LanGuard AI

One-Pager

GFI LANGUARD · GESTIONE DELLE VULNERABILITÀ E DELLE PATCH · PER BANCHE E ISTITUZIONI FINANZIARIE

Ogni endpoint senza patch è un rilievo d'audit in attesa di verificarsi.

GFI LanGuard esegue la scansione, valuta e applica le patch a ogni dispositivo della tua rete — quindi trasforma automaticamente i risultati in evidenze di conformità pronte per l'audit.

70,000+ **Tracciamento dei problemi noti**

Ogni scansione viene confrontata con un database continuamente aggiornato di vulnerabilità note — oltre che con porte aperte, patch mancanti e configurazioni di sistema — per tutti i sistemi operativi presenti nella rete.

IL CICLO CONTINUO

SCANSIONE
Identifica ogni dispositivo sulla rete e inventaria software, hardware, porte aperte, condivisioni, servizi in esecuzione e utenti connessi — su Windows, Linux, macOS e VM, con funzionalità limitate sui dispositivi mobili e di rete.

REPORT
Genera report di conformità programmati, mappati su PCI DSS, HIPAA, SOX, GLBA e ISO/IEC 27001 e 27002, forniti con cadenza prestabilita — evidenze d'audit che il tuo team non deve preparare manualmente.

RISOLUZIONE
Distribuisce automaticamente le patch mancanti o — previa approvazione — su sistemi operativi supportati e oltre 60 applicazioni di terze parti, anche in ambienti protetti senza connessione a Internet.

VALUTAZIONE
Incrocia ogni dispositivo con un database di oltre 70.000 vulnerabilità note per evidenziare patch mancanti e vulnerabilità prima che vengano sfruttate.

Poi il ciclo si ripete — con la frequenza che imposti tu.

DISTRIBUZIONE E RESILIENZA

APPLICAZIONE PATCH IN AMBIENTI ISOLATI (AIR-GAPPED)
Esegue scansioni e applica le patch in ambienti protetti senza connessione a Internet.

Isolamento per tenant
Ogni WAN Agent funziona su un tenant autenticato mediante certificato e comunica tramite connessioni SSL.

MULTIPIATTAFORMA
Windows, Linux, macOS, VM, dispositivi mobili e di rete — un'unica console

ARCHITETTURA DI DISTRIBUZIONE

Le scansioni possono essere eseguite lato server o tramite un agent leggero. Un Relay Agent estende la copertura alle filiali; gli utenti remoti utilizzano il WAN Agent sicuro, con ogni cliente isolato nel proprio tenant autenticato tramite certificato su connessioni SSL — nessuna terza parte può modificarlo e non esiste un'infrastruttura condivisa tra i clienti. Il tuo amministratore mantiene il controllo.

MAPPATURA DELLA CONFORMITÀ — BASELINE GLOBALE

Vista della baseline globale qui sotto — estendila al quadro normativo specifico della tua istituzione utilizzando lo stesso motore di reportistica.

Baseline globale — Principi del Comitato di Basilea; ISO/IEC 27001 & 27002	La scansione continua e programmata delle vulnerabilità e la distribuzione delle patch su tutta la rete, unitamente ai report nativi mappati su ISO/IEC 27001 e 27002, costituiscono i controlli che forniscono allerta precoce e evidenze d'audit che gli esaminatori si aspettano — ovunque tu operi.**	**Supporta**
Stati Uniti — PCI DSS, HIPAA, SOX, GLBA	I report di conformità automatizzati mappano ciascun requisito nominato, inclusa la finestra di 30 giorni per le patch critiche prevista dal Requisito 6.3.3 di PCI DSS v4.0.1 — evidenze d'audit, non una certificazione.††	**Capacità**
Unione Europea — DORA (Regolamento (UE) 2022/2554), Articolo 9(1) — Gestione del rischio ICT	L'articolo 9(1) richiede l'identificazione e la risoluzione continuativa delle vulnerabilità ICT. Il ciclo di scansione-valutazione-risoluzione di LanGuard è un controllo tecnico che supporta tale requisito.§	**Capacità**
Regno Unito / Canada / Australia / Singapore — FCA/PRA Operational Resilience (UK); OSFI B-13 (Canada); APRA CPS 234 (Australia); MAS TRM (Singapore), o il tuo equivalente locale	Ciascuno richiede evidenze che tu sia in grado di identificare e risolvere le vulnerabilità tecnologiche in un servizio critico per il business — lo stesso motore di scansione e gestione delle patch, orientato al tuo quadro normativo.	**Capacità**

Copyright © GFI USA, LLC. Tutti i diritti riservati.