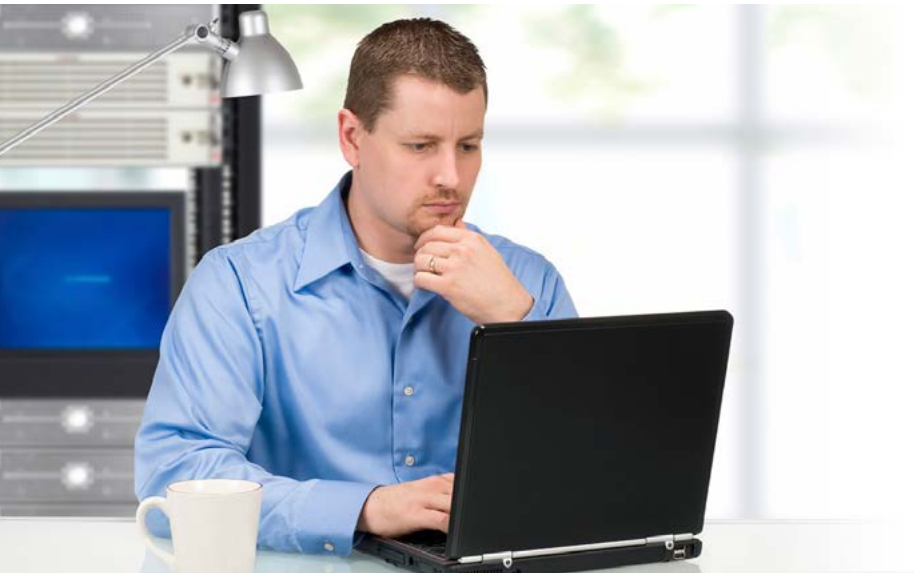
FICHE TECHNIQUE



FortiAnalyzer™
Centralisation de l'enregistrement, des analyses et de la génération de rapports

FortiAnalyzer

FortiAnalyzer 200D, 400E, 1000E, 2000E, 3000E, 3000F, 3500E, 3500F, 3900E et FAZ-VM

Les réseaux d'entreprise sont en évolution constante du fait de la croissance organisationnelle et des exigences réglementaires et commerciales. Il en résulte des montagnes de données issues des appliances de sécurité, une absence de visibilité et un contexte historique de menaces dynamiques. Étant donné le paysage des menaces actuel, ces dernières peuvent rester indétectées pendant un temps extrêmement long.

Visibilité instantanée, réponse rapide aux incidents

C'est là qu'intervient Fortinet Security Fabric, pour une protection unifiée de bout en bout — en déployant les Enterprise Firewalls de Fortinet pour combattre les menaces persistantes avancées et en ajoutant FortiAnalyzer pour étendre la structure de sécurité, pour une visibilité accrue et des informations d'alerte de sécurité robustes, à la fois interactives et automatisées.

FortiAnalyzer vous permet de collecter, d'analyser et de mettre en relation les données des journaux de votre réseau distribué d'Enterprise Firewalls de Fortinet de manière centralisée, de voir tout le trafic de pare-feu et de générer des rapports à partir d'une seule console. Avec un abonnement au service FortiGuard Indicator of Compromise (IOC), vous pouvez obtenir une liste de priorités des hôtes compromis de façon à pouvoir intervenir rapidement.

Fonctionnalités et avantages clés

Recherches et rapports centralisés	Une expérience de recherche et de rapports simple et intuitive, à la manière de Google, sur le trafic réseau, les menaces, les activités du réseau et les tendances au sein de ce dernier.
Indicators of Compromise (IOC) automatisés	Analyse des journaux de sécurité pour la détection des menaces automatisée.
Vues historiques et en temps réel de l'activité du réseau	Affichage d'une synthèse des applications, des sources, des destinations, des sites Web, des menaces de sécurité, des modifications administratives et des événements système.
Gestion d'événements légère	Les définitions d'événements de sécurité prédéfinies sont facilement personnalisables avec des alertes automatisées.
Intégration transparente avec Fortinet Security Fabric	Assure la mise en relation avec les journaux de FortiClient, FortiSandbox, FortiWeb et FortiMail, etc., pour une visibilité renforcée.

