STORMSHIELD ENDPOINT SECURITY

LA SEULE SOLUTION FOURNISSANT UNE PROTECTION AVÉRÉE CONTRE LES ATTAQUES CIBLÉES ET LES APT

À PROPOS

Arkoon et Netasq, filiales à 100% d'Airbus Defence and Space CyberSecurity, opèrent la marque Stormshield et proposent tant en France qu'à l'international des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

WWW.STORMSHIELD.EU

Téléphone
09 69 32 96 29

Page de contact email

Reposant sur une technologie unique d'analyse du système, Stormshield Endpoint Security est la seule solution fournissant une protection avérée contre les attaques ciblées et les APT, mêmes inconnues.

Transparente, parfaitement adaptée aux déploiements à grande échelle, Stormshield Endpoint Security intègre en un seul agent tous les services de sécurité requis pour la protection des postes et des serveurs, du contrôle des périphériques au chiffrement des disques.

PROBLÉMATIQUE

Nos entreprises font désormais face à des attaques avancées, en perpétuelle progression, et dont les conséquences peuvent s'avérer dramatiques. Plus que jamais, elles doivent s'adapter à ce contexte et trouver des solutions de protection et de surveillance innovantes. Depuis maintenant 11 ans, la suite Stormshield Endpoint Security permet d'anticiper les menaces en proposant non seulement une suite de modules complète pour la sécurité générale des postes de travail, mais également une technologie exclusive de protection contre l'exploitation des APTs qui a prouvé son efficacité en conditions réelles. Avec 93% des vulnérabilités Windows XP pro-activement bloquées, Stormshield Endpoint Security s'offre les meilleures statistiques vérifiables du marché, tout en conservant un taux de faux-positifs extrêmement faible.

BÉNÉFICES CLIENTS

- La seule technologie anti-APT ayant prouvé son efficacité contre les exploitations de vulnérabilités inconnues.
- Une prise en charge globale de la problématique de la fuite de données au travers des modules Device Control, APT Protection et Encryption.
- Un module Core Defense couvrant tous les besoins de sécurité de base tels que le contrôle applicatif, firewall, HIPS, NIPS, etc.
- Des politiques de sécurité s'adaptant de façon dynamique au contexte du poste.
- Une architecture s'intégrant simplement, des agents faciles à déployer, et une console d'administration centralisée.

COMPOSANTS LOGICIELS

- **Agent**
- **Serveur**
- **Console d'administration**

PRÉ-REQUIS SYSTÈMES

Pour l'agent

- Pentium IV : 3 Ghz
- Mémoire : 512 Mo (minimum), 1 Go (recommandée)
- Espace disque : 250 Mo (90 Mo avec les logs de l'agent)
- Espace disque nécessaire de l'antirivus : 400 Mo
- Systèmes d'exploitation : Windows XP SP3 (32bits), Windows Vista SP2 (32bits), Windows 7 SP1 (32/64bits), Windows Server 2003 (32bits), Windows Server 2008 (32bits), Windows Server 2008 R2 (64bits)

Pour le serveur d'administration

- Processeur cadencé à 1 Ghz minimum
- Mémoire : 1 Go minimum
- Espace disque nécessaire avec l'antivirus : 2 Go minimum
- Systèmes d'exploitation : Windows Server 2003 R2 (32/64bits), Windows Server 2008 SP2 (32bits), Windows Server 2008 R2 (64bits)

APT PROTECTION

- 3ème génération de protection contre les vulnérabilités : différentes couches de détection du produit permettant d'identifier chaque attaque.
- Une implémentation propre au produit de la technologie ASLR sur les anciens systèmes d'exploitation (Windows XP).
- Amélioration de la technologie ASLR pour détecter les techniques malicieuses courantes permettant de déjouer cette protection.
- Contre mesure contre les attaques de type heap spraying qui détournent l'usage de Javascript.
- Contrôle de l'état de la mémoire.
- Analyse fine du code des processus pour identifier les exécutions en mode noyau qui n'étaient pas prévues dans le code de l'application.
- Et bien d'autres encore : honeypot, prévention ret-lib-c, détection pass-the-hash, etc.

DEVICE CONTROL

- Suivi complet des opérations sur tout type de périphérique amovibles.
- Droits d'accès granulaires à des périphériques de stockage amovibles.
- Contrôle des accès en lecture seule et en écriture au niveau du type de fichier.
- Chiffrement des données stockées sur des périphériques amovibles.
- Contrôle Bluetooth, 3G/4G, connectivité wifi, validation protocolaire.
- Validation de l'utilisation du VPN aux points d'accès publics.

CORE DEFENSE

- Protection HIPS : analyse comportementale continue des exécutables, système d'auto-apprentissage pour les applications légitimes, protections contre le keylogging et l'élévation de privilèges, détection de rootkit.
- Firewall avec protection réseau : prévention de l'empoisonnement cache ARP, de l'utilisation illégitime des sessions, de l'usurpation d'identité, etc.
- Contrôle des applications : contrôle de l'installation et de l'exécution des applications, validation de listes blanches d'applications ou des listes noires, protection contre la fermeture des applications, accès aux fichiers de contrôles et aux registres.

ENCRYPTION

- Chiffrement complet du disque transparent.
- Politiques de gestion du chiffrement centralisée et basée sur le fichier/dossier.
- Effacement de fichiers sécurisés et nettoyage de fichiers d'échanges.
- Certification FIPS140-02.

ANTIVIRUS

- Détecte et nettoie tous les types de virus connus.
- Analyse de fichiers en temps réel ou sur demande.
- Analyse les mails avant qu'ils n'atteignent votre boîte de réception.
- Gestion du module en tout transparence par la console de management Stormshield Endpoint Security.

Arkoon Network Security
1 place Verrazzano - CS 30603 69258 - Lyon Cedex 09