- طراحی و پیاده سازی راهکارهای جامع امنیتی
- ارزیابی امنیتی سازمان , Penetration Test
- راهکارهای مدیریت پهنای باند و WAN Optimization
- مانیتورینگ شبکه
- راهکارهای جامع پیام رسانی و ارتباطی
- راهکارهای جامع پشتیبان گیری و مجازی سازی
- راهکارهای VDI و انتشار برنامه
- برگزار کننده دوره های آموزشی

معرفی

گسترش روز افزون شبکه‌های کامپیوتری، مسائل و نیازهای مهمی همچون مدیریت، امنیت، نگهداری و یکپارچه سازی سیستمها را در پی دارد. شرکت رایان سامانه آرکا با در نظر گرفتن این نیازها و با هدف ارایه راهکارهای جامع برای نیازهای ICT کشور در سال ۱۳۸۳ تاسیس گردید. این شرکت، با بهره گیری از تجارب متخصصین برجسته شبکه و ارتباطات و با در اختیار داشتن نمایندگی محصولات معتبر و شناخته شده در سطح جهان، خدمات گسترده ای در زمینه پیاده سازی، مشاوره و ارایه راهکارهای جامع فن آوری اطلاعات به ویژه در زمینه امنیت، مدیریت، پیام رسانی و سهمیه بندی پهنای باند ارایه می‌نماید و در حال حاضر مفتخر هستیم که این محصولات و خدمات را به بیش از ۲۵۰۰ مرکز شامل وزارتخانه ها، سازمانها، دانشگاهها و شرکتهای بزرگ کشور ارائه نموده ایم.

راهکارها و خدمات

راهکارها و خدمات آرکا

ارایه راهکارهای جامع امنیتی

محافظت شبکه‌های کامپیوتری و منابع شبکه در مقابل تهدیدات و خطرات، امری حیاتی برای تداوم و بقای هر سازمانی می‌باشد. شرکت رایان سامانه آرکا با ارایه طرح جامع امنیتی چند لایه، شبکه ها و اجزای آن را در مقابل خطرات و تهدیدهای اینترنتی و تهدیدات داخلی محافظت می‌کند. این طرح شامل آنتی ویروس، دستگاههای مدیریت تهدید یکپارچه UTM، فایروال WAF و مدیریت وصله و امنیت نقاط انتهایی Endpoint Security (DLP) می‌باشد.

مانیتورینگ و آنالیز شبکه و امنیت شبکه ، تست نفوذپذیری

پیاده سازی مرکز عملیات شبکه و امنیت به منظور مانیتورینگ شبکه و امنیت شبکه با استفاده از تجهیزات و نرم افزارهای پیشرفته و همچنین تست نفوذ پذیری به منظور کشف نقاط آسیب پذیر شبکه و ارائه راهکارهای اصلاحی به همراه سیاست های امنیتی مبتنی بر ISMS جهت رفع نقاط آسیب پذیر از جمله خدمات تخصصی این شرکت است.

با استفاده از محصولات قدرتمند مانیتورینگ، کلیه اجزای شبکه و سرورها مورد نظارت قرار گرفته و خطاها و رخدادهای امنیتی و گزارشهای آن از طریق ایمیل و SMS در اختیار مدیر شبکه قرار می‌گیرد.

ایمن سازی

ایمن سازی (Hardening) به معنای مقاوم سازی است و به منظور تامین امنیت بیشتر روی سیستمها و دفاع در عمق، ایمن سازی روی آنها انجام میگیرد. ایمن سازی در لایه های مختلفی مانند سیستم عامل، وب سرور، پایگاه داده، لایه کاربر و لایه فیزیکی انجام میشود. برخی از اهداف ایمن سازی عبارت است از: جلوگیری از نفوذ غیرمجاز به سیستم عامل، کاهش ریسکهای امنیتی، جلوگیری از آلوده شدن سیستم عامل به انواع ویروس، و جلوگیری از قطع سرویس‌دهی سیستم ها. برای مثال، کارهایی مانند انجام بروزرسانیهای امنیتی، حذف سرویسهای غیرضروری، و استفاده از فایروال برخی از اعمالی است که در فرآیند ایمن سازی انجام میگیرد.

