LanGuard AI

Resumo de uma página

GFI LANGUARD · GERENCIAMENTO DE VULNERABILIDADES E PATCHES · PARA BANCOS E INSTITUIÇÕES FINANCEIRAS

Todo endpoint sem patches aplicados é uma constatação de auditoria prestes a ocorrer.

GFI LanGuard varre, avalia e implanta patches em todos os dispositivos da sua rede — e transforma o resultado em evidências de conformidade prontas para auditoria, automaticamente.

70,000+ **Rastreamento de Vulnerabilidades Conhecidas**

Cada varredura é verificada contra um banco de dados continuamente atualizado de vulnerabilidades conhecidas — além de portas abertas, patches ausentes e configuração do sistema — em todos os sistemas operacionais da sua rede.

O CICLO CONTÍNUO

VARREDURA
Identifica todos os dispositivos na rede e inventaria software, hardware, portas abertas, compartilhamentos, serviços em execução e usuários conectados — em Windows, Linux, macOS, VMs e, de forma limitada, em dispositivos móveis e de rede.

RELATÓRIO
Gera relatórios de conformidade agendados, mapeados para PCI DSS, HIPAA, SOX, GLBA e ISO/IEC 27001 e 27002, entregues com periodicidade definida — evidência de auditoria que sua equipe não precisa montar manualmente.

REMEDIAÇÃO
Implanta patches ausentes automaticamente ou mediante aprovação, em sistemas operacionais suportados e em mais de 60 aplicações de terceiros — inclusive em ambientes seguros sem conexão com a internet.

AVALIAÇÃO
Cruza as informações de cada dispositivo com o banco de dados de mais de 70.000 problemas conhecidos para identificar patches ausentes e vulnerabilidades antes que sejam exploradas.

Então o ciclo se repete — no cronograma que você definir.

IMPLEMENTAÇÃO E RESILIÊNCIA

APLICAÇÃO DE PATCHES EM AMBIENTES ISOLADOS
Faz varreduras e implanta patches em ambientes seguros sem conexão com a internet.

ISOLADO POR TENANT
Cada WAN Agent é executado em seu próprio tenant autenticado por certificado, via SSL.

MULTIPLATAFORMA
Windows, Linux, macOS, VMs, dispositivos móveis e de rede — um console

ARQUITETURA DE IMPLEMENTAÇÃO

As varreduras são executadas em modo servidor ou por meio de um agente leve. Um Relay Agent estende a cobertura a filiais; usuários remotos usam o WAN Agent seguro, com cada cliente isolado em seu próprio tenant autenticado por certificado via SSL — nenhuma outra parte pode modificá-lo, e não há infraestrutura compartilhada entre clientes. Seu administrador mantém o controle.

MAPEAMENTO DE CONFORMIDADE — REFERENCIAL GLOBAL

Visão do referencial global abaixo — estenda-a ao quadro regulatório específico da sua instituição usando o mesmo mecanismo de relatórios.

Referencial Global — Princípios do Comitê da Basileia; ISO/IEC 27001 & 27002	Varredura contínua e agendada de vulnerabilidades e implantação de patches em toda a rede, além de relatórios nativos mapeados para ISO/IEC 27001 & 27002, são os controles de alerta precoce e evidência de auditoria que os examinadores esperam — em todos os locais onde você opera.**	**Compatível com**
Estados Unidos — PCI DSS, HIPAA, SOX, GLBA	Relatórios automatizados de conformidade mapeiam para cada requisito nomeado, incluindo a janela de 30 dias para patches críticos do Requisito 6.3.3 do PCI DSS v4.0.1 — evidência de auditoria, não uma certificação.††	**Capacidade**
União Europeia — DORA (Regulamento (UE) 2022/2554), Artigo 9(1) — Gestão de Risco TIC	O Artigo 9(1) exige a identificação e remediação contínuas de vulnerabilidades TIC. O ciclo de varredura-avaliação-remediação do GFI LanGuard é um controle técnico que suporta esse requisito.§	**Capacidade**
Reino Unido / Canadá / Austrália / Singapura — FCA/PRA Operational Resilience (Reino Unido); OSFI B-13 (Canadá); APRA CPS 234 (Austrália); MAS TRM (Singapura), ou seu equivalente local	Cada um exige evidências de que você pode identificar e remediar vulnerabilidades tecnológicas em um serviço crítico para o negócio — o mesmo mecanismo de varredura e aplicação de patches direcionado ao seu quadro regulatório.	**Capacidade**

Copyright © GFI USA, LLC. Todos os direitos reservados.