

Total Security de WatchGuard

Protection réseau complète dans une solution unique et facile à déployer

Total Security.

Un pare-feu à filtrage dynamique de paquets, même s'il est crucial, n'est tout simplement plus suffisant. La réalité est là : chaque réseau a besoin d'un arsenal complet de moteurs d'analyse pour se protéger contre les logiciels espions et les virus, les applications malicieuses et la perte de données, en passant par les ransomwares, les botnets, les menaces persistantes avancées et les logiciels malveillants de type zero day. Une solution de sécurité réseau réellement performante pourra couvrir tous les aspects de la prévention, de la détection, de la corrélation des menaces d'aujourd'hui (et de la réponse à y apporter), mais aussi de celles de demain, au fur et à mesure de leur évolution. La plateforme de sécurité réseau primée de WatchGuard propose non seulement la suite la plus complète de contrôles de sécurité unifiée actuellement disponible sur le marché, mais elle a également toujours été la première à offrir des solutions permettant de faire face aux nouvelles menaces réseau et celles en constante évolution, notamment les logiciels malveillants et les ransomwares.

Simplicité totale.

Bien plus que de simples moteurs d'analyse de sécurité. Chez WatchGuard, nous estimons que la simplicité est la clé d'une adoption réussie de nouvelles technologies. Ainsi, tous nos produits sont non seulement faciles à configurer et à déployer initialement, mais ils sont également axés sur la gestion centralisée afin de rationaliser et faciliter la gestion continue des stratégies et des réseaux. La sécurité est certes complexe, mais aucune raison que sa gestion le soit également.

Performance totale.

Toutes les entreprises, quelle que soit leur taille, doivent surveiller la performance. La lenteur des analyses de sécurité peut affecter la capacité d'un réseau à faire face à un volume de trafic élevé. Certaines entreprises sont ainsi forcées de réduire leur niveau de protection afin de maintenir une excellente performance, mais les solutions de WatchGuard ne vous demandent jamais de choisir entre la sécurité et la rapidité. En exploitant la puissance du traitement multinœuds, la plateforme de WatchGuard est conçue pour offrir le débit le plus rapide lorsqu'il est nécessaire, et ce même avec tous les contrôles de sécurité activés. Notre plateforme peut exécuter tous les moteurs d'analyse simultanément, assurant une protection optimale et un débit ultrarapide.

Visibilité totale.

Du comité de direction à un site distant, les décisions critiques relatives à la sécurité doivent souvent être prises très rapidement afin d'éviter tout dommage. Vous devez par ailleurs savoir ce qui se passe non seulement sur votre réseau, mais également au niveau des différents appareils situés à l'intérieur et en dehors du pare-feu. La visibilité englobe bien plus que des données. La visibilité est obtenue lorsque ces données sont converties en des informations appropriées et facilement exploitables. L'ajout de WatchGuard Host Sensor, disponible via le service de sécurité Threat Detection and Response, permet d'assurer la surveillance et la détection continues des événements et de répondre immédiatement aux menaces au niveau des postes de travail. La plateforme de visibilité réseau primée de WatchGuard, Dimension, recueille les données de l'ensemble des dispositifs de votre réseau et les présente sous la forme d'informations exploitables immédiatement. Grâce à Dimension, vous pouvez identifier des tendances comportementales, détecter les menaces réseau potentielles, bloquer les usages inappropriés, surveiller l'état du réseau et bien plus encore.

Sécurité de pointe



Simplicité



Performance optimale



Visibilité des menaces



Future-Proofed Durabilité



Services de sécurité de WatchGuard

WatchGuard propose le portefeuille le plus complet de services de sécurité réseau, des traditionnels IPS, Anti-virus, contrôle d'application, anti-spam, filtrage d'URLaux services plus avancés permettant de vous protéger contre les logiciels malveillants avancés, les ransomwares et la perte de données sensibles. WatchGuard offre également une série complète de services de visibilité réseau et de gestion.

