FICHE PRODUIT

FortiSandbox™

FortiSandbox 500F, 1000F, 2000E, 3000E, machine virtuelle, hébergement cloud et cloud public

FortiSandbox est un outil ultra-performant reposant sur l'intelligence artificielle. Il s'agit de l'un des composants de la solution anti-intrusions informatiques de Fortinet, intégrée à la plateforme Fortinet Security Fabric. Cette solution permet aux entreprises de lutter contre les cybermenaces ciblées qui sont en forte croissance comme les ransomwares (logiciels rançon), les crypto-malware et les autres menaces sévissant sur les vastes surfaces d'attaque. FortiSandbox permet de réagir en temps réel, via la détection et la neutralisation automatisées des logiciels malveillants 0-day.

Large couverture de la surface d'attaque avec Security Fabric

Protection efficace contre les attaques ciblées avancées grâce à une architecture intégrée et évolutive sécurisant les réseaux, les e-mails, les applications web et les terminaux, de l'infrastructure locale jusqu'au cloud, ainsi que les dispositifs de supervision (ICS) en environnements OT (Operational Technology)

Détection et neutralisation automatisées des logiciels malveillants 0-day les plus évolués

Grâce à son intégration native et à ses API ouvertes, FortiSandbox automatise la réception d'objets depuis les points de protection de Fortinet et d'autres fournisseurs. Le partage des renseignements sur les menaces est également réalisé de manière automatique, en temps réel, pour réagir immédiatement en cas de cybermenaces.

Un outil reconnu et certifié

FortiSandbox est constamment soumis à des tests rigoureux, réalisés en conditions réelles par des experts indépendants tels *NSS Labs Breach Detection Systems* (BDS), *Breach Prevention Systems* (BPS), and *ICSA Labs Advanced Threat* Defense (ATD). FortiSandbox obtient invariablement les meilleures notes en matière de neutralisation des menaces connues et inconnues.

Protection contre les intrusions informatiques pour

- Télétravail
- Succursales
- Campus
- Datacenters
- Cloud public (AWS, Azure)

Certifications indépendantes

NSS LABS RECOMMENDED

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Services de sécurité FortiGuard

www.fortiguard.com

Assistance mondiale FortiCare 24h/24, 7j/7

support.fortinet.com

FONCTIONALITÉS

Analyse anti-malware grâce au sandboxing et à l'intelligence artificielle

Complétez vos défenses avec l'analyse sandboxing en deux étapes faisant appel à l'intelligence artificielle. Les fichiers suspects et à risque sont soumis à une première étape d'analyse identifiant avec rapidité les logiciels malveillants connus et émergents, grâce à l'analyse statique de FortiSandbox boostée par l'intelligence artificielle. La deuxième étape de l'analyse s'effectue en environnement confiné, afin de déterminer le cycle de vie complet des attaques. L'IA comportementale identifie en continu de nouvelles techniques utilisées par les hackers et met ensuite automatiquement à jour les indicateurs comportementaux signalant une menace. Le moteur de détection d'analyse dynamique FortiSandbox devient ainsi plus efficace et plus performant contre les nouvelles menaces 0-day.

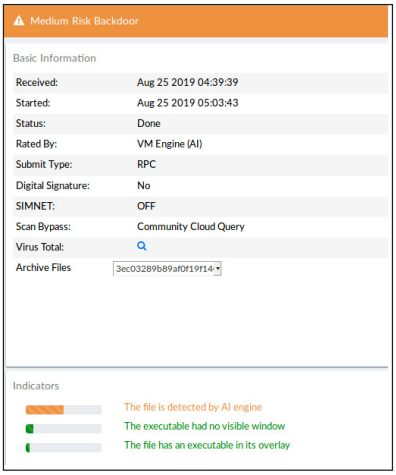

Schéma 1 : Analyse dynamique reposant sur l'intelligence artificielle

Rapports et outils d'investigation basés sur Mitre ATT&CK

FortiSandbox fournit un rapport d'analyse détaillé mappant les techniques de malware sur le cadre de références Mitre ATT&CK, grâce à de puissants outils d'investigation intégrés. FortiSandbox permet aux équipes SecOps (opérations de sécurité) de télécharger les paquets capturés, les fichiers originaux, les journaux de traceurs, les screenshots de malware et les IOC conformes STIX 2.0.