مرکز عملیات امنیت

مرکز عملیات امنیت شبکه، (SOC)مجموعه ای از خدمات و مکانی است جهت مانیتورینگ ۲۴*۷ سرویس ها و ارتباطات شبکه به منظور کشف تهدیدات و رخدادهای امنیتی مرتبط با دارایی های اطلاعاتی سازمان و پاسخ گویی بلدرنگ به آن که از سه جز اصلی نیروی‌انسانی (People)، محصولات و تجهیزات گوناگون امنیتی (Technology) و فرآیند و رویه‌های متنوع (Process) تشکیل گردیده است، رصد یکپارچه و جامع امنیتی شبکه علاوه بر فراهم نمودن آگاهی وضعیتی از طریق شناسایی، مهار و رفع تهدیدات ، باعث می‌شود تا مدیران تحلیل دقیق‌تری از وضعیت امنیتی شبکه و میزان خطرپذیری آن بدست آورده و به اصلاح روش‌ها، سیاست‌ها و راهکارهای امنیتی سازمان بپردازند.

راهکارهای جامع پیام رسانی و ارتباطی

این شرکت محصولات جامع و قدرتمندی در خصوص ایمیل سرور، و ارتباطات VOIP ارایه می‌کند. ایمیل سرور ارایه شده این شرکت، یک نرم افزار بسیار جامع و قدرتمند بوده و انتخاب بزرگترین سازمانها و دانشگاههای ایران است. در زمینه VOIP ، این شرکت با ارایه تجهیزات مورد نیاز، بستر ارتباطی صوتی و تصویری مقرون به صرفه در اختیار سازمانها قرار می‌دهد.

تست نفوذپذیری

امروز بسیاری از سازمانها هزینه های گزافی را جهت برقراری سیستم های امن در شبکه های خود صرف می کنند. در مقابل برخی سازمانهای دیگر هنوز به اهمیت این امر پی نبرده اند. انجام آزمونهای نفوذ پذیری نه تنها برای سازمانهای دسته دوم بلکه برای سازمانهایی که اقدام به برقراری سیستم های امن نموده اند نیز توصیه می شود. چرا که حتی در صورت پرداخت هزینه واستقرار چنین سیستم هایی نیاز به کنترل دائمی سیستم از لحاظ امنیتی امری اجتناب ناپذیر تلقی می گردد. ارزیابی امنیتی روشی است که توسط آن قادر خواهیم بود تا آسیب پذیری های موجود در شبکه و وب سایت خود را شناسایی کرده و پیش از آنکه نفوذگران واقعی به سیستم وارد شوند، امنیت شبکه خود را افزایش دهیم. این روش با استفاده از ارزیابی جنبه های مختلف امنیتی کمک می کند تا با کاهش دادن ریسک های امنیتی موجود در شبکه، سیستم عامل ها و برنامه های کاربردی، احتمال نفوذ غیر مجاز به شبکه را کاهش دهیم.

طراحی امنیتی

با افزایش روز افزون تهدیدات امنیتی ، طراحی امن شبکه و استفاده از تجهیزات امنیتی به منظور بالا بردن سطح ایمنی سرویس ها و خدمات ارایه شده توسط سازمان یکی از ملزومات شبکه های امروزی می باشد ، بدین منظور بازنگری معماری شبکه ، نیازسنجی ، نصب ، پیاده سازی و پیکربندی تجهیزات امنیتی اعم از فایروالهای شبکه ، فایروالهای لایه وب ، لایه کاربردی و دیتابیس نیازمند نیروهای متخصص می باشد . تیم تخصصی مدافع امنیت با داشتن نیروهای متخصص در زمینه امنیت و شبکه شما را در این امر یاری سازد.

