FortiAnalyzer

Les cybermenaces sont dynamiques. Elles évoluent sans cesse. Face à elles, les organisations manquent cruellement de visibilité sur leur environnement informatique. Résultat : les violations de données et autres cyberviolations mettent en moyenne plus de 100 jours à être détectées. Chaque fois qu'une entreprise est visée par une intrusion, elle se retrouve à la merci des pirates. Des informations sensibles ou confidentielles sur des clients sont alors susceptibles de fuiter. FortiAnalyzer permet d'intercepter les cybermenaces sur l'ensemble de la surface d'attaque. Il fournit une visibilité accrue, des informations précises, des renseignements en temps réel sur les menaces, des analyses exploitables, une analyse de sécurité CNP-SOC ainsi qu'une mise en perspective opérationnelle utilisable par l'écosystème Security Fabric de Fortinet.

Analyse centralisée

Corrélation d'événements et détection avancée des cybermenaces - Pour permettre aux administrateurs informatiques d'identifier les cybermenaces et de les contrer, sur l'ensemble du réseau.

Tableaux de bord NOC-SOC - Des tableaux de bord NOC-SOC personnalisables permettent la gestion, la surveillance et le contrôle de votre réseau.

Performances évolutives et déploiements flexibles - Prise en charge de milliers d'agents FortiGate et FortiClient™. Extension dynamique du stockage en fonction des besoins. FortiAnalyser est déployé individuellement ou optimisé pour une opération spécifique.

Fortinet Security Fabric peut fournir une protection unifiée de bout en bout : les firewalls Fortinet Enterprise luttent contre les menaces persistantes avancées, tandis que FortiAnalyzer offre une visibilité accrue et émet des alertes de sécurité exploitables, automatisées.

FortiAnalyzer vous permet de collecter, d'analyser et de corréler les données de logs de votre réseau distribué de firewalls Fortinet Enterprise, depuis un poste central. Vous pouvez visualiser le trafic firewall et générer des rapports depuis une console unique. Associé à un abonnement au service FortiGuard Indicator of Compromise (IOC), FortiAnalyzer peut fournir une liste hiérarchisée des hôtes compromis, pour vous aider à réagir rapidement.

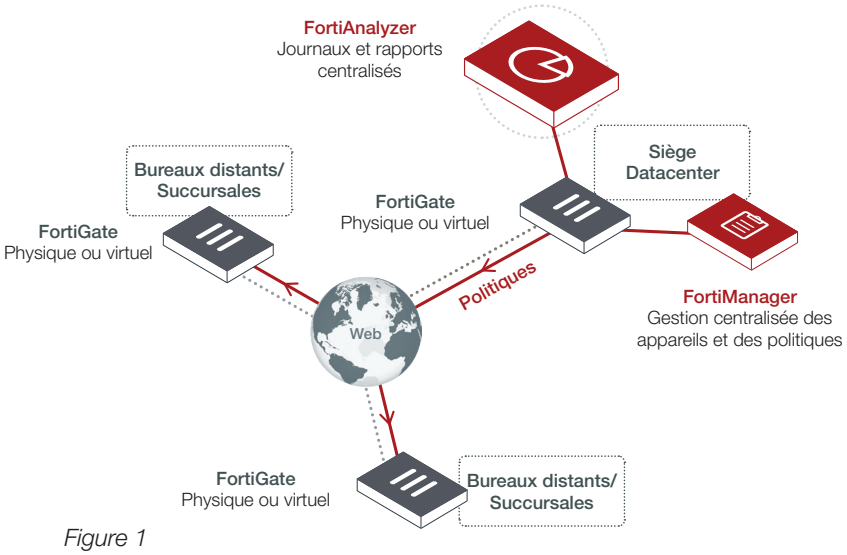

Figure 1

Caractéristiques

- Recherche et rapports centralisés - Expérience de recherche simple et intuitive, de type Google. Rapports sur le trafic réseau, sur les menaces, les activités et les tendances propres au réseau.
- Indicateurs de compromission automatisés (IOC) - Analyse des journaux de sécurité à l'aide de FortiGuard IOC Intelligence pour la détection APT.
- Aperçus en temps réel et historiques de l'activité réseau - Résumé des applications, sources, destinations, sites web, cybermenaces, modifications administratives et événements système.
- Gestion simplifiée des événements : les définitions d'événements de sécurité prédéfinies sont facilement personnalisables, grâce à des alertes automatisées.
- Intégration facile à l'écosystème Security Fabric de Fortinet - Corrélation avec les journaux de FortiClient, FortiSandbox, FortiWeb et FortiMail, pour une visibilité accrue.

