FICHE TECHNIQUE

Gamme FortiSandbox™

Neutralisation proactive et multicouche des menaces

FortiSandbox

Les cybercriminels les plus ingénieux arrivent de plus en plus à contourner les solutions classiques de protection contre les logiciels malveillants et à introduire des menaces persistantes avancées au cœur des réseaux. Ces attaques extrêmement ciblées déjouent les dispositifs de détection de signature en place en dissimulant leur nature malveillante de différentes façons : compression, chiffrement, polymorphisme, etc. La liste des techniques employées est encore longue. Certaines ont même commencé à contourner les environnements « Sandbox » virtuels au moyen de la détection des machines virtuelles (VM), de « bombes à retardement », etc. Pour combattre les attaques d'aujourd'hui, une approche complète et intégrée est nécessaire, allant au-delà d'une simple protection contre les logiciels malveillants, d'un environnement Sandbox virtuel ou d'un système de surveillance isolé.

FortiSandbox combine avec efficacité des fonctions de détection et de neutralisation proactives, des informations exploitables sur les menaces et un déploiement simple et intégré. La solution repose sur un environnement Sandbox unique à deux niveaux, complété par la technologie Fortinet primée de protection contre les logiciels malveillants et par les fonctionnalités FortiGuard de veille intégrées en option. Le savoir-faire acquis au fil des années par Fortinet dans le domaine des menaces est désormais mis à disposition sur site via FortiSandbox.

Détection et neutralisation proactives

Les codes suspects sont soumis à des préfiltres multicouches avant l'exécution dans le système d'exploitation virtuel en vue d'une analyse comportementale détaillée. Ces préfiltres très efficaces incluent un filtrage par notre moteur antivirus (AV), des requêtes sur les bases de données de menaces dans le Cloud et une simulation indépendante du système d'exploitation avec un émulateur de code, le tout suivi par une exécution dans l'environnement d'exécution virtuel entier. Si un code malveillant est détecté, les résultats servent à la création de signatures de protection contre les logiciels malveillants et à la mise à jour des autres bases de données de menaces.

Informations exploitables

Toutes les classifications (code malveillant et risque élevé/moyen/faible) sont présentées dans un tableau de bord intuitif. Des informations complètes sur les menaces, générées suite à l'exécution virtuelle (activité système, efforts d'exploitation, trafic Web, téléchargements consécutifs, tentatives de communication, etc.), sont disponibles dans des journaux et rapports extrêmement détaillés.

Déploiement simple

FortiSandbox prend en charge l'inspection d'un grand nombre de protocoles dans une même solution unifiée et simplifie ainsi l'infrastructure et les opérations réseau. Par ailleurs, la solution s'intègre avec FortiGate en tant que nouvelle fonctionnalité au sein de l'infrastructure de sécurité existante.

L'association idéale entre neutralisation proactive, visibilité avancée sur les menaces et reporting complet.

Principales caractéristiques

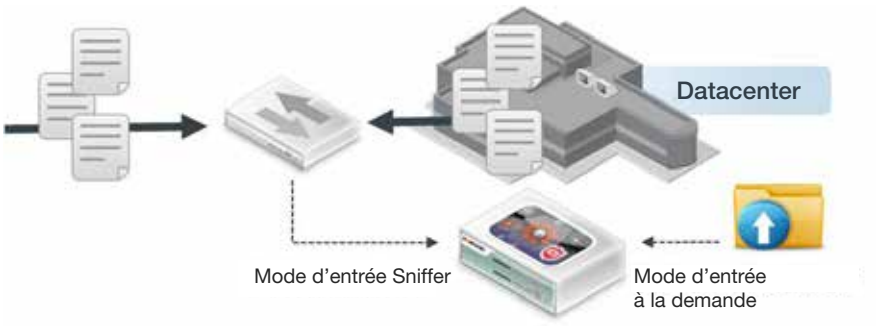
- Environnement d'exécution virtuel sécurisé pour révéler les menaces inconnues
- Préfiltres multicouches uniques pour une détection rapide et efficace des menaces
- Reporting détaillé pour une visibilité totale sur le cycle de vie des menaces
- Inspection de nombreux protocoles dans une appliance unique pour simplifier le déploiement et réduire les coûts
- Intégration avec FortiGate pour renforcer plutôt que pour dupliquer l'infrastructure de sécurité
- Sécurité validée par des tests NSS BDS (Breach Detection Systems)

OPTIONS DE DÉPLOIEMENT

FortiSandbox est l'appliance d'analyse des menaces la plus flexible du marché. Elle offre en effet diverses options de déploiement pour répondre aux configurations et exigences spécifiques des clients. Les entreprises peuvent également mettre en œuvre les trois options d'entrée en parallèle.

