

از امنیت بالای وب لذت ببرید

راهکارهای کنترل دسترسی به اینترنت،
پالایش وب و پالایش اینترنت

کیفیت در فیلترینگ وب
امنیت جامع وب
قیمت عالی
هزاران مشتری

عادت های وب گردی کاربران را کنترل کرده و بر دانلودهای آنها بصورت بلادرنگ نظارت نمایید

تحقیقی که توسط موسسه IDC صورت گرفته است نشان می دهد ۴۰٪ از دسترسی کارکنان به اینترنت ربطی به کار آنها ندارد. از آنجا که قطع کامل اینترنت در ادارات عملی نمی باشد، نرم افزارهای کنترل دسترسی و نظارت بر اینترنت مدیران شبکه را قادر می سازند استفاده های متفرقه از اینترنت را کاهش دهند. GFI WebMonitor با ارائه توانایی کنترل و نظارت بر دسترسی کاربران بصورت بلادرنگ به شما کمک می کند که کارایی کارکنان سازمان را ارتقا بخشیده و به شما اطمینان خواهد داد که فعالیت های وب گردی کارکنان در ارتباط با نیازهای کسب و کار بوده و کلیه فایل های دانلود شده عاری از ویروس و دیگر بدافزارها می باشند.

GFI WebMonitor از پایگاه داده دسته بندی وب سایتها بنام WebGrade استفاده می کند که با استفاده از آن می توانید گروه های مختلف وب سایت مانند بزرگسالان، بازی های آنلاین، ایمیل های شخصی، وب سایت های مسافرتی، شبکه های اجتماعی را کنترل و دسترسی به آنها را محدود کنید. این پایگاه داده عظیم بیش از ۲۸۰,۰۰۰,۰۰۰ آدرس اینترنتی را شامل می شود که بصورت روزانه نیز بروز رسانی می گردد.

مزایا

- افزایش بهره وری با کنترل عادات وبگردی کارکنان
- تدوین و اجرای سیاست های مصرف اینترنت متمرکز
- بیشینه کردن استفاده از پهنای باند از طریق سهمیه زمانی پهنای باند و نگهداری موقت صفحات
- محافظت بلادرنگ از شبکه در برابر دانلودهای خطرناک از طریق چند موتور آنتی ویروس
- جلوگیری از نشت اطلاعات از طریق وب سایت های مهندسی اجتماعی
- بررسی ترافیک رمز شده HTTPS به منظور امنیت بیشتر
- کمک به اجرای مسئولیت های قانونی

صرف اینترنت در شبکه خود را نظارت، کنترل و ایمن نمایید
با استفاده از GFI WebMonitor شما می توانید:

- « بر وب گردی و دانلودهای کاربران از طریق گزارش های تعاملی و چند سطحی نظارت نمایید.
- « مصرف اینترنت کاربران را کنترل کرده و بهره وری کارکنان را از طریق محدود کردن دسترسی به وب سایت های غیر کاری افزایش دهید.
- « زیرساخت شبکه خود را از طریق اطمینان از عاری بودن فایل های دانلود شده از ویروس، جاسوس افزار و دیگر بدافزارها ایمن نمایید.

GFI WebMonitor در سه نسخه در دسترس است:
نسخه Web Filter:

شامل امکان کنترل وبگردی کاربران بر اساس سهمیه زمانی و پهنای باند و همچنین فیلترینگ صفحات وب بر اساس آدرس URL و دسته بندی وب سایت ها می شود.

نسخه WebSecurity:

شامل کنترل و پوشش وجود ویروس در فایل های دانلود شده از طریق چند موتور ضد ویروس و ضد phishing و کنترل MSN/Live مستر می باشد.

نسخه UnifiedProtection:

شامل ادغام دو نسخه WebFilter و WebSecurity می باشد.

ویژگی هایی که در تمام نسخه ها در دسترس می باشند:

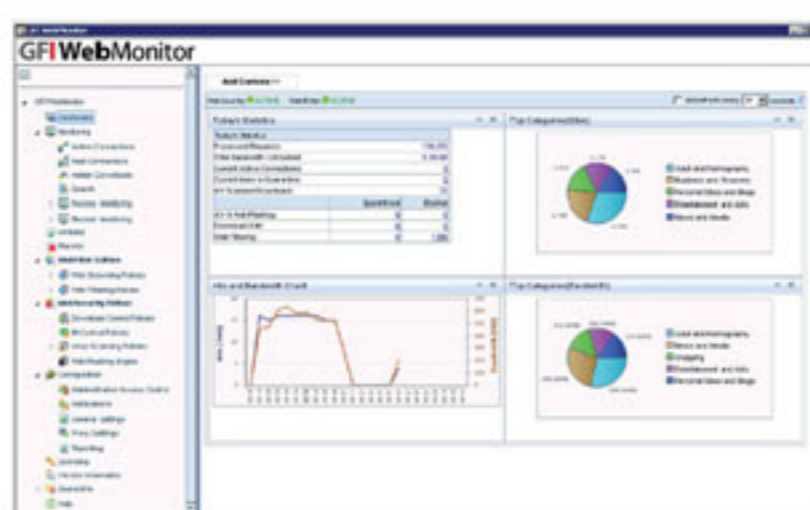
- « امکان دسترسی کنترل شده به واسط پیکربندی و نظارت برنامه.
- « نظارت یا قطع دسترسی یک ارتباط بصورت بلادرنگ.
- « نظارت یا قطع دانلود پنهان برنامه های کاربردی.
- « امکان تعریف فهرست سفید و فهرست سیاه.
- « امکان تعریف استثنائات در سیاست ها
- « پوشش HTTPS
- « ذخیره سازی صفحات وب
- « پنهان سازی اطلاعات شخصی
- « پشتیبانی از محیط های مجازی

نسخه WebFilter

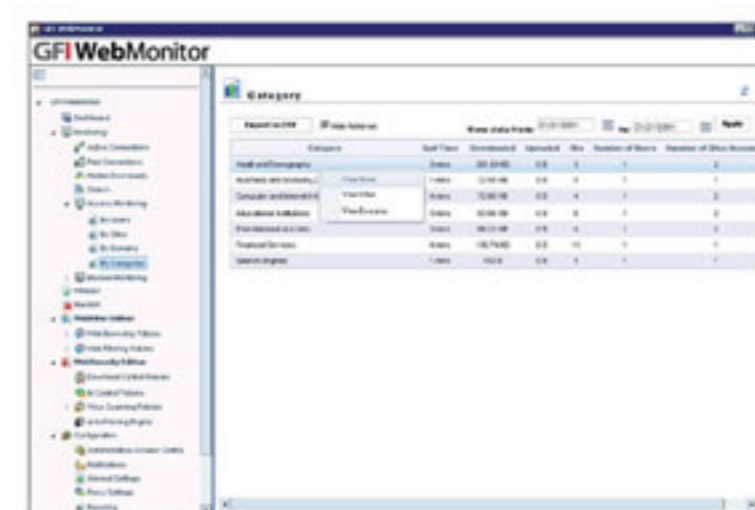
اعمال سیاست های فیلترینگ صفحات وب با دسته بندی بیش از ۲۶۰ میلیون آدرس URL

با استفاده از GFI WebMonitor می توانید سیاستهای فیلترینگ وب متفاوتی تعریف نموده و به کاربران اجازه دسترسی به وب سایت های مختلف را بر اساس آدرس IP یا شناسه کاربری بدهید یا ندهید. دسته بندی وب سایت ها با استفاده از پایگاه داده WebGrade صورت می پذیرد که تعداد بسیاری از URL ها در زبانهای مختلف را شامل شده و بیش از ۲۸۰ میلیون دامنه مختلف را پوشش می دهد. با توجه به تغییر مداوم طبیعت وب، در صورت مشاهده URL هایی که در پایگاه داده محلی دسته بندی نشده اند، GFI WebMonitor درخواستی مبنی بر دسته بندی این URL ها را به سرورهای GFI ارسال می کند. در صورت شناسایی یک URL دسته بندی نشده، آدرس آن پردازش شده و به پایگاه داده افزوده می گردد.

نرم افزار GFI WebMonitor همچنین در نسخه GFI WebMonitor for ISA/TMG به عنوان یک نسخه اختصاصی برای Microsoft ISA/TMG Server در دسترس می باشد.



GFI WebMonitor dashboard



Granular monitoring of Internet access

اعمال سیاست های وبگردی بر اساس سهمیه بندی پهنای باند و زمان

همچنین با استفاده از این ابزار قادر خواهید بود سیاست های وبگردی را با توجه به سهمیه بندی زمانی و پهنای باند بر اساس شناسه کاربری یا آدرس IP کاربران خود پیاده سازی نمایید. برای مثال، می توانید به یک کاربر امکان مرور وب سایت های خبری تا یک ساعت در روز یا دانلود حداکثر 100MB در هفته را بدهید. این قبیل سیاست ها برای وب سایت های خاص یا برای دسته ای از وب سایتها قابل تعریف و اجرا می باشند.

اعمال جستجوی ایمن

با استفاده از GFI WebMonitor این امکان وجود دارد که جستجوی ایمن در موتورهای جستجو را بصورت اجباری به اجرا گذاشت. این گزینه معمولاً در سطح کاربر قابل تنظیم بوده و کاربر می تواند این امکان را غیرفعال نماید، در عین حال در زمان فعال سازی این امکان تنظیمات شخصی کاربر باطل شده و تنظیمات بکار رفته توسط مدیر سیستم فعال می گردند.

نسخه WebSecurity

اعمال سیاست های کنترل دانلود کاربران بر اساس شناسه کاربری / شناسه گروه / آدرس IP و نوع فایل ها

شما می توانید با توجه به سیاست های امنیتی سازمان مطبوع خود، چندین سیاست کنترل دانلود فایل بر اساس شناسه کاربری / شناسه گروه / آدرس IP تعریف نمایید. برای مثال مدیر شبکه می تواند سیاستی تعریف نماید که طی آن کارمندان قادر به دانلود فایل های اجرایی، آرشو های ZIP، فایل های تصویری و فایل های صوتی نباشند.

محافظت در برابر فیشینگ

تمامی وب سایت هایی که کاربر سعی بر دسترسی به آنها را دارد، می توانند بوسیله یک پایگاه داده حاوی URL های وب سایت های فیشینگ که بصورت خود کار بروز می شوند مورد بررسی قرار گیرند. در صورتی که وب سایت درخواستی در فهرست URL های فیشینگ یافت شد، مسدود شده و پیغامی در این زمینه به کاربر نمایش داده می شود.

کنترل MSN

از طریق اعمال سیاست های کنترل IM می توانید پیام ها و فایل های ورودی / خروجی Live Messenger را نظارت و مسدود نمایید.

