

Verfügbar in  
folgenden Sprachen



**Microsoft**  
GOLD CERTIFIED  
Partner

# GFI LANguard

Netzwerksicherheits-Scanner, Port-Scanner und  
Patch-Management



- Richtungsweisende Technologie
- Attraktives Preisangebot
- Über **20.000** Kunden

## Die führende Lösung für Netzwerksicherheits-Scans und Schwachstellen-Management

GFI LANguard ermöglicht das Aufspüren, Bewerten und Beheben von Sicherheitsschwachstellen im Netzwerk. Bereits über 20.000 Kunden vertrauen auf den mehrfach ausgezeichneten Netzwerk- und Port-Scanner, um ihre IT-Umgebung mit nur minimalem Verwaltungsaufwand zu schützen. Systemverantwortliche kennen das Problem: Aufgaben wie Schwachstellen-Scans, Patch-Management und Netzwerk-Audits müssen oft getrennt voneinander mit unterschiedlichen Produkten bewältigt werden. GFI LANguard hingegen vereint diese drei tragenden Elemente des Schwachstellen-Managements in einem Paket. Administratoren erhalten per zentrale Konsole einen vollständigen Überblick über den Schutz der IT-Umgebung – und können Systeme einfacher und effektiver absichern.

## Schwachstellen-Scans

Beim Scannen des Netzwerkssamt virtuellen Umgebungen kommen mehr als 15.000 Schwachstellen-Checks und -bewertungen zum Einsatz, die unter anderem auf den Branchenstandards OVAL (Open Vulnerability and Assessment Language) und SANS Top 20 (SysAdmin, Audit, Network, Security) beruhen. Regelmäßige Überprüfungen des Sicherheitsstatus der IT-Umgebung helfen, Lücken zu schließen, bevor sie ausgenutzt werden können. Stellen Sie beispielsweise auch fest, ob Rechner anfällig für den Conficker-Wurm sind und wo bereits eine Infizierung erfolgt ist, sofern kein Schutz bestand.

### VORTEILE

- **Bietet leistungsfähige Netzwerksicherheits- und Port-Scans sowie Netzwerk-Audits**
- **Kontrolliert das gesamte Netzwerk, darunter auch virtuelle Umgebungen, mit über 15.000 Schwachstellen-Checks und -bewertungen**
- **Mindert Betriebskosten durch Zentralisierung von Schwachstellen-Scans, Patch-Management und Netzwerk-Audits**
- **Liefert automatisierte Funktionen für dauerhaften Netzwerkschutz ohne hohen Administrationsaufwand**
- **Bietet Audit-Funktionen zur umfassenden Darstellung des Netzwerk- und Port-Schutzes**
- **Beliebtester kommerzieller Sicherheits-Scanner für Microsoft Windows (bereits zweimal in Folge Sieger bei Nmap-Anwenderumfrage) und "Best of TechEd"-Gewinner 2007 in der Kategorie "Sicherheit"**



## Schwachstellen-Management mit einer integrierten Lösung

GFI LANguard vereint die drei tragenden Elemente des Schwachstellen-Managements – Sicherheits-Scans, Patch-Management und Netzwerk-Audits –, die über eine einzelne, integrierte Konsole verfügbar sind. Scans des gesamten Netzwerks spüren sämtliche potenziellen Gefahren auf. Darüber hinaus bieten umfassende Reporting-Funktionen zur Berichterstellung wertvolle Hilfe bei Bewertung und Behebung der ermittelten Schwachstellen.

- Schwachstellen-Scans
- Patch-Management und Schwachstellen-Behebung
- Netzwerk- und Software-Audits

### Schwachstellen-Scans

Im Rahmen der Sicherheitsüberprüfungen werden mehr als 15.000 Schwachstellen kontrolliert und bewertet sowie alle IP-Adressen des Netzwerks untersucht. Führen Sie Scans für unterschiedliche Betriebssysteme (Windows, Macintosh, Linux) und sogar virtuelle Umgebungen durch, und analysieren Sie Sicherheitseinstellungen und -status Ihres Netzwerks. So lassen sich Lücken aufspüren und schließen, bevor sie von Hackern missbraucht werden können.

### Erkennung virtueller Maschinen

Bei Scans werden auch virtuelle Maschinen erkannt und entsprechend angezeigt. Aktuell unterstützt werden die Virtualisierungslösungen VMware und Virtual PC.

### Definition individueller Schwachstellen-Checks

Ein intuitiver Assistent hilft bei der einfachen Erstellung eigener Schwachstellen-Checks. Selbst komplexe Checks lassen sich einrichten. Die mitgelieferte Skript-Engine unterstützt Python und VBScript; ein Skript-Editor und -Debugger vereinfacht die Entwicklung zusätzlich.

