PROTECTION AVANCÉE CONTRE LES MENACES

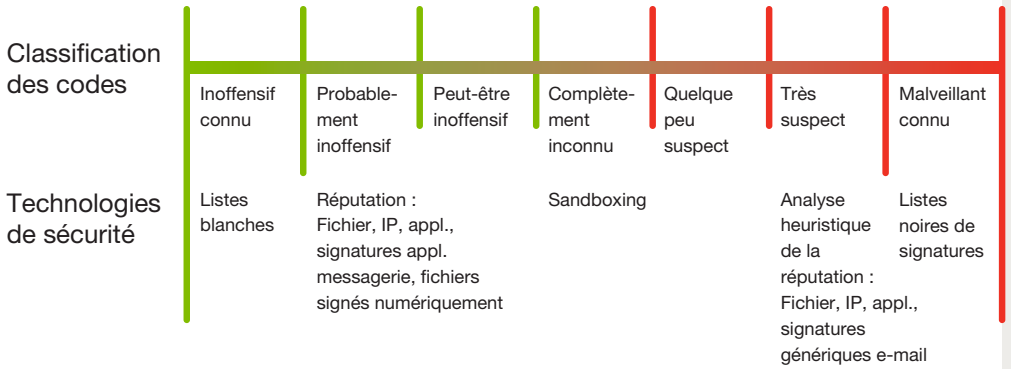
Protégez votre entreprise contre les attaques avancées. La technologie Sandbox est capable de détecter les menaces susceptibles d'échapper aux autres systèmes de sécurité en les incitant à se démasquer.

Pourquoi utiliser la technologie Sandbox pour votre protection ?

Les entreprises mises à mal par des menaces persistantes avancées (APT) ne cessent de défrayer la chronique. La technologie Sandbox est la dernière solution à la mode prônée pour vous protéger contre ces menaces. Pourquoi ? Pourquoi la technologie Sandbox ? Quels avantages une solution de Sandbox vous offre-t-elle par rapport aux couches de sécurité existantes ?

Une solution de Sandbox vous donne l'occasion de prédire l'avenir, d'anticiper l'inconnu.

Le monde n'est pas tout noir ou tout blanc, tout bon ou tout mauvais. Les codes qui s'exécutent sur votre réseau sont de natures très diverses et englobent aussi bien des codes inoffensifs connus que des codes malveillants connus. Mais de nombreux codes sont tout simplement inconnus. Vous disposez probablement déjà d'un certain nombre de technologies de sécurité pour protéger votre entreprise contre les codes malveillants et vous aider à identifier les codes inoffensifs. Toutefois, comme la plupart des entreprises, vous êtes toujours à la merci de l'inconnu. Et cette zone d'incertitude n'est pas à prendre à la légère.



Avantages

- Prévention des atteintes à la sécurité des données par des attaques avancées
- Détection des menaces persistantes avancées
- Découverte des logiciels malveillants inconnus jusqu'à présent
- Blocage d'un nombre plus important d'attaques de spearphishing (ou harponnage)
- Amélioration de l'efficacité de votre solution NGFW, UTM ou de la passerelle de messagerie sécurisée

SECURED BY **FORTIGUARD**®

Le rapport 2014 Verizon Breach Report indique 1 367 brèches de sécurité et plus de 63 000 incidents de sécurité en 2013. La technologie Sandbox vous offre en définitive un moyen d'effacer la zone d'incertitude et d'identifier ainsi les attaques inconnues jusqu'à présent, qui sont susceptibles d'échapper aux technologies de sécurité classiques.

Comment la technologie Sandbox s'intègre-t-elle dans les nombreuses couches de sécurité déjà en place ?

Examinons le cycle de vie d'une attaque et le rôle joué par les technologies de sécurité dans la protection d'une entreprise.