نسخه UnifiedProtection

نسخه UnifiedProtection ترکیبی از تمامی امکانات دونه نسخه WebFilter و WebSecurity را در خود دارد

نیازمندی های سیستم :

- « Windows Server 2003/2008, Windows XP/Vista/7
- « Internet Explorer 7 or later
- « .NET Framework 2.0 or later

نیازمندی های سیستم برای ISA/TMG Server

- « ISA Server 2004/2006/Forefront TMG
- « Internet Explorer 7 or later
- « .NET Framework 2.0 or later

Download your free trial from <http://www.gfi.com/webmon>



GFI WebMonitor™
Web security, monitoring and Internet access control

GFI WebMonitor™
Web security, monitoring and Internet access control



نظارت بر سلامت سیستم

قوانین و ملاحظات قانونی

بازرسی های
جرم شناسانه

امنیت شبکه و
سیستم های اطلاعاتی

افزایش uptime

امنیت مضاعف

قیمت رقابتی

داده ها را نظارت کنید، تحلیل و نظارت داده ها آسان خواهد شد.

حجم زیادی از اطلاعات تولید شده فایل های ثبتی سیستمی (لاگ: log) برای مدیران سیستم منبعی از اطلاعات پربهاست، یک مدیریت کارآمد ضمن اینکه بر قابلیت های یک سازمان می افزاید به قابلیت اطمینان شبکه، سیستم های منبع و در دسترس بودن بالای آن ها کمک می کند. به منظور دستیابی به امنیت کافی، اعتبار و تداوم کسب و کار به تحلیل و مدیریت اطلاعات log یک شبکه گسترده در زمان واقعی نیاز است اما صدها و هزاران مدخل log هر روز تولید می شود که مدیریت آن ها کاری چالش زا است.

GFI EventsManager باعث تسهیل در کارهای مدیریت و کاهش هزینه ها می گردد. این ابزار با جمع آوری، به نظم درآوردن، تحلیل، طبقه بندی و یکپارچه سازی اطلاعات log از تمامی منابع شبکه، میزان فعالیت و بروز ماندن سیستم ها را افزایش می دهد. همچنین این سیستم با مدیریت عملکردهای و زیرساخت IT به صورت تحلیل فعال و در زمان واقعی، مدیریت این وظایف عظیم را امکان پذیر می سازد و باعث واکنش سریع تر و هدفمندتر به مسائل و مشکلات برخاسته از این وظایف می گردد. در هم آمیختگی به خصوص تحلیل اطلاعات log با مدیریت فعال IT نه تنها نوع مشکلات را به شما نشان می دهد بلکه به شناسایی دلیل بروز مشکلات از یک کنسول مشابه نیز کمک می کند.

مزایا

« حفاظت از سیستم به واسطه شناسایی و تحلیل حوادث امنیتی به وقوع پیوسته در تحلیل اطلاعات log

« ارتقاء امنیت به واسطه مدیریت اقدامات، مکانیسم ها و اپلیکیشن های مرتبط با امنیت

« کاهش هزینه ها و افزایش بهره وری به واسطه مدیریت اتوماتیک IT

« شناخت و درک حوادث رخ داده در فضای IT سیستم شما

« فعال و بروز نگه داشتن شبکه و شناسایی مشکلات مربوط به داشبورد و هشدارهای زمان واقعی

« کمک به آرشیو منظم وظایف از طریق سرور SQL، بازبینی های Oracle و SNMPTrap که توسط سرورها، مسیر یاب ها، فایروال ها، سویچ ها، سیستم های تلفن، PC ها و غیره بوجود آمده اند.

« نظم درونی این سیستم طبقه بندی، مدیریت و هشداردهی خارج از عرف مربوط به اطلاعات log را امکان پذیر می سازد.

امدادهای GFI EventsManager

- « جمع آوری اطلاعات از تمامی منبع مجازی به صورتی کاملاً جزئی و عمیق
- « دستیابی به جزئیات اطلاعات مربوط رویدادهای فضاهای مختلف به کمک انواع log های پشتیبانی شده
- « ردیابی و گزارش دهی در خصوص فعالیت های سرور Oracle و SQL مانند تغییر تبیل های DB، تلاش جهت دستیابی به اطلاعات بدون نیاز به امتیازات به خصوص
- « فراهم آوردن منابع اطلاعاتی قابل اعتماد جهت بررسی موارد چالش آفرین

GFI EventsManager جهت مدیریت رویدادها و اطلاعات امنیتی

GFI EventsManager توانایی تحلیل اطلاعات log امنیتی در زمان واقعی را دارا می باشد. از این روش شما قادر خواهید بود حوادث امنیتی را شناسایی کرده و به منظور پیدا کردن فرد مسئول، به تحلیل جزئیات بدست آمده بپردازید. در همین زمان، شما می توانید بر ساختار، موجودیت و عملکرد خدمات، اپلیکیشن ها و مکانیسم های امنیتی و همچنین فعالیت های کاربران نظارت کنید.

GFI EventsManager برای نظارت و مدیریت بر عملکردها و زیرساخت IT

به کمک GFI EventsManager شما قادر خواهید بود در دسترس بودن، عملکرد، کاربری و اجرای کل زیرساخت IT شامل پروتکل های شبکه، ابزارهای شبکه، زیرساخت شبکه، سرورها، خدمات، اپلیکیشن ها را در زمان واقعی و از یک کنسول واحد را به طرز فعالانه ای تحت مدیریت قرار دهید. همچنین شما توانایی مدیریت فایروال ها، سنسورها، مسیر یاب ها و اتفاقات به وقوع پیوسته توسط سرور Microsoft ISA، SharePoint، Exchange Server، SQL Server و IIS و جلوگیری از رویداد حوادث شبکه را دارا خواهید بود. برای مثال شما می توانید ایمیل ها، درگاه های SMTP، موجود بودن MAPI، بلاک های نامطلوب هارد دیسک، فضای دیسک را غیره را نیز تحت مدیریت خود در آورید.

ادغام یکپارچه و منسجم نظارت فعال IT و تحلیل اطلاعات log امتیازات منحصر به فردی همراه خود دارد. در این حالت نه تنها شما از زمان بروز مشکلات (از طریق نظارت فعال IT) آگاه خواهید شد بلکه می توانید در سریع ترین زمان ممکن دلایل بروز مشکلات (از طریق تحلیل log) در یک کنسول واحد را شناسایی نمایید.

GFI EventsManager برای پاسخ دهی منظم

GFI EventsManager با ارائه مجموعه اطلاعات log، نظم دهی و انسجام چند لایه ای نقش مهمی در زمینه بازایی اطلاعات موجود log و نیازمندی های مربوط به نظارت های سازمانی قانون گذار به شرح زیر ایفا می کند:

Basel II، استاندارد امنیتی داده های PCI، قانون Sarbanes-Oxley، قانون GrammLeach-، قانون Billiey، FISMA، قانون ۱۹۹۹ USA Patriot، Turnbull Guidance، قانون حفاظت از اطلاعات انگلستان، EU DPD.

System requirements

- » Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, Windows Server 2012
- » .NET framework 2.0
- » Microsoft Data Access Components (MDAC) 2.8 or later

GFI EventsManager برای نظارت های قانونی

زمانی که روند منظم کارها از مسیر خود خارج می شود و در زمان نیاز به بررسی های قانونی در دعوی قضایی که ساز و کارهای الکترونیک را در برمی گیرد اطلاعات log می تواند منبع رجوع بسیار مهمی باشد و سوابق اطلاعات مربوط به کاربری های سیستم های الکترونیک را به تفصیل ارائه نماید. قابلیت GFI EventsManager در ارائه اطلاعات log کل شبکه جهت بررسی های قانونی که به صورت زمانبندی ساعتی قابل انجام است شما را از هزینه های بازبینی و مشاوره های پرهزینه خارج از سازمان معاف می کند.

نظارت عمقی و جزئی بر رویدادها

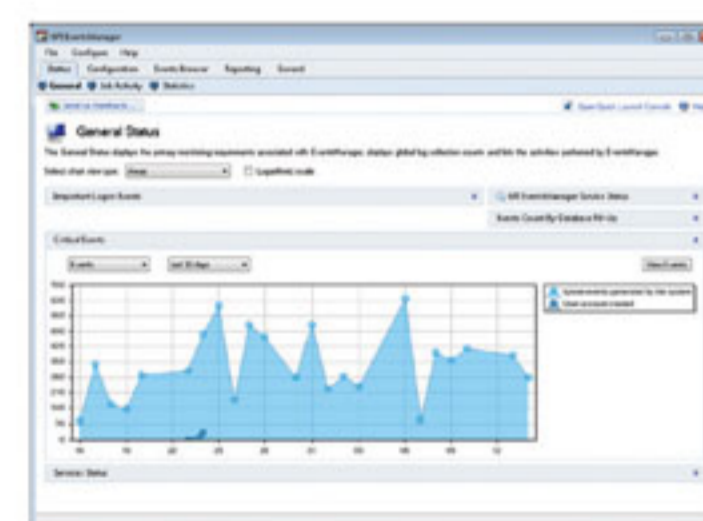
GFI EventsManager جهت نظارت بر طیف گسترده ای از ابزارها و سیستم ها از طریق logging متمرکز و تحلیل انواع log به کمک شما می آید. مدیران سیستم می توانند اطلاعات را در تفصیلی ترین حالت ممکن جمع آوری کرده و با تحلیل آن ها، بدون نیاز به هرگونه اطلاعات اضافی تصمیمات خود را اتخاذ نمایند.

تحلیل اطلاعات log شبکه گسترده

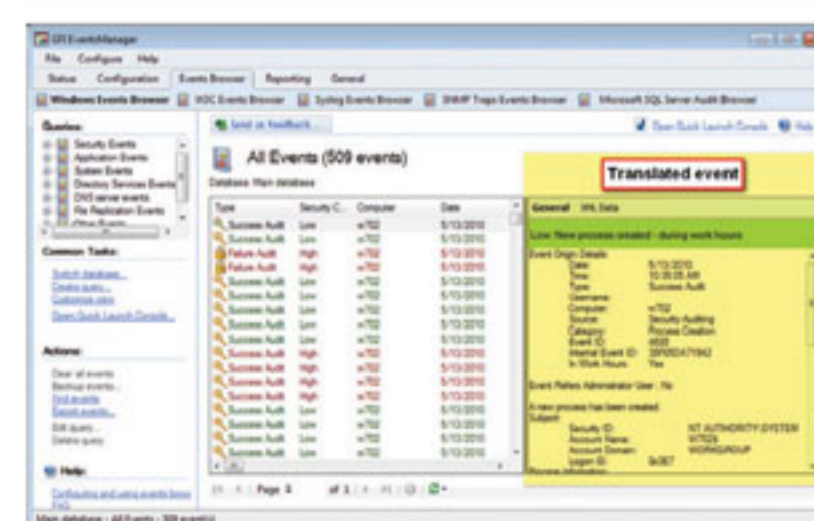
شما به عنوان یک مدیر شبکه در خصوص log های پنهان و انبوه که تحلیل اطلاعات log را به کاری ماجراجویانه تبدیل می کند از تجربه لازم برخوردار هستید. GFI EventsManager امکان مدیریت و کنترل اطلاعات log ورودی از سرورهای شبکه گسترده (ویندوز، لینوکس/یونیکس، AIX، سیستم عامل مک و غیره)، سرورهای گوناگون (سرورهای وب، سرورهای دیتابیس، سرورهای فایل، سرورهای اپلیکیشن، سرورهای دسترسی از راه دور، سرورهای مجازی سازی و غیره)، اپلیکیشن ها (هر اپلیکیشن که log های متنی بوجود می آورد)، ابزارهای زیرساخت شبکه (مسیر یاب ها، سویچ ها، فایروال ها)، ابزارهای امنیتی شبکه (IDS، راهکارهای IPS)، ابزارهای عمومی شبکه (هر ابزار مجهز به SNMP) را امکان پذیر می سازد.

