

SALES GUIDE

Offering network security audit *with GFI LanGuard MSP*



GFI Software™

Overview

In cyber warfare, where hackers continually exploit new vulnerabilities, organizations must proactively safeguard their networks. GFI LanGuard provides a robust and comprehensive solution for conducting network security audits, empowering businesses to stay secure and compliant.

The vitality of network security audits

A network security audit is a fundamental process that enables organizations to assess their overall security posture, ensuring robust protection against potential threats. By conducting regular audits, businesses adopt a proactive defense strategy rather than merely reacting to security incidents. Additionally, it aids in adhering to compliance regulations, reinforcing the integrity of data and network infrastructure.

GFI LanGuard: Your trusted network security partner

As a leading network security auditing tool, GFI LanGuard equips organizations with unparalleled visibility and control. Its advanced features enable the effective detection of vulnerabilities and swift deployment of patches to fortify network defenses.

Empowering MSPs with 'Pay Per Scan' licensing

Nowadays, an increasing number of businesses are opting to delegate security audits to Managed Service Providers (MSPs) rather than relying on in-house teams. This preference stems from the recognition that MSPs are more proficient in implementing security best practices, owing to their extensive experience working with multiple organizations.

To support MSPs in conducting comprehensive network security audits, GFI offers a 'pay per scan' monthly licensing option for GFI LanGuard, the details of which you can find in the [MSP Licensing Guide for GFI LanGuard](#).

Conducting a network security audit: A comprehensive approach

Before initiating the audit process, careful planning is essential. Consider the following steps:

- **Time range and scope:** Define the audit timeline and the specific scope of the assessment.
- **Security audit checklist:** Customize a comprehensive security audit checklist tailored to your customer's needs.

3 Offering network security audit with GFI LanGuard MSP

- **Identify needed tools:** Determine the necessary tools, and GFI LanGuard will be your essential partner in this process.
- **Auditing team setup:** Establish a dedicated team to manage and oversee the audit process efficiently.

Below is a sample network security audit checklist that you can use as a starting point and tailor according to your customers' needs:

- ✓ Audit scope
- ✓ Identify sensitive data and its location
- ✓ Make sure users are accessing internet safely
- ✓ Identify threats
- ✓ Ensure the safety of sensitive data
- ✓ Perform penetration testing
- ✓ Inspect servers
- ✓ Review and edit internal policies
- ✓ Access your current backup strategies
- ✓ Reinforce firewalls
- ✓ Reevaluate your password and access strategies
- ✓ Check the procedures of management system
- ✓ Reevaluate security software
- ✓ Ensure all OS and 3rd party SW is up to date
- ✓ Review logs and log monitoring system
- ✓ Identify vulnerabilities
- ✓ Remove unwanted applications
- ✓ Look for unauthorized access points

Frequency of network audits: An essential consideration

As an MSP offering network security audits, remember that network security is an ongoing commitment rather than a one-time task. Regular network scanning and fresh audit reports are crucial to addressing and mitigating security issues. Therefore, for ultimate security, it is recommended that customers avail [vulnerability and patch management as a service](#), which you as an MSP can deliver.

Benefits of using GFI LanGuard for network audits

GFI LanGuard collects a wide variety of information from the endpoints, which can help tick a huge range of items from the audit checklist. Some of its key operations include:

- **Network device audit:** Identify and assess all active devices in your network, allowing you to understand potential points of entry for attackers.
- **Patch management:** GFI LanGuard enables the detection and remediation of missing patches across various operating systems and applications, including Windows OS, MAC, Linux, and third-party software.

4 Offering network security audit with GFI LanGuard MSP

- **Vulnerability assessment:** Perform comprehensive vulnerability assessments on operating systems, network devices, mobile devices, and third-party applications to proactively address security gaps.
- **Software and hardware inspection:** Gain insights into deployed software and hardware to ensure compliance and reduce exposure to security risks.
- **Built-in compliance reporting:** Easily generate compliance reports, streamlining the process of meeting regulatory requirements.

For more information, refer to our guide [How to perform a network security audit](#).

Safeguard your network with GFI LanGuard

With GFI LanGuard's powerful network security auditing capabilities, organizations can ensure their networks are resilient against cyber threats. Protect your valuable assets, data, and reputation by leveraging GFI LanGuard's innovative features.

For more information or to schedule a GFI LanGuard network audit, contact us at sales@gfi.com



All product names and companies mentioned may be trademarks or registered trademarks of their respective owners.

All information in this document was valid to the best of our knowledge at the time of its publication.

The information contained in this document may be changed without prior notice.