DATASHEET

GFI LanGuard

Close the door on patch vulnerabilities

Keeping your network safe starts with being aware of all the elements that make it up. GFI LanGuard delivers this visibility, lets you assess where there may be potential vulnerabilities, and gives you the means how to patch them. GFI LanGuard offers these powerful capabilities in an easy-to-use and easy-to-deploy application.

- **See your network and where threats get in**—Automatically discover all the elements of your network: computers, laptops, mobile phones, tablets, printers, servers, virtual machines, routers and switches.
- **Find the gaps that threats exploit**—Scan your network for missing patches. Over 5,000 patches are released every year; any one may be the flaw hackers target. Find the gaps in Microsoft, MacOS, Linux operating systems. Identify missing patches in web browsers and 3rd party software such as Adobe, Java, and 60 more major vendors.
- **Patch the holes that make you vulnerable**—GFI LanGuard lets you deploy patches centrally and automatically, or by deploying agents on machines so they do it and save server processing. Don't depend on individuals to keep your perimeter patched. Control which patches you install and roll-back patches if you find problems. Install more than just security patches: many patches fix bugs to help applications run better.
- **Report on compliance & vulnerability requirements**—Compliance regulations have many requirements to ensure financial, health, or other personal data is secure in networks and systems. Get the automated, formatted reports auditors need to demonstrate compliance for the multiple requirements in PCI DSS, HIPAA, SOX, GLBA, PSN, and CoCo regulations.

GFI™
Aurea SMB Solutions

For a full list of contact details worldwide, please visit: www.gfi.com/contact-us

Patch management across multiple operating systems

GFI LanGuard is compatible with Microsoft®, Mac OS X® and Linux®, operating systems, as well as many third-party applications like Apple QuickTime®, Adobe®, Mozilla® Firefox®, and more. Scan your network automatically or on demand. Auto-download missing patches or roll-back patches.

Patch management for multiple web browsers

GFI LanGuard is the first solution that automates patching for all major web browsers running on Windows® systems: Microsoft Internet Explorer® Mozilla Firefox®, Google Chrome™ Apple Safari® and Opera™.

Detect vulnerabilities before hackers do

GFI LanGuard network security scanner can identify more than 60,000 vulnerabilities. It scans devices, identifies and categorizes security vulnerabilities, recommends a course of action and gives you the tools to solve the problem. The graphic threat level indicator provides an intuitive, weighted assessment of the vulnerability status of scanned devices.

Web-based reporting

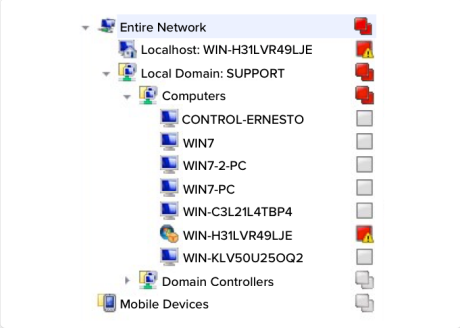
The web-based reporting interface is through a secure (https) connection supported by all major browsers. Customers with large networks can install multiple GFI LanGuard instances (sites) and one web console that provides centralized view and aggregated reporting across all instances.

Track latest vulnerabilities and missing updates

GFI LanGuard ships with a thorough vulnerability assessment database, including standards such as OVAL (11,500+ checks) and SANS Top 20. This database is regularly updated with information from BugTraq, SANS Corporation, OVAL, CVE and others. The auto-update system keeps it continuously up-to- date with newly released Microsoft security updates and vulnerability checks.

Integrates with third-party security apps

GFI LanGuard integrates with more than 4,000 critical security applications, including: antivirus, anti-spyware, firewall, anti-phishing, backup client, VPN client, URL filtering, patch management, web browser, instant messaging, peer-to-peer, disk encryption, data loss prevention and device access control. It provides status reports and lists of instant messaging or peer-to-peer applications installed on your network. It also rectifies any issues that require attention such as triggering antivirus or anti-spyware updates.



Check vulnerabilities on networked devices

GFI LanGuard keeps your switches, routers, access points and printers secure from attack. It also supports vulnerability scanning on smartphones and tablets running Windows®, Android™ and iOS®, plus a number of network devices such as printers, routers and switches from manufacturers like HP®, Cisco® and many more.

Know what's happening on your network

GFI LanGuard's network auditing gives you a comprehensive view of your network – including connected USB devices smartphones and tablets, as well as installed software, open shares, open ports, weak passwords and any hardware information. Secure your network by closing ports, deleting obsolete users or disabling wireless access points.

Security audits

The interactive dashboard provides a summary of the current network security status and a history of all relevant changes in the network over time. Drill down through information, from network-wide security sensors to individual security scan results.

Run agent-less or agent-based modes

GFI LanGuard can be configured to run in agent-less or agent-based mode. Agent technology enables automated network security audits and distributes the scanning load across client machines.

Try free for 30 days

© 2021 GFI Software. All rights reserved. The names of actual companies and products mentioned herein may be trademarked by their respective owners.