GFI LanGuard™

Twój wirtualny doradca do spraw bezpieczeństwa IT

GFI LanGuard to wielokrotnie nagradzane rozwiązanie, które zdobyło zaufanie firm na całym świecie. Aplikacja ta pozwala skanować, wykrywać, oceniać oraz usuwać luki bezpieczeństwa w sieci oraz podłączonych do niej urządzeniach. Daje ona kompletny obraz bezpieczeństwa sieciowego i pomaga je utrzymywać przy minimalnym wysiłku.

- ✓ **Zarządzanie poprawkami Skanowanie luk w zabezpieczeniach**
- ✓ **Raportowanie zgodności Audyt sieci**
- ✓ **Informacje o bezpieczeństwie sieciowym**

Dowiedz się więcej i rozpocznij DARMOWY OKRES PRÓBNY

www.gfi.com/languard

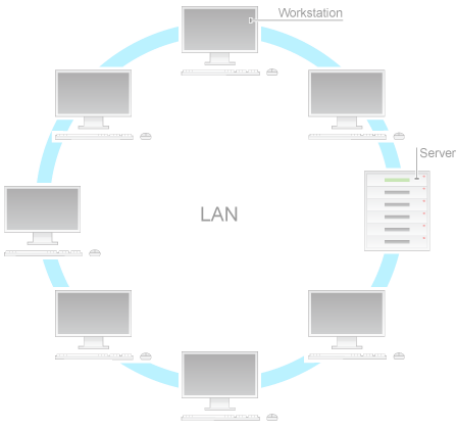
Sun Capital Sp. z o.o.

ul. Ołtaszyńska 92C/6
53-034 Wrocław
tel.: +48 071 360-81-00
sprzedaz@suncapital.pl

www.suncapital.pl

Skanowanie, wykrywanie, ocenianie oraz usuwanie luk w naszej sieci

Internet jest narzędziem absolutnie niezbędnym dla większości firm. Odcięcie od Sieci oznaczałoby całkowitą izolację – co, zdaniem niektórych, wcale nie było by takie złe. Badania firmy IDC wykazały bowiem, że nawet 40% aktywności sieciowej pracowników nie dotyczy ich obowiązków zawodowych. Ponadto w Internecie niezwykle łatwo natknąć się na złośliwy kod, a cyberprzestępcy za wszelką cenę próbują włamać się do sieci użytkowników. Oprogramowanie do monitorowania Internetu i kontroli dostępu znacznie podnosi produktywność, zapobiega włamaniom i chroni sieć przed licznymi zagrożeniami.



Przegląd korzyści

- ✓ Scentralizowane zarządzanie poprawkami, ocena podatności na zagrożenia i audyt sieci
- ✓ Zautomatyzowana instalacja poprawek dla systemów operacyjnych Microsoft®, Mac OS® X, Linux® oraz aplikacji firm trzecich
- ✓ Ponad 50 tys. sprawdzeń podatności przeprowadzanych w sieciach: na komputerach, smartfonach, tabletach, drukarkach, routerach i przełącznikach oraz w środowiskach wirtualnych
- ✓ Wspomaga zachowanie zgodności ze standardem PCI DSS oraz innymi przepisami dotyczącymi bezpieczeństwa (np. HIPAA, CIPA, SOX, GLB/GLBA, PSN CoCo)

Pełna lista korzyści na stronie:
www.gfi.com/languard

Wymagania systemowe

Windows Server 2003, 2008/2008 R2, 2012 oraz Windows XP (SP 2), Vista, 7, 8.
Microsoft .NET Framework 3.5
W przypadku skanowanych urządzeń Mac: system operacyjny Mac OS X w wersji 10.5 lub wyższej.
Zarządzanie poprawkami jest możliwe w następujących dystrybucjach Linuksa: RedHat Enterprise Linux 5 +, CentOS 5 +, Ubuntu 10.04 +, Debian 6 +, OpenSuse 11.2 +, SUSE Linux Enterprise 11.2 + oraz Fedora 19 +.
Powłoka Secure shell (SSH) – wymagana dla urządzeń opartych na platformie UNIX; stanowi część większości najpopularniejszych dystrybucji Linuksa.

