FERTINET®

FortiSandbox™

Multi-layer proactive threat mitigation

Today's most sophisticated cybercriminals are increasingly bypassing traditional antimalware solutions and inserting advanced persistent threats deep within networks. These highly targeted attacks evade established signature-based detection by masking their malicious nature in many ways — compression, encryption, polymorphism, the list of techniques goes on. Some have even begun to evade virtual "sandbox" environments using VM detection, "time bombs" and more. Fighting today's attacks requires a comprehensive and integrated approach — more than antimalware. More than a virtual sandbox. More than a separate monitoring system.

FortiSandbox offers a robust combination of proactive detection and mitigation, actionable threat insight and easy, integrated deployment. At its foundation is a unique, dual-level sandbox which is complemented by Fortinet's award-winning antimalware and optional integrated FortiGuard threat intelligence. Years of Fortinet threat expertise is now packaged up and available on site via FortiSandbox.

Proactive Detection and Mitigation

Suspicious codes are subjected to multi-layer pre-filters prior to execution in the virtual OS for detailed behavioral analysis. The highly effective pre-filters include a screen by our AV engine, queries to cloud-based threat databases and OS-independent simulation with a code emulator, followed by execution in the full virtual runtime environment. Once a malicious code is detected, results are submitted for antimalware signature creation as well as updates to other threat databases.

Actionable Insight

All classifications — malicious and high/medium/low risk — are presented within an intuitive dashboard. Full threat information from the virtual execution — including system activity, exploit efforts, web traffic, subsequent downloads, communication attempts and more — is available in rich logs and reports.

Easy Deployment

FortiSandbox supports inspection of many protocols in one unified solution, thus simplifies network infrastructure and operations. Further, it integrates with FortiGate as a new capability within your existing security framework.

The ultimate combination of proactive mitigation, advanced threat visibility and comprehensive reporting.

- Secure virtual runtime environment exposes unknown threats
- Unique multi-layer pre-filters for fast and effective threat detection
- Rich reporting for full threat lifecycle visibility
- Inspection of many protocols in one appliance simplifies deployment and reduces cost
- Integration with FortiGate enhances rather than duplicates security infrastructure
- Validated security with NSS BDS (Breach Detection Systems) testing

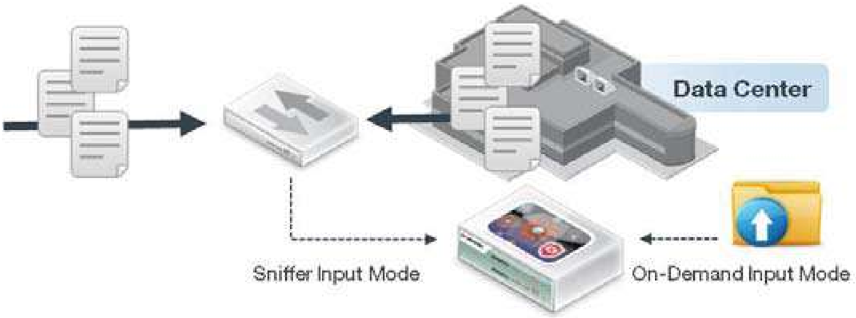
NSS LABS RECOMMEND

DEPLOYMENT OPTIONS

The FortiSandbox is the most flexible threat analysis appliance in the market as it offers various deployment options for customers' unique configurations and requirements. Organizations can also have all three input options at the same time.

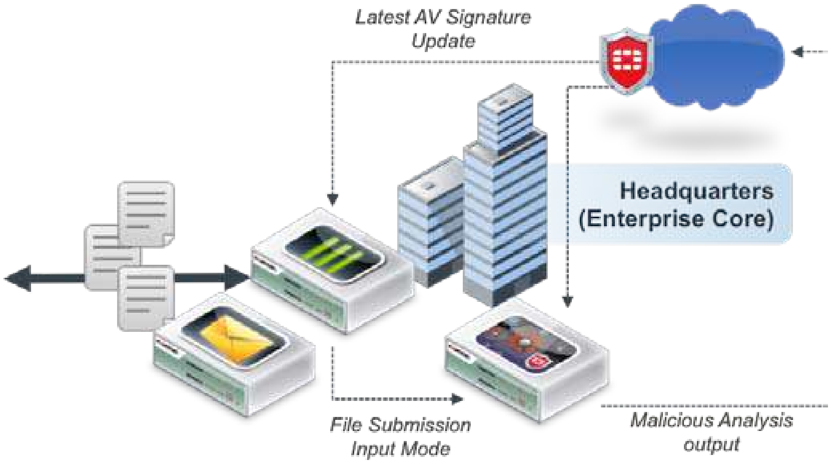
Standalone

This deployment mode relies on inputs from spanned switch ports and/or administrators' on-demand file uploads using the GUI. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from various vendors.