FORTINET SECURITY FABRIC

Fortinet Security Fabric protège les entreprises de l'IdO jusqu'au cloud. FortiAnalyzer recueille et met en relation les informations réseau et de sécurité de la structure et les présente à partir d'une console de gestion unique.

forti.net/sf

CARACTÉRISTIQUES PRINCIPALES

FortiView — Une visibilité réseau puissante

- Un tableau interactif personnalisable permet de pointer et résoudre rapidement les problèmes
- Vues synthétiques et intuitives du trafic réseau, des menaces, des applications et bien plus encore
- Vues granulaires des utilisateurs sans fil, des points d'accès non autorisés et des vulnérabilités des terminaux
- Visualisation avec graphiques à bulles et Threat Map géographique
- Exploration permettant de suivre la trace des pirates, de remonter les transactions et d'obtenir plus d'informations exploitables

FortiGuard Indicators of Compromise — Moteur de corrélation automatisé

- Analyse les journaux de sécurité FortiGate pour identifier les modèles de trafic suspects
- Système de défense contre les violations automatisé qui surveille en permanence votre réseau à la recherche de potentielles attaques
- Présentation d'une liste de priorités des hôtes compromis nécessitant une intervention
- IOC améliore l'approche de sécurité et aide les organisations à se protéger grâce à une détection précise des menaces avancées

Rapport

- Plus de 28 modèles intégrés avec exemples de rapports prêts à l'emploi
- Génération de rapport sur demande ou à échéance fixe, avec notification automatisée par e-mail et vue Calendrier
- Formats de rapport flexibles : HTML/CSV/XML/PDF
- Rapports personnalisés : plus de 300 graphiques intégrés pour des rapports personnalisés et un concepteur de graphique intuitif permettant de créer facilement tableaux et graphiques à partir des résultats des recherches dans les journaux

Moniteur et alerte

- Surveillance active de votre réseau en temps réel afin d'identifier les questions, les problèmes et les attaques
- Plus de 20 définitions d'événements intégrées prêtes à l'emploi et totalement personnalisables
- Notification d'alerte automatisée pour une réponse rapide
- Exploration des détails des événements pour une investigation sans délai

Mutualisation avec gestion flexible des quotas

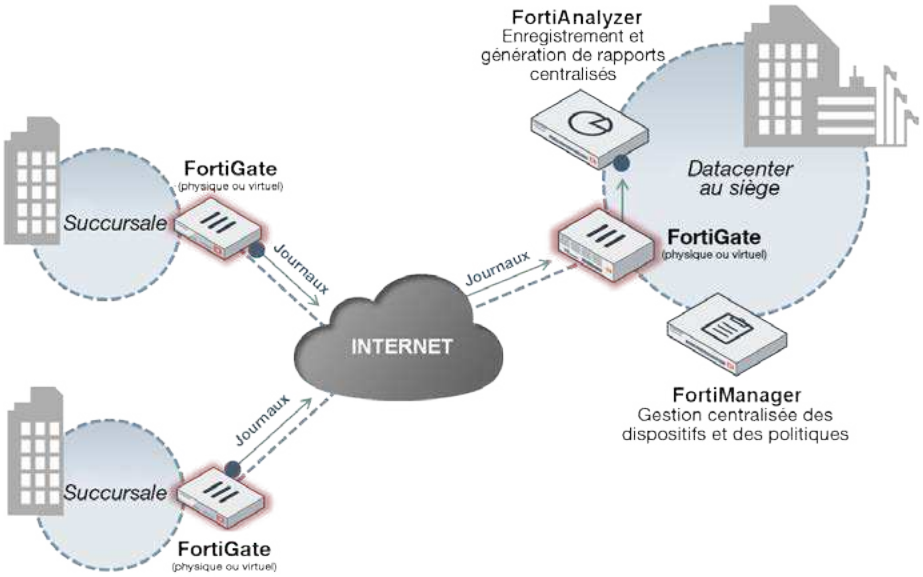
- Politique de données de journaux analytiques/ archives temporelles par domaine administratif (ADOM)
- Gestion automatisée des quotas en fonction de la politique définie
- Graphiques de tendances pour guider la configuration de la politique et la surveillance des usages

Récupération de journaux pour analyse détaillée

- Récupération des journaux archivés pour examiner les données historiques dans le cadre d'une analyse détaillée
- Options de récupération flexibles : récupération de tous les journaux ou de ceux sélectionnés sur une période donnée
- Facilité de configuration : la récupération est définie à distance entre client et serveur, en quelques clics

