



Strengthening network security with GFI LanGuard and GFI Clearview

In the face of rapidly evolving cyber threats, organizations must prioritize network security to safeguard critical assets and sensitive data. A comprehensive security approach requires a combination of vulnerability management and network monitoring solutions. This document explores the security perspective of using GFI LanGuard in collaboration with GFI ClearView. The collaboration between these solutions enhances network security by proactively identifying vulnerabilities and optimizing incident response measures.

Understanding GFI LanGuard

GFI LanGuard is a robust vulnerability assessment and patch management solution designed to identify and remediate network vulnerabilities, missing patches, and security loopholes across diverse systems and applications. By performing automated network scans, LanGuard helps organizations maintain a strong security posture and mitigate potential risks.

Emphasizing GFI Clearview

GFI Clear view is a powerful network monitoring tool that offers real-time visibility into network traffic, bandwidth utilization, and application performance. It aids IT teams in optimizing network performance and promptly troubleshooting issues.

By using GFI LanGuard in collaboration with GFI Clearview, a relationship that fortifies network security is established. The data gathered from both of the solutions can be fed into systems such as SIEM. This allows the SIEM system to enhance and supplement the existing alerts and reports. This collaboration empowers IT teams with enriched insights and proactive measures to enhance network security comprehensively.

Key benefits

Vulnerability detection

GFI LanGuard provides information of the vulnerabilities present on all devices, software installations, hardware inventory. By correlating data from GFI Clearview (e.g. top hosts or top applications) with vulnerability information from GFI LanGuard, IT teams can prioritize vulnerabilities based on their potential impact on network performance and security. This collaboration streamlines incident response and remediation efforts, reducing the window of opportunity for attackers.

Threat detection with improved visibility into application behavior

GFI ClearView provides detailed insights into application usage and behavior, helping IT teams identify suspicious application activities. This list of applications can also be correlated with the software inventory provided by GFI LanGuard to make sure that all applications are covered from the vulnerability perspective and from the traffic perspective. This knowledge enables proactive security measures and enhances overall network security. Furthermore, GFI ClearView can work alongside firewalls to optimize their performance and ensure that security rules and policies are correctly enforced. By analyzing network traffic, GFI ClearView can help identify bottlenecks and prioritize firewall rules to enhance overall security effectiveness.

Robust reporting

The built-in compliance reports provided by GFI LanGuard together with the valuable information provided by GFI ClearView can be used to provide evidence of the network security posture of the organization. Helping them prove how they are compliant with different security requirements. The combination of historical vulnerability data from GFI LanGuard and long-term network traffic data from GFI Clearview enables IT teams to conduct trend analysis over time. This helps in identifying recurring security patterns, assessing the effectiveness of security measures, and making data-driven decisions to improve the overall security strategy.

The use of GFI LanGuard in collaboration with GFI Clearview empowers organizations with a powerful security duo that combines vulnerability management with real-time network visibility. This collaboration ensures the proactive identification and remediation of vulnerabilities, ultimately strengthening network security. By leveraging the synergies between them, organizations can establish a comprehensive security framework that defends against emerging threats and safeguards sensitive data and critical assets.