FortiSandbox fournit des renseignements détaillés sur les menaces, ainsi que des recommandations après examen des fichiers (voir figure 2).

Les équipes SecOps peuvent choisir d'enregistrer une vidéo de l'ensemble de l'interaction avec le malware ou d'interagir manuellement avec celui-ci en environnement simulé.

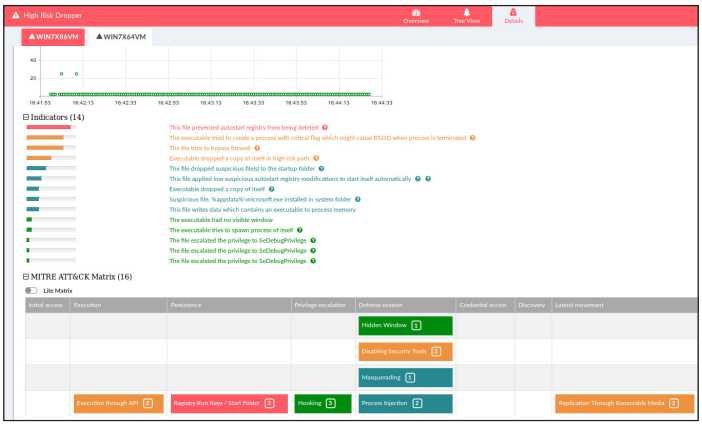

Schéma 2 : Cadre Mitre ATT&CK avec outils intégrés

Protection automatisée contre les intrusions informatiques

FortiSandbox, protection automatisée, présente une installation ultra-simplifiée et des capacités d'intégration uniques du fait de son intégration aux produits Security Fabric. Lorsqu'un code malveillant est identifié, FortiSandbox transmet les scores de risque obtenus.

Les données récoltées localement sont partagées en temps réel avec les solutions de Fortinet, des partenaires FabricReady et des fournisseurs tiers afin de neutraliser la nouvelle menace détectée. Ces données peuvent ensuite être transmises en option aux chercheurs du FortiGuard Labs, pour mieux protéger les organisations du monde entier. Le schéma 3 illustre les étapes du processus automatisé de neutralisation des cybermenaces.

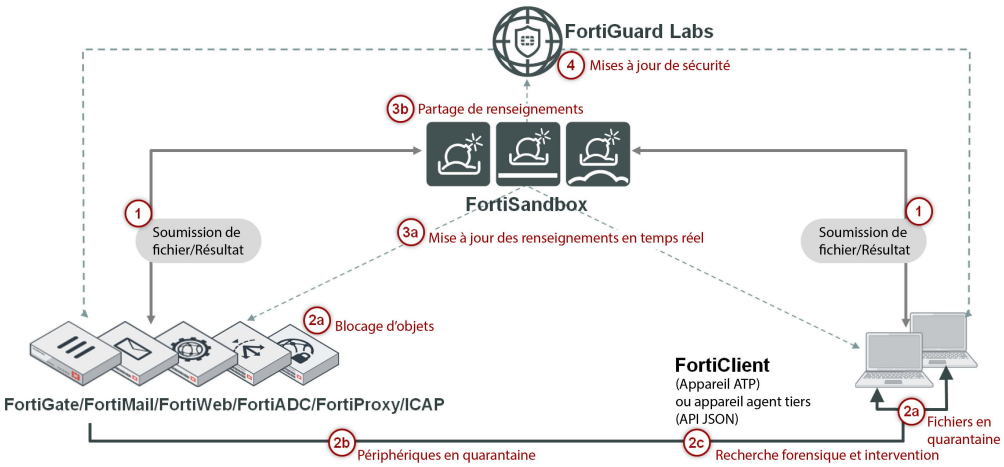

Schéma 3 : Processus de neutralisation des menaces de FortiSandbox

Requête

1. Soumission de fichiers pour analyse et résultats

Neutralisation des cybermenaces

2a. Blocage des objets sur le périphérique chargé de soumettre le fichier. Blocage des fichiers sur le poste de travail

