GFI Software™
Smartly engineered for greater IT

GFI LanGuard, la solution récompensée adoptée par des entreprises du monde entier.

Partie de la famille de produits **GFI Security**

Gestion des correctifs Analyse des vulnérabilités

Audit du réseau Aperçu de la sécurité du réseau

Il vous permet d'analyser, de détecter, d'évaluer et de corriger les failles de sécurité de votre réseau et des périphériques connectés. Fournit une image complète de votre réseau et aide à maintenir la sécurité avec une gestion minimale.

Allez plus loin et commencez votre évaluation GRATUITE :

gfsfrance.com/languard

Microsoft Partner
Gold Application Development
Silver Midmarket Solution Provider

Gestion des correctifs

GFI LanGuard permet une gestion complète des correctifs de sécurité et autres pour les systèmes d'exploitation Microsoft, Mac OS X, les distributions majeures de Linux et des applications tierces. Il peut également automatiser l'application de correctifs pour tous les principaux navigateurs web.

Il prend en charge de nombreuses applications tierces populaires comme Apple QuickTime®, Adobe® Acrobat®, Adobe® Flash® Player, Adobe® Reader®, Adobe® Shockwave® Player, Mozilla Firefox®, Mozilla Thunderbird®, Java™ Runtime et beaucoup d'autres.

Evaluation des vulnérabilités

Les audits de sécurité vérifient plus de 60 000 évaluations de vulnérabilité grâce à une base de données étendue, de qualité industrielle qui comprend OVAL (plus de 11 500 contrôles) et les normes SANS Top 20.

Une technologie innovante d'agent permet de répartir la charge d'analyse et de remédiation à travers les machines. Particulièrement utile dans les réseaux d'entreprise.

Les analyses de vulnérabilité sont multi-plateformes (Windows, Mac OS, Linux™) et les machines virtuelles sont également prises en charge. En outre, GFI LanGuard peut vérifier les smartphones et les tablettes, les imprimantes, les commutateurs et les routeurs de fabricants tels que HP, Cisco, 3Com, Dell, SonicWALL, Juniper, NETGEAR, Nortel, Alcatel, IBM D-Link et Linksys.

Un indicateur graphique du niveau de menace fournit une évaluation intuitive, pondérée de l'état de vulnérabilité de votre infrastructure. Toute vulnérabilité détectée peut être gérée en choisissant remédier, ignorer, reconnaître et recatégoriser.

Audit du réseau

Une fois que vous avez effectué l'analyse des vulnérabilités et appliqué les correctifs sur vos systèmes, vous pouvez utiliser la fonction d'audit de GFI LanGuard pour tout connaître sur l'état de sécurité de votre réseau.

Les audits peuvent inclure la vérification des périphériques USB connectés, les smartphones et tablettes, les versions et types de logiciels, le nombre de partages ouverts, les ports ouverts, les mots de passe faibles, les utilisateurs ou les groupes qui ne sont plus en usage et l'intégrité des systèmes Linux sur votre réseau.

Tableaux de bord :

A côté de l'interface standard GFI LanGuard, le produit inclut également une interface de reporting qui permet aux administrateurs de vérifier l'état de la sécurité de leur réseau à partir de n'importe quel appareil connecté dans le monde.

Les clients avec de grands réseaux peuvent installer plusieurs instances de GFI LanGuard et une console web qui offre une vue centralisée et des rapports agrégés sur toutes les instances. Cela permet une évolutivité quasiment illimitée. Le logiciel s'intègre également avec Active Directory pour les informations d'identification et d'authentification, et les clients peuvent configurer différents utilisateurs avec différents droits d'utilisation.

GFI LanGuard prend également en charge des rapports détaillés, y compris des rapports techniques, de gestion et de conformité spécifiques aux normes (PCI-DSS, HIPAA, CIPA, SOX, etc.).

Liens rapides :

Systèmes d'exploitation pris en charge : www.gfsfrance.com/languard-supported-os/
Applications prises en charge : www.gfsfrance.com/languard-supported-apps/
Matériel pris en charge : www.gfsfrance.com/languard-supported-devices/

Commencez votre évaluation gratuite sur **gfsfrance.com/languard**

Avantages en un coup d'œil

Gestion des correctifs, évaluation des vulnérabilités et audit de réseau. centralisés

Application automatique des correctifs pour les systèmes d'exploitation Microsoft®, Mac OS® X, Linux® et des applications tierces

Plus de 60 000 évaluations de vulnérabilité effectuées sur l'ensemble des réseaux, y compris les ordinateurs, les smartphones, les tablettes, les imprimantes, les routeurs, les commutateurs et même les environnements virtuels

Aide pour la conformité avec PCI DSS et autres réglementations de sécurité (par ex. HIPAA, CIPA, SOX, GLB/GLBA, PSN CoCo)

Configuration requise

Windows Server 2003, 2008/2008 R2, 2012/2012 R2 et Windows XP (SP 2), Vista, 7, 8, 10

Microsoft .NET Framework 4.5.1

Mac OS X version 10.5 ou ultérieur pour les cibles Apple Mac

Linux est pris en charge pour les systèmes cibles systèmes avec : RedHat Enterprise Linux 5+, CentOS 5+, Ubuntu 10.04+, Debian 6+, OpenSuse 11.2+, SUSE Linux Enterprise 11.2+ et Fedora 19+.

Secure shell (SSH): nécessaire pour les cibles d'analyse UNIX ; inclus par défaut dans toutes les distributions majeures de Linux.

GFI LanGuard est disponible en :

anglais, italien, allemand, japonais, chinois traditionnel et simplifié

GFI Software™
www.gfsfrance.com

Pour une liste complète des bureaux et détails de contact de GFI dans le monde, veuillez visiter : www.gfsfrance.com/contact-us