سایر مشخصه ها:

- « هشداردهی و نظارت بر اطلاعات log در زمان واقعی به صورت ۲۴ ساعت روز، هفت روز هفته و ۳۶۵ روز سال
- « موتورهای قدرتمند جستجو و اسکن اطلاعات
- « دسترسی جزئی، بازبینی شده و کنترل شده به اطلاعات log
- « جمع بندی اطلاعات log توزیع شده در یک WAN به درون دیتابیس و یا آرشیو اتوماتیک تمامی مدخل های log
- « مدیریت اطلاعات log مرتبط با مسائل قانونی
- « داشبورد قدرتمند
- « نسخه های فیلترینگ پیشرفته رویدادهای شامل قانون یک کلیک و تعریف فیلتر
- « گزارشهای اطلاعات کلیدی امنیت که در شبکه شما اتفاق می افتد
- « پشتیبانی از ابزارهای جدید
- « عملکرد چندگانه جهت پاسخ دهی به نیازمندی های شرکتی متفاوت
- « رفع نویز و اختلالات جزئی
- « برنامه ریزی و توزیع اتوماتیک گزارش ها از طریق ایمیل
- « رویدادها قابل تبدیل به فایل های HTML می باشند
- « پشتیبانی از محیط های مجازی



GFI EventsManager management console



Makes cryptic logs easier to understand

Download your free trial from <http://www.gfi.com/faxmaker>



GFI EventsManager

Log data analysis and IT management



GFI EventsManager

Log data analysis and IT management

GFI LanGuard®

سه آرزوی شما را بر آورده می کند:

«مدیریت وصله های امنیتی
«ارزیابی آسیب پذیری ها
«بازرسی شبکه



حفظ امنیت شبکه
متناسب با نیازهای شما
افزایش کارایی

GFI LanGuard مشاور امنیت مجازی شما

GFI LanGuard به شما امکان می دهد تا آسیب پذیری های شبکه را پوشش، شناسایی، ارزیابی و اصلاح نموده و با کمترین مشکلی شبکه خود را ایمن نمایید. همچنین این ابزار به شما امکان می دهد تصویر کاملی از وضعیت شبکه خود به دست آورده و هر چه سریعتر و موثر تر به شبکه ای امن تر دسترسی پیدا کنید.

GFI LanGuard راهکاری است که تاکنون موفق به اخذ جوایز بسیار از مراجع معتبر مختلف گشته و به وسیله هزاران مشتری در سراسر دنیا مورد استفاده قرار گرفته است.



مزایا

- « امنیت شبکه جامع و فراگیر
- « نصب خودکار وصله های امنیتی محصولات مایکروسافت، MacOS و دیگر برنامه های کاربردی
- « اجرای بیش از ۵۰۰۰۰ ارزیابی امنیتی در سراسر شبکه شامل کامپیوترها، چاپگرها، روترها، سوئیچ ها و حتی محیط های مجازی
- « امکان انتشار اسکریپت و نصب نرم افزارهای اختصاصی در سطح شبکه
- « با ارائه گزینه های اجرای عملیات بصورت خودکار به شما کمک می کنند حفاظت از امنیت شبکه با کمترین زحمت مدیریتی اجرا شود
- « به حداقل رساندن زمان
- « کمک به مدیران جهت انطباق با استاندارد PCI DSS و دیگر قوانین امنیتی بین المللی نظیر (HIPAA, SOX, GLB, GLBA), e.g., (GCSx CoCo)
- « کاهش مجموع هزینه های خرید و مالکیت نرم افزارهای امنیتی با قیمت های کاملا رقابتی
- « متمرکز سازی پوشش آسیب پذیری های شبکه، مدیریت وصله های امنیتی و بازرسی شبکه در یک ابزار

مدیریت وصله های امنیتی

GFI LanGuard شبکه شما را پوشش کرده و تمام عملکرد و ابزارهای لازم جهت نصب و مدیریت وصله های نرم افزاری در خصوص نسخه های مختلف سیستم عامل ها و محصولات مایکروسافت را ارائه می دهد. همچنین GFI LanGuard امکان دانلود و نصب خودکار وصله های نرم افزاری و همچنین بازگرداندن حالت برنامه کاربردی به زمان قبل از نصب وصله های نرم افزاری نصب شده را فراهم می نماید. می توانید این ابزار را به شکل سفارشی نیز اجرا نمایید که نتیجه آن برخورداری مداوم از محیطی پیکربندی شده و ایمن در برابر آسیب پذیری ها خواهد بود.

GFI LanGuard امکان مدیریت وصله های نرم افزاری را برای برنامه های کاربردی غیر مایکروسافتی نیز فراهم آورده و مدیران شبکه را قادر می سازد به همان روشی که برای نرم افزارهای مایکروسافتی به کار می گیرند وصله های نرم افزاری را برای نرم افزارهای پشتیبانی شده توسط GFI LanGuard، شناسایی، دانلود و نصب نمایند. GFI LanGuard مدیریت وصله نرم افزاری را برای بسیاری از برنامه های کاربردی عمومی نظیر Apple Quicktime, Adobe Acrobat, Adobe flash player, Adobe Reader, Mozilla Firefox, Java Runtime و ... پشتیبانی می نماید.

برای داشتن فهرستی از این اطلاعات به آدرس زیر مراجعه فرمائید:
<http://kbase.gfi.com/showarticle.asp?id=KBID003469>

همچنین GFI LanGuard بصورت خودکار بروز رسانی وصله های نرم افزاری مرورگرهای وب اصلی از قبیل Apple Safari, Google Chrome, Mozilla Firefox, IE و Opera که روی سیستم عامل های ویندوز کار میکنند را انجام می دهد.

ارزیابی آسیب پذیری ها

طی بازرسی های امنیتی انجام شده که به وسیله پایگاه داده بسیار گسترده و قوی از آسیب پذیری های امنیتی با همکاری استانداردهای OVAL (بیش از ۵۰۰۰ آزمون) و SANS Top 20 صورت گرفت، بیش از ۵۰۰۰۰ آسیب پذیری مشخص گردید.

استفاده از این ابزارها امکان اسکن توزیع شده را روی ماشین های مختلف فراهم می آورد. البته به دلیل پراکنده بودن آسیب پذیری ها هم این روش، روشی مطلوب خواهد بود. به ویژه در شبکه های بزرگ و سازمان هایی با سایت های چندگانه.

قابلیت انجام چند پوشش همزمان (Windows, Mac, Linux) در همه محیط های ممکن از جمله محیط های مجازی فراهم است ضمن آنکه به غیر از کامپیوترها، چاپگرها، سوئیچ ها و روترها از محصولات شرکت هایی مانند پی بی و سیسکو نیز اسکن می شوند. قابلیت اجرای آزمون آسیب پذیری

با استفاده از صفحات تنظیم بسیار ساده و امکان تعریف گروه بندی دستگاه ها و گروه بندی آزمون ها از دیگر امکانات این برنامه است.

قابلیت ایجاد انواع مختلفی از پوشش ها و آزمون های امنیتی به سادگی، ارائه شاخص گرافیکی تعیین کننده سطح مخاطره پذیری که وضعیت آسیب پذیری کامپیوتر یا کامپیوترهای پوشش شده را از طریق ارائه نتایج ارزیابی بصورت درجه بندی شده و بصری فراهم می کند نیز از دیگر امکانات قابل ذکر است.

بازرسی شبکه

پس از اینکه شبکه را برای یافتن آسیب پذیری ها پوشش نمودید و وصله های امنیتی را روی سیستم ها نصب کردید می توانید از قابلیت بازرسی GFI LanGuard به منظور یادگیری هرچیز در خصوص وضعیت امنیتی شبکه از قبیل USB ها و دیگر ابزارهای قابل حملی در شبکه موجود هستند و یا نرم افزارهایی که در شبکه نصب شده اند (مجاز و غیر مجاز) قابلیت بازرسی سخت افزاری گسترده، تعداد فایل های به اشتراک گذاشته شده، پورت های باز، کلمات عبور ضعیف، کاربران و گروه های بلا استفاده و وضعیت امنیت سیستم های لینوکس در شبکه خود استفاده نمایید.

