GFiLANguard

Network vulnerability and port scanner, patch management and network auditing

Network security scanner, port scanner and patch management

GFI LANguard is an award-winning network and security scanner used by over 20,000 customers that allows you to scan your network and ports to detect, assess and rectify security vulnerabilities with minimal administrative effort. As an administrator, you have to deal separately with problems related to vulnerability issues, patch management and network auditing, at times using multiple products. However, with GFI LANguard these three pillars of vulnerability management are addressed in one package, allowing you to have a complete picture of your network set-up and maintain a secure network state faster and more effectively.

GFI LANguard performs network scans using vulnerability check databases based on OVAL and SANS Top 20, providing over 15,000 vulnerability assessments when your network, including virtual environments, is scanned. GFI LANguard allows you to analyze your network security state and take action to secure the network before it is compromised.

When a network scan is complete, GFI LANguard's patch management capabilities give you all the functionality and tools you need to effectively deploy and manage patches on all machines across different Microsoft operating systems and products in 38 languages. Apart from automatically downloading missing Microsoft security updates, you can also automatically deploy the missing Microsoft patches or service-packs throughout your network at the end of scheduled scans.

GFI LANguard's network auditing function tells you all you need know about your network by retrieving hardware information on memory, processors, display adapters, storage devices, motherboard details, printers, and ports in use. Using baseline comparisons you can check whether any hardware was added/removed since last scan. GFI LANguard can also identify and report on unauthorized software installations and provide alerts or else automatically uninstall these unauthorized applications whenever they are detected on the network.

Benefits

Why use GFI LANguard?

- Powerful network, security and port scanner with network auditing capabilities
- Over 15,000 vulnerability assessments carried out across your network, including virtual environment
- Reduces the total cost of ownership by centralizing vulnerability scanning, patch management and network auditing
- Automated options help to retain a secure network state with minimal administrative effort
- Network-wide auditing functions provides a complete picture of network and port security set-up
- • #1 Windows commercial security scanner (voted by Nmap users for two years running) and Best of TechEd 2007 (security).

Integrated vulnerability management solution

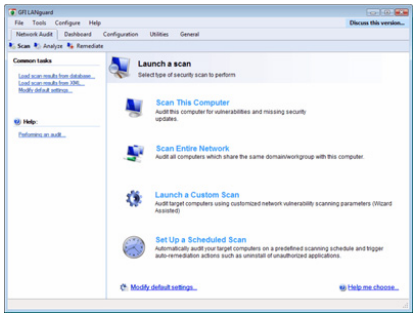
GFI LANguard is an award-winning solution that addresses the three pillars of vulnerability management: security scanning, patch management and network auditing through a single, integrated console. By scanning the entire network, it identifies all possible security issues and using its extensive reporting functionality provides you with the tools you need to detect, assess, report and rectify any threats.

- Vulnerability scanning
- Patch management and remediation
- Network and software auditing.

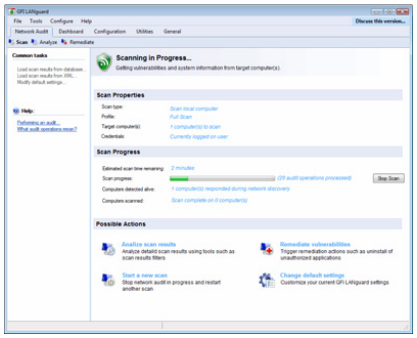
Vulnerability scanning

During security audits, over 15,000 vulnerability assessments are made and networks are scanned IP by IP. GFI LANguard gives you the capability to perform multi-platform scans (Windows, Mac OS, Linux) across all environments including Virtual Machines and to analyze your network's security set-up and status. This ensures that you are able to identify and rectify any threats before hackers manage to do so.

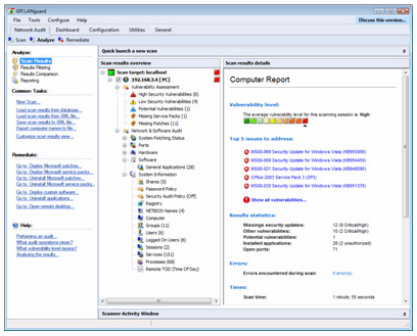
GFI LANguard



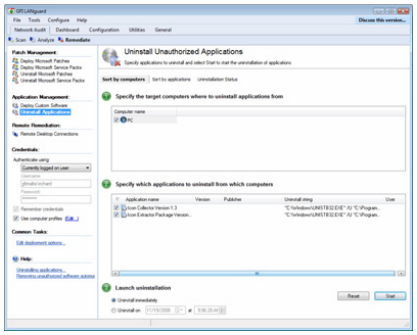
Launch a new scan



GFI LANguard full scan in progress

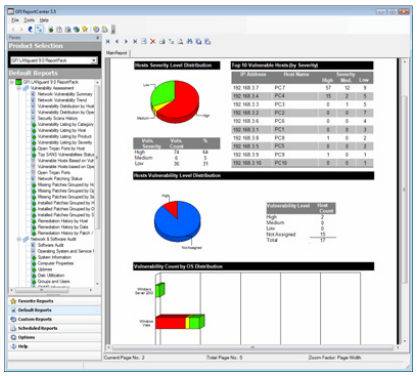


GFI LANguard scan results



Uninstall unauthorized applications

GFI LANguard ReportPack



Executive report showing network vulnerability summary

Detection of Virtual Machines

GFI LANguard can now detect whether a scanned machine is rear or virtual. Currently both VMware and Virtual PC software are supported.

set-up your own custom vulnerability checks

GFI LANguard allows you to easily create custom vulnerability checks through simple wizard-assisted set-up screens. The wizard is also powerful enough to allow building of complex vulnerability checks. The scripting engine is also compatible with Python and VBScript. GFI LANguard includes a script editor and debugger to help with script development.