- **Étape 1 :** Le pirate commence par une reconnaissance de sa cible. Il conçoit ensuite un e-mail ingénieux, qui contient souvent un code (ou fichier) malveillant. Il envoie ensuite ce message à la cible. C'est là que votre solution antispam/antiphishing est censée intervenir pour bloquer le message. Mais si ce n'est pas le cas : l'e-mail parvient à la cible et le pirate peut alors espérer que celle-ci clique sur le lien malveillant.

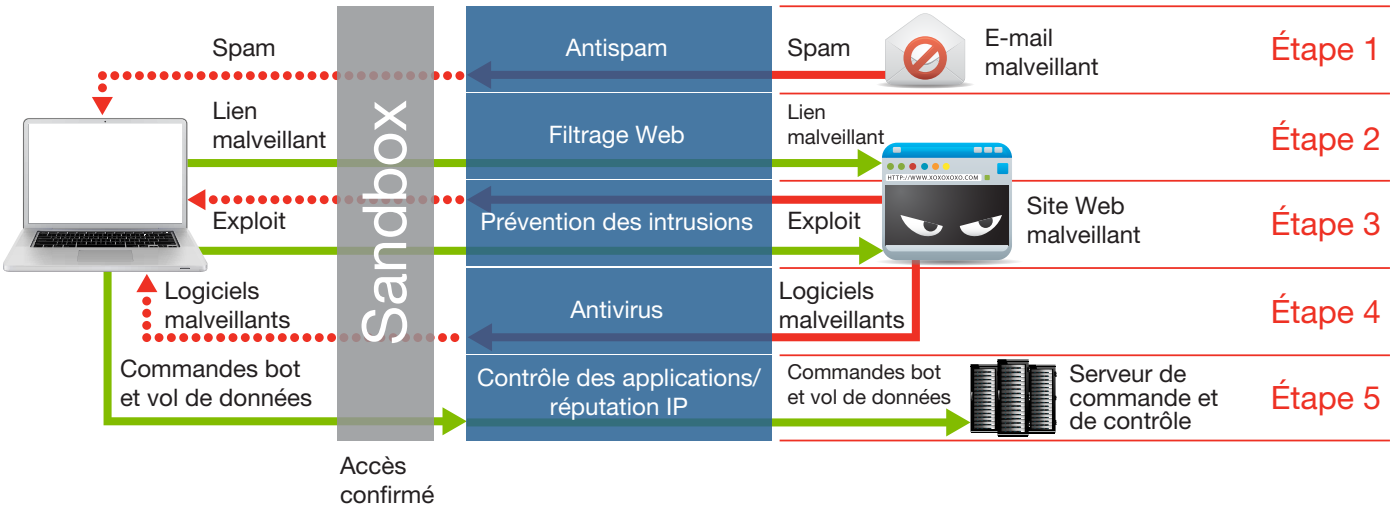
- **Étape 2 :** Si la cible clique sur le lien, le trafic est acheminé vers un site Web en vue de l'établissement de la communication. C'est là que votre filtre Web est censé bloquer le trafic. Mais si ce n'est pas le cas : ce site Web malveillant commence à attaquer votre entreprise.

- **Étape 3 :** Les attaques (exploits) lancées par le site Web malveillant visent généralement à obtenir un accès au système de la cible. C'est là que votre système de prévention des intrusions (IPS) tente de bloquer les attaques. Mais s'il n'y parvient pas : une brèche est alors ouverte et le site peut introduire un logiciel malveillant dans votre entreprise.

- **Étape 4 :** Dès lors que le logiciel malveillant cherche à s'infiltrer, votre programme de protection contre les logiciels malveillants est censé vous protéger. Mais si ce n'est pas le cas : un code exécutable est introduit dans votre système où il peut s'exécuter.

- **Étape 5 :** Une fois le code malveillant exécuté, il cherche généralement à accéder aux identifiants de connexion et effectue un balayage latéral pour trouver les données sensibles de votre entreprise, qu'il récupère/transfère ensuite. Mais pour pouvoir accomplir sa mission, il doit extraire ces données vers un serveur de commande et de contrôle. C'est là que vos systèmes de contrôle des applications, d'analyse de réputation IP, de détection des botnets et autres dispositifs de protection entrent en action. Mais si ces technologies ne parviennent pas à bloquer ce trafic sortant : votre sécurité est compromise.

