



GFI LANguard

Network Security Scanner

Network vulnerability scanning, patch management and auditing

GFI LANguard Network Security Scanner (N.S.S.) is an award-winning solution that allows you to scan, detect, assess and rectify any security vulnerabilities on your network. As an administrator, you often have to deal separately with problems related to vulnerability issues, patch management and network auditing, at times using multiple products. However, with GFI LANguard N.S.S., these three pillars of vulnerability management are addressed in one package. Using a single console with extensive reporting functionality, GFI LANguard N.S.S.'s integrated solution helps you address these issues faster and more effectively.

GFI LANguard N.S.S. makes use of state of the art vulnerability check databases based on OVAL and SANS Top 20, providing over 15,000 vulnerability assessments when your network is scanned. GFI LANguard N.S.S. gives you the information and tools you need to perform multi-platform scans across all environments, to analyze your network's security health and effectively install and manage patches on all machines across different operating systems and in different languages. This results in a consistently configured environment that is secure against all vulnerabilities.

Voted the best commercial network security scanner by users of Nmap for two years running, named the winner in the Patch Management category in TechTarget's 2006 'Products of the Year' awards, and voted the winner in the security category of the Best of TechEd Awards 2007, GFI LANguard N.S.S. is the most complete vulnerability management solution in one convenient integrated package. GFI LANguard N.S.S. is an essential, cost-effective solution for businesses to safeguard their systems and networks from hacker attacks and security breaches.

Benefits

Why use GFI LANguard N.S.S.?

- Over 15,000 vulnerability assessments carried out across your network
- Reduces the total cost of ownership by centralizing vulnerability scanning, patch management and network auditing
- Provides customizable reports of scans performed across the whole network including applications and resources
- Helps IT administrators secure their networks faster and more effectively
- Prevents downtime and business losses due to vulnerability exposure
- #1 Windows commercial security scanner (voted by Nmap users for two years running) and Best of TechEd 2007 (security).

■ Integrated vulnerability management solution

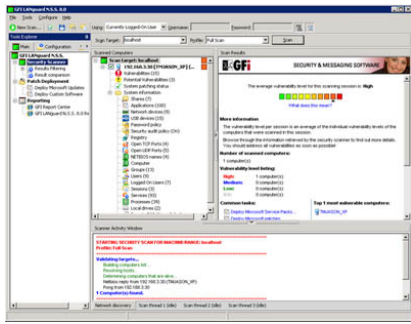
GFI LANguard Network Security Scanner (N.S.S.) is an award-winning solution that addresses the three pillars of vulnerability management: security scanning, patch management and network auditing through a single, integrated console. By scanning the entire network, it identifies all possible security 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
- Network and software auditing.

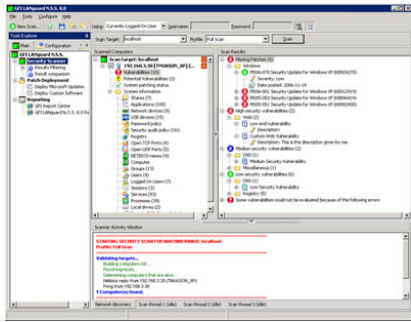
Vulnerability scanning

During security audits, over 15,000 vulnerability assessments are made and networks are scanned IP by IP. GFI LANguard N.S.S. gives you the capability to perform multi-platform scans (Windows, Mac OS, Linux) across all environments and to analyze your network's security health from a single source of data. This ensures that you are able to identify and rectify any threats before hackers manage to do so.

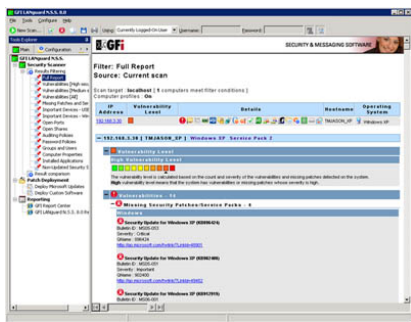
GFI LANguard Network Security Scanner



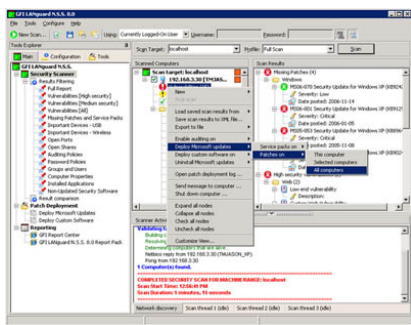
GFI LANguard Network Security Scanner main screen



Indicates vulnerabilities found

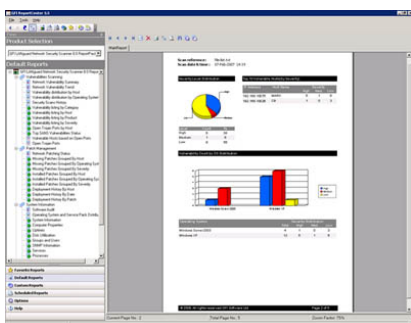


Extensive HTML security reports



Easily deploy patches network-wide

GFI LANguard Network Security Scanner ReportPack



Executive report showing network vulnerability summary

■ Identify security vulnerabilities and take remedial action

GFI LANguard N.S.S. scans computers, identifies and categorizes security vulnerabilities, recommends a course of action and provides tools that enable you to solve these issues. GFI LANguard N.S.S. 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.

■ Extensive, industrial-strength vulnerabilities database

GFI LANguard N.S.S. 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 N.S.S. 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.

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

GFI LANguard N.S.S. 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 N.S.S. 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!

■ Setup your own custom vulnerability checks

GFI LANguard N.S.S. allows you to easily create custom vulnerability checks through wizard-assisted custom-vulnerability condition setup screens. You can also write complex vulnerability checks using the GFI LANguard N.S.S. VBScript-compatible script engine. GFI LANguard N.S.S. includes a script editor and debugger to help with script development.

■ Easily analyze and filter scan results

GFI LANguard N.S.S. 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

When a scan is complete, GFI LANguard N.S.S. 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 N.S.S. you can easily deploy missing service packs and patches network-wide. GFI LANguard N.S.S. 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 N.S.S. 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.

■ Deploys custom/third party software and patches network-wide

Besides deploying patches and service packs, GFI LANguard N.S.S. enables you to easily deploy third party software or patches network-wide. You can use this feature to deploy client software, update custom or non-Microsoft software, virus updates and more. The custom software deployment feature means you can do without Microsoft SMS, which is too complex and expensive for small to medium sized networks.

Network and software auditing

GFI LANguard N.S.S.'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. 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.

■ Automatically receive alerts of new security holes

GFI LANguard N.S.S. can perform scheduled scans (for instance daily or weekly) and can automatically compare results to previous scans. Any new security holes or security setup changes discovered on your network are emailed to you for analysis. This enables you to quickly identify newly-created shares, installed services, installed applications, added users, newly-opened ports and more.

■ Scan and retrieve OS data from Linux systems

It is possible to remotely extract OS data from Linux-based systems and scan results are presented in the same way as for Windows-based computers. This means that both Linux and Windows-based computers can be analyzed in a single scanning session! GFI LANguard N.S.S. includes numerous Linux security checks including rootkit detection. GFI LANguard N.S.S. can use SSH Private Key files instead of the conventional password string credentials to authenticate to Linux-based target computers.

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 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

GFI
www.gfi.com