دیگر ویژگی ها:

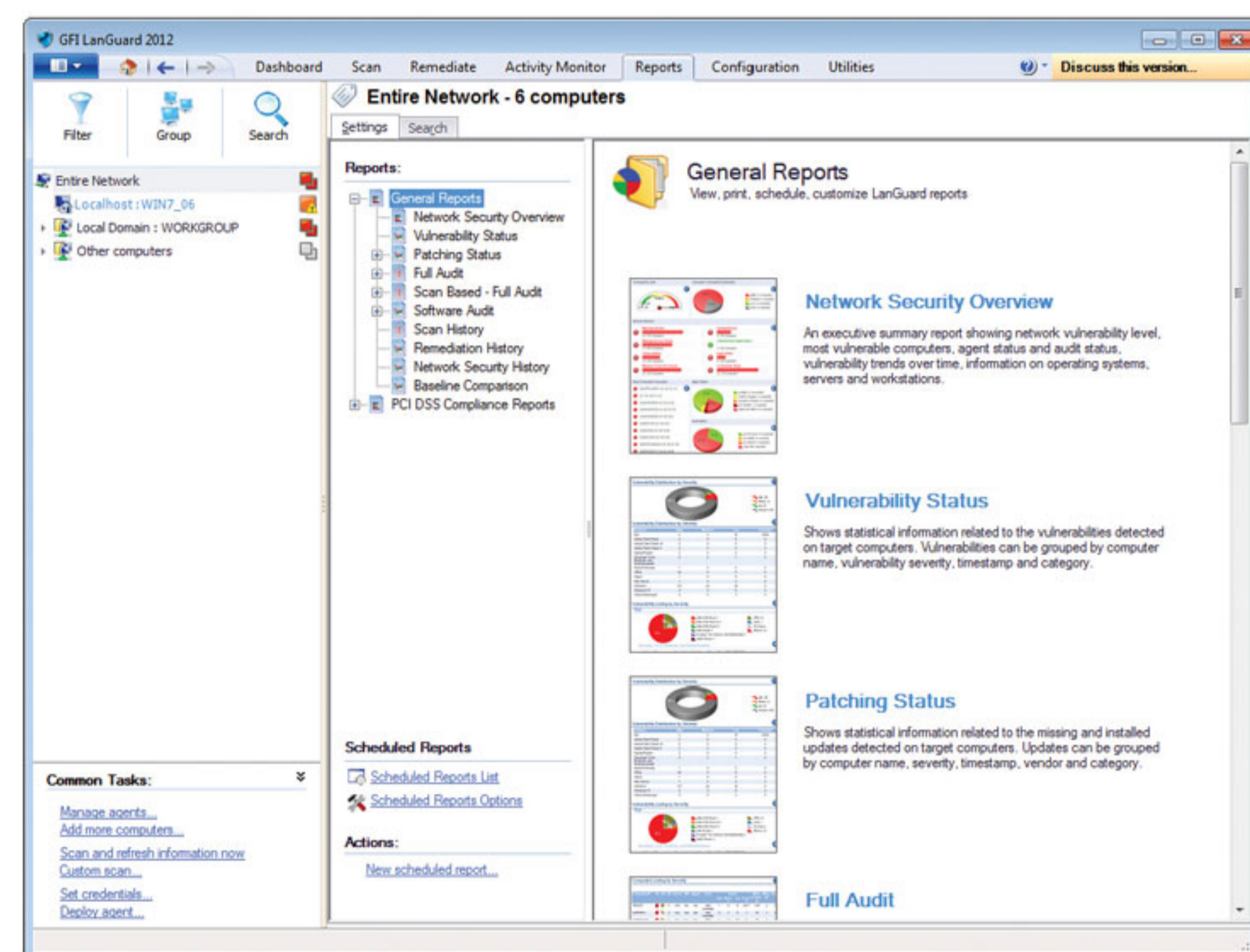
- « ادغام با بیش از ۲۵۰۰ برنامه کاربردی امنیتی حیاتی.
- « دارای یک داشبورد قدرتمند که بازرسی های امنیتی را به منظور ارائه یک نتیجه کلی در خصوص وضعیت امنیت شبکه پردازش می نماید.
- « گزارش های تشریحی شامل اطلاعات مدیریتی و مقایسه ای و منطبق بر استانداردهایی نظیر SOX و HIPAA و PCI-DSS.
- « پشتیبانی از Wake-on-LAN، روشن کردن کامپیوتر و خاموش کردن آن برای اسکن و صرفه جویی در انرژی.

امکانات مورد نیاز:

- « Microsoft Windows 7, server 2008 R2, Visat, 2003, XP (SP2)
- « Microsoft .NET Framework Version 3.5
- « Secure Shell (SSH) – required for UNIX-Based scan targets; this is included by default in all major Linux OS distributions.



GFI LanGuard dashboard



GFI LanGuard reporting

نرم افزار با زبان کشورهای زیر در دسترس می باشد



Download your free trial from <http://www.gfi.com/languard>



راهکار جامع ضد هرزنامه و امنیت ایمیل برای شرکت های کوچک و متوسط



پالایش ضد هرزنامه چند لایه

امنیت ایمیل با موتور
ضد ویروس چندگانه

قیمت رقابتی

حفاظت از شبکه در مقابل هرزنامه ها و سایر ویروس ها و تهدیدات سایبری

موثر ترین راه مقابله با ارسال کنندگان هرزنامه استفاده از GFI MailEssentials به عنوان یک راهکار ضد هرزنامه برجسته می باشد. این ابزار با استفاده از دو موتور ضد هرزنامه و با کمترین نیاز به پیکربندی تخصصی امکان شناسایی و جلوگیری بیش از ۹۹٪ هرزنامه ها را به مدیر شبکه می دهد. همچنین این ابزار از قیمت بسیار مناسبی نیز سود می برد.

مدیران شبکه می توانند مطمئن باشند که نرخ شناسایی هرزنامه در این ابزار با بیشترین نرخ ممکن خواهد بود. همچنین GFI MailEssentials نرخ تشخیص اشتباه پایینی دارد.

GFI MailEssentials می تواند ایمیل های فیشینگ را شناسایی و مسدود نماید و ابزارهای مدیریتی زیر را به سرور ایمیل شما بیفزاید: تکذیب نامه ها (disclaimers)، نظارت بر ایمیل ها، گزارش اینترنتی ایمیل ها، فهرست سرورها، پاسخ خودکار بر اساس سرورها و داندلود POP3.

مزایا

« پشتیبانی از برجسته ترین پلتفرم های انتقال پیام شامل: ۲۰۰۳، ۲۰۰۷، ۲۰۱۰ Microsoft Exchange و Lotus Domino

« نرخ شناسایی هرزنامه بسیار بالا (بیش از ۹۹٪) از طریق استفاده از فناوری های ضد هرزنامه متنوع.

« اسکن ویروس ها با موتورهای ضد ویروس چندگانه

« نصب بر روی سرور بدون نیاز به نصب نرم افزار های سمت کاربر

« راهکار ضد هرزنامه چند لایه با قیمت عالی

GFI MailEssentials دارای سه ویرایش مختلف است:

نسخه UnifiedProtection: نوعی راهکار فراگیر مبتنی بر سرور است که از شبکه شما در برابر هرزنامه، ویروس، و دیگر تهدیدات ایمیلی حفاظت می کند. نرخ کشف هرزنامه این راهکار بیش از ۹۹٪ بوده و حداقل خطای مثبت را داشته و تا پنج موتور آنتی ویروس دارد.
نسخه آنتی اسپم یا ضد هرزنامه: نوعی راهکار ضد هرزنامه و ضد فیشینگ است.
نسخه EmailSecurity: متضمن نوعی امنیت چند لایه در برابر ویروس ها و دیگر بدافزارهای ایمیلی است.

امکانات موجود در نسخه های UnifiedProtection و Anti-Spam

حفاظت کامل در برابر هرزنامه ها

GFI MailEssentials نوعی راهکار ضد هرزنامه گواهی شده توسط VBSpam است که با بکارگیری موتورهای متعدد ضد هرزنامه مانع از هرز رفتن تولید و بهره‌وری کاربران می شود و سطح بالایی از حفاظت در برابر هرزنامه ها را ایجاد می کند.

با مدیریت خود کار لیست سفید تعداد خطاهای مثبت کاهش می یابد

راهکار GFI MailEssentials شامل یک ابزار مدیریتی لیست سفید خودکار مجوز است که اسامی دریافت کنندگان ایمیل را به لیست سفید می افزاید و می توان اسامی موجود در این لیست را بر اساس نام دامنه، آدرس های ایمیلی و کلیدواژه طبقه بندی نمود.

این راهکار از کاربران در برابر تهدید ناشی از ایمیل های فیشینگ حفاظت می کند

ماژول ضد فیشینگ MailEssentials تهدیدات ناشی از ایمیل های فیشینگ را از طریق مقایسه محتوی هرزنامه با پایگاه داده ای URL های فیشینگ که به صورت مستمر به روزرسانی می شوند، شناسایی و مسدود می نماید تا مطمئن شود که تمامی ایمیل های جدید فیشینگ کشف شده اند. این راهکار همچنین کلیدواژه های اصلی فیشینگ را در هر ایمیلی که برای سازمان شما ارسال شود بررسی می کند.

دیگر قابلیت ها:

« موتور ضد هرزنامه SpamRazer

« تکنیک ضد هرزنامه لیست خاکستری برای تشخیص ایمیل های هرزنامه ای نشأت گرفته از سرورهای ایمیلی نامطلق با RFC است.

« فیلترینگ بی‌زین یا اقتصادسنجی: از نوعی راهکار ریاضی مبتنی بر ایمیل های قانونی و هرزنامه های شناخته شده به عنوان روشی مؤثر برای تشخیص هرزنامه استفاده می کند.

« بررسی بلاک لیست دی ان اس های متفرقه (DNSBL)

امکانات موجود در نسخه های UnifiedProtection و EmailSecurity

بررسی ویروس ها از طریق موتورهای اسکن متعدد

GFI MailEssentials از موتورهای آنتی ویروس متعدد برای اسکن کردن ایمیل های دریافتی استفاده می کند که به میزان قابل توجهی متوسط زمان مورد نیاز برای بدست آوردن جدیدترین ویروس ها را کاهش داده و امکان واکنش سریع به تهدیدات و مقابله با آن ها را فراهم می کند. این راهکار از طریق موتورهای آنتی ویروس متعدد شانس بهتری را برای ایجاد سازکار دفاعی مناسب در لحظه مناسب و برای مقابله با جدیدترین حملات فراهم می کند.

مجهز به آنتی ویروس های GFI VIPRE و BitDefender

موتور وایپر با بهره گیری از نوعی فناوری پیشرفته با سرعت بسیار بالا تهدیدات را اسکن نموده و از این طریق حجم بالایی از اطلاعات را برای یافتن تهدیدات بدافزاری در بازه زمانی کوتاه و کمترین اثرگذاری روی عملکرد سیستم کاربران تحلیل می کند. بیت دیفندر نیز نوعی موتور آنتی ویروس بسیار سریع، منعطف و پیشرفته است که قابلیت تشخیص و اسکن نمودن طیف گسترده ای از فرمتها را دارا می باشد. MailEssentials به صورت خودکار فایل های تعریفی بیت دیفندر و وایپر را بررسی و به روزرسانی می کند. علاوه بر این دو، سه موتور دیگر نیز به عنوان امکانات اضافی برای آن در نظر گرفته شده اند.

اسکن تروجان ها و فایل های اجرایی مخرب

اسکنر تروجان و فایل های اجرایی راهکار MailEssentials با استفاده از نوعی هوش داخلی سطح خطر فایل های اجرایی را تخمین می زند که این کار نیز از طریق تجزیه فایل های مذکور و تشخیص عملکرد احتمالی آن به صورت در لحظه انجام می گیرد. در پایان نتایج تحلیل های انجام گرفته با پایگاه داده ای اقدامات مخرب مقایسه شده و فایل های اجرایی با فعالیت مشکوک توسط اسکنر قرنطینه می شود. این فعالیتها می توانند در قالب ارزیابی یک مودم، ایجاد ارتباطات شبکه ای یا ارزیابی دفترچه آدرس ها صورت بگیرند.

