LanGuard

DATOVÝ LIST

Zavřete dveře před zranitelnostmi

Udržování bezpečnosti vaší sítě začíná tím, že si uvědomíte všechny prvky, které ji tvoří. GFI LanGuard poskytuje tento přehled, umožňuje vyhodnotit, kde se mohou vyskytovat potenciální zranitelnosti, a dává vám prostředky, jak je opravit. GFI LanGuard nabízí tyto výkonné funkce ve snadno použitelné a snadno nasaditelné aplikaci.

Podívejte se na svou síť a kudy se do ní dostávají hrozby

Automaticky objevujte všechny prvky vaší sítě: počítače, notebooky, mobilní telefony, tablety, tiskárny, servery, virtuální stroje, routery a přepínače.

Najděte mezery využívané hrozbami

Skenujte svou síť na chybějící záplaty. Každý rok je vydáno více než 5 000 oprav; kterákoli z nich může řešit chyby, na které cílí hackeři. Najděte mezery v operačních systémech Microsoft, MacOS a Linux. Identifikujte chybějící opravy ve webových prohlížečích a softwaru od třetích stran, jako jsou Adobe, Java a od 60 dalších předních dodavatelů.

Zalepte díry, které vás činí zranitelnými

GFI LanGuard vám umožňuje nasazovat záplaty centrálně a automaticky nebo nasazením agentů na počítače, aby to udělali a ušetřili výpočetní kapacitu serveru. Nespoléhejte se na jednotlivce, že udrží váš perimetr opravený. Určujte, které opravy nainstalujete, a v případě problémů opravy vraťte zpět. Instalujte více než jen bezpečnostní záplaty: mnoho záplat opravuje aplikace, aby běžely lépe.

Získejte požadované přehledy o souladu s předpisy a opravách chyb zabezpečení

Zákony o zajištění souladu s předpisy obsahují mnoho požadavků na zajištění bezpečnosti finančních, zdravotních nebo jiných osobních údajů v sítích a systémech. Získejte automatizované, formátované přehledy, které auditoři potřebují k prokázání shody s mnoha požadavky předpisů PCI DSS, HIPAA, SOX, GLBA, PSN a CoCo.

Požádejte o Demo

Správa oprav napříč více operačními systémy

GFI LanGuard je kompatibilní s operačními systémy Microsoft®, Mac OS X® a Linux®, stejně jako s mnoha aplikacemi třetích stran, jako jsou Apple QuickTime®, Adobe®, Mozilla® Firefox® a další. Skenujte svou síť automaticky nebo na vyžádání. Automaticky stahujte chybějící opravy nebo opravy vracejte zpět.

Správa oprav pro více webových prohlížečů

GFI LanGuard je první řešení, které automatizuje záplatování všech hlavních webových prohlížečů běžících v systémech Windows®: Microsoft Internet Explorer® Mozilla Firefox®, Google Chrome™ Apple Safari® a Opera™.

Odhalte zranitelnost dříve, než to udělají hackeři

Skener bezpečnosti sítě GFI LanGuard dokáže identifikovat více než 60 000 zranitelností. Skenuje zařízení, identifikuje a kategorizuje slabá místa zabezpečení, doporučí postup a poskytne vám nástroje k vyřešení problému. Grafický indikátor úrovně ohrožení poskytuje intuitivní, vážené hodnocení stavu zranitelnosti skenovaných zařízení.

Webová tvorba přehledů

Webové rozhraní pro tvorbu přehledů se používá prostřednictvím zabezpečeného připojení (https), které podporují všechny hlavní prohlížeče. Zákazníci s rozsáhlými sítěmi mohou nainstalovat více instancí (lokalit) GFI LanGuard a jednu webovou konzoli, která poskytuje centralizovaný přehled a souhrnný reporting pro všechny instance.

Sledujte nejnovější zranitelnosti a chybějící aktualizace

GFI LanGuard je dodáván s důkladnou databází posouzení zranitelností včetně standardů OVAL (více než 11 500 kontrol) a SANS Top 20. Tato databáze je pravidelně aktualizována informacemi z databází společností BugTraq, SANS Corporation, OVAL, CVE a dalších. Systém automatických aktualizací ji neustále aktualizuje pomocí nově vydaných aktualizací zabezpečení a kontrol zranitelností od společnosti Microsoft.

Integrace s bezpečnostními aplikacemi třetích stran

GFI LanGuard se integruje s více než 4 000 kritickými bezpečnostními aplikacemi, mezi které patří: antivirus, antispyware, firewall, anti-phishing, zálohovací klient, VPN klient, URL filtrování, správa záplat, webový prohlížeč, rychlé zasílání zpráv, peer-to-peer, šifrování disků, prevence ztráty dat a řízení přístupu k zařízením. Poskytuje zprávy o stavu a seznamy aplikací pro rychlé zasílání zpráv nebo peer-to-peer aplikací nainstalovaných ve vaší síti. Také řeší všechny problémy, které vyžadují pozornost, jako je spouštění aktualizací antiviru nebo antispywaru.

Kontrolujte zranitelnosti na síťových zařízeních

GFI LanGuard chrání vaše přepínače, směrovače, přístupové body a tiskárny před útoky. Podporuje také skenování zranitelností v chytrých telefonech a tabletech se systémy Windows®, Android™ a iOS® a v řadě síťových zařízení, jako jsou tiskárny, směrovače a přepínače od výrobců jako HP®, Cisco® a mnoha dalších.

Mějte přehled o dění ve vaší síti

Síťový audit GFI LanGuard vám poskytne komplexní přehled o vaší síti – včetně připojených USB zařízení, chytrých telefonů a tabletů, stejně jako o nainstalovaném softwaru, otevřených sdíleních, otevřených portech, slabých heslech a veškerých informacích o hardwaru. Zabezpečte síť uzavřením portů, odstraněním zastaralých uživatelů nebo zakázáním bezdrátových přístupových bodů.

Bezpečnostní audity

Interaktivní ovládací panel poskytuje přehled o aktuálním stavu zabezpečení sítě a historii všech relevantních změn v síti v průběhu času. Procházejte si podrobně informace, od celosíťových bezpečnostních senzorů až po výsledky jednotlivých bezpečnostních skenů.

Spouštějte režimy bez agenta nebo založené na agentovi

GFI LanGuard lze nakonfigurovat pro provoz v režimu bez agenta nebo s agentem. Technologie agentů umožňuje automatizované audity zabezpečení sítě a rozděluje zátěž skenování mezi klientské počítače.

✨ GFI LanGuard CoPilot

Objevte novou úroveň síťové bezpečnosti s GFI LanGuard, nyní rozšířenou o GenAI insights a Configuration Assistant. Naše upgrady nově definují ochranu pro chytřejší, rychlejší a na míru šitou obranu. GenAI proniká hluboko do souvislostí zranitelností a optimalizuje ochranu vašich kritických bodů. Je to víc než jen zabezpečení - je to využitelná inteligence. Konfigurační asistent přizpůsobuje nastavení vašim potřebám a zefektivňuje zabezpečení bez složitostí. zabezpečení. Okamžitě se přizpůsobuje a blokuje vznikající hrozby úpravou filtrů obsahu za chodu. Vaše citlivá data zůstanou chráněna, dodržování předpisů zůstane zachováno a riziko se minimalizuje.