Fonctionnalités-clés

Intervention en cas de cyberincident

Avec la fonctionnalité d'intervention post-incident, FortiAnalyzer vous permet de gérer les événements suspects et d'identifier les postes de travail infectés. Grâce aux gestionnaires d'événements par défaut ou personnalisés, vous détectez instantanément les activités malveillantes. La mise en quarantaine des appareils est automatisée, grâce à l'automatisation FOS intégrée. L'intégration aux plateformes ITSM vous permet de rationaliser la détection, le suivi des incidents, la collecte et l'analyse des preuves. Vous comblez ainsi les lacunes de votre centre des opérations de sécurité et renforcez votre cyberprotection globale.

FortiView - Visibilité accrue sur le réseau

Un tableau de bord interactif personnalisable vous aide à identifier rapidement les problèmes, à partir de représentations intuitives du trafic réseau, des menaces et des applications (Fig 2). FortiView constitue un système de surveillance complet pour votre réseau. À partir d'une seule interface, vous visualisez les données en temps réel et les données historiques. FortiView enregistre et monitore les menaces réseau, filtre les données sur plusieurs niveaux, suit les activités administratives, et plus encore.

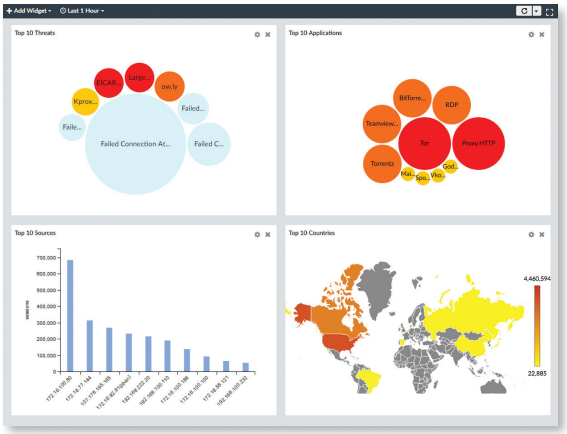

Figure 2

Indicateurs de compromission

Le résumé des indicateurs de compromission (IOC) liste les utilisateurs dont l'utilisation web apparaît comme douteuse. Il fournit plusieurs types de données : adresses IP, nom de l'hôte, groupe, système d'exploitation, évaluation globale des menaces, aperçu cartographique et nombre de menaces. Pour générer les indicateurs de compromission, FortiAnalyzer analyse les journaux des filtres web de chaque utilisateur au regard de sa base de données sur les menaces. Lorsqu'une correspondance avec une cybermenace est trouvée, un score de menace est attribué à l'utilisateur. FortiAnalyzer agrège les scores de menace d'un utilisateur final pour émettre un avis sur les indicateurs globaux de compromission de l'utilisateur en question. Le résumé des indicateurs de compromission est produit via le filtre web UTM des appareils FortiGate et l'abonnement FortiAnalyzer à FortiGuard, de manière à synchroniser la base de données locale sur les menaces et la base de données FortiGuard.

Rapports

La fonction Rapports vous permet générer des rapports de données personnalisés. FortiAnalyzer propose plus de 30 modèles de rapports intégrés, prêts à l'emploi. Des rapports-types, présentés en exemples, vous permettent d'identifier le modèle adapté à vos besoins. Obtenez des rapports à la demande ou selon un calendrier prédéfini, avec des notifications automatisées par e-mail, des téléchargements et un agenda faciles à gérer. Créez des rapports personnalisés avec plus de 300 types de graphiques et tableaux intégrés. Ces rapports sont disponibles dans plusieurs formats : PDF, HTML, CSV et XML.