SERVICES DE SÉCURITÉ ESSENTIELS



SERVICE DE PRÉVENTION D'INTRUSIONS (IPS)

IPS utilise constamment des signatures mises à jour pour analyser le trafic sur tous les protocoles majeurs afin de fournir une protection en temps réel contre les menaces réseau, notamment les logiciels espions, les injections SQL, les attaques de script inter sites, et les dépassements de tampon.



SERVICE D'AUTORITÉ DE RÉPUTATION (REPUTATION ENABLED DEFENSE, RED)

Un puissant service de recherche de réputation basé sur le Cloud qui protège les utilisateurs du Web contre les sites malveillants et les botnets, tout en améliorant considérablement le traitement Web en général.



ENDPOINT DISCOVERY

Ce service de découverte réseau par abonnement pour les appli-ances Firebox génère une carte visuelle de tous les nœuds sur votre réseau afin de pouvoir aisément voir où vous pourriez être menacé.



ANTI-VIRUS DE PASSERELLE (GAV)

Utilisez nos signatures constamment mises à jour pour identifier et bloquer les logiciels espions, virus, chevaux de Troie, vers, rogue-ware et menaces combinées connus, y compris les nouvelles variantes de virus connus. Parallèlement, une analyse heuristique identifie les constructions de données et actions suspectes afin de ne laisser passer aucun virus inconnu.



WEBBLOCKER (FILTRAGE D'URL)

Outre le blocage automatique de sites malveillants connus, les outils de filtrage granulaire du contenu et des URL vous permettent de bloquer tout contenu inapproprié, de conserver de la bande passante réseau et d'augmenter la productivité des employés.



CONTRÔLE D'APPLICATION

Autorisez, bloquez ou restreignez l'accès à des applications de façon sélective en fonction du service, de la fonction d'un utilisateur et de l'heure de la journée, puis découvrez en temps réel les personnes qui accèdent à votre réseau et les types d'accès.



SPAMBLOCKER (ANTI-SPAM)

Détection des courriers indésirables en temps réel pour se protéger contre les attaques. Notre spamBlocker (anti-spam) est tellement rapide et efficace qu'il peut analyser jusqu'à 4 milliards de messages par jour.

SERVICES DE SÉCURITÉ AVANCÉS



APT BLOCKER – UNE PROTECTION AVANCÉE POUR LUTTER CONTRE LES LOGICIELS MALVEILLANTS

APT Blocker utilise une « sandbox » (bac à sable) primé de nouvelle génération pour détecter et bloquer les attaques les plus sophistiquées, notamment les ransomwares, attaques zero day et autres malwares avancés.



PRÉVENTION DES PERTES DE DONNÉE (DLP)

Ce service permet d'éviter les fuites de données accidentelles en analysant les fichiers texte et autres types de fichiers courants afin d'y détecter toute fuite d'informations sensibles du réseau.



DIMENSION COMMAND

Dimension traduit les données recueillies depuis toutes les appli-ances sur votre réseau en informations exploitables sur le réseau et sur les menaces. Dimension Command vous permet de réagir afin de réduire ces menaces instantanément, et ce à partir d'une seule et même console centrale.



THREAT DETECTION AND RESPONSE

Assure la corrélation des événements de sécurité du firewall jusqu'aux postes de travail grâce à l'analyse des menaces, afin de détecter et de classer les attaques des logiciels malveillants et ainsi prendre des mesures immédiates pour les bloquer. Améliore la visibilité en faisant évoluer votre modèle de sécurité existant au-delà de la simple prévention pour y ajouter la corrélation, la détection et la réponse.

Une approche unifiée de la sécurité

Les PME et les entreprises multisites continuent d'être les victimes des menaces avancées, lesquelles ont de graves conséquences sur leurs opérations commerciales et sur la continuité de leur activité quels que soient leurs déploiements de sécurité existants. Aucun contrôle de sécurité unique, ou sous-ensemble de contrôles, ne suffit. Plus vous instaurez de niveaux de protection contre une attaque, plus votre défense globale est efficace, même lorsque de nouvelles menaces contournent l'une des protections en place.