### Umfangreiche Datenbank zu Sicherheitsproblemen

Im Lieferumfang von GFI LANguard ist eine vollständige Datenbank mit Schwachstellenkontrollen und -bewertungen enthalten, darunter mehr als 2.000 branchenweit anerkannte OVAL-Checks (Open Vulnerabilities Assessment Language) und Scans zu SANS-Top-20-Sicherheitslücken. Die Datenbank wird regelmäßig mit neuen Informationen von BugTraq, der SANS Corporation, OVAL, CVE und anderen Quellen zur Informationssicherheit aktualisiert. Informationen zu neu veröffentlichten Sicherheits-Updates von Microsoft sowie Schwachstellen-Checks von GFI und anderen Sicherheitsquellen (z. B. OVAL-Datenbank) werden automatisch zur Verfügung gestellt.

## Identifizierung von Sicherheitsschwachstellen und Einleitung von Gegenmaßnahmen

GFI LANguard scannt alle Netzwerkrechner, schlüsselt identifizierte Sicherheitslücken in verschiedene Gefahrenkategorien auf und bietet Hinweise sowie Tools zur Problembekämpfung. Eine leicht verständliche grafische Darstellung des Gefährdungsgrads erlaubt die rasche Bewertung des Schutzes einzelner Computer oder des gesamten Netzwerks. Gegebenenfalls werden Links oder zusätzliche Informationen bereitgestellt, die beim Schließen einer speziellen Lücke helfen können – z. B. eine BugTraq-ID oder eine Artikel-ID der Microsoft Knowledge Base.

## Funktionskontrolle von Sicherheitsanwendungen wie Antiviren- und Anti-Spyware-Lösungen

Stellen Sie fest, ob unterstützte Sicherheitsanwendungen wie Antiviren- und Anti-Spyware-Programme mit aktuellen Signaturdateien arbeiten und ihre Scans korrekt verrichten. So können beispielsweise die Konfigurationseinstellungen der Security-Produkte kontrolliert werden um zu überprüfen, ob wichtige Funktionen wie Echtzeit-Scans aktiviert sind.

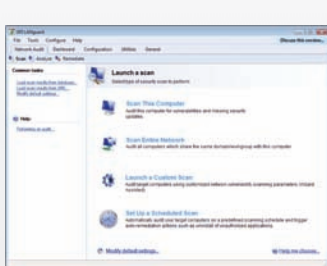
## Problemlose Anpassung von Scans und Schwachstellen-Checks

Scans lassen sich mühelos für die Suche nach unterschiedlichen sicherheitsrelevanten Informationen anpassen. Hierzu zählen Freigaben auf Arbeitsplatzrechnern, Richtlinien für Sicherheitsüberwachungen und Passwörter oder auch Computer, auf denen einzelne Patches oder Service Packs fehlen. Ebenso möglich ist die Suche nach folgenden potenziellen Schwachstellen:

- **Offene Ports:** GFI LANguard sucht nach nicht benötigten, offenen Ports und stellt sicher, dass keine Ports unter der Kontrolle von Hackern stehen.
- **Ungenutzte Konten lokaler Benutzer und Gruppen:** Es werden nicht länger verwendete Benutzerkonten hervorgehoben, die aus Sicherheitsgründen gelöscht oder deaktiviert werden sollten.
- **Unerwünschte Anwendungen:** Erstellen Sie eine Blacklist mit unerwünschten oder gefährlichen Programmen, bei deren Identifizierung eine Warnung erfolgen soll.
- **Gefährliche USB-Geräte und Funkverbindungen/-knoten:** Lassen Sie alle per USB oder Funkverbindung angekoppelten Geräte aufspüren und sich bei verdächtigen Aktivitäten benachrichtigen.
- u. v. m.

## Systemanforderungen

- Windows 2000 (SP4), Windows XP (SP2; x86- und x64-Edition), Windows Server 2003 (x86- und x64-Edition), Windows Vista (x86- und x64-Edition) oder Windows Server 2008 (x86- und x64-Edition)
- Unterstützung von optionalem Microsoft Small Business Server (SBS) 2003/2008
- Microsoft .NET Framework 2.0 oder höher
- Für Scans von Linux-Computern: aktiviertes Secure Shell (SSH) – standardmäßig im Lieferumfang jeder Linux-Distribution enthalten
- Ggf. Änderung der Firewall-Konfiguration erforderlich, siehe Knowledge-Base-Artikel:  
<http://kbase.gfi.com/showarticle.asp?id=KBID002344>.



Starten eines neuen Scans



Vollständiger Scan

↓ Weitere Informationen und eine kostenfreie Testversion stehen zum Abruf bereit auf <http://www.gfi.com/de/lannetscan/>

### Kontakt

#### Malta

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

#### GB

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

#### Asien/Pazifikraum/Südastralien

Tel +61 8 8273 3000  
Fax +61 8 8273 3099  
sales@gfiap.com

Weitere Niederlassungen von GFI: <http://www.gfi.com/de/company/contact.htm>

**Microsoft**  
GOLD CERTIFIED  
Partner

**GFI**