مدیریت امنیت اطلاعات

امروزه امنیت اطلاعات، بزرگترین چالش در عصر فناوری اطلاعات محسوب می‌شود و حفاظت از اطلاعات در مقابل دسترسی غیر مجاز، تغییرات، خرابکاری و افشاء، امری ضروری و اجتناب ناپذیر به شمار می‌رود. از این رو، امنیت دارایی‌های اطلاعاتی، برای تمامی سازمان‌ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش است. سیستم مدیریت امنیت اطلاعات یا Information Security Management – (ISMS System)سیستمی است جهت شناسایی، برطرف سازی و مدیریت آسیب پذیری‌ها، تهدیدها و مخاطرات امنیتی موجود در فضای اطلاعات و سرویس دهی سازمان‌ها. امروزه سازمان‌ها بسیاری از فرصت‌های کسب و کار را به دلیل نداشتن محیط امن و قابل اطمینان برای اطلاعات پر ارزش خود یا مشتری، از دست می‌دهند. هدف اصلی این سیستم برقراری مکانیسمی جهت حفاظت از فرصتها و به حداقل رساندن احتمال وقوع تهدیدات امنیتی اعم از تهدیدات داخلی سازمان، تهدیدات خارجی سازمان، تهدیدات اتفاقی، تهدیدات ناشی از خطاهای عمدی و غیر عمدی است. ایجاد بستری امن جهت تولید، پردازش، انتقال و نگهداری از اطلاعات سازمان و حصول اطمینان برای مشتریان داخلی و خارجی، تأمین کنندگان، ذینفعان، شرکای تجاری و سازمان‌های بالادستی در راستای حفظ محرمانگی، صحت و در دسترس بودن اطلاعات از دیگر اهداف این سیستم محسوب می‌شود.

راهکارهای جامع مجازی سازی و پشتیبان گیری

درحوزه مجازی سازی امکان استفاده از امکانات و قابلیت‌های ارزشمند این تکنولوژی در سه سطح سرور، نرم‌افزارهای کاربردی (همانند نرم‌افزارهای مهندسی) و دسکتاپ کاربران قابل طراحی و پیاده‌سازی می‌باشد. در اجرای مجازی سازی از تکنولوژی های روز دنیا (مانند VMware و Citrix و Hyper-V) استفاده می‌شود. با استفاده از راهکارهای پیشرفته و جامع سخت افزاری و نرم افزاری برای ذخیره سازی، پشتیبان گیری و بازیابی اطلاعات و بازیابی سیستم عامل، این مشکل را به صورت شگفت آوری حل کرده است، طوریکه در اسرع وقت، اوضاع به روال عادی بر می‌گردد.

راهکارهای VDI و انتشار برنامه

در راهکار VDI ، برنامه های کاربردی/ سیستم عامل بر روی یک یا چند سرور اجرا شده و کاربران به جای نصب مجدد آن بر روی کامپیوتر خود، از برنامه های سرور استفاده می‌کنند. برنامه های منتشر شده از روی سرور، از طریق مرورگر اینترنت و همچنین تین کلاینتها برای افراد مجاز قابل دسترس و قابل اجرا می باشد. این راهکار از حیث مدیریتی و صرفه جویی اقتصادی از مزایای متعددی مانند عدم نیاز به خرید مجوز نرم افزارها، نگهداری آسان برنامه ها، امنیت فوق العاده و ... برخوردار است.

