LanGuard AI

Ficha informativa

GFI LANGUARD · GESTIÓN DE VULNERABILIDADES Y PARCHES · PARA BANCOS E INSTITUCIONES FINANCIERAS

Cada endpoint sin parchear es un hallazgo de auditoría a la espera de producirse.

GFI LanGuard escanea, evalúa y parchea cada dispositivo de su red — y convierte automáticamente los resultados en evidencia de cumplimiento lista para auditoría.

70,000+ **Seguimiento de problemas conocidos**

Cada análisis se compara con una base de datos de vulnerabilidades conocidas actualizada continuamente —además de puertos abiertos, parches faltantes y configuración del sistema— en todos los sistemas operativos de su red.

EL CICLO CONTINUO

ESCANEO
Identifica cada dispositivo de la red y realiza un inventario del software, hardware, puertos abiertos, recursos compartidos, servicios en ejecución y usuarios conectados —en Windows, Linux, macOS, VMs y con cobertura limitada en dispositivos móviles y de red.

INFORME
Genera informes de cumplimiento programados correspondientes a PCI DSS, HIPAA, SOX, GLBA e ISO/IEC 27001 y 27002, entregados con la periodicidad establecida — evidencia de auditoría que su equipo no tiene que recopilar manualmente.

REMEDIACIÓN
Despliega los parches faltantes de forma automática o previa aprobación, en los sistemas operativos compatibles y en más de 60 aplicaciones de terceros —incluso en entornos aislados sin conexión a Internet.

EVALUACIÓN
Contrasta cada dispositivo con la base de datos de más de 70.000 problemas conocidos para detectar parches faltantes y vulnerabilidades antes de que sean explotadas.

Luego el ciclo se repite —según la programación que usted defina.

DESPLIEGUE Y RESILIENCIA

PARCHEO EN ENTORNOS AISLADOS
Escanea y despliega parches en entornos aislados sin conexión a Internet.

AISLAMIENTO POR TENANT
Cada WAN Agent se ejecuta en su propio tenant autenticado mediante certificado, sobre SSL.

MULTIPLATAFORMA
Windows, Linux, macOS, VMs, dispositivos móviles y de red —una única consola

ARQUITECTURA DE DESPLIEGUE

Los escaneos se ejecutan desde servidor o mediante un agente ligero. Un Relay Agent extiende la cobertura a sucursales; los usuarios remotos usan el seguro WAN Agent, con cada cliente aislado en su propio tenant autenticado por certificado sobre SSL —ninguna otra parte puede modificarlo y no existe infraestructura compartida entre clientes. Su propio administrador mantiene el control.

MAPEO DE CUMPLIMIENTO — LÍNEA BASE GLOBAL

Vista de la línea base global a continuación —extiéndala al régimen específico de su institución utilizando el mismo motor de informes.

Línea base global — Principios del Comité de Basilea; ISO/IEC 27001 y 27002	El escaneo continuo y programado de vulnerabilidades y el despliegue de parches a nivel de red, junto con informes nativos mapeados a ISO/IEC 27001 y 27002, son los controles de alerta temprana y la evidencia de auditoría que los examinadores esperan —en cualquier lugar donde opere.**	**Compatibilidad**
Estados Unidos — PCI DSS, HIPAA, SOX, GLBA	Los informes de cumplimiento automatizados se corresponden con cada requisito nombrado, incluyendo el plazo de 30 días para parches críticos del Requisito 6.3.3 de PCI DSS v4.0.1 —evidencia de auditoría, no una certificación.††	**Capacidad**
Unión Europea — DORA (Reglamento (UE) 2022/2554), Artículo 9(1) — Gestión del riesgo TIC	El Artículo 9(1) exige la identificación y corrección continuas de vulnerabilidades TIC. El ciclo de escaneo-evaluación-remediación de GFI LanGuard es un control técnico que respalda ese requisito.§	**Capacidad**
Reino Unido / Canadá / Australia / Singapur — Resiliencia Operativa FCA/PRA (Reino Unido); OSFI B-13 (Canadá); APRA CPS 234 (Australia); MAS TRM (Singapur), o su equivalente local	Cada uno espera evidencia de que puede identificar y remediar vulnerabilidades tecnológicas en un servicio crítico para el negocio —el mismo motor de escaneo y parcheo, orientado a su régimen regulatorio.	**Capacidad**

Copyright © GFI USA, LLC. Todos los derechos reservados.