LanGuard AI

Jednostránkový přehled

GFI LANGUARD · Řízení zranitelností a správa záplat · Pro banky a finanční instituce

Každé koncové zařízení bez nainstalovaných záplat je auditním nálezem, který jen čeká na odhalení.

GFI LanGuard skenuje, vyhodnocuje a aplikuje záplaty na každé zařízení ve vaší síti — a výsledky automaticky přemění na důkazy o souladu připravené pro audit.

70,000+ **Sledování známých zranitelností**

Každé skenování je porovnáváno s průběžně aktualizovanou databází známých zranitelností — kontroluje také otevřené porty, chybějící záplaty a konfiguraci systému — napříč všemi operačními systémy ve vaší síti.

NEUSTÁLÝ CYKLUS

SKENOVÁNÍ
Identifikuje každé zařízení v síti a eviduje software, hardware, otevřené porty, sdílené složky, běžící služby a přihlášené uživatele — na platformách Windows, Linux a macOS, na virtuálních strojích (VM) a omezeně i na mobilních a síťových zařízeních.

NÁPRAVA
Nasazuje chybějící záplaty automaticky nebo po schválení na podporovaných operačních systémech a u více než 60 aplikací třetích stran — včetně zabezpečených prostředí bez připojení k internetu.

HODNOCENÍ
Porovnává každé zařízení s databází více než 70 000 známých zranitelností, aby odhalil chybějící záplaty a zranitelnosti dříve, než budou zneužity.

ZPRÁVA
Generuje naplánované zprávy o souladu mapované na PCI DSS, HIPAA, SOX, GLBA a ISO/IEC 27001 a 27002, doručované v nastaveném intervalu — auditní důkazy, které váš tým nemusí sestavovat ručně.

Pak se cyklus opakuje — podle rozvrhu, který nastavíte.

NASAZENÍ A ODOLNOST

Nasazování záplat v odizolovaných sítích
Provádí skenování a nasazuje záplaty v zabezpečených prostředích bez připojení k internetu.

Izolace pro jednotlivé tenanty
Každý WAN Agent běží v samostatném tenantovi ověřeném certifikátem přes SSL.

Meziplatformní
Windows, Linux, macOS, virtuální stroje (VM), mobilní a síťová zařízení — jedna konzole

ARCHITEKTURA NASAZENÍ

Skeny probíhají na serveru nebo prostřednictvím lehkého agenta. Relay Agent rozšiřuje pokrytí do poboček; vzdálení uživatelé používají zabezpečený WAN Agent, přičemž každý zákazník je izolován ve vlastním tenantovi ověřeném certifikátem přes SSL — žádná jiná strana jej nemůže měnit a mezi zákazníky není sdílená infrastruktura. Váš administrátor si zachovává kontrolu.

MAPOVÁNÍ SOULADU — GLOBÁLNÍ VÝCHOZÍ ÚROVEŇ

Níže uvedená globální výchozí úroveň — rozšiřte ji o specifika vaší instituce pomocí stejného nástroje pro generování zpráv.

Globální výchozí úroveň — principy Basilejského výboru pro bankovní dohled; ISO/IEC 27001 a 27002	Nepřetržité, plánované skenování zranitelností a nasazování záplat v celé síti, spolu s nativně mapovanými reporty na ISO/IEC 27001 a 27002, představují včasné varování a auditní důkazy, které auditoři očekávají — ve všech zemích, kde působíte.**	**Podporuje**
Spojené státy — PCI DSS, HIPAA, SOX, GLBA	Automatizované zprávy o souladu mapují každý uvedený požadavek, včetně požadavku PCI DSS v4.0.1 (Requirement 6.3.3), který stanovuje 30denní lhůtu pro kritické záplaty — auditní důkazy, nikoli certifikace.††	**Schopnost**
Evropská unie — DORA (nařízení (EU) 2022/2554), článek 9(1) — řízení ICT rizik	Článek 9(1) vyžaduje průběžnou identifikaci a nápravu zranitelností ICT. Cyklus skenování–hodnocení–nápravy řešení GFI LanGuard je technickou kontrolou podporující tento požadavek.§	**Schopnost**
Spojené království / Kanada / Austrálie / Singapur — FCA/PRA Operational Resilience (UK); OSFI B-13 (Kanada); APRA CPS 234 (Austrálie); MAS TRM (Singapur), nebo váš místní ekvivalent	Každý z nich očekává důkazy, že dokážete identifikovat a napravit technologické zranitelnosti v provozně kritické službě — stejný skenovací a záplatovací mechanismus nasměrovaný na vaše předpisy.	**Schopnost**

Copyright © GFI USA, LLC. Všechna práva vyhrazena.