2b. Appareils en quarantaine

2c. Enquête approfondie et intervention

Mise à jour

3a. Transfert des indicateurs de compromission aux appareils intégrés

3b. Partage optionnel des analyses avec FortiGuard

4. Protection améliorée pour tous les clients/appareils

Options de déploiement

Déploiement facile

FortiSandbox, solution unifiée, prend en charge l'inspection de nombreux protocoles et simplifie ainsi l'infrastructure et les opérations réseau. FortiSandbox s'intègre à Security Fabric, en créant un niveau de protection avancée supplémentaire.

FortiSandbox est l'appliance d'analyse des menaces la plus flexible du marché. Elle propose diverses options de déploiement afin de répondre aux configurations et besoins de chaque client, qui peut choisir de combiner ces options.

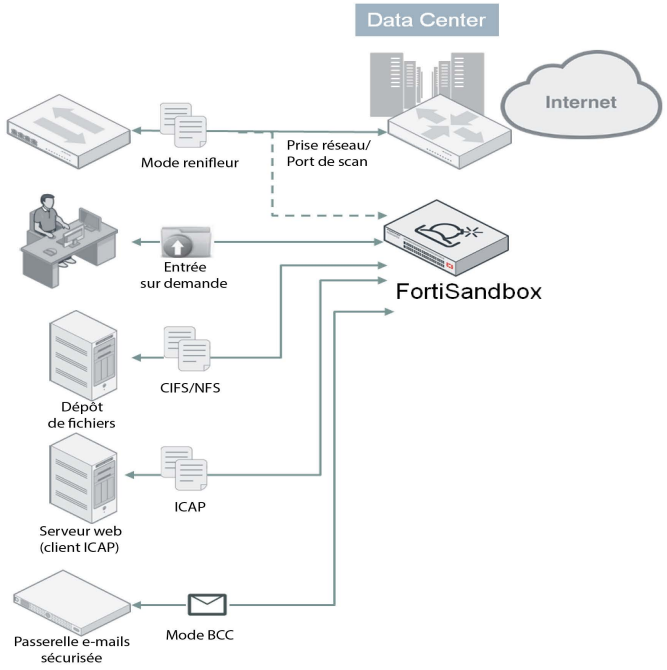

Schéma 4 : Déploiement autonome

Déploiement autonome

Ce mode de déploiement FortiSandbox prend en charge les ports de commutation, les prises réseau et les e-mails via le mode BCC. Le déploiement autonome propose également, en fonction des besoins, l'upload de fichiers ou l'analyse de répertoires (CIF, NFS, AWS S3 et Azure Blob) via l'interface graphique. Cette approche convient parfaitement à l'amélioration des protections multi-fournisseurs.

Déploiement integré

FortiSandbox assure un fonctionnement intégré avec les solutions FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (agent ATP) et Fabric-Ready Partner. Cette solution fonctionne également avec les solutions d'autres fournisseurs, via ICAP ou API JSON.

Il devient ainsi possible d'intercepter et de soumettre des contenus suspects à FortiSandbox. FortiSandbox permet de neutraliser les cyber menaces en temps opportun et de produire des rapports.

Plusieurs FortiSandbox peuvent également fonctionner de manière intégrée pour un partage instantané des renseignements en temps réel. Ce type d'inégration peut notamment profiter aux grandes entreprises déployant plusieurs FortiSandbox dans différentes régions du monde. Ce modèle automatisé sans contact est idéal pour une protection globale, au-delà des frontières et des fuseaux horaires.

