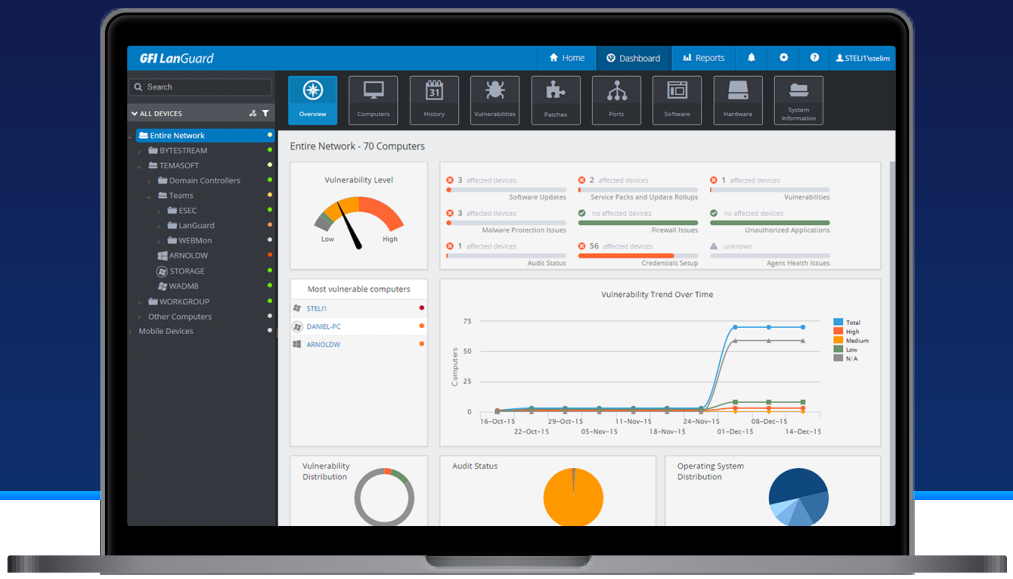
FICHE TECHNIQUE

LanGuard



Éliminez les vulnérabilités liées aux correctifs

La sécurité de votre réseau commence par le fait de connaître tous les éléments qui le composent. GFI LanGuard offre cette visibilité, vous permet d'évaluer où des vulnérabilités potentielles sont susceptibles d'exister et vous donne les moyens de les corriger. GFI LanGuard offre ces puissantes capacités dans une application facile à utiliser et à déployer.

- **Visualisez votre réseau ainsi que les points d'entrée des menaces** — Détectez automatiquement tous les éléments de votre réseau : ordinateurs de bureau et portables, téléphones mobiles, tablettes, imprimantes, serveurs, machines virtuelles, routeurs et commutateurs.
- **Trouvez les lacunes que les menaces exploitent** — Recherchez les correctifs manquants sur votre réseau. Plus de 5 000 correctifs sont publiés chaque année; quiconque peut être la cible de pirates informatiques. Détectez les lacunes dans les systèmes d'exploitation Microsoft, MacOS et Linux. Identifiez les correctifs manquants dans les navigateurs Web et les logiciels tiers tels qu'Adobe, Java et de 60 autres fournisseurs majeurs.
- **Comblez les lacunes qui vous rendent vulnérable** — GFI LanGuard vous permet de déployer des correctifs de manière centralisée et automatique, ou d'installer des agents sur les appareils afin qu'ils le fassent, ce qui permet d'économiser les ressources du serveur. Ne comptez pas sur les personnes pour l'application des correctifs dans votre environnement. Contrôlez les correctifs que vous installez et les correctifs de restauration si vous rencontrez des problèmes. Installez plus que de simples correctifs de sécurité : de nombreux correctifs corrigent les bogues pour aider les applications à mieux fonctionner.
- **Rapport sur les exigences en matière de conformité et de vulnérabilité** — Les réglementations de conformité énoncent de nombreuses exigences pour garantir la sécurité des données financières, de santé ou d'autres données à caractère personnel dans les réseaux et les systèmes. Obtenez des rapports formatés et automatisés dont les auditeurs ont besoin pour démontrer la conformité aux exigences multiples des réglementations PCI DSS, HIPAA, SOX, GLBA, PSN et CoCo.

GFI Software™

Pour obtenir la liste complète des coordonnées dans le monde entier, veuillez consulter le site: www.gfi.com/contact-us

Gestion des correctifs sur plusieurs systèmes d'exploitation

GFI LanGuard est compatible avec les systèmes d'exploitation Microsoft®, Mac OS X® et Linux®, ainsi qu'avec de nombreuses applications tierces comme Apple QuickTime®, Adobe®, Mozilla® Firefox® et bien plus encore. Analysez votre réseau automatiquement ou à la demande. Téléchargez automatiquement les correctifs manquants ou ceux de restauration.