*FortiGate/FortiMail Integrated

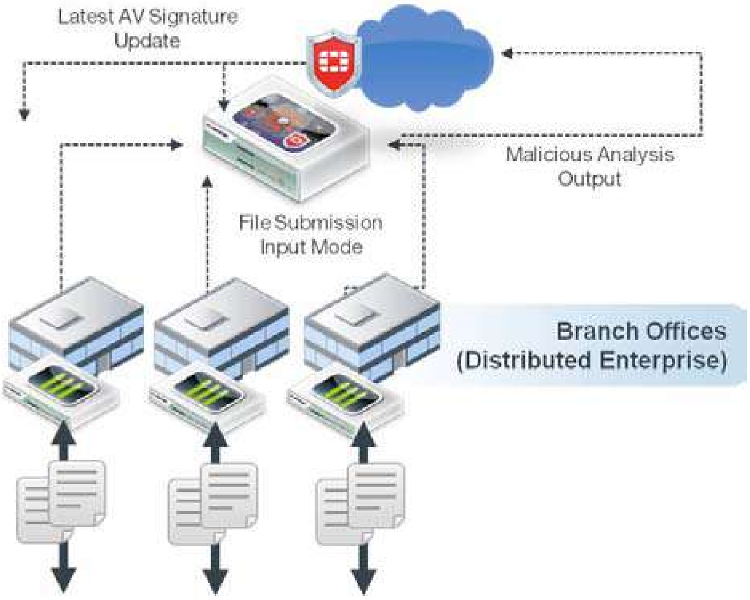
The FortiGate, as the Internet security gateway, can be set up to submit suspicious files to the FortiSandbox. This seamless integration reduces network complexity and expands the applications and protocols supported including SSL encrypted ones such as HTTPS.


Latest AV Signature Update
Headquarters (Enterprise Core)
File Submission Input Mode
Malicious Analysis output

* Requires: FortiOS V5.0.4+, FortiMail V5.1+

Distributed FortiGate Integrated

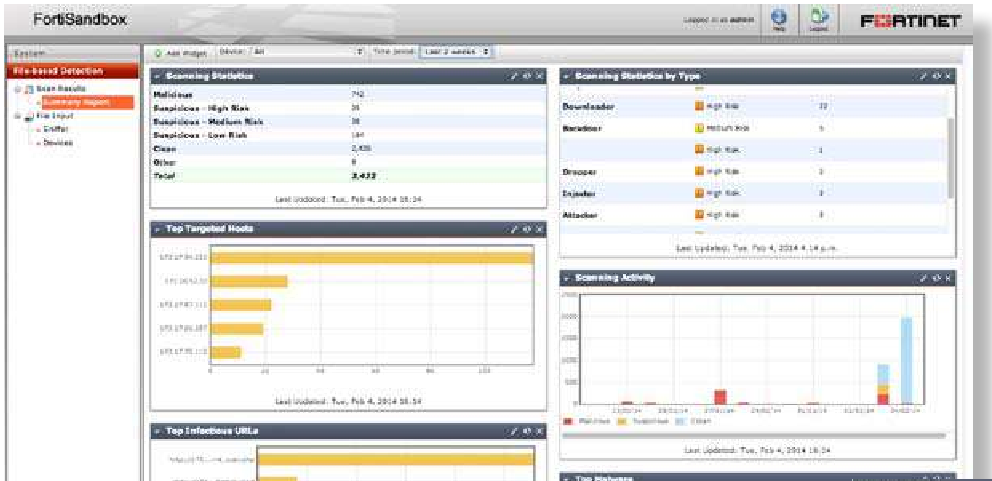
This deployment is attractive for organizations that have distributed environments, where FortiGates are deployed in the branch offices and submit suspicious files to a centrally-located FortiSandbox. This setup yields the benefits of lowest TCO and protects against threats in remote locations.