Transmission des journaux pour intégration tierce

- Transmission des journaux vers des systèmes tels qu'un serveur Syslog, un serveur de journaux CEF ou un système FortiAnalyzer à des fins de stockage à long terme, d'analyse détaillée ou de conformité réglementaire
- Configuration flexible : tous les journaux sont transmis ou, grâce à des filtres, uniquement ceux présentant un intérêt, selon la configuration choisie
- Contrôle des champs des journaux envoyés aux serveurs Syslog ou CEF



SPÉCIFICATIONS

	FORTIANALYZER 200D	FORTIANALYZER 400E	FORTIANALYZER 1000E
Capacité et performances			
Go/Jour d'enregistrement	5	75	300
Vitesse d'analyse (journaux/s)	120	500	4 000
Vitesse de collecte (journaux/s)	350	725	6 000
Appareils/VDOM/ADOM (maximum)	150	200	2 000
Options prises en charge			
Indicators of Compromise (IOC) FortiGuard	Oui	Oui	Oui
Fonctions FortiManager (jusqu'à 20 appareils)	Non	Non	Oui
Spécifications matérielles			
Format	1 U (montage en rack)	1 U (montage en rack)	2 U (montage en rack)
Nombre total d'interfaces	4 GbE	4 GbE	2 GbE
Capacité de stockage	1 To (1 x 1 To)	12 To (4 x 3 To)	24 To (8 x 3 To)
Disques durs amovibles	Non	Oui	Oui
Niveaux RAID pris en charge	Aucun	RAID 0/1/5/10	RAID 0/1/5/6/10/50/60
Niveau RAID par défaut	—	10	50
Alimentations remplaçables à chaud redondantes	Non	Non	Oui
Dimensions			
Hauteur x largeur x longueur (pouces)	1,8 x 17,1 x 13,9	1,7 x 17,2 x 19,8	3,5 x 17,2 x 25,2
Hauteur x largeur x longueur (cm)	4,5 x 43,3 x 35,2	4,3 x 43,7 x 50,3	8,9 x 43,7 x 68,4
Poids	13,4 lb (6,1 kg)	31 lb (14,1 kg)	52 lb (23,6 kg)
Données environnementales			
Alimentation électrique c.a.	100–240 V c.a., 50–60 Hz, 6 A max.	100–240 V c.a., 60–50 Hz	100–240 V c.a., 60–50 Hz
Consommation électrique (moyenne)	60 W	93 W	192,5 W
Dissipation thermique	205 BTU/h	456 BTU/h	920 BTU/h
Température d'exploitation	32 à 104 °F (0 à 40 °C)	41 à 95 °F (5 à 35 °C)	41 à 95 °F (5 à 35 °C)
Température de stockage	-13 à 158 °F (-35 à 70 °C)	-40 à 140 °F (-40 à 60 °C)	-40 à 140 °F (-40 à 60 °C)
Humidité	5 à 95 % sans condensation	8 à 90 % sans condensation	8 à 90 % sans condensation
Altitude d'exploitation	Jusqu'à 7 400 ft (2 250 m)	Jusqu'à 7 400 ft (2 250 m)	Jusqu'à 7 400 ft (2 250 m)
Conformité			
Certifications sécurité	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