Autonome

Ce mode de déploiement repose sur les données d'entrée en provenance des ports de switch répartis ou les téléchargements de fichiers à la demande effectués par les administrateurs au moyen de l'interface utilisateur graphique. C'est l'infrastructure la plus adaptée pour l'ajout de fonctionnalités de sécurité aux systèmes de protection contre les menaces proposés par différents fournisseurs.



*Intégration avec FortiGate/ FortiMail

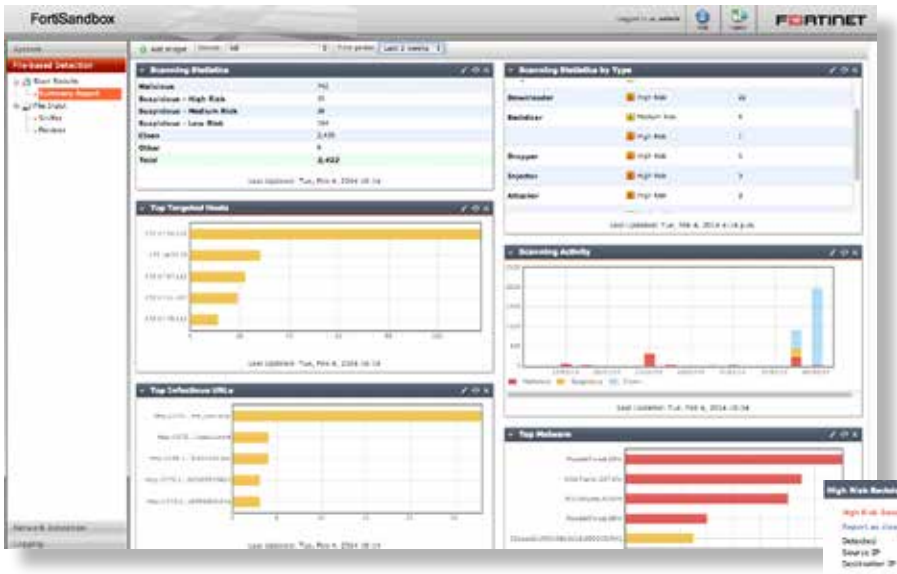
En tant que passerelle de sécurité Internet, la solution FortiGate peut être configurée de manière à envoyer les fichiers suspects à FortiSandbox. Cette intégration transparente réduit la complexité du réseau et permet de prendre en charge davantage d'applications et de protocoles, y compris ceux faisant l'objet d'un chiffrement SSL comme HTTPS.

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

Intégration avec des solutions FortiGate distribuées

Ce déploiement convient plus particulièrement aux entreprises dotées d'environnements distribués, où des solutions FortiGate sont déployées dans les succursales et envoient les fichiers suspects à un environnement FortiSandbox centralisé. Cette configuration bénéficie du TCO (ou coût total de possession) le plus faible et assure une protection contre les menaces sur les sites distants.

