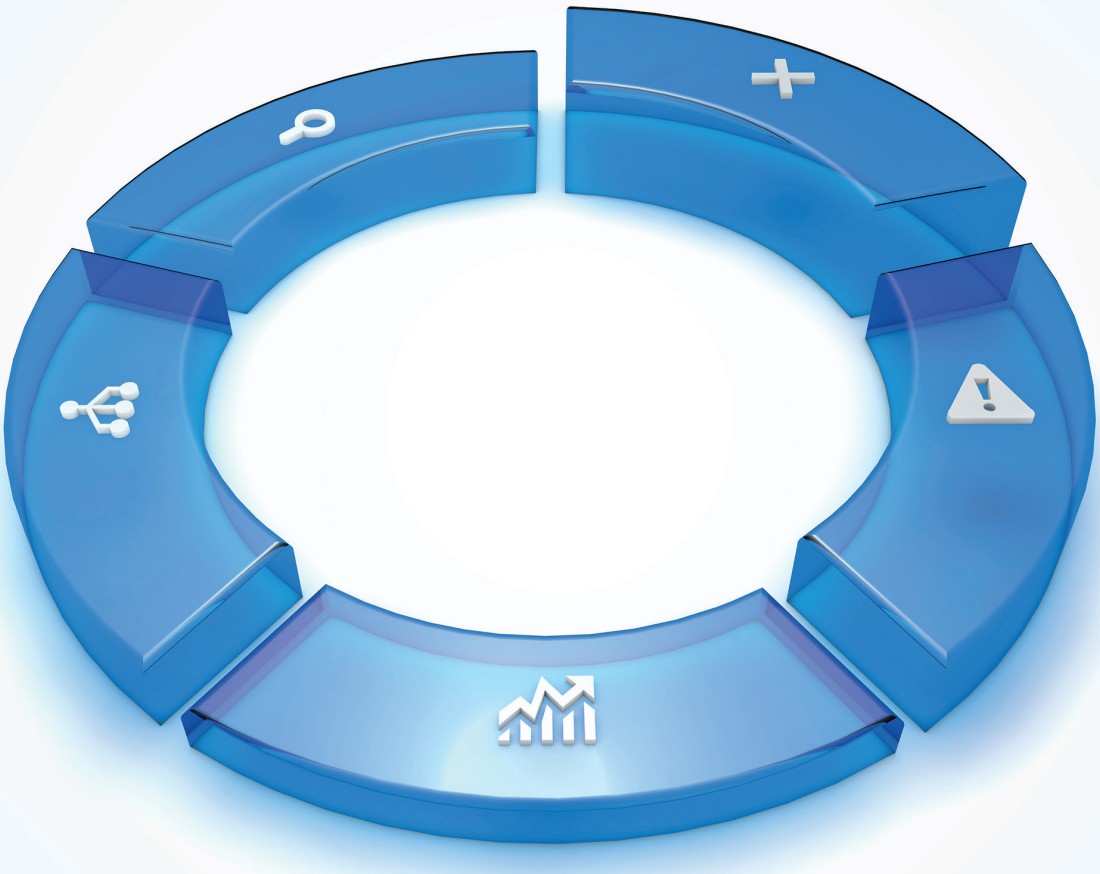
Your virtual IT security consultant



Patch management
Vulnerability scanning
Compliance reporting
Network auditing
Network security insights

Find out more and start your FREE trial:

gfi.com/languard

Microsoft Partner
Gold Application Development
Silver Midmarket Solution Provider

GFI LanGuard™
Network security scanner and patch management

GFI LanGuard is an award-winning solution trusted by businesses worldwide. Allowing you to scan, detect, assess and rectify security vulnerabilities in your network and connected devices. It provides a complete picture of your network and helps maintain security with minimal effort.

Patch management

GFI LanGuard enables complete patch management of security and non-security patches to Microsoft operating systems, Mac OS X, major Linux distributions and third-party applications. It can also automate patching for all major web browsers too.

It supports many popular third-party applications such as Apple QuickTime®, Adobe® Acrobat®, Adobe® Flash® Player, Adobe® Reader®, Shockwave® Player, Mozilla Firefox®, Mozilla Thunderbird®, Java™ Runtime and many more.

Vulnerability assessment

Security audits check for over 60,000 vulnerability assessments using an extensive, industrial strength vulnerabilities database incorporating OVAL (11,500+ checks) and SANS Top 20 standards.

Innovative agent technology allows the scanning and remediation load to be distributed across machines. Particularly useful in enterprise networks.

Vulnerability scans are multi-platform (Windows, Mac OS, Linux™) and virtual machines are also supported. Additionally, GFI LanGuard can audit smart phones and tablets, printers, switches and routers from manufacturers such as HP, Cisco®, 3Com, Dell, SonicWALL, Juniper, NETGEAR, Nortel, Alcatel, IBM D-Link and Linksys.

A graphical threat level indicator provides an intuitive, weighted assessment of the vulnerability status of your infrastructure. Any detected vulnerabilities can be managed by selecting to remediate, ignore, acknowledge or 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.

Audits can include checking for connected USB devices, smartphones and tablets, software types and versions, the number of open shares, open ports, weak passwords, users or groups no longer in use and the security health status of Linux systems on your network.

Other features:

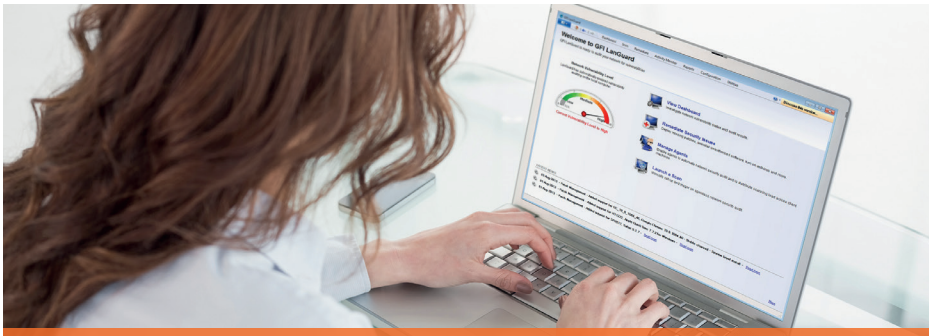
GFI LanGuard has a powerful dashboard that provides a complete summary of network security status. Integration with over 4,000+ critical security applications ensures the latest updates and definitions are in always place.

GFI LanGuard also supports extensive reporting, including technical, managerial and compliance standard-specific reports (PCI-DSS, HIPAA, CIPA, SOX, etc.).

Wake-on-LAN support is also standard. GFI LanGuard can power devices on and off before and after scanning – saving energy and maximizing convenience.

Quick links:

Supported Operating systems: www.gfi.com/languard-supported-os/
Supported Applications: www.gfi.com/languard-supported-apps/
Supported Hardware: www.gfi.com/languard-supported-devices/



Start your free trial at **gfi.com/languard**

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 60,000 vulnerability assessments carried out across networks, including computers, smartphones, tablets, printers, routers, switches and virtual environments

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

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

System requirements

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

Microsoft .NET Framework 3.5

Mac OS X version 10.5 or greater required for Apple Mac-based targets

Linux patching is supported for target systems having: RedHat Enterprise Linux 5+, CentOS 5+, Ubuntu 10.04+, Debian 6+, OpenSuse 11.2+, SUSE Linux Enterprise 11.2+ and Fedora 19+.

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:

English, Italian, German, Japanese, Traditional and Simplified Chinese

GFI®
www.gfi.com

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