Surveillance et alertes

Les gestionnaires d'événements définissent les messages à extraire des journaux et à afficher dans le module de gestion des événements. Vous devez préalablement activer un gestionnaire d'événements pour commencer à générer des événements. Vous pouvez configurer des gestionnaires d'événements pour un périphérique spécifique, pour tous les périphériques ou pour une unité locale FortiAnalyzer. Il est possible de créer des gestionnaires d'événements pour FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox et pour les serveurs syslog. Un gestionnaire peut être configuré de manière à envoyer des alertes par adresse e-mail, communauté SNMP ou serveur syslog.

Centre d'exploitation du réseau (NOC) et Centre d'exploitation de la sécurité (SOC)

FortiAnalyzers NOC-SOC est un centre de gestion qui vous aide à sécuriser l'ensemble de votre réseau en fournissant des données relatives aux journaux et aux cybermenaces. Le SOC vous aide à protéger votre réseau, vos sites web, vos applications, vos bases de données, vos serveurs et centres de données grâce à un monitoring centralisé des cybermenaces, des cyberévénements et de l'activité réseau. Vous pouvez utiliser des tableaux de bord et widgets FAZ prédéfinis ou personnalisés, via une interface unique, pour une intégration facile au sein de votre Security Fabric. (Fig 3)

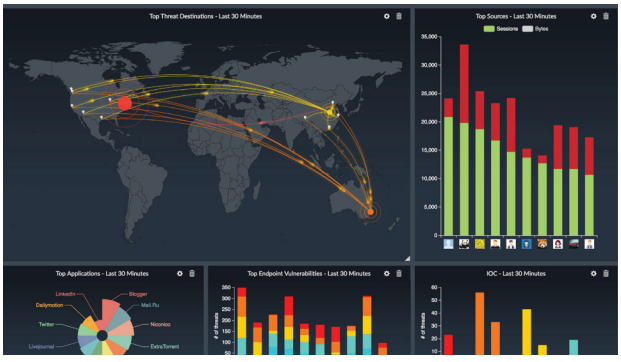

Figure 3

Récupération des logs pour expertise forensique

L'extraction des journaux permet de transférer les journaux archivés d'un appareil FortiAnalyzer à un autre. Cela permet aux administrateurs d'exécuter des requêtes et des rapports incluant des données historiques. Ce type de procédé peut s'avérer particulièrement utile en cas de recherche forensique. Un périphérique FortiAnalyzer peut être serveur ou client de récupération. Il peut jouer les deux rôles pour récupérer les données du journal pour un périphérique spécifique et une période de temps déterminée, sur la base de filtres prédéfinis. Les données récupérées sont ensuite indexées et peuvent être utilisées pour des analyses et des rapports.

Transfert de logs pour intégration tierces

Vous pouvez transférer les journaux d'une unité FortiAnalyzer vers une autre unité FortiAnalyzer, vers un serveur syslog ou vers un serveur Common Event Format (CEF). Le client est l'unité FortiAnalyzer qui transmet les journaux à un autre appareil. Le serveur est l'unité FortiAnalyzer, le serveur syslog ou le serveur CEF qui reçoit les logs. Le client transfère les journaux vers une autre unité ou un autre serveur, mais conserve une copie locale des journaux. La copie locale est soumise aux politiques définies pour les données des journaux archivés. Les journaux sont transmis en temps réel ou presque, au fur et à mesure qu'ils sont reçus. Les fichiers de contenu transférés comprennent : les fichiers DLP, les fichiers de quarantaine de l'anti-virus et les captures de paquets IPS.