دیگر امکانات:

« حذف خودکار دستورات HTML و حفاظت از کاربر در برابر ویروس های HTML و حملات انجام شده از طریق ایمیل های HTML

« با استفاده از اسکنر تروجان و فایل های اجرایی و سازوکارهای کنترل ویروس نورمن، مکافی و کسپرسکی، سیستم شما در برابر نرم افزارهای جاسوسی حفظ خواهد شد تا امنیت در بالاترین سطح ممکن برقرار شود.

« ارسال ایمیل های قرنطینه شده با استفاده از رابط تعدیلگر قدرتمند از هر نقطه ای در شبکه

« امکانات موجود در تمامی نسخه ها

« گزارش دقیق و در لحظه از اطلاعات گرافیکی مبتنی بر وب

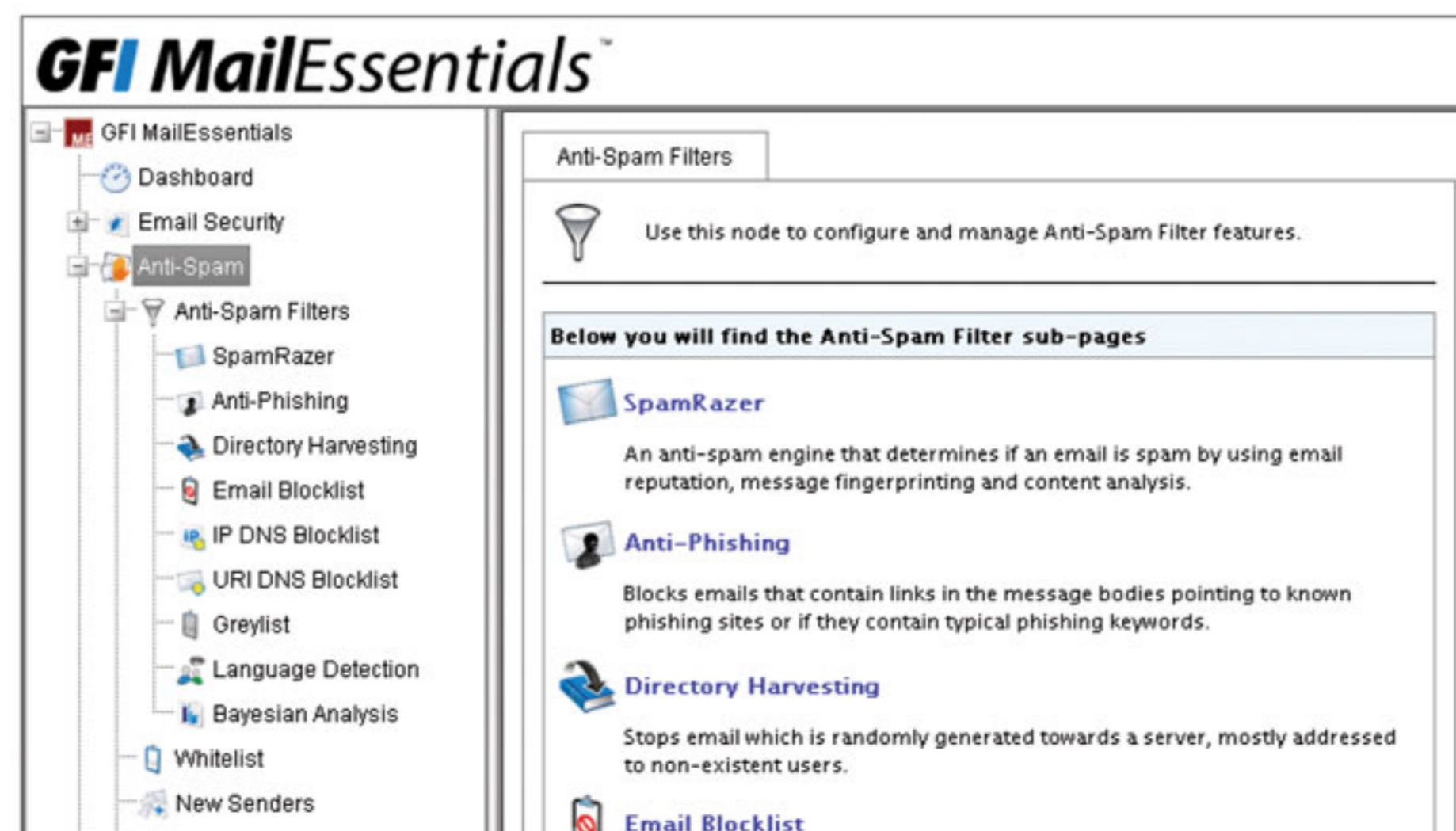
« فیلترینگ پیشرفته محتویات

« پشتیبانی از محیط های مجازی

« تشخیص برنامه های VSAPI ساخته شده توسط شرکت های دیگر

« رابط کاربری مبتنی بر وب

« پشتیبانی کامل از Unicode



GFI MailEssentials anti-spam filters

Download your free trial from <http://www.gfi.com/mes>



GFI MailEssentials™

Anti-spam solution for Exchange/SMTP/Lotus



GFI MailEssentials™

Anti-spam solution for Exchange/SMTP/Lotus

ثبت فعالیت دسترسی حافظه های جانبی به شبکه شما

علاوه بر مسدود نمودن دسترسی به رسانه های ذخیره سازی قابل حمل، GFI EndPointSecurity، کلیه فعالیت های کاربر در رابطه با این ابزارها را به SQL سرور مرکزی و سرور ثبت وقایع ارسال می نماید. هر زمان که کاربر به سیستم وارد می شود، فهرستی از فایل هایی که به آنها دسترسی پیدا می کند تهیه می گردد.



سایر ویژگی ها:

- « نظارت بر شبکه را متمرکز کرده، تجهیزات متصل شده به شبکه را شناسایی نموده و وظایف متنوعی را اجرا می کند.
- « دارای صفحه مخصوص ایجاد خط مشی.
- « امکان گزارش گیری روزانه و هفتگی.
- « امکان محافظت خودکار از دستگاه هایی که به تازگی شناسایی می شوند.
- « قابلیت دریافت و نصب SQL Express در صورت خودکار اگر سرور مرکزی پایگاه داده ها در دسترس نباشد.
- « کنترل دسترسی پیشرفته و ایجاد لیست سیاه و سفید.
- « امکان نظارت و اخطار بلادرنگ.
- « گزارش کامل در خصوص استفاده از دستگاه ها با اضافه کردن GFI Report Back Agent
- « امکان نصب نامحسوس Agent
- « امکان اعطای مجوز موقت دسترسی به دستگاه.
- « بررسی و شناسایی فهرستی از قطعات که قبلاً استفاده شده اند یا در حال استفاده می باشند.
- « Agentهای محافظت شده توسط کلمه عبور از دستکاری تنظیمات ممانعت کرده و از امکان Agent ضد دستکاری در Windows 7 پشتیبانی می کنند.
- « پشتیبانی از Windows 7 BitLocker To Go
- « امکان ارسال پیام های شخصی شده به کاربر در زمان مسدود کردن دسترسی های او.
- « امکان مشاهده فعالیت کاربران و موارد استفاده از دستگاه ها از طریق یک پایگاه داده.
- « امکان پاک کردن اطلاعات قدیمی تر از یک زمان تعیین شده توسط مدیر شبکه.
- « قابلیت دسته بندی کاربران بر اساس گروه، دامین...
- « پشتیبانی از سیستم های عامل در زبانهای رایج
- « و قابلیت های دیگر!...



جلوگیری از سرقت اطلاعات و نفوذ نرم افزار های مخرب در صورت

داشتن نرم افزار امنیتی EndPoint

متأسفانه بیشتر شرکتها تا زمانی که اتفاق بدی برایشان نیفتد از تهدیدات موجود غافل هستند و یا آنها را نادیده می گیرند. با توجه به تحقیق صورت گرفته به سفارش GFI و توسط eMedia در ایالات متحده تعداد بسیار کمی از شرکت های متوسط به تجهیزات و حافظه های قابل حمل به عنوان یک مخاطره بزرگ توجه داشتند در حالی که کمتر از ۲۰٪ از آنها اقدام به پیاده سازی راهکارهای نرم افزاری جهت جلوگیری از این مخاطرات کرده بودند. نکته کلیدی مدیریت دستگاه های جانبی قابل حمل این است که راهکاری امنیتی در نقطه پایانی نصب گردد و امکان کنترل و نظارت در خصوص اینکه کدام دستگاه ها، توسط چه کسانی در حال استفاده هستند یا استفاده شده اند و چه داده هایی به آنها منتقل شده است را به مدیران شبکه بدهد.

استفاده از دستگاه های قابل حمل در شبکه را با GFI EndPointSecurity کنترل نمایید.

GFI EndPointSecurity مدیران شبکه را قادر می سازد دسترسی و ثبت فعالیت کاربران را در خصوص موارد زیر بصورت فعال مدیریت کنند:

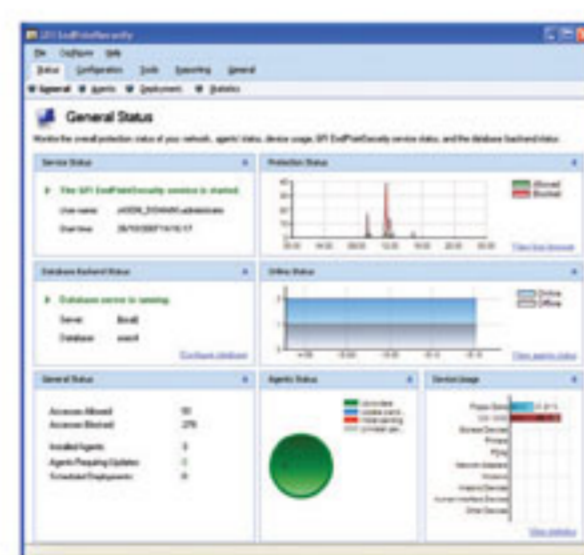
- « پخش کننده های صوتی تصویری از جمله iPod Creative Zen و ...
- « حافظه های USB CompactFlash، کارت های حافظه، لوح فشرده و دیسک ها و دیگر حافظه های جانبی قابل حمل.
- « PDAها، گوشی های موبایل iPhone، تلفن های هوشمند و سایر وسایل ارتباطی مشابه.
- « کارت های شبکه، لپ تاب ها و سایر وسایل ارتباطی در شبکه.