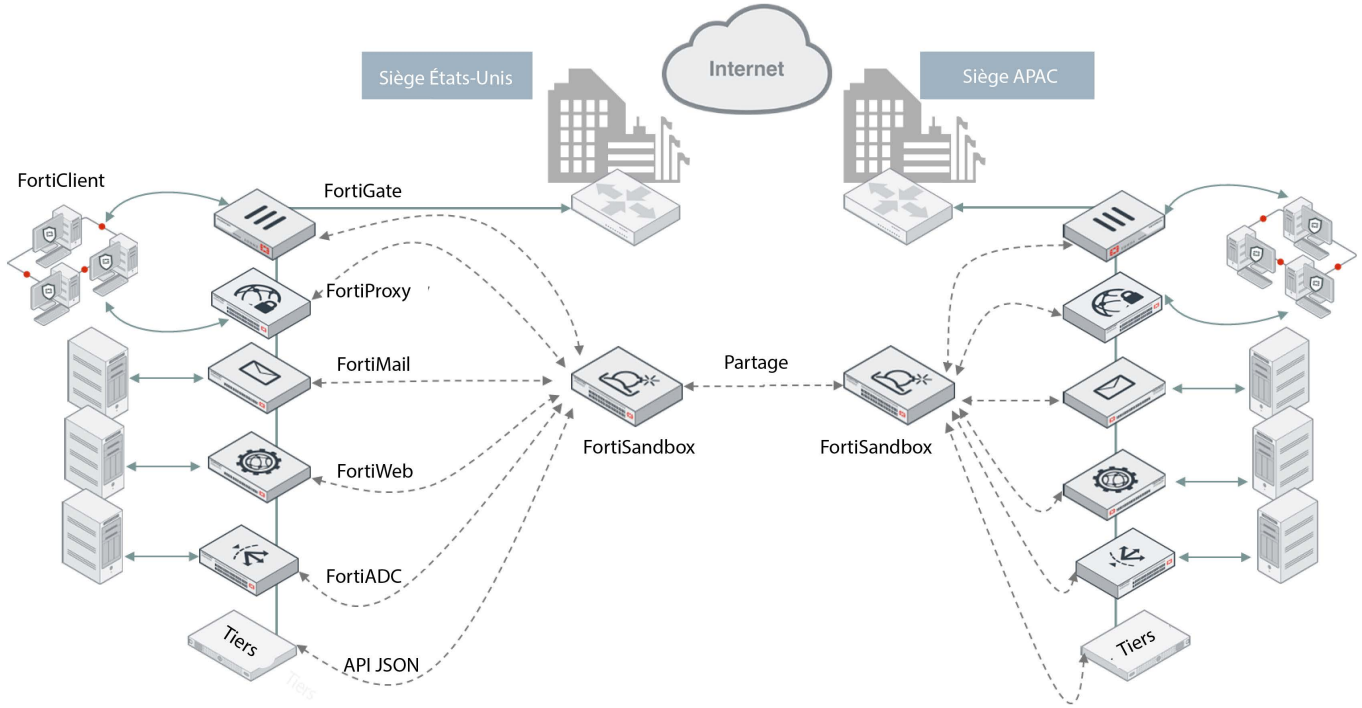

Schéma 5 : Déploiement intégré

Résumé des caractéristiques

ADMINISTRATION

- ✓ Prise en charge des configurations WebUI et CLI
- ✓ Création de plusieurs comptes administrateurs
- ✓ Sauvegarde et restauration des fichiers de configuration
- ✓ Notification par e-mail lorsque des fichiers malveillants sont détectés
- ✓ Rapport hebdomadaire (diffusion mondiale et administrateurs FortiGate)
- ✓ Page de recherche centralisée pour créer des conditions de recherche personnalisées
- ✓ Mises à jour automatiques et fréquentes des signatures
- ✓ Vérification automatique et téléchargement de nouvelles images de machines virtuelles
- ✓ Surveillance de l'état des machines virtuelles
- ✓ Authentification Radius pour les administrateurs

RÉSEAU/DÉPLOIEMENT

- ✓ Prise en charge du routage statique
- ✓ Fichier d'entrée : Mode Offline/sniffer, téléchargement de fichiers à la demande, soumission de fichiers à partir d'un ou plusieurs appareils intégrés
- ✓ Possibilité de créer un réseau simulé pour les fichiers numérisés afin d'y accéder dans un environnement réseau fermé.
- ✓ Prise en charge du clustering haute-disponibilité
- ✓ Surveillance des ports pour le basculement en cluster

