

- Offre une sécurité réseau robuste et proactive
- Assure votre défense contre les menaces nouvelles ou inconnues
- Élimine la fenêtre de vulnérabilité
- Offre une bien meilleure sécurité que les produits basés uniquement sur les signatures



Technologie écologique

L'actif le plus puissant du système de défense de votre réseau

WatchGuard® vous fournit une véritable protection contre les menaces Zero Day grâce aux fonctions de l'architecture Intelligent Layered Security (ILS) de ses appliances de gestion unifiée des menaces Firebox®X, qui bloquent les attaques nouvelles ou inconnues sans avoir besoin de signatures.

Qu'entend-on par attaque « Zero Day » ?

À l'heure actuelle, on parle beaucoup de la protection « Zero Day » dans le domaine de la sécurité informatique. En réalité, tous les fournisseurs n'offrent pas le même degré de protection.

- Les menaces Zero Day sont des attaques nouvelles ou inconnues contre lesquelles il n'existe pas encore de correctif (patch) ou de signature.
- La protection contre les attaques Zero Day vous défend contre les attaques nouvelles ou inconnues avant que leur vulnérabilité ne soit découverte et que l'exploit ne soit créé et lancé.

L'architecture du Firebox®X comprend une vraie protection intégrée Zero Day

L'architecture Intelligent Layered Security du Firebox X combine des fonctions de sécurité capables de défendre votre réseau contre tous les types d'attaques et de le protéger contre leurs variantes avant même qu'elles ne soient connues. Ces fonctions sont notamment:

- **la détection des anomalies du protocole**, qui bloque le trafic malveillant non conforme aux standards du protocole,
- **le filtrage** qui signale et élimine du système les fichiers à haut risque comme les fichiers .exe et script, virus, spywares et chevaux de Troie, en inspectant entièrement le paquet,
- **l'analyse des comportements** qui décèle et bloque le trafic des hôtes ayant un comportement suspect, notamment les attaques de déni de service (DoS) ou déni de service distribué (DDoS) ainsi que les scans de ports ou d'adresses.

Ce qu'apportent les signatures à une solution de sécurité

Certains fournisseurs prétendent assurer une protection Zero Day, mais en réalité leurs solutions de sécurité reposent uniquement sur l'analyse des signatures.

Or les technologies de sécurité fondées sur les signatures prennent l'empreinte de chaque nouvelle attaque après son apparition. Par conséquent, la protection ne se fait que lorsque cette nouvelle empreinte ou signature est ajoutée au système. Il ne s'agit nullement d'une protection Zero Day. Par nature, les signatures sont réactives ; elles ne vous protègent pas contre les attaques nouvelles ou inconnues sans mise à jour.

La recherche de signatures offre une couche de protection granulaire contre les spywares, virus, vers, chevaux de Troie et menaces mixtes, en décelant le code malveillant au sein des fichiers et du trafic essentiels pour l'entreprise. Mais cette technique n'est que l'un des éléments d'une solution complète de gestion unifiée des menaces.

22 des 30 virus les plus importants apparus entre 2003 et 2006, y compris leurs variantes, ont été bloqués par défaut par le Firebox®, protégeant ainsi nos clients avant même que les signatures ne soient disponibles.*

La fenêtre de vulnérabilité

Les solutions reposant sur les signatures bloquent ce qui a déjà été identifié. Mais à partir du moment où un nouvel exploit est lancé, votre réseau reste exposé jusqu'au développement et au déploiement de la signature ou du correctif adéquat.

