SOPHOS
Security made simple.

Sophos Sandstorm

Une protection Next-Gen avancée contre les menaces en toute simplicité

Sophos fait figure de leader dans la lutte contre les malwares avec l'utilisation de technologies de pointe très efficaces telles que l'émulation JavaScript et l'analyse comportementale en temps réel. Bien que la protection antimalware classique demeure essentielle comme première ligne de défense, les entreprises ont besoin d'outils supplémentaires pour lutter contre les ransomwares et les malwares ciblés d'aujourd'hui.

Sophos Sandstorm est une solution de sécurité contre les ransomwares et les menaces persistantes avancées (APT) qui vient compléter la gamme de produits Sophos. Elle détecte, bloque et répond aux menaces avancées non identifiées par les autres solutions de manière rapide et précise, en utilisant notre technologie Next-Gen de sandboxing basée sur le Cloud.

Principaux avantages

- Intégration transparente à votre solution de sécurité Sophos
- Opérationnel en quelques minutes seulement
- Protection contre les ransomwares et les APT, les malwares inconnus et les attaques ciblées
- Intelligence sur les menaces permettant une meilleure prise de décisions
- Rapports granulaires, centrés sur les incidents

Protection avancée contre les attaques ciblées

Maintenez votre réseau à l'abri des ransomwares et des malwares inconnus qui dérobent vos données. Grâce à la technologie puissante next-gen de sandboxing basée sur le Cloud, vous pouvez détecter, bloquer et répondre aux menaces APT et zero day de manière rapide et précise.

Notre mot d'ordre : la simplicité

Sophos Sandstorm s'intègre parfaitement à votre solution de sécurité Sophos. Il suffit de mettre à jour votre abonnement, d'appliquer la politique Sandstorm et vous êtes instantanément protégé contre les attaques ciblées. Vous êtes opérationnel immédiatement.

Bloquer les menaces avancées que les autres ne parviennent pas à détecter

Détectez les ransomwares et les menaces inconnues spécifiquement conçues pour échapper aux appliances de sandboxing de première génération. Notre approche de l'émulation complète du système fournit le plus haut niveau de visibilité sur le comportement des malwares inconnus et de détection des attaques malveillantes que les solutions concurrentes ne parviennent pas à identifier.

Rapports approfondis

Accélérez la réponse aux menaces avancées grâce à l'analyse simple des violations centrées sur les incidents. Nous vous fournissons des informations sur les APT prioritaires en corrélant les preuves et données. Cette approche permet à la fois de réduire les fausses alertes et de vous faire gagner du temps.

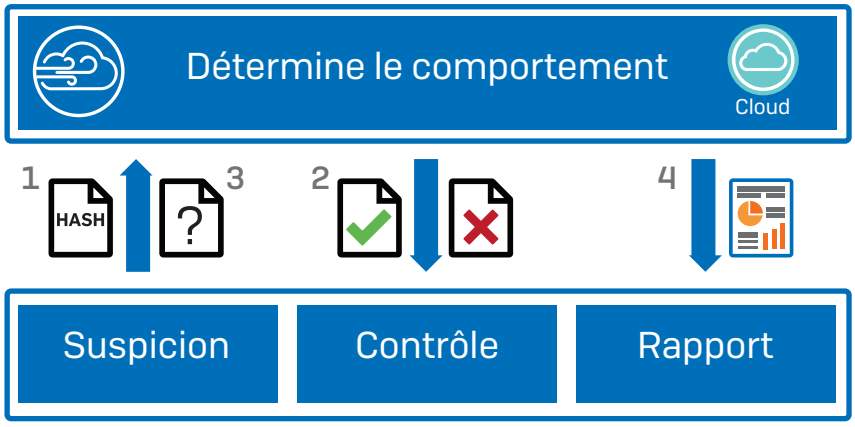
Des performances ultra-rapides

Votre solution de sécurité Sophos pré-filtre le trafic avec une grande précision et soumet seulement les fichiers suspects à Sandstorm, garantissant un minimum de latence et d'impact sur les utilisateurs.

Fonctionnalités de Sophos Sandstorm

- Intégration complète au tableau de bord de votre solution de sécurité Sophos
- Inspecte les fichiers exécutables et les documents contenant du contenu exécutable
  - Exécutables Windows (dont .exe, .com, et .dll).
  - Documents Word (dont .doc, .docx, docm et .rtf).
  - Document PDF
  - Archives contenant des types de fichiers listés ci-dessus (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet).
  - Prend en charge plus de 20 types de fichiers
- Analyse dynamique des comportements des malwares qui exécute les fichiers en environnements réels
- Rapports approfondis sur les fichiers malveillants et possibilité de débloquer un fichier depuis le tableau de bord
  - Durée d'analyse moyenne inférieure à 120 secondes
  - Options flexible de politiques de sécurité pour les utilisateurs et les groupes selon le type de fichier, exclusions et actions selon les résultats des analyses
  - Prend en charge les liens de téléchargement

Fonctionnement



1. La solution de sécurité Sophos analyse les fichiers en fonction de tous les contrôles de sécurité classiques (par exemple, signatures antimalware, URL malveillantes, etc.). Si le fichier est un exécutable ou contient du contenu exécutable et qu'il n'est pas téléchargé depuis un site Web fiable, le fichier est considéré comme étant suspect. La solution de sécurité Sophos envoie le hachage du fichier suspect à Sophos Sandstorm pour déterminer s'il a été analysé précédemment.
2. Si le hachage fichier a été analysé précédemment, Sophos Sandstorm transmet l'intelligence sur la menace à la solution de sécurité Sophos. Ici, le fichier est envoyé à l'appareil de l'utilisateur ou bloqué selon les informations fournies par Sophos Sandstorm.
3. Si le hachage n'a pas été analysé auparavant, une copie du fichier suspect est envoyée à Sophos Sandstorm. Ici, le fichier est neutralisé et son comportement est surveillé. Une fois l'analyse pleinement effectuée, Sophos Sandstorm transmet l'intelligence sur la menace à la solution de sécurité Sophos. Encore une fois, le fichier est délivré à l'appareil de l'utilisateur ou bloqué selon les informations fournies par Sophos Sandstorm.
4. La solution de sécurité Sophos utilise l'intelligence détaillée fournie par Sophos Sandstorm pour créer des rapports approfondis sur chaque incident de menace.

Essai gratuit

Inscrivez-vous pour participer à une évaluation gratuite de 30 jours sur sophos.fr/sandstorm

Équipe commerciale France
Tél. : 01 34 34 80 00
Emaill : info@sophos.fr

Oxford, Royaume-Uni

11/2016 DS-FR (SM)

SOPHOS