Modes Analyzer-Collector

Les unités FortiAnalyzer peuvent être déployées en mode Analyzer ou Collector. Des unités fonctionnant sous des modes différents peuvent fonctionner en synergie, de manière à améliorer les performances globales de réception, d'analyse et de reporting. En mode Collector, la tâche principale d'une unité consiste à transférer les journaux des périphériques connectés vers un Analyzer et à archiver ces journaux. L'Analyzer délègue la tâche de réception des journaux au Collector afin de pouvoir se concentrer sur l'analyse des données et la génération de rapports. Ce type de fonctionnement permet d'optimiser les performances de réception des logs du Collector. (Figure 4)

Architecture multitenant avec gestion flexible des quotas

Politiques de fonctionnement gérables par domaine d'administration (ADOM) pour l'archivage et l'analyse des données selon des critères temporels. Gestion automatisée des quotas. Graphiques de tendances permettant de guider l'élaboration des politiques de fonctionnement et le suivi du monitoring.

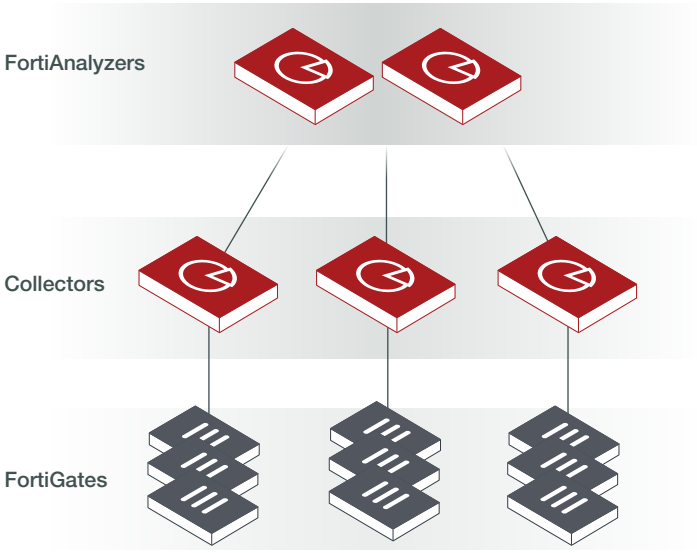

Figure 4

FortiAnalyzer VM

FortiAnalyzer-VM intègre le logging, l'analyse et le reporting réseau au sein d'un système unique, pour une connaissance accrue des événements réseau liés à la cybersécurité. FortiAnalyzer-VM est une version logicielle de l'appliance matérielle FortiAnalyzer. Elle est conçue pour fonctionner sur de nombreuses plateformes de virtualisation. FortiAnalyzer-VM offre toutes les fonctionnalités de l'appliance matérielle FortiAnalyzer.

FortiAnalyzer-VM fournit aux organisations de toutes tailles une riche palette de fonctionnalités : analyse centralisée des événements de sécurité, recherches forensiques, rapports, archivage de contenu, exploration des données, mise en quarantaine des fichiers malveillants et évaluation des vulnérabilités. Les données de sécurité provenant de vos appareils Fortinet et autres dispositifs sont collectées, corrélées et analysées, géographiquement et chronologiquement. Vous obtenez ainsi un aperçu simplifié et consolidé de votre cyberprotection.

Spécifications

	FAZ-VM-BASE	FAZ-VM-Go1	FAZ-VM-Go5	FAZ-VM-Go25	FAZ-VM-Go100	FAZ-VM-Go500	FAZ-VM-Go2000
CAPACITÉS ET PERFORMANCES							
Go/jour de logs	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/VDOMs (Maximum)	10 000	10 000	10 000	10 000	10 000	10 000	10 000
Indicateur de compromission (IOC) FortiGuard	✓	✓	✓	✓	✓	✓	✓
PRÉ-REQUIS RELATIFS À L'HYPERVISEUR							
Prise en charge de l'hyperviseur	VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.0/6.5/6.5/6.7, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+ et Open Source Xen 4.1+, KVM sur Redhat 6.5+ et Ubuntu 17.04, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI)						
Prise en charge de l'interface réseau (Minimum / Maximum)	1 / 4						
vCPU (Minimum / Maximum)	2/ Illimité						
Prise en charge de la mémoire (Minimum / Maximum)	4 Go / Illimité						