Extensive, industrial-strength vulnerabilities database

GFI LANguard ships with a complete and thorough vulnerability assessment database, which includes standards such as OVAL (2,000+ checks) and SANS Top 20. This database is regularly updated with information from BugTraq, SANS Corporation, OVAL, CVE and others. Through its auto-update system, GFI LANguard is always kept updated with information about newly released Microsoft security updates as well as new vulnerability checks issued by GFI and other community-based information repositories such as the OVAL database.

Identify security vulnerabilities and take remedial action

GFI LANguard scans computers, identifies and categorizes security vulnerabilities, recommends a course of action and provides tools that enable you to solve these issues. GFI LANguard also makes use of a graphical threat level indicator that provides an intuitive, weighted assessment of the vulnerability status of a scanned computer or group of computers. Wherever possible a web link or more information on a particular security issue is provided, such as a BugTraq ID or a Microsoft Knowledge Base article ID.

Ensures that third party security applications such as anti-virus and anti-spyware offer optimum protection

GFI LANguard also checks that supported security applications such as anti-virus and anti-spyware software are updated with the latest definition files and are functioning correctly. For example, you can ensure that supported security applications have all key features (such as real-time scanning) enabled.

Easily creates different types of scans and vulnerability tests

You can easily configure scans for different types of information; such as open shares on workstations, security audit/password policies and machines missing a particular patch or service pack. You can scan for different types of vulnerabilities to identify potential security issues. These include:

- **Open ports:** GFI LANguard scans for unnecessary open ports and checks that no port hijacking is in force.
- **Unused local users and groups:** Remove or disable User accounts no longer in use.
- **Blacklisted applications:** Identify unauthorized or dangerous software and add to blacklists of applications you want to associate with a high security vulnerability alert.
- **Dangerous USB devices, wireless nodes and links:** Scans all devices connected to USB or wireless links and alerts you of any suspicious activity.
- And much more!

Easily analyze and filter scan results

GFI LANguard enables you to easily analyze and filter scan results by clicking on one of the default filter nodes. This enables you to identify, for example, machines with high security vulnerabilities or machines that are missing a particular service pack. Custom filters can also very easily be created from scratch or customized. You can also export scan results data to XML.

Patch management and remediation

When a scan is complete, GFI LANguard gives you all the functionality and tools you need to effectively install and manage patches on all machines across different Microsoft operating systems and products in 38 languages. Click here to view a full list. GFI LANguard also allows auto-downloads of missing patches as well as patch roll-back. Custom software can also be deployed. This results in a consistently configured environment that is secure against all vulnerabilities.

Automatically deploy network-wide patch and service pack management

With GFI LANguard you can easily deploy missing service packs and patches network-wide. GFI LANguard is the ideal tool to monitor that Microsoft WSUS is doing its job properly and it performs tasks WSUS does not such as deploying Microsoft Office and custom software patches. GFI LANguard also provides you with new features such as patch auto-download and patch rollback. It is also Unicode compliant and able to support patch management in all the 38 languages currently supported by Microsoft. The network administrator also has the option to either to manually approve each patch or set all Microsoft updates as approved. If patches are approved manually the network administrator can choose to receive email notifications when new Microsoft updates are available.

Automatic remediation of unauthorized applications

Remediation operations can be triggered automatically at the end of scheduled scans. Apart from reporting on all installed applications, GFI LANguard 9 allows the user to define which applications are authorized or not authorized to be installed on the network. This list of applications can be easily defined for each scanning profile using the Applications Inventory Tool. During a scan, any unauthorized applications are identified and (optionally) uninstalled automatically by GFI LANguard. An integrated Auto-Uninstall Validation tool is provided to help identify which of the detected applications support silent uninstall and can thus be safely and automatically uninstalled.

Network and software auditing

GFI LANguard's auditing function tells you all you need know about your network – what USB devices are connected, what software is installed, any open shares, open ports and weak passwords in use and hardware information. The solution's in-depth reports gives you an important and real-time snapshot of your network's status. Scan results can be easily analyzed using filters and reports, enabling you to proactively secure the network by closing ports, deleting users or groups no longer in use or disabling wireless access points.

Extended Hardware auditing facility

GFI LANguard can now show detailed information about the hardware configuration of all the scanned machines on your network. All devices from the "Device Manager" tool from windows operating systems are retrieved including motherboard, processors, memory, storage devices, display adapters, and much more. Using baseline comparisons you can now check whether any hardware was added/removed since last scan.

System requirements

- Windows 2000 (SP4), XP (SP2), 2003, VISTA operating system
- Internet Explorer 5.1 or higher
- Client for Microsoft Networks component – included by default in Windows 95 or higher
- Secure Shell (SSH) – this is included by default in every Linux OS distribution pack.

Awards

Download your evaluation version from http://www.gfi.com/lannetscan/

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 2205 2000
Fax +356 2138 2419
sales@gfi.com

Microsoft GOLD CERTIFIED Partner

www.gfi.com