Latest AV Signature Update
Malicious Analysis Output
File Submission Input Mode
Branch Offices (Distributed Enterprise)

FEATURES

VM Sandboxing

Complement your established defenses with cutting-edge capability — analyzing suspicious and high-risk files in a contained environment to uncover the full attack lifecycle using system activity and callback detection.



Scanning Statistics

Malicious	742
Suspicious - High Risk	35
Suspicious - Medium Risk	38
Suspicious - Low Risk	164
Clean	2,435
Other	8
Total	3,422

Last Updated: Tue, Feb 4, 2014 15:24

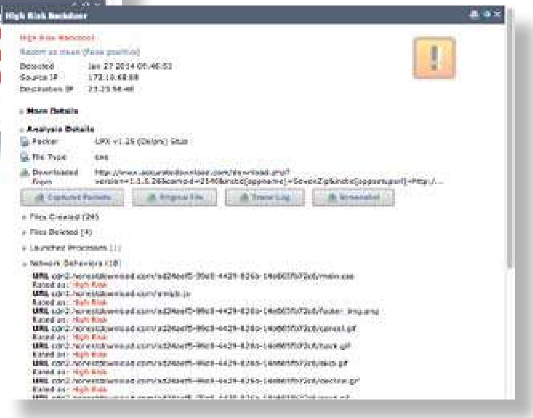
Scanning Statistics by Type

Downloader	High Risk	22
Backdoor	Medium Risk	5
	High Risk	1
Dropper	High Risk	3
Injector	High Risk	2
Attacker	High Risk	8

Last Updated: Tue, Feb 4, 2014 4:14 p.m.

Dashboard widgets — real-time threat status

Detailed file analysis report



High Risk Backdoor

Report as clean (false positive)

Detected	Jan 27 2014 05:46:53
Source IP	172.16.68.88
Destination IP	23.23.58.48

Main Details

Analysis Details

Packer	UPX v1.25 (Delphi) Stub
File Type	exe
Downloaded From	[illegible]

Files Created (24)

Files Deleted (4)

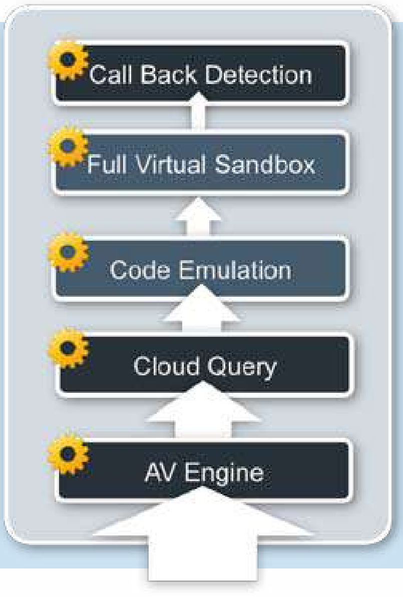
Launched Processes (1)

Network Behaviors (18)

URL [illegible]/main.exe
Rated as: High Risk
URL [illegible]
Rated as: High Risk
URL [illegible]
Rated as: High Risk
URL [illegible]/cancel.gif
Rated as: High Risk
URL [illegible]/back.gif
Rated as: High Risk
URL [illegible]
Rated as: High Risk
URL [illegible]
Rated as: High Risk

File Analysis Tools

Reports with captured packets, original file, tracer log and screenshot provide rich threat intelligence and actionable insight after files are examined. This is to speed up remediation and updated protection.



Multi-tiered file processing optimizes resource usage that improves security, capacity and performance

AV Engine

- Applies top-rated (95%+ Reactive and Proactive) AV Scanning. Serves as an efficient pre-filter.