CARACTÉRISTIQUES

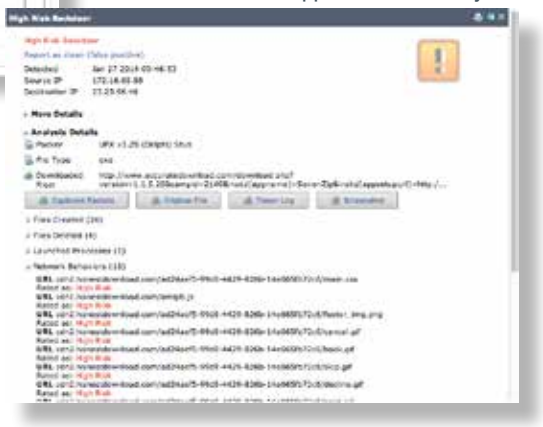


Widgets de tableau de bord — état des menaces en temps réel

Sandbox sur VM

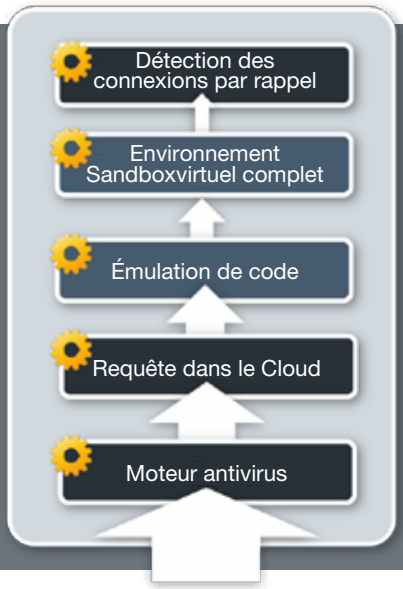
Complétez votre système de défense par des fonctionnalités de pointe permettant d'analyser les fichiers suspects et à haut risque dans un environnement confiné afin de découvrir le cycle de vie complet d'une attaque sur la base de l'activité système et de la détection des connexions par rappel.

Rapport détaillé d'analyse des fichiers



Outils d'analyse des fichiers

Les rapports avec les paquets capturés, le fichier d'origine, le journal de suivi et une capture d'écran procurent une excellente visibilité sur les menaces et des informations exploitables une fois les fichiers examinés. Cela permet d'accélérer le processus de neutralisation et de mettre à jour la protection.



Le traitement multi-niveaux des fichiers optimise l'utilisation des ressources et améliore la sécurité, la capacité et les performances

Moteur antivirus

- Applique une analyse antivirus de haut niveau (proactive et réactive à plus de 95 %). Sert de préfiltre efficace.

Requête dans le Cloud

- Contrôle en temps réel des dernières informations sur les logiciels malveillants
- Accès à des informations partagées pour une détection instantanée des logiciels malveillants

Émulation de code

- Simule rapidement l'activité prévue
- Indépendant du système d'exploitation et à l'abri de tout contournement/brouillage

Environnement Sandbox virtuel complet

- Environnement d'exécution sécurisé en vue d'une analyse/évaluation comportementale
- Révèle des informations complètes sur le cycle de vie des menaces

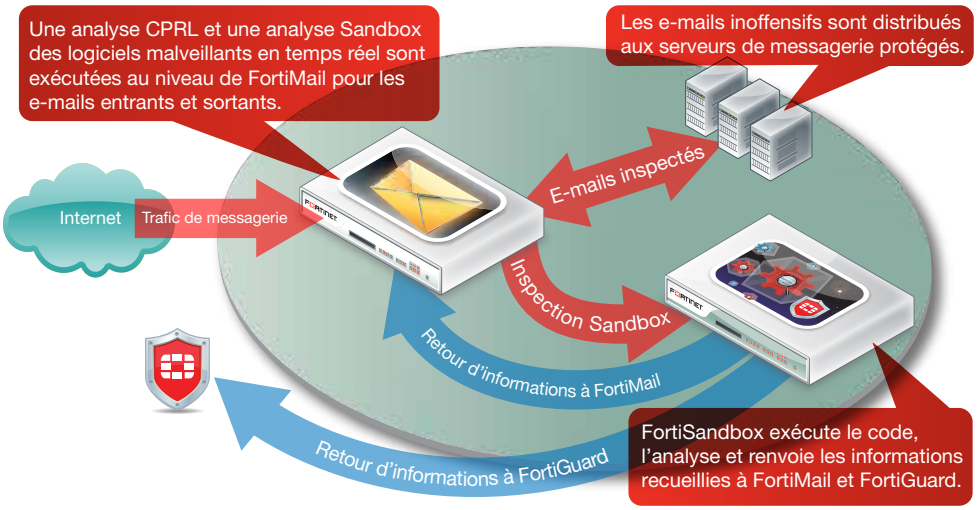
Détection des connexions par rappel

- Identifie la cible ultime, les connexions par rappel et les tentatives d'extraction

CARACTÉRISTIQUES

Neutralisation avec FortiMail

De nombreuses menaces avancées commencent par un e-mail ciblé qui contient un logiciel malveillant personnalisé. À cela s'ajoute l'ingénierie sociale qui incite l'utilisateur à ouvrir ce message. C'est pourquoi les entreprises complètent leur passerelle de messagerie sécurisée par un système de Sandbox intégré. Plus précisément, la passerelle de messagerie sécurisée met les messages en attente pendant qu'une analyse supplémentaire est réalisée dans cet environnement d'exécution confiné. Elle applique ensuite les politiques appropriées sur la base des résultats obtenus.