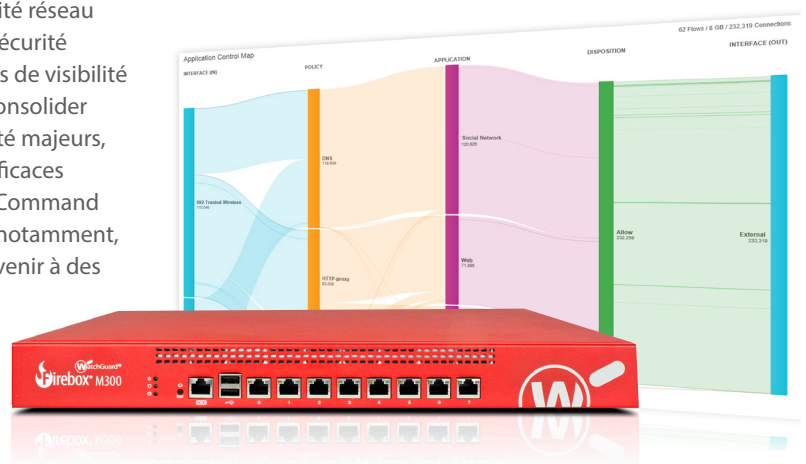
Avec Total Security Suite, les entreprises de toutes tailles peuvent bénéficier de fonctions de prévention, de détection, de corrélation et de réponse avancées, du périmètre jusqu'aux terminaux. ThreatSync, notre moteur Cloud de corrélation et de scoring des menaces, collecte les données d'événement réseau provenant de plusieurs services de sécurité sur la Firebox, y compris APT Blocker, Reputation Enabled Defense, Gateway AntiVirus et WebBlocker. Ces données sont mises en corrélation avec l'activité malveillante détectée via WatchGuard Host Sensor et nos fonctionnalités avancées d'analyse des menaces, afin d'offrir une vue unifiée de votre environnement et d'attribuer une notation complète basée sur le niveau de gravité de la menace.

Mieux encore, tous ces avantages en matière de sécurité sont disponibles dans l'ensemble de notre réseau de partenaires MSSP via une offre unique comprenant une référence, une licence et une appliance.



La puissance de la visibilité

WatchGuard Dimension est une solution de visibilité de la sécurité réseau basée sur le Cloud incluse de série dans chaque plateforme de sécurité réseau de WatchGuard. Elle propose une suite de puissants outils de visibilité et de génération de rapports qui permettent d'identifier et de consolider instantanément les menaces, problèmes et tendances de sécurité majeurs, accélérant ainsi la capacité à définir des stratégies de sécurité efficaces sur l'ensemble du réseau. L'activation de la fonction Dimension Command débloque l'accès à une variété de fonctions de contrôle réseau, notamment, les modifications de configuration en un clic, la possibilité de revenir à des configurations précédentes, l'accès direct à des appliances individuelles par le biais d'une IU Web et des outils de gestion VPN. La connaissance apporte le pouvoir, et la visibilité permet d'acquérir la connaissance.



Passer d'un pare-feu dynamique standard à une plateforme d'analyse complète à 7 couches a été crucial pour nous. Nous sommes parvenus à ajouter IPS/IDS, le filtrage d'application, la détection de malware, l'antivirus de passerelle, le filtrage Web et toutes les autres fonctions de sécurité proposées par WatchGuard. Dans cette appliance unique, nous avons réussi à associer de nombreuses fonctions de sécurité, qui, en tant qu'unités autonomes, ne seraient pas intéressantes d'un point de vue financier.