Zarządzanie poprawkami

GFI LanGuard pozwala na kompleksowe zarządzanie poprawkami zabezpieczeń i poprawkami niezwiązanymi z zabezpieczeniami, przeznaczonymi dla systemów operacyjnych firmy Microsoft, systemu Mac OS X, głównych dystrybucji Linuksa oraz aplikacji firm trzecich. Umożliwia także automatyzację instalacji poprawek dla wszystkich głównych przeglądarek internetowych.

GFI LanGuard obsługuje wiele aplikacji firm trzecich, w tym m.in. Apple QuickTime®, Adobe® Acrobat®, Adobe® Flash® Player, Adobe® Reader®, Shockwave® Player, Mozilla Firefox®, Mozilla Thunderbird® oraz Java™ Runtime.

Skanowanie podatności na zagrożenia

W ramach audytów bezpieczeństwa wykonywanych jest ponad 50 tys. sprawdzeń podatności z wykorzystaniem obszernej, profesjonalnej bazy zagrożeń, wykorzystującej standardy OVAL (ponad 10 000 sprawdzeń) oraz SANS Top 20.

Innowacyjna technologia agentowa pozwala rozłożyć obciążenie wynikające ze skanowania i usuwania podatności na wiele urządzeń. Jest to szczególnie przydatne w przypadku sieci korporacyjnych.

Mechanizm skanowania obsługuje wiele platform (Windows, Mac OS, Linux™), a także maszyny wirtualne. Ponadto GFI LanGuard potrafi sprawdzać bezpieczeństwo smartfonów, tabletów, drukarek, przełączników oraz routerów różnych producentów, w tym HP, Cisco®, 3Com, Dell, SonicWALL, Juniper, NETGEAR, Nortel, Alcatel, IBM oraz Linksys.

Graficzny, ważony wskaźnik poziomu zagrożenia w intuicyjny sposób przedstawia podatność infrastruktury na zagrożenia. Wykryte podatności można usunąć, zignorować, zaakceptować lub zaklasyfikować jako normalne zjawisko.

Audyt sieci

Po przeskanowaniu sieci pod katem podatności na zagrożenia oraz zainstalowaniu poprawek można skorzystać z funkcji audytu, aby uzyskać szczegółowe informacje na temat stanu bezpieczeństwa sieci.

Audyt może obejmować sprawdzenie podłączonych urządzeń USB, smartfonów i tabletów, rodzajów i wersji oprogramowania, liczby udostępnionych zasobów, otwartych portów, słabych haseł, nieaktywnych użytkowników lub grup oraz stanu bezpieczeństwa systemów linuksowych w sieci.

Inne funkcje:

Aplikacja GFI LanGuard pozwala korzystać z zaawansowanego panelu nawigacyjnego, który przedstawia pełne zestawienie informacji o stanie bezpieczeństwa sieci. Integracja z ponad czterema tysiącami aplikacji o krytycznym dla bezpieczeństwa znaczeniu gwarantuje wykorzystanie najnowszych aktualizacji oraz definicji.

GFI LanGuard pozwala też tworzyć szczegółowe raporty, w tym raporty techniczne, zarządcze oraz dotyczące zgodności z konkretnymi normami (m.in. PCI-DSS, HIPAA, CIPA oraz SOX).

Aplikacja obsługuje funkcję Wake-on-LAN. Może uruchamiać urządzenia przed skanowaniem i wyłączać je po zakończeniu skanowania, tym samym oszczędzając energię i zapewniając maksymalną wygodę.

Szybkie linki:

Obsługiwane systemy operacyjne: www.gfi.com/languard-supported-os/
Obsługiwane aplikacje: www.gfi.com/languard-supported-apps/
Obsługiwany sprzęt: www.gfi.com/languard-supported-devices/

SUNCAPITAL
ul. Ołtaszyńska 92C/6
Wrocław, 53-034
Tel.: +48 (0) 71 360-81-00
Fax: +48 (0) 71 794-93-76
sprzedaz@suncapital.pl