FortiMail envoie et met en file d'attente tout contenu suspect

RÉSUMÉ DES CARACTÉRISTIQUES

Administration

Prise en charge des configurations WebUI et CLI

Création de plusieurs comptes administrateur

Sauvegarde et restauration des fichiers de configuration

Notification par e-mail en cas de détection d'un fichier malveillant

Rapport hebdomadaire envoyé à une liste de diffusion et aux administrateurs FortiGate

Page de recherche centralisée permettant aux administrateurs d'établir des conditions de recherche personnalisées

Mises à jour automatiques fréquentes des signatures

Surveillance de l'état des machines virtuelles

Gestion réseau/déploiement

Prise en charge du routage statique

Fichiers en entrée : mode hors ligne/sniffer, téléchargement de fichiers à la demande, soumission de fichiers par des Devices intégrés

API basée sur le Web qui permet aux utilisateurs de télécharger des échantillons à analyser indirectement

Possibilité de créer un réseau simulé pour l'accès du fichier analysé dans un environnement réseau fermé

Intégration de Devices :
- Soumission de fichiers : FortiGate, FortiMail
- Mise à jour de l'hôte de base de données : FortiManager
- Logging à distance : FortiAnalyzer, Syslog Server

Protection avancée contre les menaces

Sandbox de système d'exploitation virtuel :
- Instances Windows simultanées
- Techniques anti-contournement : sleep calls, requêtes sur les processus et le registre
- Détection des connexions par rappel : visite d'URL malveillantes, communication de commande et de contrôle botnet et trafic de piratage en provenance des logiciels malveillants activés
- Téléchargement des paquets capturés, fichier d'origine, journal de suivi et capture d'écran

Taille de fichier illimitée prise en charge, possibilité de configurer une taille de fichier maximale

Types de fichiers pris en charge :
- Archives : .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj
- Fichiers exécutables (par exemple : .exe, .dll), PDF, Microsoft Office Document et Javascript
- Fichiers multimédias : .avi, .mpeg, .mp3, .mp4

Protocoles/applications pris en charge :
- Mode sniffer : HTTP, FTP, POP3, IMAP, SMTP, SMB
- Mode intégré avec FortiGate : HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM et leurs versions équivalentes avec chiffrement SSL
- Mode intégré avec FortiMail : SMTP, POP3, IMAP

Détection des menaces réseau en mode sniffer : identification des activités de botnet et des attaques réseau, visite d'URL malveillantes

Possibilité d'envoyer automatiquement des fichiers suspects au service de Cloud pour analyse manuelle et création de signatures

Surveillance et rapport

Widgets de surveillance en temps réel (consultables en fonction de la source et options relatives à la période) : statistiques des résultats d'analyse, activités d'analyse (dans le temps), principaux hôtes ciblés, principaux logiciels malveillants, principales URL infectieuses, principaux domaines de rappel

Observateur d'événements avec vue détaillée : tableau dynamique avec contenu des actions, nom du logiciel malveillant, classement, type, source, destination, heure de détection et chemin de téléchargement

Logging : interface utilisateur graphique, téléchargement du fichier journal BRUT

Génération de rapports sur les fichiers malveillants : rapports détaillés sur les caractéristiques et comportements de fichiers — modification de fichier, comportements des processus, du registre, du réseau, snaptshot de VM

Analyse ultérieure : fichiers téléchargeables — exemple de fichier, journaux de suivi Sandbox et capture PCAP