چگونه کار می کند؟

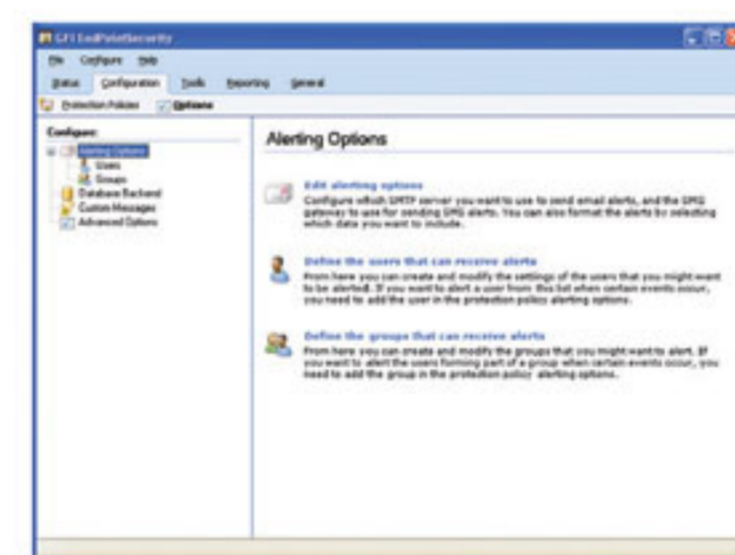
GFI EndpointSecurity به منظور کنترل دسترسی یک Agent کوچک بر روی ماشین مقصد نصب می کند. حجم این Agent تنها 1.2MB بوده و هرگز کاربر از وجود آن با خبر نخواهد شد. همچنین GFI EndpointSecurity از یک ابزار نصب راه دور مبتنی بر فن آوری GFI LanGuard سود می برد که به شما امکان می دهد این Agent را با اجرای چند کلیک در کل شبکه نصب نمایید. پس از نصب Agent Active Directory را مورد بررسی قرار داده و به محض ورود کاربر به سیستم، دسترسی های تعریف شده برای هر کاربر را به آن اعمال می کند. اگر کاربر جزو گروهی که اجازه دسترسی به آن داده شده نباشد، دسترسی او به دستگاه مورد نظر مسدود می گردد.

شبکه خود را در برابر مخاطرات ناشی از رسانه های ذخیره سازی قابل حمل محافظت کرده و دسترسی کاربران به آنها را مدیریت نمایید.

با استفاده از GFI EndPointSecurity می توانید بصورت مرکزی دسترسی کاربران به رسانه های ذخیره سازی را غیرفعال کرده و از سرقت اطلاعات و یا ورود بدافزارهایی از قبیل ویروس ها و اسب های تراوا به شبکه توسط کاربر ممانعت نمایید. گرچه شما می توانید از طریق تنظیمات BIOS، دسترسی به حافظه های قابل حمل از قبیل CD یا فلاپی را غیرفعال نمایید اما این راهکار در دنیای واقعی غیرعملی به حساب می آید چراکه برای حذف این سیاست امنیتی ناچار خواهید بود بصورت حضوری به هر سیستم مراجعه کرده و بصورت موقت این ابزارها را فعال نمایید، از طرف دیگر کاربران حرفه ای قادر به هک BIOS هستند. GFI EndPointSecurity به شما امکان کنترل سطح وسیعی از دستگاه های مختلف را می دهد.



GFI EndPointSecurity Management Console



GFI EndPointSecurity configuration options

- امکانات مورد نیاز:
- « Operating system: Windows 2000 (SP4), XP, 2003, Vista, 7 and 2008 (x86 and x64 versions)
 - « Internet Explorer 5.5 or Later
 - « .NET Framework Version 2.0
 - « Port: TCP Port 1116 (Default)
 - « Database backend: SQL Server 2008/2005/2000; if this is not available, GFI EndPointSecurity can automatically download, install and configure a version of SQL Server Express.

Download your free trial from <http://www.gfi.com/endpointsecurity>



GFI EndPointSecurity™
Control of USB sticks, iPods and other endpoint devices

شما می توانید نسخه آزمایشی این محصول را از این آدرس دریافت نمایید تا در صورت رضایت به صورت کامل تهیه فرمائید.
<http://www.gfi.com/endpointsecurity>

GFI EndPointSecurity™
Control of USB sticks, iPods and other endpoint devices

استفاده کنترل نشده از USBها،
پخش کننده های MP3 و PDAها،
درهای شبکه را به سوی ویروسها و سرقت اطلاعات باز می کند.

قوی و کاربر پسند
کیفیت عالی
کنترل کامل
قیمت مناسب

کنترل جامع بر استفاده از iPodها، USBها و دیگر تجهیزات قابل حمل

افزایش استفاده از تجهیزاتی مانند iPod، حافظه های USB، تلفن های هوشمند و دیگر تجهیزات قابل حمل موجب افزایش خطر نشت اطلاعات و فعالیت های بدخواهانه در شبکه ها شده است. در حالی که اکثر شرکت های بزرگ از نرم افزار آنتی ویروس، دیواره آتش، سیستم های امنیت نامه های الکترونیکی و محتوای وب به منظور محافظت در برابر مخاطرات خارجی استفاده می نمایند، تعداد کمی از آنها متوجه هستند که کپی کردن حجم عظیمی از داده های محرمانه و حساس شرکت در یک iPod یا حافظه USB برای یک کارمند چقدر آسان بوده و هیچ کس هم از این عمل با خبر نخواهد شد این عمل همچنین به احتمال قوی موجب انتشار ویروس، بدافزار و نرم افزارهای غیرقانونی در شبکه خواهد شد. راه سختگیرانه جلوگیری از این اتفاقات قفل کردن تمامی پورت های USB می باشد اما این روش نه پایدار و نه عملی خواهد بود.



مزایا



« جلوگیری از سرقت نشت اطلاعات به وسیله کنترل دسترسی به تجهیزات حافظه قابل حمل با کمترین زحمت.

« جلوگیری از انتشار نرم افزار های مخرب و غیر مجاز در شبکه.

« مدیران شبکه را قادر می سازد دستگاه های جانبی را بر اساس کلاس، پسوند فایل، پورت فیزیکی یا کد شناسایی قطعه مسدود نمایند.

« به مدیران شبکه امکان میدهد تا در بازه های زمانی مشخص اجازه دسترسی به پورت و یا دستگاه خاصی را صادر نمایند.

« اگر امکان نصب سرور پایگاه داده وجود نداشته باشد، می تواند SQL Express را به صورت خودکار دریافت و نصب نماید.



شناسایی مشکلات آرشیو اطلاعات ایمیلی شرکت از طریق گزارشهای Maillnsights

سوابق ایمیل‌های شما یکی از حیاتی‌ترین منابع اطلاعاتی شرکت به حساب می‌آید. الگوی گزارش‌دهی Maillnsights در آرشیوگر ایمیل GFI به شما کمک می‌کند تا با استخراج داده‌ها از آرشیو ایمیل خود ظرفیت شکافت‌های امنیتی و خطرات قانونی را شناسایی نمایید.

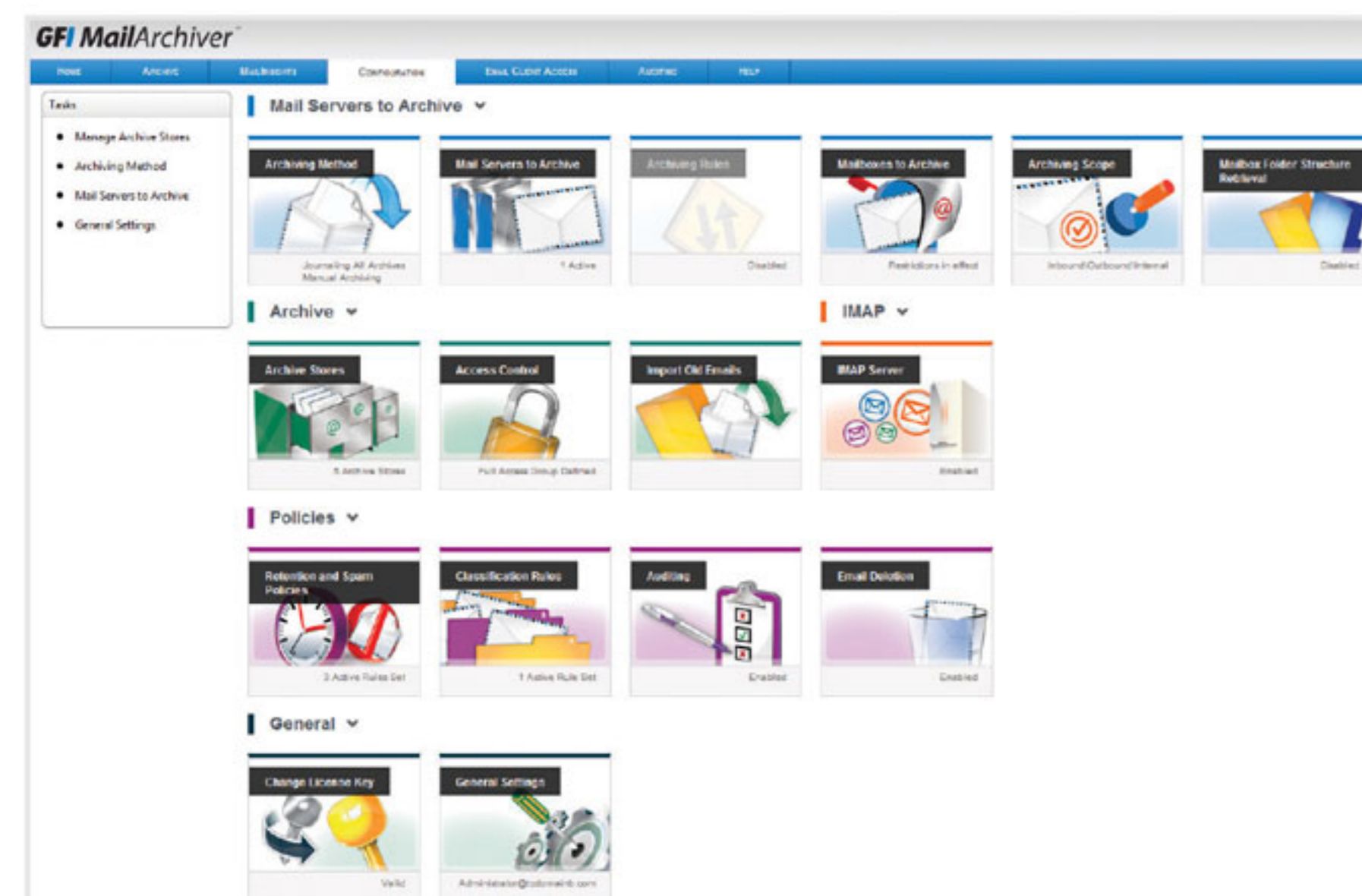
- « کدامیک از کاربران شما بیشترین میزان ارسال ایمیل را دارند؟
- « چه کسانی از اشتراک ایمیل شرکت جهت ارسال ایمیل‌های مهم استفاده می‌کنند؟
- « سریع‌ترین و کندترین پاسخ‌گویان به ایمیل‌های شما چه کسانی هستند؟
- « چه کسانی از منبع ذخیره‌سازی ایمیل برای فایل‌های نامناسب استفاده می‌کنند؟
- « چه کسانی در ایمیل‌های خود از زبان‌های نامناسب استفاده می‌کنند؟
- « کدامیک از کاربران از ایمیل شرکت برای کارهای استخدایمی و جستجوی شغل استفاده می‌کنند؟
- « چه کسی اطلاعات شغلی شما را در اختیار رقبا قرار می‌دهد؟