Les technologies antispam, de filtrage Web, de prévention des intrusions, antivirus, de contrôle des applications et d'analyse de réputation IP sont des protections nécessaires. Mais elles ne suffisent pas à arrêter les attaques les plus sophistiquées d'aujourd'hui. Elles reposent sur l'identification d'indicateurs connus (mais diversifiés) d'attaque, au moyen de signatures, d'analyses heuristiques ou de filtres de réputation. Le véritable danger, ce sont les attaques inédites ou celles capables de se dissimuler au travers de techniques d'encapsulation, de chiffrement ou autres méthodes de contournement. Si vous complétez votre système combiné de sécurité par la technologie Sandbox, vous ajoutez une couche de protection qui peut détecter tout code malveillant, même inconnu jusqu'alors, en l'incitant à se démasquer dans l'environnement Sandbox.



Qu'est-ce que la technologie Sandbox ?

Il s'agit d'un environnement sécurisé et isolé qui reproduit l'environnement d'exploitation d'un utilisateur et dans lequel vous pouvez exécuter un code, l'observer et l'évaluer sur la base de son activité plutôt que de ses caractéristiques. Vous pouvez lancer des fichiers exécutables et confiner tout trafic réseau ou élément susceptible de dissimuler des logiciels malveillants au sein d'un environnement Sandbox. Cet environnement sécurisé permet d'exécuter et d'observer les codes malveillants, notamment les opérations sur fichier/disque, les connexions réseau, les changements de configuration du registre/système, etc.

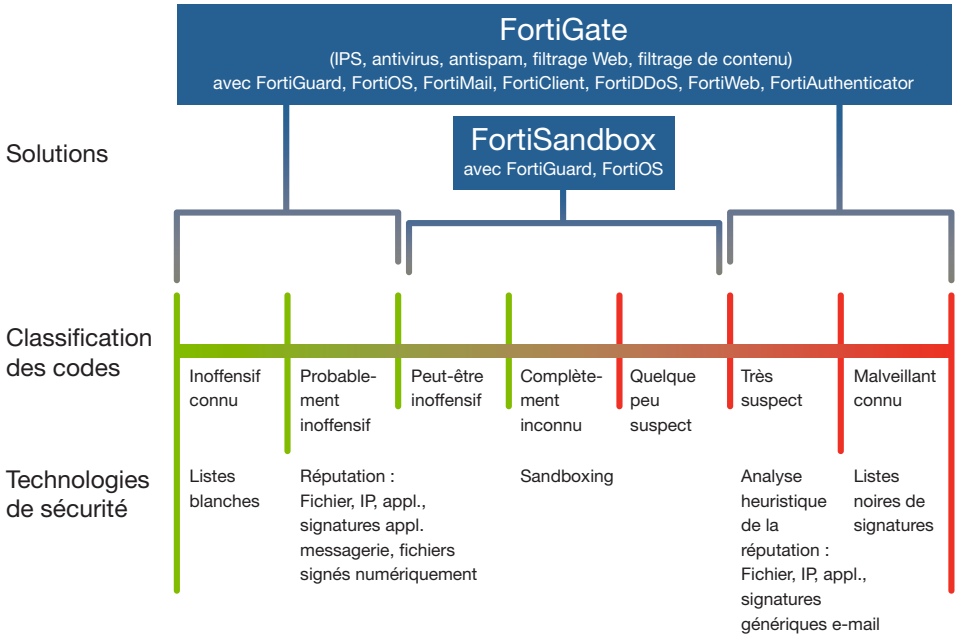
Pourquoi la solution FortiSandbox est-elle si rapide et si efficace ?