SPÉCIFICATIONS

	FSA-1000D	FSA-3000D
Matériel		
Format	2 U	2 U
Nombre total d'interfaces réseau	6 ports RJ45 GbE, 2 emplacements SFP GbE	4 ports RJ45 GbE, 2 emplacements SFP GbE 2 emplacements SFP+ 10 GbE
Capacité de stockage	4 To (max. 8 To)	8 To (max. 16 To)
Alimentation électrique	2 alimentations redondantes	2 alimentations redondantes
Système		
Sandbox sur VM (fichiers/heure)	160	560
Analyse antivirus (fichiers/heure)	6 000	15 000
Nombre de VM	8	28
Dimensions		
Hauteur x largeur x longueur (pouces)	3,5 x 17,2 x 14,5	3,3 x 19,0 x 29,7
Hauteur x largeur x longueur (mm)	89 x 437 x 368	84 x 482 x 755
Poids	27,60 lbs (12,52 kg)	71,5 lbs (32,5 kg)

	FSA-1000D	FSA-3000D
Données environnementales		
Consommation électrique (moyenne / maximale)	115 / 138 W	392 / 614,6 W
Courant maximal	100 V/5 A, 240 V/3 A	110 V/10 A, 220 V/5 A
Dissipation thermique	471 BTU/h	2 131,14 BTU/h
Source d'énergie	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz
Humidité	5 à 95 % sans condensation	20 à 90 % sans condensation
Plage de températures d'exploitation	32 à 104 °F (0 à 40 °C)	50 à 95 °F (10 à 35 °C)
Plage de températures de stockage	-13 à 158 °F (-25 à 70 °C)	-40 à 149 °F (-40 à 65°C)
Conformité		
Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	

	FSA-VM
Configuration matérielle requise	
Hyperviseur pris en charge	VMware ESXi version 5.0 ou supérieure
CPU virtuels (min. / max.)	4 / illimité (Fortinet recommande de mettre en œuvre un nombre de vCPU correspondant au nombre de machines virtuelles Windows +4.)
Mémoire virtuelle (min. / max.)	8 Go / illimité
Stockage virtuel (min. / max.)	30 Go / 16 To
Nombre total d'interfaces réseau virtuelles (min.)	6
Système	
Sandbox sur VM (fichiers/heure)	En fonction du matériel
Analyse antivirus (fichiers/heure)	En fonction du matériel
Nombre de VM	Entre 2 et 52 (mise à niveau au moyen des licences appropriées)

INFORMATIONS DE COMMANDE

Produit	Référence	Description
FortiSandbox 1000D	FSA-1000D	Système Advanced Threat Protection — 6 ports RJ45 GbE, 2 emplacements SFP GbE, alimentation redondante, 6 licences Windows XP et 2 licences Windows 7 incluses
FortiSandbox 3000D	FSA-3000D	Système Advanced Threat Protection — 4 ports RJ45 GbE, 2 emplacements SFP GbE, alimentation redondante, 22 licences Windows XP et 6 licences Windows 7 incluses
FortiSandbox-VM	FSA-VM-BASE	Licence de base pour FortiSandbox-VM empilable. Comprend (1) licence VM Windows XP et (1) licence VM Windows 7. Extension maximale de FSA-VM limitée à un total de 52 machines virtuelles.
Accessoires en option	**Référence**	**Description**
Module transceiver SX SFP 1 GbE	FG-TRAN-SX	Module transceiver SX SFP 1 GbE pour tous systèmes dotés d'un emplacement SFP ou SFP/SFP+.
Module transceiver LX SFP 1 GbE	FG-TRAN-LX	Module transceiver LX SFP 1 GbE pour tous systèmes dotés d'un emplacement SFP ou SFP/SFP+.
Module transceiver SFP+ 10 GbE courte portée	FG-TRAN-SFP+SR	Module transceiver SFP+ 10 GbE courte portée pour tous systèmes dotés d'un emplacement SFP ou SFP/SFP+.
Module transceiver SFP+ 10 GbE longue portée	FG-TRAN-SFP+LR	Module transceiver SFP+ 10 GbE longue portée pour tous systèmes dotés d'un emplacement SFP ou SFP/SFP+.

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

SIÈGE SOCIAL MONDIAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1 408 235 7700
www.fortinet.com/sales

SUCCURSALE EMEA
120, rue Albert Caquot
06560, Sophia Antipolis,
France
Tél. : +33 (0)4 89 87 05 10

SUCCURSALE APAC
300 Beach Road 20-01
The Concourse
Singapore 199555
Tél. : +65 6513 3730

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