

Protection du Poste Client et des Données

Les menaces les plus dangereuses pour la sécurité des entreprises aujourd'hui se situent au niveau des postes de travail, ordinateurs portables et autres périphériques utilisés par les employés sur le terrain, en déplacement et au bureau. Respecter les nouvelles réglementations, déjouer les attaques et protéger l'information sur ces systèmes mal contrôlés sont autant de casse-têtes pour les administrateurs informatiques.

SkyRecon Systems relève le défi avec StormShield Security Suite, sa solution éprouvée et saluée par de nombreuses récompenses internationales. Offrant une protection à 360 degrés, complète et cohérente, ce système modulaire intègre en un agent unique tous les services de sécurité requis sur le poste de travail. StormShield permet ainsi aux organisations de toutes tailles de protéger les postes des collaborateurs contre les attaques connues et inconnues, les intrusions et le vol de données sensibles, sans perturber le travail de l'utilisateur.



Pourquoi les postes de travail sont-ils vulnérables ?

Les postes de travail sont devenus les composants les plus exposés. Ouverts sur l'Internet, souvent utilisés en dehors du périmètre sécurisé de l'entreprise, manipulés par des utilisateurs peu conscients des risques, ils sont aujourd'hui le point de mire principal des attaques externes à l'organisation. Chaque semaine, les médias en témoignent : vols d'ordinateur portable contenant des données confidentielles, attaques par keylogger (enregistreurs de frappe) ayant permis l'accès à des informations sensibles, virus furtif ou attaque par déni de service (DOS) immobilisant une grande entreprise...

Autre fait marquant, des incidents graves de sécurité peuvent être causés par des employés contrariés, des collaborateurs qui installent des applications non autorisées contenant des failles de sécurité, répondent à des messages de hameçonnage, ou téléchargent des contenus illicites. L'utilisateur contribue largement à faire du poste de travail le « maillon faible » de la politique de sécurité de l'entreprise. Pourtant, les administrateurs doivent pouvoir sécuriser et contrôler les postes sans pour autant bloquer ni gêner l'utilisateur dans son activité.

La nécessité d'une protection intégrée au niveau du poste de travail

Aujourd'hui, la quasi-totalité des entreprises est équipée d'un antivirus sur chaque poste. Cependant, une majorité d'entre elles continue à subir des coûts financiers directement induits par des incidents de sécurité sur ces postes. Pourquoi ces entreprises ne sont-elles donc pas protégées ? Des études récentes ont montré que le nombre de systèmes dans le monde infectés par des vers permettant le contrôle à distance (« botnet ») avait

augmenté de 29 %, de 23 % en ce qui concerne les chevaux de Troie et de 54 % en termes de perte d'informations dues au vol d'une clé USB ou d'autres périphériques de stockage.

Ceci s'explique par le caractère borné des solutions de sécurité du poste de travail, qui se limitent à l'antivirus ou au chiffrement par exemple. Ces technologies sont certes efficaces, mais elles ne se limitent qu'au problème qu'elles traitent et laissent ainsi le poste de travail vulnérable à quantité d'autres menaces.

Empiler divers produits de sécurité n'est pas non plus une solution acceptable, pour des raisons de compatibilité, de performance, de coût et de complexité d'administration.

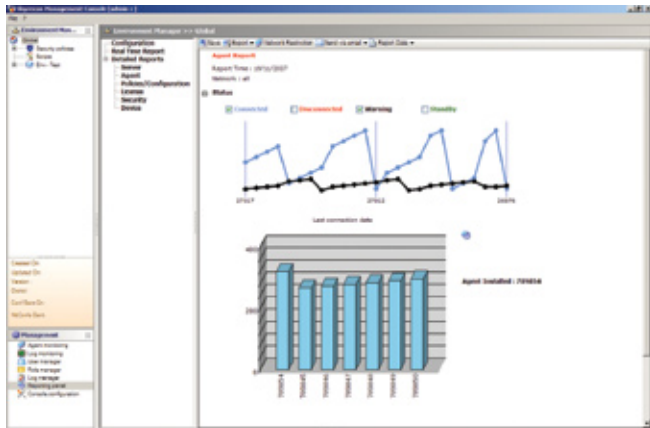
StormShield Security Suite

StormShield restitue aux directions informatiques le contrôle du poste de travail, en permettant aux administrateurs de définir des politiques de sécurité et d'usage des postes de travail, applicables dans l'entreprise comme en situation de mobilité.