INTÉGRATION DES SYSTÈMES

- ✓ Soumission des fichiers : FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy et FortiClient (agent ATP)
- ✓ Mise à jour de la base de données sur les menaces dynamiques :
  - FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy et FortiClient (agent ATP)
  - Mises à jour périodiques dynamiques vers les entités enregistrées
  - Somme de contrôle des fichiers et base de données des URL malveillantes
- ✓ Mise à jour du proxy de la base de données pour FortiManager
- ✓ Identification à distance : FortiAnalyzer, FortiSIEM, serveur syslog
- ✓ API JSON, pour l'automatisation de l'upload des échantillons et des indicateurs de logiciels malveillants exploitables, à des fins de remédiation.
- ✓ Intégration certifiée par des experts indépendants : CarbonBlack, Ziften, SentinelOne
- ✓ Partage des indicateurs de compromission entre différents FortiSandbox.

PROTECTION AVANCÉE CONTRE LES MENACES

- ✓ Détection des nouvelles menaces des ransomwares et des malwares protégés par mots de passe
- ✓ Analyse du code statique identifiant les menaces présentes dans le code inactif
- ✓ Analyse heuristique basée sur les comportements et la réputation
- ✓ Environnement de test du système d'exploitation virtuel :
- ✓ Analyse comportementale basée sur l'intelligence artificielle
  - Instances concomitantes
  - Systèmes d'exploitation pris en charge : Windows XP*, Windows 7, Windows 8.1, Windows 10, MacOS et Android
  - Techniques anti-évasion : appels en sommeil, requêtes de processus et de registre
  - Détection des rappels : visite d'URL malveillantes, communication botnet C&C et trafic provenant de logiciels malveillants activés.
  - Capture de paquets, fichiers originaux, journaux des traceurs et captures d'écran
  - Environnement de test en mode interactif

* Prise en charge en machine virtuelle personnalisée

- ✓ Type de fichier pris en charge :
  .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, .html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
- ✓ Protocoles/applications pris en charge :
  - Mode sniffer : HTTP, FTP, POP3, IMAP, SMTP, SMB
  - Mode BCC : SMTP
  - Mode intégré avec FortiGate : HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM et leur versions chiffrées SSL équivalentes
  - Mode intégré avec FortiMail : SMTP, POP3, IMAP
  - Mode intégré avec FortiWeb : HTTP
  - Mode intégré avec le client ICAP : HTTP
- ✓ Personnalisation des machines virtuelles pour qu'elles prennent en charge différents types de fichiers
- ✓ Trafic d'images des machines virtuelles isolé du trafic système
- ✓ Détection des menaces réseau en mode renifleur : identification des activités du botnet et des attaques réseau, des visites d'URL malveillantes
- ✓Analyse du partage réseau SMB/NFS et mise en quarantaine des fichiers suspects. L'analyse peut être planifiée
- ✓ Analyse des URL intégrées dans les documents
- ✓ Trafic d'images des machines virtuelles isolé du trafic système
- ✓ Possibilité de soumettre automatiquement les fichiers suspects au service cloud pour analyse manuelle et création de signature
- ✓ Possibilité de transférer des fichiers vers un partage réseau pour une analyse tierce ultérieure
- ✓ Liste blanche et option de liste noire (somme de contrôle des fichiers)
- ✓ Analyse et interrogation des URL à partir des e-mails et fichiers

MONITORING ET RAPPORTS

- ✓ Widgets de surveillance en temps réel (consultables par source et par période de temps) : statistiques des résultats d'analyse, activités d'analyse (au fil du temps), principaux hôtes ciblés, principaux logiciels malveillants, principales URL infectieuses, principaux domaines de callback
- ✓ Explorateur d'événements de recherche : tableau dynamique des actions, nom du malware, classification, type, source, destination, heure de détection et chemin de téléchargement.
- ✓ Logging - GUI, fichier de log RAW téléchargeable
- ✓ Génération de rapports pour les fichiers malveillants - Rapports détaillés sur les caractéristiques et les comportements des fichiers : modification de fichiers, comportements de processus, comportements du registre, comportements du réseau, snapshot des machines virtuelles, tableau chronologique des comportements.
- ✓ Analyse approfondie - Fichiers téléchargeables : échantillons, journaux de suivi du sandboxing, capture PCAP et indicateurs au format STIX

