The virtual IT security consultant for your business

- Patch management
- Vulnerability scanning
- Network auditing

GFI LanGuard™

Network security scanner and patch management

Benefits at a glance

Centralized patch management, vulnerability assessment and network auditing

Automated patching for Microsoft®, Mac OS® X, Linux® operating systems and third-party applications

Over 50,000 vulnerability assessments carried out across your network, including computers, smartphones, tablets, printers, routers, switches and even virtual environments

Automated options help you to retain a secure network state with minimal administrative effort

Assists with PCI DSS compliance and other security regulations (e.g., HIPAA, SOX, GLB/GLBA, PSN CoCo)

For a full list of GFI LanGuard benefits visit: www.gfi.com/languard

GFI LanGuard allows you to scan, detect, assess and rectify security vulnerabilities in your network and secure it with minimal administrative effort. It gives you a complete picture of your network setup, which helps you maintain a secure network faster and more effectively.

GFI LanGuard is an award-winning solution trusted by customers worldwide to deliver comprehensive network security to millions of computers in their businesses.

Patch management

GFI LanGuard manages patch deployment for both security and non-security patches to Microsoft, Mac OS X and Linux® operating systems, Microsoft applications and third-party applications – in all supported languages. It also allows auto-download of missing patches as well as patch rollback.

Custom software and scripts can be deployed, giving full flexibility to achieve a consistently configured environment that is secure against vulnerabilities.

Many popular third-party applications are supported, such as Apple QuickTime®, Adobe® Acrobat®, Adobe® Flash® Player, Adobe® Reader®, Shockwave® Player, Mozilla Firefox®, Mozilla Thunderbird®, Java™ Runtime and others.

GFI LanGuard also automates patching for all major web browsers running on Windows® systems, including Microsoft Internet Explorer®, Mozilla Firefox®, Google Chrome™, Apple Safari® and Opera™ Browser.

Please visit:
http://kb.gfi.com/articles/SkyNet_Article/KBID003469 for a full list.

Vulnerability assessment

During security audits, over 50,000 vulnerability assessments are made, using an extensive, industrial strength vulnerabilities database incorporating OVAL (8,000+ checks) and SANS Top 20 standards.

The use of agent technology allows the scanning load to be distributed across machines, and with relay agent technology the remediation load may also be distributed. This is particularly useful in multi-site and large networks.

Vulnerability scans are multi-platform (Windows, Mac OS, Linux™) and virtual machines are also supported. GFI LanGuard can also scan smart phones and tablets running iOS®, Android® and Windows Phone®, as well as other devices such as printers, switches and routers from manufacturers such as HP and Cisco® can also be scanned.

Full flexibility is offered with the ability to set up custom vulnerability checks through wizard-assisted screens, to define custom groupings of computers and to create different types of scans and tests with ease.

A graphical threat level indicator provides an intuitive, weighted assessment of the vulnerability status of a scanned computer, or group of computers, or the entire network. Any detected vulnerabilities can be managed by choosing from remediate, ignore, acknowledge and re-categorize as appropriate.

Network auditing

Once you have scanned for vulnerabilities and patched your systems, you can use the GFI LanGuard auditing function to learn everything about your network's security status, including what USB devices, smartphones and tablets are connected; what software has been installed – both authorized and unauthorized; the number of open shares, open ports, weak passwords in use; users or groups no longer in use; and the security health status of Linux systems on your network.

Other features:

Powerful dashboard that processes security audits to provide a summary of network security status.
Integration with over 2,500 critical security applications ensuring latest updates and latest definitions are in place.
Extensive reporting, including technical, managerial and compliance standard-specific reports (PCI-DSS, HIPAA, SOX, etc.)
Wake-on-LAN support – powering computers on before, and off after, scanning – saving energy and maximizing convenience.

"GFI LanGuard proved to be the solution that the National Theatre was looking for in terms of cost, efficiency and effectiveness."

Richard Bevan, National Theatre

System requirements

Windows XP (SP2), Windows Server 2003, Windows Vista, Windows Server 2008/2008 R2, Windows 7, Windows 8 and Windows Server 2012

Microsoft .NET Framework 3.5

Mac OS X version10.5 or greater required for Apple Mac-based targets

Linux patching is supported for target systems having: RedHat Enterprise Linux 5 and later, CentOS 5 and later, Ubuntu 10.04 and later, Debian 6 and later, OpenSuse 11.2 and later, SUSE Linux Enterprise 11.2 and later

Secure shell (SSH) – required for UNIX-based scan targets; this is included by default in all major Linux OS distributions.

GFI LanGuard is available in the following languages:

English, Italian, German

GFI 5042 aug13

www.gfi.com

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

Microsoft Partner
Gold Application Development
Silver Devices and Deployment
Silver Midmarket Solution Provider