LanGuard AI

ONE-PAGER

GFI LANGUARD · VULNERABILITY & PATCH MANAGEMENT · FOR BANKS & FINANCIAL INSTITUTIONS

Every Unpatched Endpoint is an Exam Finding Waiting to Happen.

GFI LanGuard scans, assesses, and patches every device on your network — then turns the result into audit-ready compliance evidence, automatically.

70,000+ Known Issues Tracked

Every scan is checked against a continuously updated database of known vulnerabilities — plus open ports, missing patches and system configuration — across every OS on your network.

THE CONTINUOUS CYCLE

SCAN
Identifies every device on the network and inventories software, hardware, open ports, shares, running services and logged-on users — across Windows, Linux, macOS, VMs, limited on mobile and network devices.

ASSESS
Cross-references each device against the 70,000+ known-issue database to surface missing patches and vulnerabilities before they're exploited.

REMEDIATE
Deploys missing patches automatically or on approval, across supported operating systems and 60+ third-party vendor applications — including in secured environments with no internet connection.

REPORT
Generates scheduled compliance reports mapped to PCI DSS, HIPAA, SOX, GLBA and ISO/IEC 27001 & 27002, delivered on a set cadence — audit evidence your team doesn't have to assemble by hand.

Then the cycle repeats — on the schedule you set.

DEPLOYMENT & RESILIENCE

AIR-GAPPED PATCHING
Scans and deploys patches in secured environments with no internet connection.

ISOLATED PER-TENANT
Each WAN Agent runs on its own certificate-authenticated tenant, over SSL

CROSS-PLATFORM
Windows, Linux, macOS, VMs, mobile and network devices — one console

DEPLOYMENT ARCHITECTURE

Scans run server-based or via a lightweight agent. A Relay Agent extends coverage to branch offices; remote users use the secure WAN Agent, with each customer isolated to its own certificate-authenticated tenant over SSL — no other party can modify it, and no shared infrastructure between customers. Your own administrator retains control.

COMPLIANCE MAPPING — GLOBAL BASELINE

Global baseline view below — extend it to your institution's specific regime using the same reporting engine.

Global Baseline — Basel Committee Principles; ISO/IEC 27001 & 27002	Continuous, scheduled vulnerability scanning and patch deployment network-wide, plus native ISO/IEC 27001 & 27002-mapped reporting, are the early-warning and audit-evidence controls examiners expect — everywhere you operate.**	**Supports**
United States — PCI DSS, HIPAA, SOX, GLBA	Automated compliance reports map to each named requirement, including PCI DSS v4.0.1 Requirement 6.3.3's 30-day critical-patch window — audit evidence, not a certification.††	**Capability**
European Union — DORA (Regulation (EU) 2022/2554), Article 9(1) — ICT Risk Management	Article 9(1) requires ongoing identification and remediation of ICT vulnerabilities. LanGuard's scan-assess-remediate cycle is a technical control supporting that requirement.§	**Capability**
UK / Canada / Australia / Singapore — FCA/PRA Operational Resilience (UK); OSFI B-13 (Canada); APRA CPS 234 (Australia); MAS TRM (Singapore), or your local equivalent	Each expects evidence you can identify and remediate technology vulnerabilities in a business-critical service — the same scan-and-patch engine, pointed at your regime.	**Capability**

Copyright © GFI USA, LLC, All rights reserved.