FortiAnalyzer 200D

FortiAnalyzer 400E

FortiAnalyzer 1000E

SPÉCIFICATIONS

	FORTIANALYZER 2000E	FORTIANALYZER 3000E	FORTIANALYZER 3000F
Capacité et performances			
Go/Jour d'enregistrement	500	800	1 600
Vitesse d'analyse (journaux/s)	7 500	15 000	35 000
Vitesse de collecte (journaux/s)	11 250	50 000	52 500
Appareils/VDOM/ADOM (maximum)	2 000	4 000	4 000
Options prises en charge			
Indicators of Compromise (IOC) FortiGuard	Oui	Oui	Oui
Fonctions FortiManager (jusqu'à 20 appareils)	Oui	Oui	Oui
Spécifications matérielles			
Format	2 U (montage en rack)	2 U (montage en rack)	3 U (montage en rack)
Nombre total d'interfaces	4 GbE, 2 x 10 GbE SFP+	4 GbE, 2 GbE SFP	4 GbE, 2 x 10 GbE SFP+
Capacité de stockage	36 To (12 x 3 To)	16 To (8 x 2 To)	48 To (16 x 3 To)
Disques durs amovibles	Oui	Oui	Oui
Gestion du stockage RAID	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
Niveau RAID par défaut	50	10	50
Alimentations remplaçables à chaud redondantes	Oui	Oui	Oui
Dimensions			
Hauteur x largeur x longueur (pouces)	3,5 x 17,2 x 25,6	3,4 x 19 x 29,7	5,2 x 17,2 x 25,5
Hauteur x largeur x longueur (cm)	8,9 x 43,7 x 64,8	8,7 x 48,2 x 75,5	13,2 x 43,7 x 64,8
Poids	58 lb (26,3 kg)	71,5 lb (32,5 kg)	76 lb (34,5 kg)
Données environnementales			
Alimentation électrique c.a.	100–240 V c.a., 60–50 Hz	100–240 V c.a., 50–60 Hz, 10 A max.	100–240 V c.a., 60–50 Hz
Consommation électrique (moyenne)	390 W	375,8 W	465 W
Dissipation thermique	1 840 BTU/h	1 947 BTU/h	1 904 BTU/h
Température d'exploitation	50 à 95 °F (10 à 35 °C)	50 à 95 °F (10 à 35 °C)	50 à 95 °F (10 à 35 °C)
Température de stockage	-40 à 158 °F (-40 à 70 °C)	-40 à 149 °F (-40 à 65 °C)	-40 à 158 °F (-40 à 70 °C)
Humidité	8 à 90 % sans condensation	20 à 90 % sans condensation	8 à 90 % sans condensation
Altitude d'exploitation	Jusqu'à 7 400 ft (2 250 m)	Jusqu'à 7 400 ft (2 250 m)	Jusqu'à 7 400 ft (2 250 m)
Conformité			
Certifications sécurité	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

FortiAnalyzer 2000E

FortiAnalyzer 3000E

FortiAnalyzer 3000F

SPÉCIFICATIONS

	FORTIANALYZER 3500E	FORTIANALYZER 3500F	FORTIANALYZER 3900E
Capacité et performances			
Go/Jour d'enregistrement	3 000	5 000	4 000
Vitesse d'analyse (journaux/s)	36 000	60 000	48 000
Vitesse de collecte (journaux/s)	60 000	90 000	75 000
Appareils/VDOM/ADOM (maximum)	10 000	10 000	10 000
Options prises en charge			
Indicators of Compromise (IOC) FortiGuard	Oui	Oui	Oui
Fonctions FortiManager (jusqu'à 20 appareils)	Oui	Oui	Oui
Spécifications matérielles			
Format	4 U (montage en rack)	4 U (montage en rack)	2 U (montage en rack)
Nombre total d'interfaces	2 GbE, 2 GbE SFP	2 GbE, 2 GbE SFP	2 GbE, 2 x 10 GbE SFP+
Capacité de stockage	24 To (12 x 2 To — 48 To maximum)	72 To (24 x 3 To)	15 To sur disque SSD (15 x 1 To SSD)
Disques durs amovibles	Oui	Oui	Oui
Niveaux RAID pris en charge	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
Niveau RAID par défaut	10	50	50
Alimentations remplaçables à chaud redondantes	Oui	Oui	Oui
Dimensions			
Hauteur x largeur x longueur (pouces)	6,9 x 19,0 x 27,2	6,9 x 19,0 x 27,2	3,5 x 17,2 x 26,9
Hauteur x largeur x longueur (cm)	17,5 x 48,2 x 69,0	17,6 x 48,2 x 69,0	8,9 x 43,7 x 68,4
Poids	77 lb (34,9 kg)	93,74 lb (42,52 kg)	52 lb (23,6 kg)
Données environnementales			
Alimentation électrique c.a.	100–240 V c.a., 50–60 Hz, 11,5 A max.	100–240 V c.a., 60–50 Hz	100–240 V c.a., 50–60 Hz, 11,5 A max.
Consommation électrique (moyenne)	465 W pour 12 DD	465 W	470 W pour 15 DD
Dissipation thermique	1 904 BTU/h	1 904 BTU/h	1 637 BTU/h
Température d'exploitation	32 à 104 °F (0 à 40 °C)	32 à 104 °F (0 à 40 °C)	50 à 95 °F (10 à 35 °C)
Température de stockage	-13 à 158 °F (-25 à 70 °C)	-13 à 158 °F (-25 à 70 °C)	-40 à 140 °F (-40 à 60 °C)
Humidité	10 à 90 % sans condensation	10 à 90 % sans condensation	5 à 95 % sans condensation
Altitude d'exploitation	Jusqu'à 7 400 ft (2 250 m)	Jusqu'à 7 400 ft (2 250 m)	Jusqu'à 7 400 ft (2 250 m)
Conformité			
Certifications sécurité	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