سایر مشخصه‌ها:

- « یافتن و بازیابی ایمیل‌ها در هر زمان که اراده کنید به سهولت و سرعت صورت می‌گیرد.
- « آرشیوگر ایمیل GFI از پشتیبانی کامل Unicode برخوردار است و بنابراین شما می‌توانید ایمیل‌ها و ضمیمات آن‌ها را به هر زبانی که باشند جستجو و بازیابی کنید.
- « با یک کلیک می‌توانید یک ایمیل را به یک جعبه ایمیل بازگردانید.
- « از طریق داشبورد مدیریت دینامیک می‌توان در کوتاه‌ترین زمان ممکن به اطلاعات کلیدی دسترسی پیدا کرد.
- « فایل‌های PST ذخیره شده در ماشین‌های کلاینت را می‌توان به منبع جدید آرشیوگر ایمیل GFI انتقال داد.
- « امکان تنظیم خط‌مشی‌های طبقه‌بندی و بازیابی ایمیل‌ها.
- « جمع‌آوری و آرشیو کردن ایمیل‌ها از سرتاسر دنیا در یک مکان جغرافیایی واحد.
- « بازیابی جعبه‌های ایمیل از آرشیو.
- « بازیابی ایمیل‌های آرشیو شده برای اطمینان از عدم تحریف و دستکاری آن‌ها.

System requirements

- » Windows® 2003 SP1/2008/R2 or later
- » Windows SBS 2003 or later
- » Access to Microsoft® Exchange Server 2003/2007/2010
- » Microsoft .NET Framework 2.0
- » Internet Information Services (IIS) – world wide web service.



Configuring GFI MailArchiver is quick and easy

تبادل یکپارچه ایمیل‌ها از طریق آرشیوگر ایمیل GFI
 آرشیوگر ایمیل GFI بدون هرگونه تأثیر نامطلوب یا خطر برای عملکرد تبادل (Exchange) به موازات Exchange کار می‌کند. GFI به کمک ثبت مشخصه‌های Exchange Server یک کپی از ایمیل‌های ثبت شده تهیه می‌کند و آن‌ها را در سرور جداگانه‌ای ذخیره‌سازی می‌نماید. این کار باعث جداسازی عملکردهای آرشیوسازی از عملکرد سرور Exchange در انتقال ایمیل می‌شود، به شما امکان می‌دهد تا فضای آزادی بیشتری در اختیار داشته باشید و در کنار اینکه به منبع آرشیو شما ثبت و اطمینان می‌بخشد عملکرد سرور Exchange را ارتقاء می‌دهد.

کاهش هزینه‌های ذخیره‌سازی و پایان مشکلات مربوط به فایل‌های PST

آرشیوگر ایمیل GFI یک کپی از ایمیل‌های شرکت را در یک مکان ذخیره‌سازی مجزا نگه می‌دارد و نیاز کاربران به آرشیوکردن ایمیل‌هایشان در فایل‌های PST روی درایوهای داخلی سیستم را از بین می‌برد. هزینه‌های ذخیره‌سازی به خصوص زمانی کاهش می‌یابد که آرشیوگر ایمیل GFI از فضاهای ذخیره‌سازی SIS جهت ذخیره کردن یک کپی از یک ایمیل ارسال شده به دریافت کنندگان متعدد و فشرده‌سازی ضمیمات ایمیل استفاده کند و زمانی که با ایمیل‌های ذخیره شده در Exchange مقایسه می‌شود نیازمندی‌های ذخیره‌سازی بسیار کمتر است.

کمک گرفتن از e-discovery و راهکارهای مجاز

آرشیوگر ایمیل GFI با فراهم آوردن امکان آرشیو کردن ایمیل‌های شرکت‌ها و تنظیم چارچوب‌های زمانی ذخیره‌سازی و عملکردهای بازیابی به سازمان‌ها کمک می‌کند تا به نیازمندی‌های همیشگی خود مانند FOIA و SOX پاسخ بدهند. تحت این شرایط و عملکردها، شرکتهای عمومی باید اطمینان حاصل کنند که کنترل‌های درونی و بازیابی‌های آن‌ها از سلامت و ایمنی برخوردار بوده و روندهای کاری آن‌ها در تولید داده‌های درست و تایید شده توانمندی لازم را دارد.

دسترسی سریع تر، ظرفیت نامحدود ایمیل و دسترسی به سابقه ایمیل‌ها بدون محدودیت زمانی

از طریق آرشیوگر ایمیل GFI عملکرد کاربران به نحو مطلوبی ارتقاء می‌یابد. راهکار آرشیوسازی قابل دسترس و نامحدود آرشیوگر ایمیل GFI به این معنی است که عملکرد سرور Exchange سریع‌تر بوده و نیاز چندانی به محدود کردن ظرفیت ایمیل برای کاربران نیست. یکپارچه بودن آن با outlook به کاربران امکان می‌دهد تا همزمان با دسترسی به ایمیل‌های جاری خود به آرشیو ایمیل‌های قبلی نیز دسترسی داشته باشند. از طریق دسترسی IMAP نیز کاربران می‌توانند از طریق یک کلاینت یا ابزار مجهز به IMAP مانند آیفون، آپد و اندروید به آرشیو خود دسترسی یابند.



Identify business issues with Maillnsights reports

GFI MailArchiver, چطور زمان شما را ذخیره می‌کند



یافتن ایمیل‌های گمشده

افزایش رضایت و احساس مسئولیت

مشکلات تجارت شما را نمایان می‌کند

آرشیوگر ایمیل GFI؛ آخرین راه نجات

ایمیل یکی از بزرگ‌ترین و حیاتی‌ترین منابع اطلاعاتی هر شرکتی به شمار می‌رود و شما هرگز نمی‌توانید کسب و کاری را بدون این ابزار ارتباطی مجسم کنید. پیام‌های ایمیلی غالباً تنها سند تراکنش‌های مهم شما هستند، از دست دادن و یا حذف یک ایمیل یا فایل ضمیمه شده مهم می‌تواند تفاوتی به اندازه موفقیت یا شکست یک مجموعه در پی داشته باشد.

از طریق آرشیوگر ایمیل GFI، ایمیل‌های تمام شرکت‌ها به طور اتوماتیک در یک فضای امن مرکزی ذخیره می‌شود که به راحتی قابل جستجو و دستیابی است. در نتیجه شرکت‌ها همیشه از اینکه اطلاعاتشان در مکانی امن و قابل مدیریت ذخیره می‌شود خیالشان راحت خواهد بود. علاوه بر این، به واسطه گزارش‌های حاصل از Maillnsights شما می‌توانید مشکلات بالقوه کسب و کار مانند شکاف‌های امنیتی، مشکلات بهره‌وری و خطرپذیری‌های قانونی از طریق استخراج اطلاعات از آرشیو ایمیل‌تان را شناسایی و رفع نمایید.

مزایا

« افزایش قابلیت‌ها و کاهش خطرپذیری‌ها از طریق یک آرشیو کامل و امن باعث ارتقاء بهره‌وری و کاهش هزینه‌های ذخیره‌سازی و نیز حذف نیاز به فایل‌های PST و نگهداری یک کپی اصلی از ایمیل و ضمیمات آن است. بر همین مبنا می‌توان سابقه ایمیل‌ها را در یک دیتابیس جداگانه ذخیره‌سازی کرد و عملکرد و مزایای سرور ایمیل را از محدوده میل باکس‌های نامحدود فراتر برد.

« به کمک گزارش‌های Maillnsights می‌توان از شکاف‌های امنیتی جلوگیری نمود و به نحو موثری به مدیریت کاربران ایمیل شرکت پرداخت.

« در هر زمان و هر مکان امکان دستیابی به ایمیل‌های حیاتی و ضمیمات آن‌ها از طریق برنامه outlook لپ‌تاپ، تلفن همراه و تبلت وجود دارد.

« مدیریت سوابق ایمیل‌های مهم شرکت به طریق امن و کارآمد از دیگر مزایای این ابزار است.

Download your free trial from <http://www.gfi.com/faxmaker>



GFI MailArchiver™
 Archiving for productivity, management and compliance

GFI MailArchiver™
 Archiving for productivity, management and compliance





هزاران مصرف کننده

قیمت رقابتی

عملکرد فوق العاده

صرفه جویی در زمان و هزینه با FaxMaker GFI

FaxMaker GFI یک سرور فکس است که ارسال و دریافت فکس را به آسانی و به طریقی مقرون به صرفه و ایمن امکان پذیر می سازد. این ابزار جدید که مشکلات مربوط به فکس های دستی را از بین برده است به کاربران امکان می دهد تا مستقیماً از طریق ایمیل یا سایر اپلیکیشن ها به ارسال و دریافت فکس مبادرت نمایند.

FaxMaker GFI با هزاران مشتری و مزایای بسیار خود بیش از ده سال است که پاسخ گوی نیازهای شرکتها در زمینه فکس است و خدمات قابل اطمینان و سازمانی آن در قیمت های بسیار رقابتی ارائه می شود. برخی از این مزایای بی شمار عبارتند از: صرف زمان کمتر جهت ارسال فکس، جمع آوری و توزیع فکس ها، صرفه جویی قابل توجه در هزینه ها و ذخیره شدن فکس های ارسالی و دریافتی در یک فرمت دیجیتال در ایمیل یا یک فایل مشخص.

مزایا

« هزینه بسیار مناسب و بازگشت سریع سرمایه (ROI)

« امکانات ایمیل به فکس و فکس به ایمیل از طریق سرورهای ایمیل مبتنی بر فین آوری ابری مانند Office 365، Gmail، Lotus Domino، Microsoft Exchange و MDaemon

« استفاده از خطوط تلفن موجود، استفاده فکس از طریق IP، اتصال به خدمات فکس آنلاین برای فکس های ترکیبی

« فکس اتوماتیک از طریق اپلیکیشن های شرکت: هر چیزی که قابل پرینت باشد امکان فکس آن نیز وجود خواهد داشت

« فکس از ایمیل، ابزارهای چندکاره، اپلیکیشن ها و ابزارهای موبایل

« رفع نیاز به چندین ماشین فکس در یک شرکت

« کاربری و تنظیم آسان

سهولت مدیریت

نصب FaxMaker GFI به آسانی انجام می پذیرد و تنها کار لازم یکپارچه سازی آن با کلاینتها، اپلیکیشن ها و راهکارهای قابل تنظیم جاری است.