FortiSandbox vise à reproduire le comportement de systèmes utilisateur réels pour exécuter un code malveillant, voire pour accélérer son exécution, de manière à le détecter. Pour évaluer les logiciels malveillants, les systèmes de Sandbox exécutent plusieurs processus d'évaluation du code avec des technologies et systèmes d'exploitation différents. FortiSandbox hiérarchise les processus d'évaluation en fonction du degré de prévalence d'un logiciel malveillant dans les différentes configurations afin d'accélérer l'identification du code malveillant.

FortiSandbox est un outil de détection particulièrement performant lorsqu'il est associé aux capacités d'exécution des dispositifs de prévention des menaces en place, tels que les systèmes de Firewall de Nouvelle Génération (NGFW) ou de gestion unifiée des menaces (UTM), ainsi qu'à une passerelle de messagerie sécurisée ou une plateforme de protection des terminaux. Les solutions Fortinet couvrent les points d'inspection en entrée, en sortie et en interne. Elles peuvent ainsi préfiltrer le trafic de façon proactive, de manière à intercepter le plus d'éléments possible (sur la base des critères connus ou fortement suspectés) et à transférer en priorité le trafic inconnu ou suspect à FortiSandbox en vue d'une inspection complémentaire. Avec cette approche collaborative, chaque produit se spécialise dans ce qu'il fait le mieux. Par exemple, la solution de Sandbox n'a pas besoin de consacrer du temps à traiter le trafic et les menaces qui peuvent être d'abord bloqués par d'autres technologies.

De nombreuses technologies propriétaires entrent en action dans la solution Fortinet. Mais une composante cruciale joue un rôle majeur dans la prévention proactive des logiciels malveillants avancés : la technologie brevetée Compact Pattern Recognition Language (CPRL) développée par FortiGuard Labs pour exécuter une inspection approfondie sur les codes. Ce langage est capable d'identifier plus de 50 000 camouflages employés par les codes malveillants connus. Si un code utilise une technique de contournement connue, CPRL peut la détecter et FortiGate peut identifier le code sans l'envoyer dans l'environnement Sandbox. Cette étape précieuse améliore considérablement les performances, car les ressources de Sandbox sont ainsi réservées au traitement du code inconnu. Cette technologie est une composante essentielle de notre solution phare FortiGate ainsi que des offres FortiMail et FortiClient. C'est la raison pour laquelle ces solutions figurent régulièrement en tête des classements établis par des organismes de tests tiers tels que Virus Bulletin, AV Comparatives, etc.

Pour améliorer la détection des menaces les plus sophistiquées, Fortinet a intégré les techniques d'analyse avancées de FortiGuard Labs dans la solution FortiSandbox. Selon le rapport NSS Labs 2014 Breach Detection Systems, le taux de détection des failles est de 99 %, avec une identification de la majorité des brèches de sécurité en moins d'une minute.