Cloud Query

- Real-time check of latest malware information
- Access to shared information for instant malware detection

Code Emulation

- Quickly simulates intended activity
- OS independent and immune to evasion/obfuscation

Full Virtual Sandbox

- Secure run-time environment for behavioral analysis/rating
- Exposes full threat lifecycle information

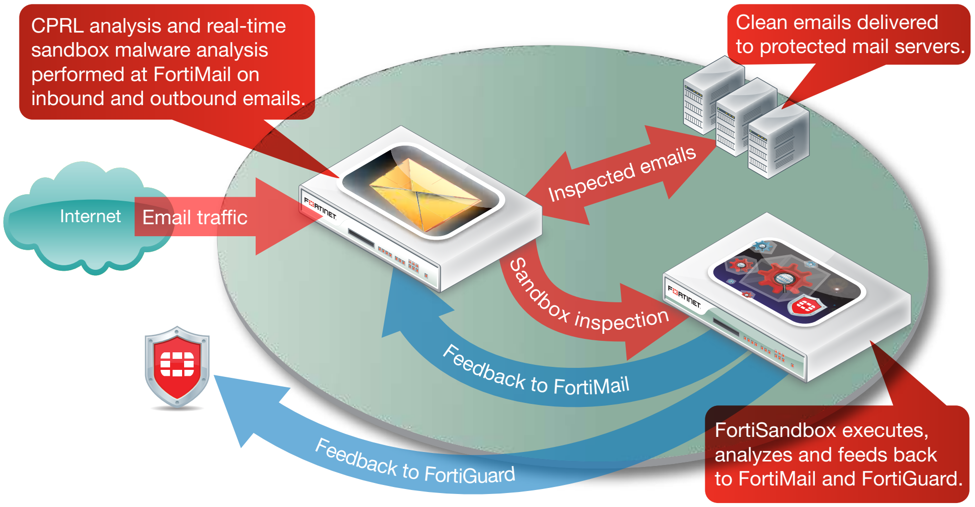
Call Back Detection

- Identifies the ultimate aim, call back and exfiltration

FEATURES

Remediation with FortiMail

With many advanced threats starting with a targeted email that contains custom malware, in addition to social engineering that entices the user to open it, organizations are extending their secure email gateway (SEG) with integrated sandboxing. Specifically, the SEG will hold messages while additional analysis is performed in this contained run-time environment and, ultimately, apply policies based on its returned findings.


CPRL analysis and real-time sandbox malware analysis performed at FortiMail on inbound and outbound emails.

Clean emails delivered to protected mail servers.

FortiSandbox executes, analyzes and feeds back to FortiMail and FortiGuard.

FortiMail submits and queues for suspicious content

FEATURES SUMMARY

Administration

Supports WebUI and CLI configurations

Multiple administrator account creation

Configuration file backup and restore

Notification email when malicious file is detected

Weekly report to global email list and FortiGate administrators

Centralized search page which allows administrators to build customized search conditions

Frequent signature auto-updates

VM status monitoring

Networking/Deployment

Static Routing Support

File Input: Offline/sniffer mode, On-demand file upload, file submission from integrated device(s)

Web-based API with which users can upload samples to scan indirectly

Option to create simulated network for scanned file to access in a closed network environment

Device Integration:
- File Submission input: FortiGate, FortiMail
- Update Database host: FortiManager
- Remote Logging: FortiAnalyzer, Syslog Server

Advanced Threat Protection

Virtual OS Sandbox:
- Concurrent Windows instances
- Anti-evasion techniques: sleep calls, process and registry queries
- Callback Detection: malicious URL visit, Botnet C&C communication and Attacker traffic from activated malware
- Download Capture packets, Original File, Tracer log and Screenshot

Unlimited file size support, maximum file size configurable

File type support:
- Archived: .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj
- Executable files (eg: .exe, .dll), PDF, Windows Office Document and Javascript
- Media files: .avi, .mpeg, .mp3, .mp4

Protocols/applications supported:
- Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
- Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL encrypted versions
- Integrated mode with FortiMail: SMTP, POP3, IMAP

Network Threat Detection in Sniffer Mode: Identify Botnet activties and network attacks, malicious URL visit

Option to auto-submit suspicious files to cloud service for manual analysis and signature creation

Monitoring and Report

Real-Time Monitoring Widgets (viewable by source and time period options): Scanning Result statistics, Scanning Activities (over time), Top Targeted Hosts, Top Malware, Top Infectious URLs, Top Callback Domains

Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time and download path

Logging — GUI, download RAW log file

Report generation for malicious files: Detailed reports on file characteristics and behaviors – File Modification, Process Behaviors, Registry Behaviors, Network Behaviors, VM snapshot

Further Analysis: Downloadable files — Sample file, Sandbox tracer logs and PCAP capture

SPECIFICATIONS

	FSA-1000D	FSA-3000D
Hardware		
Form Factor	2 RU	2 RU
Total Network Interfaces	6x GE RJ45 ports, 2x GE SFP slots	4x GE RJ45 ports, 2x GE SFP slots 2x 10 GE SFP+ Slots
Storage Capacity	4 TB (max. 8 TB)	8 TB (max. 16 TB)
Power Supplies	2x Redundant PSU	2x Redundant PSU
System		
VM Sandboxing (Files/Hour)	160	560
AV Scanning (Files/Hour)	6,000	15,000
Number of VMs	8	28
Dimensions		
Height x Width x Length (in)	3.5 x 17.2 x 14.5	3.3 x 19.0 x 29.7
Height x Width x Length (mm)	89 x 437 x 368	84 x 482 x 755
Weight	27.60 lbs (12.52 kg)	71.5 lbs (32.5 kg)

	FSA-1000D	FSA-3000D
Environment		
Power Consumption (AVG / MAX)	115 / 138 W	392 / 614.6 W
Maximum Current	100V/5A, 240V/3A	110V/10A, 220V/5A
Heat Dissipation	471 BTU/h	2131.14 BTU/h
Power Source	100–240 VAC, 60–50 Hz	100–240 VAC, 60–50 Hz
Humidity	5–95% non-condensing	20–90% non-condensing
Operation Temperature Range	32–104°F (0–40°C)	50–95°F (10–35°C)
Storage Temperature Range	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)
Compliance		
Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	

	FSA-VM
Hardware Requirement	
Hypervisor Support	VMware ESXi version 5.0 or later
Virtual CPUs (Min / Max)	4 / Unlimited (Fortinet recommends that the number of vCPUs match the number of Windows VM +4.)
Virtual Memory (Min / Max)	8 GB / Unlimited
Virtual Storage (Min / Max)	30 GB / 16 TB
Total Virtual Network Interfaces (Min)	6
System	
VM Sandboxing (Files/Hour)	Hardware Dependent
AV Scanning (Files/Hour)	Hardware Dependent
Number of VMs	2 to 52 (Upgrade via appropriate licenses)

ORDER INFORMATION

Product	SKU	Description
FortiSandbox 1000D	FSA-1000D	Advanced Threat Protection System — 6x GE RJ45, 2x GE SFP slots, redundant PSU, 6 Windows XP licenses and 2 Windows 7 licenses included.
FortiSandbox 3000D	FSA-3000D	Advanced Threat Protection System — 4x GE RJ45, 2x GE SFP slots, redundant PSU, 22 Windows XP licenses and 6 Windows 7 licenses included.
FortiSandbox-VM	FSA-VM-BASE	Base license for stackable FortiSandbox-VM. Includes (1) Windows XP and (1) Windows 7 VM license. FSA-VM maximum expansion limited to 52 total VMs.

Optional Accessories	SKU	Description
1 GE SFP SX transceiver module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX transceiver module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ transceiver module, short range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ transceiver module, long range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.