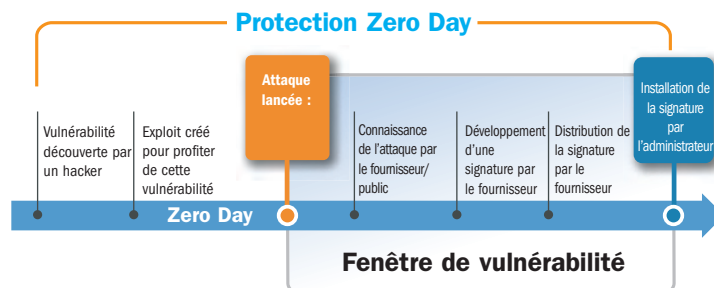
Etant donné la vitesse et le caractère destructif des attaques actuelles, quelques minutes sans protection risquent d'être catastrophiques. Or il peut se passer des heures, des jours et même des semaines avant qu'une signature ou un correctif ne soit développé et déployé, ce qui fait de la fenêtre de vulnérabilité un véritable cauchemar pour les responsables informatiques.

Une protection robuste en amont

Une vraie protection Zero Day déjà en place avant que la vulnérabilité ne soit connue, voilà ce qui est au cœur des solutions de sécurité Firebox X. N'attendez pas pour en profiter : rendez-vous sur www.watchguard.com

*Sulla base dei metodi di propagazione più comunemente utilizzati (SMTP)

WatchGuard vous protège durant la fenêtre de vulnérabilité



La protection Zero Day signifie que vous êtes protégé contre les menaces nouvelles et inconnues durant la fenêtre de vulnérabilité.

WatchGuard™

Stronger Security, Simply Done™

- **Protection multifacette entièrement intégrée**
- **La solution de sécurité la plus complète de sa catégorie**
- **Avec prévention intégrée des attaques Zero Day**
- **Des abonnements de sécurité puissants renforcent la protection dans les zones d'attaque critiques**
- **Fonctions d'administration, de contrôle et de production de journaux unifiées**



Technologie écologique

Une solide sécurité avec une protection Zero Day

Les solutions de gestion unifiée des menaces Firebox®X de WatchGuard vous offrent la sécurité la plus complète de leur catégorie et vous assurent une protection multifacette intégrée des menaces pesant sur votre réseau, notamment :

- ✓ Spywares
- ✓ Virus
- ✓ Injections SQL
- ✓ Chevaux de Troie
- ✓ Spam
- ✓ Débordement de tampon
- ✓ Vers
- ✓ Menaces mixtes
- ✓ Défis de service/Défis de service distribués
- ✓ Bots
- ✓ Exploits sur Internet
- ✓ Violations des règles de sécurité

Qu'est-ce que la gestion unifiée des menaces?

La gestion unifiée des menaces (Unified Threat Management ou UTM) constitue une tendance émergente sur le marché de la sécurité informatique. Les appliances UTM sont passées des pare-feu et réseaux virtuels privés traditionnels à des solutions dotées de nombreuses fonctions supplémentaires, notamment le filtrage des URL, le blocage du spam, la protection contre les spywares, la prévention des intrusions et l'antivirus de passerelle, sans parler des fonctions intégrées de gestion, de contrôle et de création de rapports. Autant de fonctionnalités gérées auparavant par de multiples systèmes.

La protection intégrée Zero Day à la base

Nous avons démarré avec une architecture de sécurité puissante et prête à l'emploi : l'Intelligent Layered Security (ILS) du Firebox X, qui vous offre une réelle protection Zero Day. En effet, elle défend votre réseau contre les attaques nouvelles ou inconnues avant que sa vulnérabilité ne soit découverte et que l'exploit ne soit créé et lancé. La plupart des fournisseurs vous offrent une protection reposant uniquement sur les signatures. Avec ce type de solutions réactives, les clients restent exposés aux nouveaux types de menaces jusqu'à ce que l'exploit soit connu, qu'une signature soit écrite et que la mise à jour de cette signature soit déployée.

De puissantes couches de défense qui travaillent ensemble

Avec l'ILS du Firebox X, les couches de sécurité fonctionnent de concert pour renforcer la sécurité globale de votre réseau, ce qui n'est pas le cas de la plupart des appliances UTM actuellement disponibles sur le marché. Comme les fonctions logicielles sont coordonnées, chaque composant peut participer à la structure de sécurité globale. Ainsi, lorsque le service de prévention des intrusions identifie une attaque, il peut indiquer au pare-feu ce qu'il convient de faire.

