GFI LanGuard® grants you three wishes:

» Patch management
» Vulnerability assessment
» Network auditing

Secure your network
Help prove **compliance**
Increase **productivity**

GFI LanGuard is your virtual security consultant

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 and so maintains a secure network state 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.

BENEFITS

- Comprehensive network security
- Automated patching for Microsoft®, Mac OS® X operating systems and third-party applications
- Over 50,000 vulnerability assessments carried out across your network, including computers, printers, routers, switches and even virtual environments
- Network-wide deployment of custom software and scripts
- Automated options help you to retain a secure network state with minimal administrative effort
- Minimizes disruption and downtime of computers on your network
- Assists with PCI DSS compliance and other security regulations (e.g., HIPAA, SOX, GLB/GLBA, GCSx CoCo)
- Reduced total cost of ownership (TCO) with incredibly competitive pricing
- Centralized patch management, vulnerability assessment and network auditing.

GFI LanGuard™

Network security scanner and patch management

Patch management

GFI LanGuard manages patch deployment for both security and non-security patches to Microsoft and Mac OS X 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://kbase.gfi.com/showarticle.asp?id=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 (5,000+ 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.

Scans are multi-platform (Windows, Mac OS, Linux™) and virtual machines are also supported. As well as computers on the network, 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 and other portable devices (including iPhone®, iPad® and Android™ phones) 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:

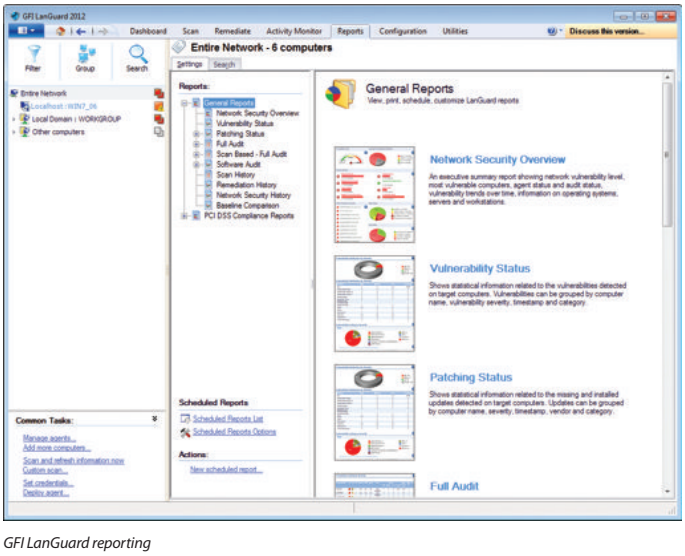
- Powerful dashboard that processes security audits to provide a summary of network security status
- Integration with over 2,500 critical security applications ensuring latest updates and latest definitions are in place
- Extensive reporting, including technical, managerial and compliance standard-specific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

System requirements

- Windows XP (SP2), 2003, Vista, 2008, 7/2008 R2 operating system – and Windows 8 (beta)
- Microsoft .NET Framework 3.5
- Mac OS X version10.5 or greater required for Apple Mac-based targets
- Secure shell (SSH) – required for UNIX-based scan targets; this is included by default in all major Linux OS distributions.

Software available in the following languages

GFI LanGuard dashboard



GFI LanGuard reporting

Download your free trial from http://www.gfi.com/languard

Microsoft Partner
Gold Independent Software Vendor (ISV)

GFI LanGuard™
Network security scanner and patch management

Contact us

Malta
Tel: +356 2205 2000
Fax: +356 2138 2419
sales@gfi.com

UK
Tel: + 44 (0)870 770 5370
Fax: + 44 (0)870 770 5377
sales@gfi.co.uk

USA
Tel: +1 (888) 243-4329
Fax: +1 (919) 379-3402
ussales@gfi.com

Asia Pacific - South Australia
Tel: +61 8 8273 3000
Fax: +61 8 8273 3099
sales@gfiap.com

For more GFI offices please visit http://www.gfi.com/company/contact.html

GFI
www.gfi.com