یکپارچه سازی با فرآیندهای جاری کسب و کار

FaxMaker GFI با ابزارهای در نظر گرفته شده و با سرور ایمیل مبتنی بر ابر ادغام می شود و به کاربران امکان می دهد تا فکس ها و پیام کوتاه/پیامهای متنی را از طریق کلاینت ایمیل خود ارسال نمایند. از این طریق هیچگونه نیازی به پرینت گرفتن، ایستادن در کنار ماشین فکس، شماره گیری و انتظار برای ارسال فکس نیست. دیگر شاهد قرار گرفتن انبوهی از برگه های در انتظار فکس روی دستگاه، جابجا شدن، افتادنشان روی زمین، گم و یا خوانده شدن آن ها توسط افراد غیرمجاز نخواهید بود. همچنین یک شرکت قادر است درست به همان صورت که ایمیل ها روی شبکه یا فایل فولدرها ذخیره شده و قابل بازیابی هستند از تمام فکس ها نیز یک نسخه پشتیبان با قابلیت جستجو تهیه کند. برنامه OCR به کاربران امکان می دهد تا با جستجوی لغات و عبارت کلیدی با سرعت بیشتری فکس ها را از آرشیو یا کلاینت ایمیل خود بازیابی نمایند.

پشتیبانی از Microsoft Exchange, Lotos Domini, سایر سروهای SMTP و راهکارهای ایمیل مبتنی بر ابر

FaxMaker GFI با Exchange Server ۲۰۰۰/۲۰۰۳/۲۰۰۷/۲۰۱۰/۲۰۱۲ استاندارد Exchange SMTP قابل یکپارچه سازی است. این اقدام ثبات و هماهنگی بیشتری بین FaxMaker GFI و نسخه ها و پکیج های خدماتی Exchange جدید ایجاد می کند. FaxMaker GFI روی سرور ایمیل یا یک ماشین مجزا قابل نصب است و نیازی به نصب هیچ نوع نرم افزاری روی خود سرور ایمیل نیست. همچنین FaxMaker GFI در Lotus Domino و سایر سروهای محبوب SMTP و راهکارهای ایمیل مبتنی بر ابر یا رایانش ابری مانند Office و Gmail نیز قابل ادغام است.

فکس های ترکیبی (Hybrid faxing)

فکس ترکیبی به شما این امکان را می دهد تا FaxMaker GFI را با خدمات دلخواه آنلاین فکس استفاده کنید و تمامی کارایی های سازمانی سرور فکس اولیه همراه با سهولت فنی خدمات فکس ابری را در اختیار تان می گذارد. با استفاده از FaxMaker GFI هیچ نیازی به خطوط تلفن، مودم ها، بردهای فکس یا یکپارچگی با PABX نیست بلکه با خورداری از خدمات پشتیبانی و ارتباط اینترنتی می توانید به سرعت کار فکس را انجام دهید. بدون استفاده از هرگونه سخت افزار شما می توانید از ارسال فکس با هزینه بسیار پایین بهره مند شوید. از آنجا که FaxMaker GFI در فضاهای مجازی قابل نصب است در فضای فیزیکی و مصرف برق صرفه جویی می کند.

فکس از طریق (FOIP) IP

FOIP شما را قادر می سازد تا از طریق زیرساخت IP به راحتی به ارسال و دریافت فکس بپردازید. FaxMaker GFI با PBX مجهز به IP کنونی شما یا فراهم آورنده خدمات VOIP که قابلیت T.38 را دارد ادغام می شود تا بدون نیاز به هرگونه سخت افزاری FOIP را ارائه کند. FaxMaker GFI FoIP می تواند جهت اجرای LCR (کمترین هزینه تماس راه دور) مورد استفاده قرار گیرد که نتیجه آن کاهش چشمگیر هزینه ها در تماس های بین المللی است. راهکار FoIP XCAPI از TE-SYSTEMS در درون FaxMaker GFI 2013 ادغام شده است. علاوه بر این، با خرید هر یک از مجوزهای FaxMaker GFI یک کانال XCAPI FoIP به صورت رایگان به شما ارائه می شود.

FaxMaker GFI از راهکار Dialogic SR140 FoIP نیز پشتیبانی می کند.

مشتری ها می توانند از نسخه آزمایشی SR140 و SR140-L به مدت ۳۰ روز استفاده نمایند.

انتقال اتوماتیک فکس و مسیریابی داخلی

FaxMaker GFI قادر است به صورت اتوماتیک فکس های واردشونده به جعبه ایمیل کاربر یا به یک پرینتر خاص که بر اساس DID/DDI/DTMF شماره گذاری شده است - خط تلفنی که فکس از طریق آن دریافت می شود - را از طریق جستجوی OCR مسیریابی نماید. فکس ها را می توان به یک فولدر مشترک انتقال داد و یا از طریق پورت نصب شده فکس به یکی از پرینترهای شبکه منتقل کرد.

پشتیبانی از ابزارهای چندکاره (MDF)

FaxMaker GFI 2013 از طریق یکپارچه شدن با Nuance eCopy ShareScan SDK قادر است از ابزارهای چندکاره ای مانند کانن، اچ پی، کونیکا مینولتا، ریکو و زیراکس پشتیبانی نماید. MDF ها هم اکنون توانایی ارسال فکس از سیستم های مشابه را دارا می باشند که این کار نیاز به چندین خط تلفن و ابزارهای زیاد را از بین می برد و ثبت، آرشیوسازی و بازیابی فکس را میسر می سازد.

یکپارچه سازی با Active Directory: کاهش وظایف مدیریتی

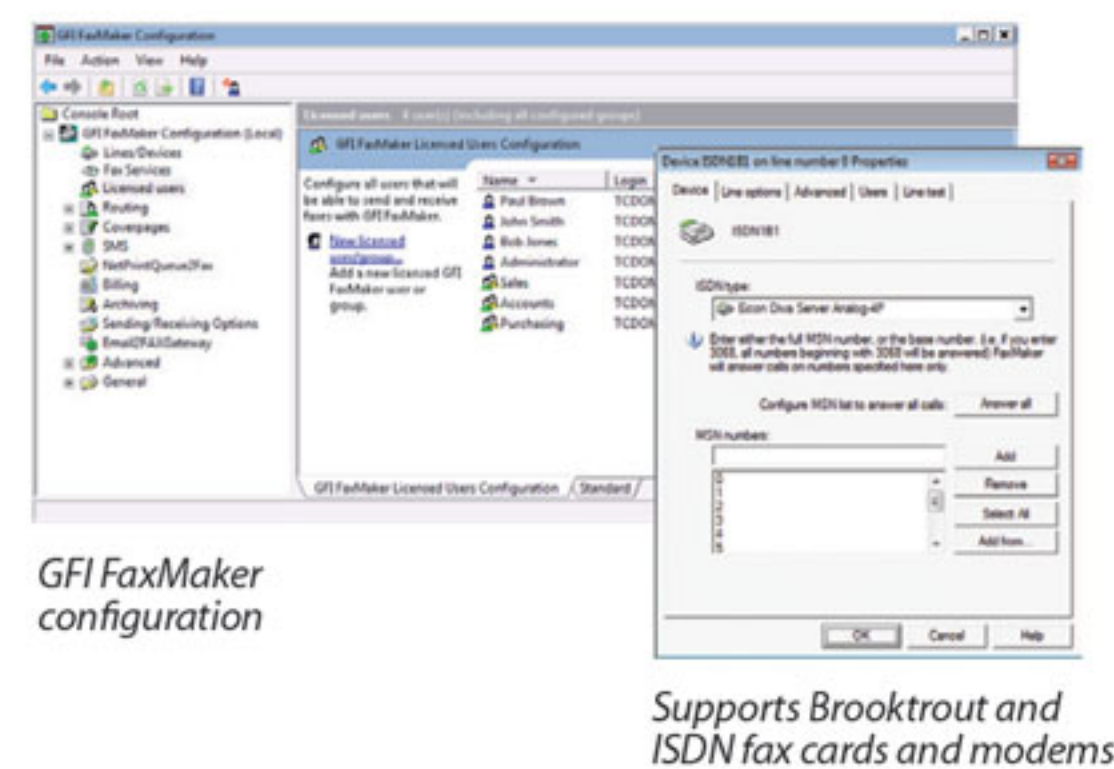
طراحی FaxMaker GFI برای Exchange/SMTP/Lotus کاملاً به صورت پایه ای صورت گرفته است بطوریکه وظایف مدیریتی این سیستم در کمترین حد ممکن می باشد. یکپارچه شدن آن با Active Directory، نیاز به مدیریت دستیابی مجزای کاربر فکس را از بین می برد. تنظیمات مرتبط با کاربران برای کاربران یا گروه های کاربری ویندوز قابل کاربرد است.

سایر مشخصه ها:

- « SMS یا درگاه متن به کاربران امکان می دهد تا پیام های متنی SMS را از Desktop های خود ارسال نمایند
- « آرشیوسازی فکس ها در GFI MailArchiver، SQL یا سایر راهکارهای آرشیوسازی
- « برنامه OCR به منظور جستجو و بازیابی سریع تر و ثبت آسان تر اطلاعات فکس ها را به متن تبدیل می کند.
- « مساعدت امکانات HIPAA
- « پشتیبانی از تماس های outlook
- « چند برابر شدن ارزش FaxMaker GFI با گزارش های قدرتمند از طریق ReportPack یکپارچه سازی شده
- « پشتیبانی از سرورها و شاخه های چندگانه ایمیل
- « پشتیبانی از Native ISDN
- « و خیلی چیزهای دیگر!

System requirements

- » A Windows 2003/2008/2012 server machine with at least 1GB of RAM and 2GHz processor
- » Support FoIP software or device AND/OR account with a supported online fax service AND/OR professional fax device; for a complete list go to: <http://kbase.gfi.com/showarticle.asp?id=KBID001220>
- » If you are installing GFI FaxMaker on a separate machine to your email server, the IIS SMTP service will need to be installed.



Supports Brooktrout and ISDN fax cards and modems

Download your free trial from <http://www.gfi.com/faxmaker>



GFI FaxMaker™
Network fax server software for Exchange/SMTP/Lotus

GFI FaxMaker™
Network fax server software for Exchange/SMTP/Lotus