La communication entre les couches réduit et affine le traitement requis par les fonctions de sécurité. Le résultat : vous avez la protection nécessaire pour assurer votre sécurité tout en optimisant votre performance.

Des options de sécurité performantes pour booster vos défenses

Nos solutions flexibles vous permettent d'ajouter facilement une ou plusieurs de nos options de sécurité supplémentaires pour renforcer votre protection dans les zones d'attaque critiques et les gérer à l'aide d'une seule console d'administration intégrée.

Ces options sont les suivantes:

- **spamBlocker**: meilleure solution de notre secteur d'activité pour différencier en temps réel les communications légitimes du spam. Il bloque jusqu'à 97% des e-mails indésirables, avec un taux de faux positifs incroyablement faible.
- **Antivirus de passerelle/service de prévention d'intrusion**: protection robuste contre les virus, spywares, chevaux de Troie et exploits sur Internet connus. Cette solution repose sur les signatures au niveau de la passerelle.
- **WebBlocker**: augmente la productivité et diminue les risques pour la sécurité en bloquant l'accès au contenu malveillant sur Internet et en gérant la navigation sur Internet de vos utilisateurs.

Rôle de l'administration intégrée

Que vous soyez novice ou expert en informatique, vous verrez que les fonctions d'administration intégrée, de contrôle interactif en temps réel et de création de rapports de nos solutions UTM vous offrent la convivialité indispensable pour configurer et gérer votre sécurité.

- Administrez de multiples appliances à partir d'un point central
- Créez et mettez rapidement en œuvre des règles de sécurité à l'échelle internationale afin de développer facilement des politiques de sécurité uniformes
- Profitez d'un contrôle interactif en temps réel et de la création de rapports
- Bénéficiez d'une seule interface intuitive pour installer et gérer toutes vos fonctions de sécurité, y compris les abonnements de sécurité

Excellente évolutivité et économie

Le recours à plusieurs appliances de sécurité et logiciels exige un investissement en temps et en argent qui vient augmenter vos coûts. Avec certaines solutions de gestion unifiée des menaces, vous devez régler des licences par utilisateur ou la production centralisée des rapports et des journaux. Avec celles de WatchGuard, vous n'avez ni coût par utilisateur, ni frais pour le logiciel d'administration, mais seulement une interface utilisateur graphique à connaître. Chaque fonction de sécurité intégrée et gérée de façon centralisée assure la protection de votre réseau pour les utilisateurs configurés derrière votre Firebox X.

Rien ne vous limite, si ce n'est votre capacité en termes de trafic. Mais lorsque celle-ci est dépassée, il vous suffit de passer au modèle supérieur par une simple clé logicielle afin de bénéficier d'une capacité et d'un débit plus élevés. Il s'agit du moyen le plus simple et le plus rentable pour protéger votre investissement dans la sécurité réseau.



Stronger Security, Simply Done™

ADRESSE: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 · SITE INTERNET: www.watchguard.com

SERVICE COMMERCIAL AUX ÉTATS-UNIS: 1.800.734.9905 · SERVICE COMMERCIAL INTERNATIONAL: +1.206.613.0895

Ce document ne contient aucune garantie expresse ou tacite. Toutes les spécifications sont susceptibles de changer et tous les futurs produits, fonctionnalités et services attendus seront fournis à partir du moment où ils seront disponibles.

©2007 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard, Firebox, Fireware, LiveSecurity et Stronger Security, Simply Done sont des marques déposées ou non de WatchGuard Technologies, Inc. aux États-Unis et/ou dans d'autres pays. Tous les autres noms de marque et marques appartiennent à leurs propriétaires respectifs. Numéro de référence : WGCE66355_101707