~ Peter Thomas

Responsable informatique, Roland UK

Une appliance, une offre, Total Security

La simplicité, telle est notre mission chez WatchGuard. Mais cette mission ne se limite pas simplement à la fabrication de nos produits et à l'élaboration de packages associés. Alors que l'ensemble de nos services sont proposés à la carte, nous nous sommes appliqués à élaborer deux packages qui simplifient le processus de prise de décision. Les packages Total Security Suite et Basic Security Suite sont uniquement disponibles avec nos appliances Firebox Série M et T. Les packages Total Security Suite et Basic Security Suite sont uniquement disponibles sur nos appliances Firebox Série M et T, ainsi que nos appliances virtuelles Firebox Cloud et FireboxV.

- La **Basic Security Suite** est composée de l'ensemble des services de sécurité réseau de base d'une appliance UTM : IPS, Anti-virus, filtrage d'URL, contrôle d'application, anti-spam, et vérification de la réputation des sites internet visités. Elle comprend également nos fonctions de management centralisé, de reporting et de visibilité réseau, ainsi que notre service de support standard 24 h/24, 7 j/7.
- La **Total Security Suite** inclut l'ensemble des services proposés avec la Basic Security Suite, ainsi que la protection avancée contre les logiciels malveillants (APT Blocker), la protection contre les fuites de données (DLP), les fonctions de visibilité réseau avancées et la possibilité d'agir face aux menaces directement depuis Dimension, notre plateforme de visibilité réseau. Elle comprend en outre le service de support supérieur Gold, 24 h/24, 7 j/7.

Produit	TOTAL SECURITY SUITE	Basic Security Suite
Pare-feu dynamique	✓	✓
VPN mobile	✓	✓
VPN pour sites distants	✓	✓
Proxies applicatifs	✓	✓
Service de prévention d'intrusions (IPS)	✓	✓
Contrôle d'application	✓	✓
WebBlocker (filtrage d'URL)	✓	✓
spamBlocker (antispam)	✓	✓
Gateway AntiVirus (antivirus de passerelle)	✓	✓
Autorité de réputation (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Prévention des pertes de données (DLP)	✓	
Dimension Command	✓	
Threat Detection & Response	✓	
Support	Gold (24 h/24, 7 j/7)	Standard (24 h/24, 7 j/7)

*Le service de sécurité Threat Detection and Response est fourni avec le bundle WatchGuard Total Security Suite. Le nombre de licences Host Sensor varie en fonction de l'appliance utilisée. Les Host Sensors peuvent également être ajoutés via une option complémentaire.

Guide de démarrage

WatchGuard possède un large réseau de revendeurs et de fournisseurs de services à valeur ajoutée. Pour bien démarrer, rendez-vous sur notre site Web afin de trouver le partenaire idéal pour votre entreprise, ou contactez-nous directement. Nous répondrons à toutes vos questions et vous mettrons en relation avec le partenaire le plus adapté à vos besoins.

- Consultez notre réseau de partenaires : findpartner.watchguard.com
- Contactez un spécialiste de la sécurité WatchGuard : www.watchguard.com/wgrd-sales/emailus
- Plus d'information sur les modes d'achat : www.watchguard.com/totalsecurity

À propos de WatchGuard

WatchGuard a déployé dans le monde entier près d'un million d'appliances de gestion des menaces multifonctions intégrées. Nos boîtiers à la signature rouge sont conçus pour être les appareils de sécurité les plus intelligents, les plus rapides et les plus performants du marché, chaque moteur d'analyse tournant à plein régime. WatchGuard, dont le siège social est situé à Seattle, possède des bureaux aux États-Unis, en Europe, en Asie-Pacifique et en Amérique latine. Visitez le site www.watchguard.com pour plus de renseignements, et consultez notre blog InfoSec, **Secplicity**, pour des informations en temps réel sur les toutes dernières menaces et sur la manière d'y faire face, présentée de manière intelligible et exploitable. Rendez-vous sur le site : www.watchguard.com/secplicity.