Spécifications

	FSA-500F	FSA-1000F	FSA-2000E	FSA-3000E
Hardware				
Format	1 RU	1 RU	2U	2 RU
Nombre total d'interfaces réseau	4 ports GE RJ45	4 ports GE RJ45, 4 slots GE SFP	4 ports GE RJ45, 2 slots 10 GE SFP+	4 ports GE RJ45, 2 slots 10 GE SFP+
Stockage	1x 1 To	2x 1 To	2x 2 To	4x 2 To
Alimentations électriques	1 PSU	1 PSU, 2 PSU en option	2 PSU redondants	2 PSU redondants
Performances systèmes				
Nombre de machines virtuelles	6*	14*	24*	56*
Débit du pré-filtre de l'environnement de test (Fichiers/heure)1	4 500	7 500	12 000	15 000
Débit du sandboxing en machine virtuelle (Fichiers/heure)	120	280	480	1 120
Débit en conditions réelles (Fichiers/heure)	600[2] 360[3]	1 400[2] 840[3]	2 400[2] 1 440[3]	5 6002 3 3603
Débit du renifleur de paquets	500 Mb/s	1 Gb/s	4 Gb/s	8 Gb/s
Dimensions				
Hauteur x Largeur x Longueur (pouces)	1,73 x 17,24 x 12,63	1,73 x 17,24 x 22,83	3,46 x 17,24 x 20,87	3,5 x 17,2 x 29
Hauteur x Largeur x Longueur (mm)	44 x 438 x 320	44 x 438 x 580	88 x 438 x 530	89 x 437 x 738
Poids de l'appareil	8,5 kg (18,72 lbs)	11,34 kg (25 lbs)	12,25 kg (27 lbs)	19,52 kg (43 lbs)
Environnement				
Consommation électrique (moyenne / maximale)	30,1 / 76,3 W	66,93 / 116,58 W	164,7 / 175,9 W	538,6 / 549,6 W
Courant maximal	100/8A, 240V/4A	100V/5A, 240V/3A	100V/8A, 240V/4A	100V/9,8A, 240V/5A
Dissipation de la chaleur	260,34 BTU/h	397,75 BTU/h	600,17 BTU/h	1 943,82 BTU/h
Source d'alimentation	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Humidité	5–90% sans condensation	5–90% sans condensation	5–90% sans condensation	8–90% sans condensation
Plage de température de fonctionnement	0–40°C (32–104°F)	0–40°C (32–104°F)	0–40°C (32–104°F)	10– 35°C (50–95°F)
Plage de température de stockage	-20–70°C (-4–158°F)	-40–70°C (-40–158°F)	-20–70°C (-4–158°F)	-40–70°C (-40–158°F)
Conformité				
Certifications	FCC Partie 15 Classe A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST			

	FORTISANDBOX-VM		FORTISANDBOX CLOUD
Configuration matérielle requise			
Prise en charge de l'hyperviseur	VMware ESXi version 5.1 et + Linux KVM CentOS 7.2 et +, AWS (Sur demande et « BYOL »)		N.A
Processeurs virtuels (Minimum / Maximum)	4 / Illimité (Fortinet recommande que le nb de vCPUs corresponde au nb de MV Windows +4)		N.A
Prise en charge de la mémoire (Minimum / Maximum)	8 Go / Illimité		N.A
Stockage virtuel (Minimum / Maximum)	30 Go / 16 To		N.A
Nombre total d'interfaces réseau virtuelles (Minimum)	6		N.A
Performances système			
Débit du renifleur de paquets	1 Gb/s		N.A
Débit du pré-filtre de l'environnement de tests (Fichiers/heure)1	Fonction du matériel		**
	Machines virtuelles locales	Machines virtuelles cloud	
Nombre de machines virtuelles	8 MV/nœud, jusqu'à 99 nœuds/cluster	5 (jusqu'à 200 MV Windows Cloud)	**
Débit du sandboxing en machine virtuelle (Fichiers/heure)	Fonction du matériel	100 (jusqu'à 4 000)	**
Débit en conditions réelles (fichiers/heure)2	Fonction du matériel	500 (jusqu'à 20 000)2	**

