

Panda GateDefender Performa

Protection périphérique en temps réel du trafic web et des emails



Des solutions périphériques traditionnelles dépassées face aux défis actuels

Le panorama actuel des menaces

Les menaces d'Internet sont de plus en plus **complexes et variées**, rendant les **protections traditionnelles obsolètes**. L'essor du Web 2.0 (réseaux sociaux, messagerie instantanée, P2P, VoIP, Spotify...) favorise la propagation des nouvelles menaces et affecte la productivité des entreprises.

Cette envolée des communications web entraîne d'autres risques encore. On compte de plus en plus de **fuites d'informations confidentielles** et de transmission de **fichiers infectés** par les entreprises. Il est aussi à craindre que les ordinateurs du réseau soient infectés par des bots, enrôlés dans un réseau de PC zombies et utilisés pour envoyer du spam, commettre des fraudes en ligne ou diffuser des codes malveillants. Dans cette éventualité, l'entreprise s'expose à des risques de poursuites judiciaires et/ou à des retombées désastreuses en termes de relations publiques.

La solution

Panda GateDefender Performa se distingue des solutions périphériques traditionnelles en étant la seule appliance de gestion sécurisée des contenus (SCM) à permettre aux entreprises de mettre en place un **cloud hybride** à la périphérie de leur réseau, fournissant une **protection hautement performante** contre les codes malveillants et le spam provenant d'Internet ainsi qu'un **blocage des activités non productives** ou **potentiellement dangereuses** sur le Web. L'intégration de la technologie cloud améliore considérablement les capacités de protection tout en réduisant la consommation des ressources au minimum. La protection est offerte via une appliance unique, à **configurer et oublier**, qui peut être déployée **en parallèle** en **quelques minutes** seulement.

Autrement dit, les entreprises disposent de toute la flexibilité et du contrôle d'une solution sur site associée à la capacité de détection en temps réel du cloud computing.

Panda GateDefender Performa comprend cinq types de protections :

- **Antimalware** : Protection cloud automatique et en temps réel contre tous les types de codes malveillants.
- **Filtrage de contenu** : Définition et application de règles de sécurité différentes dans l'entreprise.
- **Antispam** : Garde la messagerie à l'abri des courriers indésirables.
- **Contrôle des protocoles Web 2.0 (IM/P2P/VoIP/Spotify)** : Préviend l'utilisation abusive de la bande passante
- **Contrôle des accès web** : Restreint l'accès à des contenus web improductifs.

Panda GateDefender Performa est disponible sous trois modèles d'appliance différents qui couvrent les besoins de sécurité de toutes les entreprises en fonction de leur type de réseau et de leur volume de trafic.

Trafic		SB	9100	9500 Lite	9500 Large
HTTP	Mbps	40	400	550	700
	Connexions simultanées	550	9800	18000	18000
HTTPS	Mbps	17	106	145	180
	Messages/sec	40	220	400	550
SMTP	Connexions simultanées	550	9800	18000	18000
	Connexions simultanées	550	9800	18000	18000

Principaux avantages

- **Protection préventive robuste** : Près de **100% de détection** des menaces d'Internet et du spam.
- **Simplicité de déploiement et d'administration** : Configurez-le et oubliez-le. Se déploie en parallèle en quelques minutes et **s'intègre parfaitement** aux systèmes existants.
- **Augmente la productivité des salariés et du système d'informations** tout en améliorant l'expérience Internet des utilisateurs.
- **Optimisation de l'utilisation de la bande passante** et des ressources.
- **Plus grand contrôle** des administrateurs sur les flux du web et des emails.
- Aide les entreprises à respecter les **obligations et normes de sécurité**.

Principales caractéristiques

- **Technologies de protection préventive** : Intelligence Collective depuis le nuage, moteurs heuristiques et quarantaine, pour une détection optimisée des menaces.
- **Protection complète et supérieure** : Protection contre les codes malveillants et les contenus potentiellement dangereux, antispam et blocage des contenus Web improductifs. Contrôle des protocoles Web 2.0.
- **Détection des PC zombies** : Protège les postes de travail et les serveurs de messagerie contre les botnets.
- **Solution hautement évolutive** : Répartition des charges automatique et haute disponibilité.
- **Règles granulaires par profils**.
Intégration simple avec AD/LDAP.
- **Garantie de transmission du trafic** en cas de défaillance du système.
- **Qualité de Service (QoS)** : Allocation de bande passante, pour une performance optimale du réseau.
- Système de **surveillance en temps réel** et **rapports** intuitifs.



