LanGuard AI

One-Pager

GFI LANGUARD · SCHWACHSTELLEN- UND PATCH-MANAGEMENT · FÜR BANKEN UND FINANZINSTITUTE

Jeder ungepatchte Endpunkt ist ein Prüfungsbefund, der nur darauf wartet, entdeckt zu werden.

GFI LanGuard scannt, bewertet und installiert Patches auf jedem Gerät in Ihrem Netzwerk — und verwandelt das Ergebnis automatisch in prüfungsbereite Compliance-Nachweise.

70,000+ **Bekannte Schwachstellen werden nachverfolgt**

Jeder Scan wird mit einer kontinuierlich aktualisierten Datenbank bekannter Schwachstellen abgeglichen und zusätzlich auf offene Ports, fehlende Patches sowie Systemkonfigurationen überprüft — und zwar für alle Betriebssysteme in Ihrem Netzwerk.

DER KONTINUIERLICHE ZYKLUS

SCANNEN
Identifiziert jedes Gerät im Netzwerk und erfasst Software, Hardware, offene Ports, Freigaben, laufende Dienste sowie angemeldete Benutzer — auf Windows, Linux, macOS und VMs; für mobile und Netzwerkgeräte ist die Unterstützung eingeschränkt.

BERICHTEN
Erstellt geplante Compliance-Berichte, die auf PCI DSS, HIPAA, SOX, GLBA sowie ISO/IEC 27001 und 27002 abgebildet sind, und liefert diese in festgelegten Intervallen — Prüfungsnachweise, die Ihr Team nicht manuell zusammenstellen muss.

BEHEBEN
Stellt fehlende Patches automatisch oder nach Freigabe bereit — für unterstützte Betriebssysteme und mehr als 60 Anwendungen von Drittanbietern — auch in abgesicherten Umgebungen ohne Internetverbindung.

BEWERTEN
Gleicht jedes Gerät mit einer Datenbank von über 70.000 bekannten Schwachstellen ab, um fehlende Patches und Schwachstellen zu identifizieren, bevor diese ausgenutzt werden.

Dann wiederholt sich der Zyklus — nach dem von Ihnen festgelegten Zeitplan.

BEREITSTELLUNG UND RESILIENZ

PATCH-BEREITSTELLUNG IN ABGETRENNTEN UMGEBUNGEN
Scannt und stellt Patches in abgesicherten Umgebungen ohne Internetverbindung bereit.

PRO MANDANT ISOLIERT
Jeder WAN Agent läuft in einem eigenen, per Zertifikat authentifizierten Mandanten über SSL

PLATTFORMÜBERGREIFEND
Windows, Linux, macOS, VMs, Mobilgeräte und Netzwerkgeräte — eine Konsole

BEREITSTELLUNGSARCHITEKTUR

Scans werden serverbasiert oder über einen leichtgewichtigen Agenten ausgeführt. Ein Relay Agent erweitert die Abdeckung auf Zweigstellen; entfernte Nutzer verwenden den sicheren WAN Agent, wobei jeder Kunde in seinem eigenen, per Zertifikat authentifizierten Mandanten über SSL isoliert ist — keine andere Partei kann diesen verändern, und es gibt keine gemeinsame Infrastruktur zwischen Kunden. Ihr eigener Administrator behält die Kontrolle.

COMPLIANCE-ZUORDNUNG — GLOBALE BASISLINIE

Globale Basisansicht unten — erweitern Sie diese für das spezifische Regelwerk Ihrer Institution mit derselben Reporting-Engine.

Globale Basis — Prinzipien des Basler Ausschusses für Bankenaufsicht; ISO/IEC 27001 und 27002	Kontinuierliche, geplante Schwachstellen-Scans und netzwerkweite Patch-Bereitstellung sowie native, an ISO/IEC 27001 und 27002 angepasste Berichte bilden die Frühwarn- und Prüfungsnachweiskontrollen, die Prüfer erwarten — überall, wo Sie tätig sind.**	**Unterstützt**
Vereinigte Staaten — PCI DSS, HIPAA, SOX, GLBA	Automatisierte Compliance-Berichte werden jedem benannten Anforderungspunkt zugeordnet, einschließlich des 30-Tage-Fensters für kritische Patches in PCI DSS v4.0.1, Anforderung 6.3.3 — Prüfungsnachweise, keine Zertifizierung.††	**Fähigkeit**
Europäische Union — DORA (Verordnung (EU) 2022/2554), Artikel 9(1) — IKT-Risikomanagement	Artikel 9(1) verlangt die fortlaufende Identifizierung und Behebung von IKT-Schwachstellen. Der Scan-Bewertungs-Behebungszyklus von LanGuard ist eine technische Kontrollmaßnahme, die diese Anforderung unterstützt.§	**Fähigkeit**
UK / Kanada / Australien / Singapur — FCA/PRA Operational Resilience (UK); OSFI B-13 (Kanada); APRA CPS 234 (Australien); MAS TRM (Singapur) oder Ihr lokales Pendant	Alle verlangen Nachweise, dass Sie technologische Schwachstellen in geschäftskritischen Diensten identifizieren und beheben können — dieselbe Scan-und-Patch-Engine, ausgerichtet auf Ihr Regelwerk.	**Fähigkeit**

Copyright © GFI USA, LLC. Alle Rechte vorbehalten.