Remarque : toutes les valeurs de performances indiquées représentent les valeurs optimales et varient en fonction de la configuration du système.
1 Le pré-filtrage FortiSandbox est alimenté par FortiGuard Intelligence.
2 Mesure réalisée à partir du trafic web et e-mails réel, lorsque l'analyse pré-filtre et l'analyse dynamique fonctionnent de manière consécutive.

* 2(FSA-500F)/2(FSA-1000F)/4(FSA-2000E)/8(FSA-3000E)/8(FSA-3000E) : licences pour machines virtuelles Windows incluses avec le matériel, le reste étant proposé en licence de mise à niveau.
** Se reporter à la description du service FortiSandbox Cloud Service.


FortiSandbox 500F


FortiSandbox 1000F


FortiSandbox 2000E


FortiSandbox 3000E

Intégration Matrix

		FORTIGATE	FORTICLIENT	FORTIMAIL	FORTIWEB	FORTIADC	FORTIPROXY
Appliance FSA et VM	Soumission des fichiers	*FortiOS V5.0.4+	FortiClient pour Windows OS V5.4+	FortiMail OS V5.1+	FortiWeb OS V5.4+	FortiADC OS V5.0+	FortiProxy OS V1.0+
	Feedback sur l'état du fichier	*FortiOS V5.0.4+	FortiClient pour Windows OS V5.4+	FortiMail OS V5.1+	FortiWeb OS V5.4+	FortiADC OS V5.0+	FortiProxy OS V1.0+
	Rapport détaillé sur le fichier	*FortiOS V5.4+	FortiClient pour Windows OS V5.4+	FortiMail OS V5.1+	–	FortiADC OS V5.0+	FortiProxy OS V1.0+
	Mise à jour de la base de données Dynamic Threat	*FortiOS V5.4+	FortiClient pour Windows OS V5.4+	FortiMail OS V5.3+	FortiWeb OS V5.4+	FortiADC OS V5.0+	FortiProxy OS V1.0+
FortiSandbox Cloud	Soumission des fichiers	*FortiOS V5.2.3+	–	FortiMail OS V5.3+	FortiWeb OS 5.5.3+	–	FortiProxy OS V1.0+
	Feedback sur l'état du fichier	*FortiOS V5.2.3+	–	FortiMail OS V5.3+	FortiWeb OS 5.5.3+	–	FortiProxy OS V1.0+
	Rapport détaillé sur le fichier	*FortiOS V5.2.3+	–	–	–	–	FortiProxy OS V1.0+
	Mise à jour de la base de données Dynamic Threat	*FortiOS V5.4+	–	FortiMail OS V5.3+	FortiWeb OS 5.5.3+	–	FortiProxy OS V1.0+