Protection préventive de la périphérie

Près de 100% de détection du spam et des menaces d'Internet entrant et sortant du réseau dès la périphérie, grâce à l'association unique de l'Intelligence Collective, du cloud computing, de moteurs heuristiques et de technologies de dernière génération. Les protocoles les plus utilisés sont analysés en temps réel : **HTTP, HTTPS, FTP, SMTP, POP3, IMAP4 et NNTP**.

Protection complète

Panda GateDefender Performa détecte et bloque tous les types de menaces Internet avant qu'elles n'entrent dans le réseau. Il neutralise, entre autres, les virus, les vers, les chevaux de Troie, les spywares, le phishing, les outils de piratage, les arnaques, les PC zombies et les botnets, le spam, les fraudes en ligne, les exploits...

Détection des PC zombies

En détectant la présence de PC zombies parmi les postes de travail et les serveurs de messagerie, Panda GateDefender Performa évite à l'entreprise que ses systèmes soient exploités par des cyber-criminels dans des botnets et utilisés pour des actions illégales. L'entreprise réduit ainsi les risques de suites judiciaires et protège sa réputation et son image de marque.

Contrôle des accès web

Augmentation de la productivité des salariés en mettant un terme à la navigation improductive sur des sites web sans rapport avec le travail. La nouvelle protection cloud en temps réel garantit un taux de détection maximal.

Contrôle des protocoles Web 2.0

Contrôle l'utilisation des applications et protocoles grands consommateurs de bande passante (P2P / IM / Spotify / VoIP), pour améliorer la productivité des salariés et optimiser l'utilisation de la bande passante.

Amélioration de la gestion des risques

Avec les règles de sécurité granulaires par profils, les administrateurs renforcent la protection et répondent aux obligations et normes de sécurité.

Système de surveillance en temps réel

La console intuitive offre des rapports personnalisables sur chaque module de protection et des informations sur le système d'informations, par exemple quels utilisateurs tentent d'accéder à des sites bloqués par la politique de sécurité. Elle fournit également des rapports de synthèse périodiques et personnalisables.



GateDefender Performa est la solution idéale. La sécurité est maintenant une inquiétude en moins. "

Schalk Gous.
Directeur technique. TOSAS, Afrique du Sud



Grâce au filtrage Web de GateDefender, nous avons réussi à augmenter la productivité de nos salariés. "

Mike Van Fleet.
Administrateur du SI. MatchFrame Video, États-Unis



GateDefender Performa est une solution excellente qui nous fournit toutes les protections dont nous avons besoin. L'apppliance est vraiment très simple à configurer et installer dans le réseau. "

Nicholas Manefeldt.

Responsable du Système d'Informations. EDI Holdings, Afrique du Sud.

Configurer et oublier

L'apppliance fonctionnant en mode pont transparent, il n'est pas nécessaire de rediriger le trafic du réseau. Le boîtier se déploie en parallèle en quelques minutes seulement et s'intègre parfaitement aux systèmes existants (Active Directory / LDAP).

Solution hautement évolutive

La solution s'adapte simplement pour suivre le développement de l'entreprise. Le système intelligent de haute disponibilité et répartition de charges automatique assure un retour sur investissement rapide et un fonctionnement optimisé du réseau.

Flux du trafic garanti

Les modèles pour les grandes entreprises intègrent une option de contournement (by-pass) permettant d'interrompre le filtrage en cas de défaillance du système afin de laisser passer le trafic et assurer ainsi la continuité de l'activité.

Optimisation et priorisation de la bande passante

Avec la fonction QoS (Qualité de Service), les administrateurs peuvent prioriser l'utilisation de la bande passante pour un fonctionnement optimal, orienté business.

Administration centralisée

Tous les modules de protection sont gérés depuis une console web unifiée. La configuration générale est définie en temps réel de façon centralisée, pour une mise en place aisée de la politique de sécurité de l'entreprise.

Alertes et rapports en temps réel

Le système de rapports consolidés en temps réel permet d'identifier les problèmes de sécurité et de trafic, justifiant l'investissement technologique. Les alertes en temps réel garantissent aux administrateurs qu'ils sont informés dès qu'un souci de sécurité se présente.