GLOBAL HEADQUARTERS

Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE

120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE

300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE

Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Product Matrix

產品	效能	Description	作業版本
FG-FW-Base Fortinet 網路防火牆 500Mbps	網路防火牆 500Mbps	提供防火牆控管存取政策,使用者身份辨識,IPSEC VPN , SSL VPN, SLB(主機負載平衡）及 無線網路控制器（Wireless Controller）	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
FG-FW-1000-UG Fortinet 網路防火牆 頻寬升級 1Gbps	網路防火牆 頻寬升級 1Gbps		
FG-VM01/VM02/VM04/VM08 Fortinet 網路防火牆 (授權方式:依照 CPU 數量 1/2/4/8 四個授權方式出貨)	網路防火牆 支援 1 CPU		
FG-NGFW-Base Fortinet 新世代網路防火牆 500Mbps (含 FW, IPS, Application Control, AV, Web Filtering and Antispam)	新世代網路防火牆 500Mbps	提供防火牆控管存取政策,使用者身份辨識,IPSEC VPN , SSL VPN, SLB(主機負載平衡）， 無線網路控制器（Wireless Controller），入侵防禦，應用程式控管，防毒，不當網頁過濾，防垃圾郵件	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
FG-NGFW-1000-UG Fortinet 新世代網路防火牆 頻寬升級 1Gbps (含 FW, IPS, Application Control, AV, Web Filtering and Antispam)	新世代網路防火牆 頻寬升級 1Gbps		
FG-VM01/VM02/VM04/VM08 Fortinet 新世代網路防火牆 500Mbps （含 FW, IPS, Application Control, AV, Web Filtering and Antispam) (授權方式:依照 CPU 數量 1/2/4/8 四個授權方式出貨)	新世代網路防火牆 支援 1 CPU		
FMG-VM-Base Fortinet 集中管理系統	集中管理系統 10 台設備	Fortinet 防火牆管理，設定和集中派送（政策，資安防禦資料庫）的中央管理系統 r, 支援 10 台設備	Vmware Hyper-V AWS
FMG-VM-10-UG Fortinet 集中管理系統	集中管理平台設備 數量升級 - 10 台設備		
FAZ-VM-BASEFortinet 集中日誌報表系統	集中日誌報表系統	Fortinet 防火牆的集中日誌報表管理系統	Vmware Hyper-V AWS
FAZ-VM-GB1 Fortinet 集中日誌報表系統 紀錄數量升級 - 1 GB/Day	集中日誌報表系統 紀錄數量升級 - 1 GB/Day		
FSA-VM Fortinet 先進威脅防護系統 (ATP)	先進威脅防護系統 (ATP)	即時執行沙箱檢測，提供虛擬的運行環境來分析高風險或可疑的程式，研判威脅完整的生命周期，協助用戶智慧地立即偵測出既存與新興的 網路威脅。	VMware

FWB-Base Fortinet 網站應用程式防火牆(WAF) 25Mbps	網站應用程式防火牆(WAF) 25Mbps	提供網站應用程式防火牆功能（WAF）， 網頁防置換，網頁自動備份及回復等功能	Vmware Hyper-V Citrix Xen Open Xen AWS
FWB-100-UG Fortinet 網站應用程式防火牆(WAF) 頻寬升級 100Mbps	網站應用程式防火牆(WAF) 頻寬升級 100Mbps		
FWB-VM01/VM02/VM04/VM08 Fortinet 網站應用程式防火牆(WAF) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	網站應用程式防火牆(WAF) 支援 1 CPU		
FAD-Base Fortinet 主機負載平衡系統 (SLB) 1Gbps	主機負載平衡系統(SLB) 1Gbps	支援網路的主機負載平衡，全球服務負載平衡（GSLB）及線路負載平衡（LLB）等功能	VMware
FAD-1000-UG Fortinet 主機負載平衡系統 (SLB) 頻寬升級 1Gbps	主機負載平衡系統(SLB) 頻寬升級 1Gbps		
FAD-VM01/VM02/VM04/VM08 Fortinet 主機負載平衡系統(SLB) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	主機負載平衡系統(SLB) 支援 1 CPU		
FML-Base Fortinet 反垃圾郵件及郵件保全系統 100 人版	反垃圾郵件及郵件保全系統 100 人版	提供電子郵件主機功能、過濾並攔截垃圾郵件	VMware Hyper-V Citrix Xen KVM
FML-300-UG Fortinet 反垃圾郵件及郵件保全系統 使用者數量升級 300 人	反垃圾郵件及郵件保全系統 使用者數量升級 300 人		
FML-VM01/VM02/VM04/VM08 Fortinet 反垃圾郵件及郵件保全系統 (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	反垃圾郵件及郵件保全系統 支援 1 CPU		
FAC-VM-Base Fortinet 身份認證系統 (Authenticator) 100 人版	身份認證系統(Authenticator) 100 人版	整合 RADIUS、LDAP 伺服器，提供標準及安全的雙因子認證	VMWare Hyper-V
FAC-VM-100-UGFortinet 身份認證系統 (Authenticator) 使用者數量升級 100 人	身份認證系統(Authenticator) 使用者數量升級 100 人		