ارزیابی آسیب پذیری

بسیاری از سازمان‌های کوچک و بزرگ با کسب و کارهای مختلف بدون در نظر گرفتن تهدیدهای امنیتی به روز موجود در فضای مجازی و هکرهایی که هر روز بر توانای آن‌ها افزوده می‌شود، به کسب و کار خود ادامه داده و از وجود یا عدم وجود آسیب پذیری امنیتی و فنی خود مطلع نیستند. حال آنکه ممکن است یک تهدید امنیتی جدید از آسیب پذیری‌های بالقوه سازمان که از آن مطلع نیست استفاده کرده و خسارات جبران ناپذیری را به اطلاعات و خدمات شرکت وارد کند. گاهی این آسیب‌ها علاوه بر خسارات فنی اعتبار سازمان را در سطح وسیعی خدشه دار خواهد کرد و تا سال‌ها اثرات ناشی از آن در بدنه سازمان وجود خواهد داشت. بنابراین اطلاع از حفره های امنیتی بالقوه و سطح و شدت آن‌ها در سازمان‌ها امری مهم و حیاتی است. هدف از پویش آسیب‌پذیری در سازمان‌ها انجام ارزیابی وضعیت امنیتی دارایی‌های اطلاعاتی موجود در شبکه داخلی، سرویس‌های اینترنتی، نرم‌افزارهای داخلی و دیگر تجهیزات حساس و افزایش ضریب امنیت این اطلاعات است. این فرآیند به شناسایی ریسک‌های امنیت اطلاعات در فرآیند پیاده سازی سیستم مدیریت امنیت اطلاعات نیز کمک خواهد کرد. پویش آسیب‌پذیری به دنبال شناسایی نقاط آسیب‌پذیر سیستم‌های کامپیوتری بر روی یک شبکه است. بعد از شناسایی اطلاعاتی مانند نسخه سیستم عامل، لیست سرویس‌ها و برنامه های نصب شده روی میزبان، سپس آسیب‌پذیرهای موجود در سیستم عامل و سرویس‌های نصب شده روی آن را شناسایی می‌شود. در این مرحله با استفاده از برنامه‌های گوناگون پویش آسیب‌پذیری‌ها، علاوه بر شناخت میزبان‌ها و سرویس‌های فعال بر روی آن‌ها، نقاط آسیب‌پذیر موجود نیز کشف و گزارش می‌شود. ابزارهای پویش مبتنی بر شبکه، با پویش میزبان مورد نظر و ارسال ترافیک سعی در کشف نقاط آسیب‌پذیری می‌نمایند. خروجی این مرحله از ارزیابی در برگیرنده اطلاعات مناسبی راجع به آسیب‌های موجود، علت بروز آسیب‌پذیری و شیوه برطرف کردن یا کاهش مشکلات آن‌هامی‌باشد.فرآیند پویش آسیب پذیری باید به صورت مداوم و دوره‌های تعیین شده انجام شود تا از ایجاد یک حفره امنیتی یا آسیب پذیری فنی در دارایی‌ها قبل از بروز حادثه مطلع شده و آن را برطرف کرد. مستندسازی فرآیند پویش آسیب پذیری به منظور ثبت و گزارش گیری ارزیابی انجام شده از مراحل حائز اهمیت این فرآیند محسوب می‌شود که ما سعی کرده‌ایم تمامی مراحل و فعالیت‌های مربوطه را به صورت یکپارچه و مدون به سازمان‌ها ارائه دهیم.

برگزار کننده دوره های آموزش

برگزاری دوره های آموزشی شبکه(CCNA,) و امنیت شبکه CEH, CCNA Security, Security+, و مباحث میکروسافت توسط اساتید مجرب به منظور ارتقاع سطح علمی‌پرسنل بخش امنیت و شبکه سازمانها

راهکارهای جامع مدیریت و سهمیه بندی منابع مصرفی

کنترل دسترسی کاربران سازمان به منابع مصرفی مانند اینترنت و پرینت، امری بسیار ضروری بوده و همواره یکی از نیازهای مهم مدیران شبکه بوده است. این شرکت محصولات و خدماتی را جهت مدیریت پهنای باند، سهمیه بندی اینترنت به صورت حجمی و زمانی (شناور) به ازای هر کاربر/گروه و همچنین محصولاتی برای سهمیه بندی، کنترل و مدیریت پرینت ارایه می‌کند.

چرا رایان سامانه آرکا:

- ارائه راهکارهای مورد نیاز مشتریان به صورت جامع
- تیم پشتیبانی متخصص و با تجربه
- دارای نمایندگی فروش و پشتیبانی در سراسر شرکت
- نمایندگی محصولات رسمی‌و معتبر (بدون تحریم)
- ارائه پشتیبانی ۲۴ ساعته برای سرویسهای آنلاین مانند: ایمیل سرور، تجهیزات فایروال،....
- پشتیبانی عالی به گواهی بیش از ۲۵۰۰ مشتری رضایتمند.

محصولات

محصولات امنیتی آویرا

آویرا محصول کشور آلمان، جزو پیشروان امنیت محسوب می‌شود. موتور ضد ویروس آویرا سبک ترین و سریع ترین موتور ضد ویروس در دنیاست. آنتی ویروس آویرا، محصول آلمان، یک ضد ویروس فوق العاده سبک، سریع، قدرتمند و هوشمند می باشد. این آنتی ویروس انتخابی مناسب برای کاربران شخصی و شبکه های کوچک می‌باشد. محصولات سازمانی آویرا امنیت Endpoint و همچنین MS Exchange را تامین می کند.