Ces politiques peuvent être modifiées dynamiquement en fonction de la connexion au réseau, de l'identité de l'utilisateur et de la configuration de la machine, assurant ainsi une protection adaptée aux risques de sécurité du moment.

Une fois configurées et déployées à partir de la console d'administration centralisée de StormShield, les politiques ne peuvent être désactivées ou modifiées par l'utilisateur, même si ce dernier dispose de droits administrateur.

Combinant une administration simple et centralisée, un contrôle total des applications et une sécurité des données et du système d'exploitation, StormShield permet aux organisations de bénéficier d'une protection efficace, complète et économique de leur parc de PCs.



Rapport de Configuration des Politiques

Caractéristiques et bénéfices

- Solution modulaire de sécurité unique et intégrée qui permet de réduire les coûts et la complexité de l'architecture IT
- Protection complète des postes de travail pour améliorer la sécurité et la conformité aux réglementations
- Evolution des politiques en fonction du contexte et adaptation dynamique aux risques de sécurité
- Sécurité comportementale unique contre les menaces « zero-day » et les attaques inconnues
- Console d'administration permettant de surveiller le statut de l'ensemble des postes en temps réel
- Interopérabilité avec les principales solutions d'infrastructure NAC pour un contrôle d'accès réseau de bout-en-bout

Fonctionnalités

Système de prévention des intrusions (HIPS) et pare-feu

Protection basée sur des règles

- Contrôle d'accès aux applications, types de fichiers, dossiers, panneaux de configuration et clés de registre
- Contrôle des connexions des applications entrantes et sortantes

Analyse comportementale et durcissement du système

- Détecte, signale et bloque les mécanismes d'attaques génériques tels que les débordements de mémoire ou les enregistreurs de frappe
- Apprentissage du comportement des applications autorisées
- Détection et blocage des attaques « zero-day » et des malwares inconnus

Prévention des intrusions sur le réseau

- Vérification de l'intégrité des protocoles
- Détection et blocage des tentatives d'intrusion dans le réseau tels que le scan de ports et les débordements de mémoire

Contrôle d'application

- Contrôle de l'installation et de l'exécution des applications
- Mise en place de listes noires ou listes blanches
- Protection contre l'interruption des applications
- Protection de l'accès aux fichiers

Contrôle d'accès réseau

- Vérification des applications en cours d'exécution, des mises à jour des fichiers de signatures et des correctifs de sécurité
- Application des contrôles d'accès au réseau au niveau du client
- Mise à jour entièrement automatisée
- Interopérabilité avec Juniper UAC, Microsoft NAP, Cisco NAC et de nombreuses solutions VPN

Sécurité des réseaux sans fil

- Contrôle du mode ad hoc et de la connectivité Bluetooth
- Force l'utilisation du VPN dans les points d'accès publics
- Application de protocole de chiffrement et d'authentification
- Liste blanche de points d'accès WiFi autorisés
- Permet de bloquer toute connexion WiFi à l'intérieur ou à l'extérieur de l'entreprise

Contrôle des périphériques externes

- Droits d'accès aux périphériques de stockage amovibles
- Contrôle par type, modèle et numéro de série
- Contrôle des droits de lecture et d'écriture par type de fichier
- Chiffrement des données stockées sur les périphériques amovibles
- Contrôle par type de périphérique USB
- Audit des opérations effectuées sur les périphériques

Chiffrement de contenu

- Chiffrement à la volée des fichiers
- Politiques centralisées de chiffrement par répertoire et par type de fichier
- Seconde authentification optionnelle et intégration avec des systèmes tiers d'authentification forte
- Archives auto-extractibles, chiffrées et protégées par un mot de passe
- Effacement sécurisé des fichiers et nettoyage du swap

Anti-virus

- Détecte et nettoie tous les types de virus
- Protège le PC contre les logiciels espions
- Anti-rootkit: protection contre les menaces furtives

Prérequis système

Agent

Microsoft Windows® 2000 SP4, XP SP1/SP2/SP3, Vista
20 MB d'espace disque disponible

Serveur

Microsoft Windows® Server 2000, 2003, 2008

Console d'administration

Microsoft Windows® 2000, XP