* Nombre illimité de Go/jour en mode collecteur

Spécifications

	 FORTIANALYZER 200F	 FORTIANALYZER 300F	 FORTIANALYZER 400E
CAPACITÉS ET PERFORMANCES			
Go/jour de logs	100	150	200
Vitesse d'analyse soutenue (logs/sec)*	3000	4500	6 000
Débit soutenu par le collecteur (logs/sec)*	4 500	6 750	9 000
Appareils/VDOMs (Maximum)	150	180	200
Nombre maximum de jours d'analyse**	40	28	30
OPTIONS PRISES EN CHARGE			
FortiGuard Indicateur de compromission (IOC)	✓	✓	✓
SPÉCIFICATIONS HARDWARE			
Format	1 RU Montage en rack	1 RU Montage en rack	1 RU Montage en rack
Nombre total d'interfaces	2xRJ45 GE	2xRJ45 GE, 2xSFP	4x GE
Capacité de stockage	4 To (1 x 4 To)	8 To (2 x 4To)	12 To (4x 3 To)
Stockage utilisable (après RAID)	4 To	4 To	6To
Disques durs amovibles	Non	Non	✓
Niveaux RAID pris en charge	N/A	RAID 0/1	RAID 0/1/5/10
Type RAID	N/A	Logiciel	Logiciel
Niveau RAID par défaut	N/A	1	10
Alimentations Hot Swap redondantes	Non	Non	Non
DIMENSIONS			
Hauteur x Largeur x Longueur (pouces)	1,75 x 17,0 x 15,0	1,75 x 17,0 x 15,0	1,7 x 17,2 x 19,8
Hauteur x Largeur x Longueur (cm)	4,4 x 43,2 x 38,1	4,4 x 43,2 x 38,0	4,3 x 43,7 x 50,3
Poids	7,8 kg (17,1 livres)	8,6 kg (18,9 livres)	14,1 kg (31 livres)
ENVIRONNEMENT			
Alimentation en courant alternatif	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Consommation électrique (Max / Moyenne)	49 W / 114W	65W / 130W	93 W / 133W
Dissipation de la chaleur	390 BTU/h	445 BTU/h	456 BTU/h
Température de fonctionnement	0 - 40° C (32 - 104° F)	0 - 40° C (32 - 104° F)	5–35°C (41–95°F)
Température de stockage	-35 - 70° C (95 - 158° F)	-35 - 70° C (95 - 158° F)	-40–60°C (-40–140°F)
Humidité	de 20 à 90% sans condensation	de 20 à 90% sans condensation	de 8 à 90% sans condensation
Altitude de fonctionnement	Jusqu'à 2 250 m (7 400 pi)	Jusqu'à 2 250 m (7 400 pi)	Jusqu'à 3 000 m (9 842 pi)
CONFORMITÉ			
Certifications relatives à la sécurité	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB

*Débit soutenu - débit maximal constant des messages logs que la plateforme FAZ peut assurer durant au moins 48 heures, sans dégradation de la base de données SQL et des performances système.

**Nombre maximal de jours correspondant à une réception des logs continue (selon le débit soutenu spécifié). Ce nombre peut augmenter si le débit moyen est inférieur.