Gestion des correctifs pour plusieurs navigateurs Web

GFI LanGuard est la première solution qui automatise l'application de correctifs pour tous les principaux navigateurs Web fonctionnant sous Windows® : Microsoft Internet Explorer®, Mozilla Firefox®, Google Chrome™, Apple Safari® et Opera™.

Détectez les vulnérabilités avant les pirates informatiques

Le scanner de sécurité réseau GFI LanGuard peut identifier plus de 60 000 vulnérabilités. Il analyse les périphériques, identifie et classe les vulnérabilités de sécurité, recommande des mesures et vous fournit les outils nécessaires pour résoudre le problème. L'indicateur graphique du niveau de menace fournit une évaluation intuitive et pondérée de l'état de vulnérabilité des périphériques analysés.

Fonction de rapports en ligne

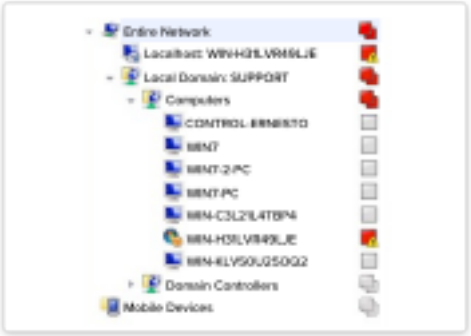
L'interface Web de génération de rapports fonctionne par le biais d'une connexion sécurisée (https) prise en charge par tous les navigateurs de premier plan. Les clients disposant de réseaux de grande ampleur peuvent installer plusieurs instances GFI LanGuard (sites) et une console Web qui fournit une vue centralisée et des rapports agrégés sur toutes les instances.

Prenez connaissance des dernières vulnérabilités et des mises à jour manquantes

GFI LanGuard s'accompagne d'une base de données exhaustive d'évaluation des vulnérabilités incluant des normes telles que OVAL (plus de 11 500 vérifications) et SANS Top 20. Cette base de données est fréquemment mise à jour avec des informations provenant de BugTraq, SANS Corporation, OVAL, CVE et d'autres. Le système d'actualisation automatique la maintient constamment à jour avec les dernières mises à jour de sécurité Microsoft et les vérifications de vulnérabilité.

S'intègre aux applications de sécurité tierces

GFI LanGuard s'intègre à plus de 4 000 applications de sécurité critiques, y compris : antivirus, anti-spyware, pare-feu, anti-phishing, client de sauvegarde, client VPN, filtrage d'URL, gestion des correctifs, navigateur Web, messagerie instantanée, peer-to-peer, chiffrement de disque, prévention des pertes de données et contrôle d'accès aux périphériques. Il fournit des rapports d'état et des listes des applications de messagerie instantanée ou peer-to-peer installées sur votre réseau. Il corrige également tous les problèmes nécessitant une attention particulière, tels que le déclenchement de mises à jour antivirus ou anti-spyware.



Vérifiez les vulnérabilités sur les périphériques en réseau

GFI LanGuard protège vos commutateurs, routeurs, points d'accès et imprimantes contre les attaques. Il prend également en charge l'analyse des vulnérabilités sur les smartphones et tablettes fonctionnant sous Windows®, Android™ et iOS®, ainsi que sur un certain nombre de périphériques réseau tels que les imprimantes, les routeurs et les commutateurs de fabricants tels que HP®, Cisco® et bien d'autres encore.

Sachez ce qui se passe sur votre réseau

L'audit de réseau de GFI LanGuard vous offre une vue complète de votre réseau — y compris les smartphones et tablettes USB connectés, ainsi que les logiciels installés, les partages ouverts, les ports ouverts, les mots de passe pas assez complexes et toute information matérielle. Sécurisez votre réseau en fermant les ports, en supprimant les utilisateurs obsolètes ou en désactivant les points d'accès sans fil.

Audits de sécurité

Le tableau de bord interactif fournit un résumé de l'état actuel de la sécurité du réseau et un historique de toutes ses modifications pertinentes au fil du temps. Parcourez les informations, des capteurs de sécurité à l'échelle du réseau aux résultats d'analyse de sécurité individuels.

Exécutez les modes sans agent ou basés sur un agent

GFI LanGuard peut être configuré pour fonctionner en mode sans agent ou en mode basé sur agent. La technologie d'agent permet d'automatiser les audits de sécurité du réseau et de répartir la charge d'analyse entre les machines clientes.

Essayez gratuitement pendant 30 jours