路攻擊，測試並加強員工的反應能力和系統的防禦機制。



激勵與認可機制

設立獎勵制度，表彰在安全實踐中表現突出的個人或團隊，激發全員的積極性。



安全納入設計在競爭市場中脫穎而出

01

差異化優勢

- 通過展示強大的安全納入設計能力，企業能在眾多競爭對手中脫穎而出，吸引注重資料安全的客戶群體。

02

客戶信任基礎

- 安全納入設計增強了客戶對品牌的信任，成為企業口碑傳播的關鍵驅動力，助力市場份額的穩步增長。

03

創新吸引力

- 將安全納入設計作為核心競爭力，企業能夠吸引尋求創新解決方案的客戶，推動業務模式的持續進化。

04

長期價值創造

- 安全納入設計不僅滿足短期合規需求，更構建了企業的長期價值，為企業贏得持續的競爭優勢。



Fortinet Fabric 廣泛集成安全納入設計所需要高效工具

安全網路



網路安全



FortiGate
新世代防火牆



FortiGate VM
虛擬防火牆



FortiCNF
雲原生防火牆



FGaaS
防火牆即服務



FortiGate
強固型新世代防火牆

企業網路



FortiSwitch
網路交換器



FortiAIOPS
AI 網路營運



FortiAP
無線基地台



FortiNAC
網路存取控制



FortiSwitch
強固型交換器



FortiExtender
LTE / 5G



FortiAP
強固型無線基地台



FortiExtender
強固型延展器



FortiManager
集中式管理

Unified SASE



安全存取



FortiSASE
安全服務邊緣
SSE



FortiGate
軟體定義廣域網路
SD-WAN



FortiClient
零信任網路存取
ZTNA



FortiProxy
安全網頁閘道器
SWG



FortiMonitor
數位體驗監看
DEM



FortiCASB
雲端存取
安全代理

雲端安全



FortiGate VM
虛擬防火牆



FortiWeb
網頁應用與
API 防護



FortiGate CNF
雲原生防火牆



FortiCNAPP
雲原生應用
保護平台



FortiADC
應用服務派送

安全營運



FortiEDR / XDR
端點偵測與回應 /
延展型偵測與回應



FortiNDR
網路偵測與回應



FortiAnalyzer
日誌記錄智能分析



FortiDeceptor
進階欺敵誘捕
技術



FortiSIEM
安全資訊與
事件管理



SOCaaS
安全營運中心
即服務



FortiRecon
數位風險保護服務
DRPS



FortiSOAR
安全協作與
自動化回應



MDR Service
託管型偵測與
回應服務



FortiAuthenticator
認證管理



FortiSandbox
智能沙箱



IR Service
事件回應服務



FortiToken
多因子認證
MFA



FortiPAM
特權帳號管理



FortiMail
安全電郵閘道器
SEG



FortiDLP
資料外洩防護



FortiTrust
身分識別