FortiAnalyzer 3500E

FortiAnalyzer 3500F

FortiAnalyzer 3900E

	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacité et performances							
Go/Jour d'enregistrement	1 incl.*	+1	+5	+25	+100	+500	+2 000
Capacité de stockage	500 Go	+500 Go	+3 To	+10 To	+24 To	+48 To	+100 To
Appareils/ADOM/VDOM pris en charge (max.)	10 000	10 000	10 000	10 000	10 000	10 000	10 000
Options prises en charge							
Indicators of Compromise (IOC) FortiGuard	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Fonctions FortiManager (jusqu'à 20 appareils)	Non	Non	Non	Non	Non	Non	Non
Configuration d'hyperviseur							
Hyperviseurs pris en charge	VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure						
Interfaces réseau prises en charge (min./max.)	1/4						
CPU virtuels (min./max.)	1/illimité						
Mémoire prise en charge (min./max.)	1 Go/illimité						

* Go/jour illimité pour déploiement en mode collecte

INFORMATIONS DE COMMANDE

Produit	Référence	Description
FortiAnalyzer 200D	FAZ-200D	Appliance d'analyse et de journaux centralisée — 4 GbE RJ45, stockage 1 To, jusqu'à 5 Go/jour d'enregistrement.
FortiAnalyzer 400E	FAZ-400E	Appliance d'analyse et de journaux centralisée — 4 GbE RJ45, stockage 12 To, jusqu'à 75 Go/jour d'enregistrement.
FortiAnalyzer 1000E	FAZ-1000E	Appliance d'analyse et de journaux centralisée — 2 GbE RJ45, stockage 24 To, double alimentation, jusqu'à 300 Go/jour d'enregistrement.
FortiAnalyzer 2000E	FAZ-2000E	Appliance d'analyse et de journaux centralisée — 4 GbE RJ45, 2 SFP+, stockage 36 To, double alimentation, jusqu'à 500 Go/jour d'enregistrement.
FortiAnalyzer 3000E	FAZ-3000E	Appliance d'analyse et de journaux centralisée — 4 GbE RJ45, 2 emplacements GbE SFP, stockage 16 To, double alimentation, jusqu'à 800 Go/jour d'enregistrement.
FortiAnalyzer 3000F	FAZ-3000F	Appliance d'analyse et de journaux centralisée — 4 GbE RJ45, 2 SFP+, stockage 48 To, double alimentation, jusqu'à 1 600 Go/jour d'enregistrement.
FortiAnalyzer 3500E	FAZ-3500E-E02S	Appliance d'analyse et de journaux centralisée — 2 GbE RJ45, 2 emplacements GbE SFP, stockage 24 To, double alimentation, jusqu'à 3 000 Go/jour d'enregistrement.
FortiAnalyzer 3500F	FAZ-3500F	Appliance d'analyse et de journaux centralisée — 2 GbE RJ45, 2 emplacements GbE SFP, stockage 72 To, double alimentation, jusqu'à 5 000 Go/jour d'enregistrement.
FortiAnalyzer 3900E	FAZ-3900E	Appliance d'analyse et de journaux centralisée — 2 GbE RJ45, 2 emplacements SFP+, stockage flash 15 To SSD, double alimentation, jusqu'à 4 000 Go/jour d'enregistrement.
FortiAnalyzer VM	FAZ-VM-BASE	Licence de base pour FortiAnalyzer VM empilable ; 1 Go/jour d'enregistrement et 500 Go de capacité de stockage. Go/jour illimités uniquement si utilisé en mode collecte. Conçu pour plates-formes VMware vSphere, Xen, KVM et Hyper-V.
	FAZ-VM-GB1	Licence de mise à niveau pour l'ajout de 1 Go/jour d'enregistrement et 500 Go de capacité de stockage.
	FAZ-VM-GB5	Licence de mise à niveau pour l'ajout de 5 Go/jour d'enregistrement et 3 To de capacité de stockage.
	FAZ-VM-GB25	Licence de mise à niveau pour l'ajout de 25 Go/jour d'enregistrement et 10 To de capacité de stockage.