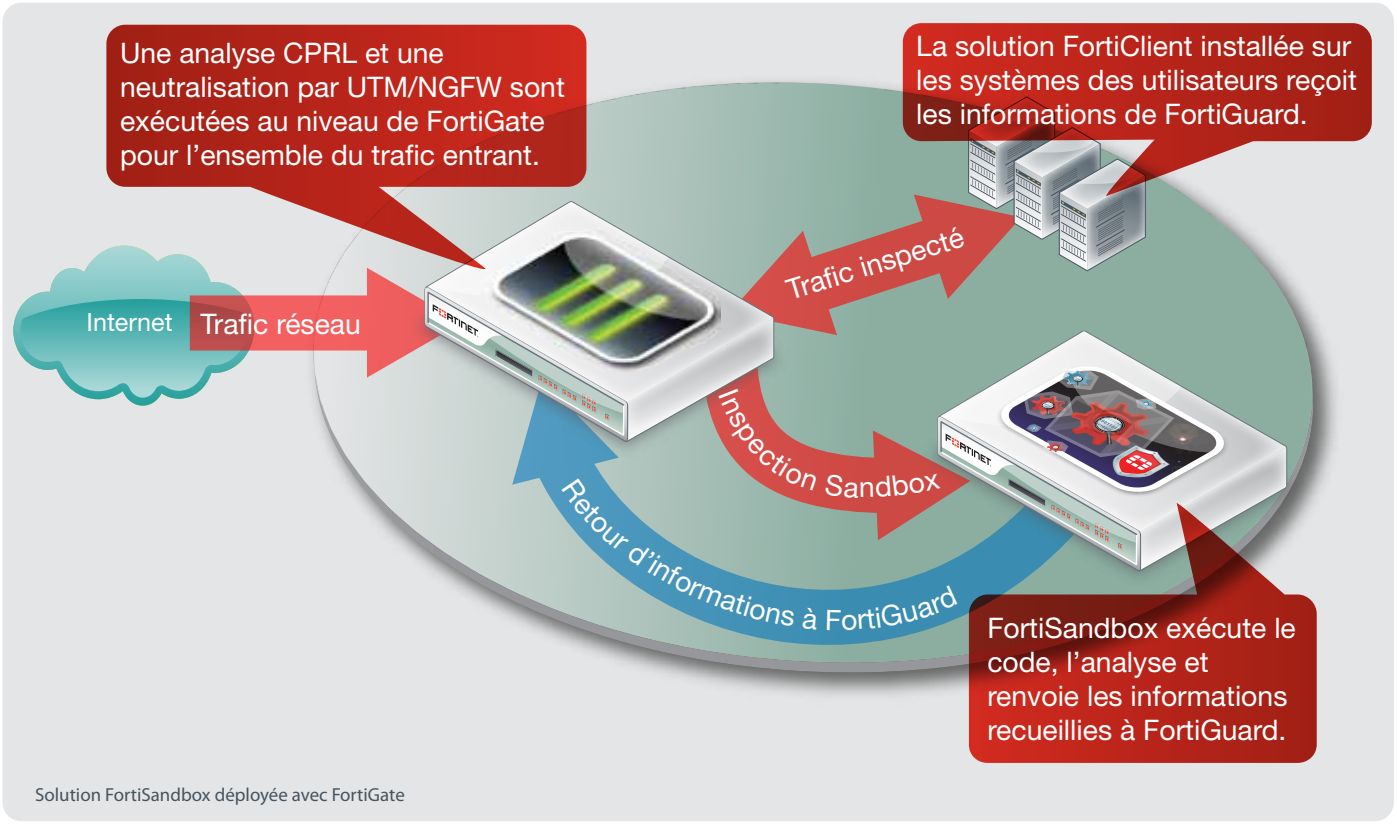
Comment choisir la bonne solution de Sandbox pour votre entreprise ?

Il vous faut une solution de Sandbox qui détecte efficacement et rapidement les failles. Veillez à choisir une solution testée et évaluée par un organisme indépendant. Ne vous fiez pas aux seuls arguments du fournisseur quant à l'efficacité et aux performances.

Vous voulez aussi que votre solution de Sandbox fonctionne en synergie avec vos autres technologies de sécurité réseau. Le but n'est pas de remplacer les technologies antispam, IPS, antivirus, de filtrage Web, d'analyse de réputation IP et de contrôle des applications intégrées dans les Firewalls de Nouvelle Génération, les passerelles de messagerie sécurisées et les plateformes de protection des terminaux. Votre solution de Sandbox doit travailler « main dans la main » avec ces technologies afin de fournir un niveau de protection supplémentaire qui peut être géré dans le cadre d'une défense coordonnée.

Enfin, la technologie Sandbox consomme énormément de ressources et les solutions proposées par les différents fournisseurs varient fortement en termes de coûts. Assurez-vous que votre solution de Sandbox offre le niveau de sécurité dont vous avez besoin pour un rapport qualité-prix correct.

Pour plus d'informations sur la technologie Sandbox de Fortinet, consultez la page http://www.fortinet.com/products/fortisandbox/index.html.



Solution FortiSandbox déployée avec FortiGate

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