*Certains modèles peuvent nécessiter une configuration CLI

Informations relatives aux commandes

Produit	Référence (SKU)	Description
FortiSandbox 500F	FSA-500F	Système avancé de protection contre les menaces - 4 x GE RJ45, 2 machines virtuelles sous licence Windows/ Linux/Android avec Win7, Win10 et 1 licence MS office incluse. Possibilité de mise à niveau jusqu'à un maximum de 6 machines virtuelles, voir SKU FSA-500F-UPG-LIC-4 et/ou FC-10-FS5HF-176-02-DD.
FortiSandbox 1000F	FSA-1000F	Système avancé de protection contre les menaces - 4 x GE RJ45, 4 x slots GE SFP, 2 machines virtuelles Windows / Linux / Android sous licence avec Win7 , Win10 et 1 licence MS office incluse. Possibilité de mise à niveau vers un maximum de 14 machines virtuelles sous licence, voir SKU FSA-1000F-UPG-LIC-6 et/ou SKU FC-10-FS1KF-176-02-DD. Alimentation redondante (en option), voir SP-FSA1000F-PS SKU.
FortiSandbox 2000E	FSA-2000E	Système avancé de protection contre les menaces - 4 x GE RJ45, 2 x slots 10GbE SFP+, alimentation redondante, 4 machines virtuelles Windows/Linux/Android sous licence avec Win7 , Win8 , Win10 et 1 licence MS office incluse. Possibilité de mise à niveau vers un maximum de 24 VM, voir SKU FSA-2000E-UPG-LIC-10 et/ ou FC-10-SA20K-176-02-DD
FortiSandbox 3000E	FSA-3000E	Système avancé de protection contre les menaces - 4 x GE RJ45, 2 x 10GbE SFP+, alimentation redondante, 8 machines virtuelles Windows/Linux/Android sous licence avec Win7 , Win8 , Win10 et (1) licences MS office incluses. Extensible jusqu'à 56 machines virtuelles, voir SKU FSA-3000E-UPG-LIC-16 et/ou FC-10-SA30K-176-02-DD.
FortiSandbox-VM	FSA-VM-00	Appliance virtuelle FortiSandbox-VM avec 0 machine virtuelle incluse et une extension maximale limitée à 8 machines virtuelles au total par nœud, jusqu'à 99 nœuds par cluster.
FortiSandbox Windows Cloud VM	FC-10-FSA01-195-02-DD	Service FortiSandbox Windows Cloud VM pour (5) machines virtuelles Windows et extension maximale limitée à (200) machines virtuelles Windows Cloud par machine virtuelle FortiSandbox.
FortiSandbox macOS Cloud VM	FC-10-FSA01-192-02-DD	Service macOS Cloud VM pour (2) macOS X machines virtuelles et extension maximale limitée à (8) macOS X machines virtuelles par FortiSandbox (Appliance / machine virtuele).
FortiSandbox Cloud Service	FC-10-XXXXX-100-02-DD	FortiGuard Advanced Malware Protection (AMP) comprenant un antivirus, un malware mobile et le service FortiSandbox Cloud. (SKU différentes selon les modèles FortiGate).
	FC-10-XXXXX-123-02-12	Abonnement au FortiSandbox Cloud Service (SKU pouvant varier selon les modèles FortiMail/FortiWeb).
	FC1-15-EMS01-298-02-DD	Abonnement à la licence FortiSandbox Cloud pour 25 appareils. Inclut l'agent Sandbox avec abonnement Sandbox On-Prem/Cloud, gestion centrale et support 24x7. (SKU pour FortiClient).
	FC1-10-XXXXX-620-02-DD	Protection SWG - Filtrage Web, filtrage DNS, contrôle des applications, DLP, AV, Botnet (IP/Domaine), Sandbox Cloud. (SKU pouvant varier selon les modèles FortiProxy).
Accessoires en option		
1 module émetteur-récepteur GE SFP SX	FG-TRAN-SX	1 module émetteur-récepteur GE SFP SX pour tous les systèmes avec slots SFP et SFP/SFP+.
1 module émetteur-récepteur GE SFP LX	FG-TRAN-LX	1 module émetteur-récepteur GE SFP LX pour tous les systèmes avec slots SFP et SFP/SFP+.
10 modules émetteur-récepteur GE SFP + courte portée	FG-TRAN-SFP+SR	10 modules émetteur-récepteur GE SFP+, courte portée pour tous les systèmes avec slots SFP+ et SFP/SFP+.
10 modules émetteur-récepteur GE SFP + longue portée GE SFP+	FG-TRAN-SFP+LR	10 modules émetteur-récepteur GE SFP+, longue portée pour tous les systèmes avec slots SFP+ et SFP/SFP+.
Alimentation en courant alternatif	SP-FSA1000F-PS	Alimentation AC pour les modules FDC-1000F, FIS-1000F, FSA-1000F uniquement.