Spécifications

	 FORTIANALYZER 800F	 FORTIANALYZER 1000E	 FORTIANALYZER 2000E
CAPACITÉS ET PERFORMANCES			
Go/jour de logs	300	600	1,000
Vitesse d'analyse soutenue (logs/sec)*	8 250	18 000	30 000
Débit soutenu par le collecteur (logs/sec)*	12 000	27 000	45 000
Appareils/VDOMs (Maximum)	800	2 000	2 000
Nombre maximum de jours d'analyse**	30	30	30
OPTIONS PRISES EN CHARGE			
FortiGuard Indicateur de compromission (IOC)	✓	✓	✓
SPÉCIFICATIONS HARDWARE			
Format	1 RU Montage en rack	2 RU Montage en rack	2 RU Montage en rack
Nombre total d'interfaces	4 x GE, 2x SFP	2x GE	4x GE, 2 x SFP+
Capacité de stockage	16 To (4x 4 To)	24 To (8x 3 To)	36 To (12x 3To)
Stockage utilisable (après RAID)	8 To	18 To	30 To
Disques durs amovibles	✓	✓	✓
Niveaux RAID pris en charge	RAID 0/1/5/10	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
Type RAID	Matériel / remplaçable à chaud	Matériel / remplaçable à chaud	Matériel / remplaçable à chaud
Niveau RAID par défaut	10	50	50
Alimentations Hot Swap redondantes	Non	✓	✓
DIMENSIONS			
Hauteur x Largeur x Longueur (pouces)	1,75 x 17,44 x 22,16	3,5 x 17,2 x 25,2	3,5 x 17,2 x 25,6
Hauteur x Largeur x Longueur (cm)	4,4 x 44,3 x 56,3	8.9 x 43,7 x 68,4	8,9 x 43,7 x 64,8
Poids	28.6 livres (13,0 kg)	52 livres (23,6 kg)	58 livres (26,3 kg)
ENVIRONNEMENT			
Alimentation en courant alternatif	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Consommation électrique (Max / Moyenne)	108W / 186W	192,5 W / 275W	293,8 W / 354W
Dissipation de la chaleur	634 BTU/h	920 BTU/h	1840 BTU/h
Température de fonctionnement	0 - 40° C (32 - 104° F)	5–35°C (41–95°F)	10 – 35°C (50–95°F)
Température de stockage	-35 - 70° C (95 - 158° F)	-40–60°C (-40–140°F)	-40–70°C (-40–158°F)
Humidité	20 à 90 % sans condensation	de 8 à 90% sans condensation	de 8 à 90% sans condensation
Altitude de fonctionnement	Jusqu'à 2 250 m (7 400 pi)	Jusqu'à 2 250 m (7 400 pi)	Jusqu'à 2 250 m (7 400 pi)
CONFORMITÉ			
Certifications relatives à la sécurité	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB

Spécifications

	FORTIANALYZER 3000F	FORTIANALYZER 3700F
CAPACITÉS ET PERFORMANCES		
Go/jour de logs	3 000	8 300
Vitesse d'analyse soutenue (logs/sec)*	42 000	100 000
Débit soutenu par le collecteur (logs/sec)*	60 000	150 000
Appareils/VDOMs (Maximum)	4 000	10 000
Nombre maximum de jours d'analyse**	30	60
OPTIONS PRISES EN CHARGE		
FortiGuard Indicateur de compromission (IOC)	✓	✓
SPÉCIFICATIONS HARDWARE		
Format	3 RU Montage en rack	4 RU Montage en rack
Nombre total d'interfaces	4x GE, 2 x SFP+	2xSFP+, 2x1GE
Capacité de stockage	48 To (16x 3 To – 48 To max)	240 To (60x4To SAS HDDs)
Stockage utilisable (après RAID)	42 To	216 To
Disques durs amovibles	✓	✓
Niveaux RAID pris en charge	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
Type RAID	Matériel / remplaçable à chaud	Matériel / remplaçable à chaud
Niveau RAID par défaut	50	50
Alimentations Hot Swap redondantes	✓	✓ ***
DIMENSIONS		
Hauteur x Largeur x Longueur (pouces)	5,2 x 17,2 x 25,5	7 x 17,2 x 30,2
Hauteur x Largeur x Longueur (cm)	13,2 x 43,7 x 64,8	17,8 x 43,7 x 76,7
Poids	34,5 kg (76 livres)	53,5 kg (118 livres)
ENVIRONNEMENT		
Alimentation en courant alternatif	100–240V AC, 50–60 Hz, 11,5 Amp Maximum	100-240V AC, 60-50 Hz
Consommation électrique (Max / Moyenne)	449 W / 541W for 12 HDD	850 W / 1423,4W
Dissipation de la chaleur	1846,5 BTU/h	4858 BTU/h
Température de fonctionnement	10–35°C (50–95°F)	10–35°C (50–95°F)
Température de stockage	-40–70°C (-40–158°F)	-40–70°C (-40–158°F)
Humidité	8–90% sans condensation	8%-90% sans condensation
Altitude de fonctionnement	Jusqu'à 2 250 m (7 400 pi)	Jusqu'à 2 233 m (7 000 pi)
CONFORMITÉ		
Certifications relatives à la sécurité	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB

*** 3700F doit être connecté à une source d'alimentation 200V - 240V.

Informations relatives aux commandes

PRODUIT	RÉFÉRENCE	DESCRIPTION
FortiAnalyzer 200F	FAZ-200F	Appliance centralisée de journalisation et d'analyse - 2xRJ45 GE, 4 To de stockage, jusqu'à 100 Go/jour de logs.
FortiAnalyzer 300F	FAZ-300F	Appliance centralisée de journalisation et d'analyse - 2xRJ45 GE, 8 To de stockage, jusqu'à 150 Go/jour de logs.
FortiAnalyzer 400E	FAZ-400E	Appliance centralisée de journalisation et d'analyse - 4x GE RJ45, 12 To de stockage, jusqu'à 200 Go/jour de logs.
FortiAnalyzer 800F	FAZ-800F	Appliance centralisée de journalisation et d'analyse - 4 x GE, 2x SFP, 16 To de stockage, jusqu'à 300 Go/jour de logs.
FortiAnalyzer 1000E	FAZ-1000E	Appliance centralisée de journalisation et d'analyse - 2x GE RJ45, 24 To de stockage, double alimentation, jusqu'à 650 Go/jour de journalisation.
FortiAnalyzer 2000E	FAZ-2000E	Appliance centralisée de journalisation et d'analyse - 4x GE RJ45, 2 x SFP+, 36 To de stockage, double alimentation, jusqu'à 1 000 Go/jour de journalisation.
FortiAnalyzer 3000F	FAZ-3000F	Appliance centralisée de journalisation et d'analyse - 4x GE RJ45, 2 x SFP+, 48 To de stockage, double alimentation, jusqu'à 3 000 Go/jour de logs.
FortiAnalyzer 3700F	FAZ-3700F	Appliance centralisée de journalisation et d'analyse - 2x SFP+, 2x1GE slots, 240 To de stockage, jusqu'à 8 300 Go/jour de logs.
FortiAnalyzer VM	FAZ-VM-BASE	Licence de base pour FortiAnalyzer-VM empilable ; 1 Go/jour de logs et 500 Go de capacité de stockage. Nombre illimité de Go/jour lorsqu'utilisé en mode collecteur uniquement. Conçu pour toutes les plateformes prises en charge.
	FAZ-VM-Go1	Licence de mise à niveau pour l'ajout d'1 Go/jour de journaux et de 500 Go de capacité de stockage.
	FAZ-VM-Go5	Licence de mise à niveau pour l'ajout de 5 Go/jour de logs et de 3 To de capacité de stockage.
	FAZ-VM-Go25	Licence de mise à niveau pour l'ajout de 25 Go/jour de logs et de 10 To de capacité de stockage.
	FAZ-VM-Go100	Licence de mise à niveau pour l'ajout de 100 Go/jour de logs et de 24 To de stockage.
	FAZ-VM-Go500	Licence de mise à niveau pour l'ajout de 500 Go/jour de logs et de 48 To de stockage.
	FAZ-VM-Go2000	Licence de mise à niveau pour l'ajout de 2 To/jour de logs et de 100 To de stockage.
	FortiAnalyzer AWS Sur demande	https://aws.amazon.com/marketplace/pp/B01N5K7210/ref=portal_asin_url
	FortiAnalyzer Azure Sur demande	https://azuremarketplace.microsoft.com/en-us/marketplace/apps/fortinet.fortianalyzer
FortiGuard Indicateurs de compromission (IOC) - Abonnement	FC-10-[code modèle]-149-02-DD	Licence d'abonnement d'un an pour les indicateurs de compromission FortiGuard (IOC).

SIÈGE
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
États-Unis
Tél.: +1.408.235.7700
www.fortinet.com/sales

BUREAU DES VENTES
EMEA
905, rue Albert Einstein
06560 Valbonne
France
Tél.: +33.4.8987.0500

BUREAU DES VENTES
APAC
8 Temasek Boulevard
#12-01 Suntec Tower Three
Singapore 038988
Tél.: +65.6395.2788

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

FST-PROD-DS-GT5H2

FG-500E-DAT-R13-201808