	FAZ-VM-GB100	Licence de mise à niveau pour l'ajout de 100 Go/jour d'enregistrement et 24 To de capacité de stockage.
	FAZ-VM-GB500	Licence de mise à niveau pour l'ajout de 500 Go/jour d'enregistrement et 48 To de capacité de stockage.
	FAZ-VM-GB2000	Licence de mise à niveau pour l'ajout de 2 To/jour d'enregistrement et 100 To de capacité de stockage.
FortiAnalyzer VM pour AWS	FAZ-VM-BASE-AWS	Licence de base pour FortiAnalyzer VM empilable ; 1 Go/jour d'enregistrement et 500 Go de capacité de stockage. Go/jour illimités uniquement si utilisé en mode collecte. Conçu pour plate-forme Amazon Web Services (AWS).
	FAZ-VM-GB1-AWS	Licence de mise à niveau pour l'ajout de 1 Go/jour d'enregistrement et 500 Go de capacité de stockage.
	FAZ-VM-GB5-AWS	Licence de mise à niveau pour l'ajout de 5 Go/jour d'enregistrement et 3 To de capacité de stockage.
	FAZ-VM-GB25-AWS	Licence de mise à niveau pour l'ajout de 25 Go/jour d'enregistrement et 10 To de capacité de stockage.
	FAZ-VM-GB100-AWS	Licence de mise à niveau pour l'ajout de 100 Go/jour d'enregistrement et 24 To de capacité de stockage.
	FAZ-VM-GB500-AWS	Licence de mise à niveau pour l'ajout de 500 Go/jour d'enregistrement et 48 To de capacité de stockage.
	FAZ-VM-GB2000-AWS	Licence de mise à niveau pour l'ajout de 2 To/jour d'enregistrement et 100 To de capacité de stockage.
FortiAnalyzer VM pour Azure	FAZ-VM-BASE-AZ	Licence de base pour FortiAnalyzer VM empilable ; 1 Go/jour d'enregistrement et 500 Go de capacité de stockage. Go/jour illimités uniquement si utilisé en mode collecte. Conçu pour plate-forme Azure.
	FAZ-VM-GB1-AZ	Licence de mise à niveau pour l'ajout de 1 Go/jour d'enregistrement et 500 Go de capacité de stockage.
	FAZ-VM-GB5-AZ	Licence de mise à niveau pour l'ajout de 5 Go/jour d'enregistrement et 3 To de capacité de stockage.
	FAZ-VM-GB25-AZ	Licence de mise à niveau pour l'ajout de 25 Go/jour d'enregistrement et 10 To de capacité de stockage.
	FAZ-VM-GB100-AZ	Licence de mise à niveau pour l'ajout de 100 Go/jour d'enregistrement et 24 To de capacité de stockage.
	FAZ-VM-GB500-AZ	Licence de mise à niveau pour l'ajout de 500 Go/jour d'enregistrement et 48 To de capacité de stockage.
	FAZ-VM-GB2000-AZ	Licence de mise à niveau pour l'ajout de 2 To/jour d'enregistrement et 100 To de capacité de stockage.
Fonctions de gestion des modules complémentaires FortiAnalyzer	FAZ-MGMT20	Licence d'ajout de fonctions FortiManager jusqu'à 20 appareils (série 1000 et au-delà — matériel uniquement).
Abonnement à FortiGuard Indicator of Compromise (IOC)	FC-10-[code modèle] -149-02-DD	Licence d'abonnement pour 1 an à FortiGuard Indicator of Compromise (IOC).

SIÈGE SOCIAL INTERNATIONAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1.408.235.7700
www.fortinet.com/sales

SUCCURSALE EMEA
905 rue Albert Einstein
06560 Valbonne
Alpes-Maritimes, France
Tél. : +33.4.8987.0500

FRANCE
TOUR ATLANTIQUE
11ème étage, 1 place de la Pyramide
92911 Paris La Défense Cedex
France
Ventes: +33-1-8003-1655

SUCCURSALE APAC
300 Beach Road 20-01
The Concourse
Singapour 199555
Tél. : +65.6395.2788

SUCCURSALE AMÉRIQUE LATINE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
États-Unis
Tél. : +1.954.368.9990

FST-PROD-DS-AZ
FAZ-DAT-R25-201608