آویرا در تستهای مختلف Virus Bulletin وAV-Comparatives و AV-Test نتایج بسیار عالی کسب کرده است.

جایزه بهترین آنتی ویروس سال ۲۰۱۶ از سوی AV-Comparatives به آویرا تعلق گرفت.

محصولات امنیتی سازمانی

شرکت کوییک هیل، محصولات امنیتی سازمانی خود را تحت عنوان Seqrite ارایه می کند. عمده محصولات این شرکت عبارتند از Endpoint Security و تجهیزات UTM .

کوییک هیل براآنتی‌ویروس کویک هیل (شریک تجاری طلایی شرکا مایکروسافت و همچنین شریک تجاری شرکا اینتل) می باشد و با بیش از ۲۰ سال سابقه فعالیت، از جمله شرکت های پیشرو در حوزه محصولات ضدویروس می باشد. این شرکت ترکیبی از بهترین فن آوری‌های امنیتی جهان را در محصولات آنتی ویروس خود مورد استفاده قرار داده است.

برخی از ویژگی های Seqrite Endpoint Security

کنترل برنامه‌های کاربردی - وب فیلترینگ وب‌سایت‌ها- جلوگیری از دزدی اطلاعات -مدیریت دارایی‌ها - نظارت بر فعالیت -محافظت در برابر اسپم - محافظت IDS/IPS - اسکن آسیب‌پذیری - محافظت دیوار آتش - Tune up - محافظت از فیشینگ ها - محافظت از مرورگر کاربران - داشبورد جدید - تاریخچه لایسنس - انتقال مجدد گروه ها و مشترکین - سهولت در توسعه و نگهداری - اخطار از طریق Email و SMS- مدیریت سیاست‌گذاری بر روی گروه ها - مدیریت سرورهای بروزرسانی چندگانه - کنترل تجهیزات جانبی پیشرفته

سامانه مدیریت دسترسی خاص
Privileged Access Management

امروزه با گسترش زیرساخت‌های شبکه، افزایش تجهیزات فعال و برون سپاری و پیمانکاری بخش‌های عظیمی از سازمان‌ها از یک سو و نگرانی مسائل امنیتی در خصوص دسترسی راهبران سیستم و نیز الزامات داده شده از سوی سازمان‌های بالادستی همچون افتا و بانک مرکزی باعث گردیده تا سامانه مدیریت دسترسی خاص (PAM) بیشترین توجه را به خود جلب کرده و در صدر اولویت‌های سازمان‌ها قرار گیرد.

محصول PAM ارائه شده توسط شرکت ARCON NET به نام ARCOS در لیست ارائه شده توسط Gartner دارای امتیاز بسیار بالا بوده و رقابت شدیدی با سایر محصولات مشابه همچون CyberArk ، BeyondTrust و Dell در این حوزه را دارا می باشد. با توجه به پیاده‌سازی و استفاده در بسیاری از موسسات مالی و اعتباری و وزارت‌خانه‌های سرتاسر دنیا، این محصول به بلوغ کامل رسیده و هم اکنون توان اتصال به بیش از ۵۰۰۰۰ تجهیز را داشته و نیز قابلیت ارتباط برقرار نمودن با تمامی محصولات بومی را توسط بخش تحقیق و توسعه این شرکت جهت ایجاد اتصال‌گر اختصاصی دارا می‌باشد.

مدیریت یکپارچه تهدیدات

UserGate UTM، امکاناتی مانند فایروال، تشخیص نفوذ، ضد ویروس، ضد اسپم و فیلتر محتوا و قابلیت های VPN را به صورت یکپارچه فراهم می‌کند که می‌تواند به راحتی نصب و به روز شود. همچنین برای استفاده شرکت های بزرگ، ویژگی های پیشرفته‌ای مانند کنترل دسترسی مبتنی بر هویت، تعادل بار، کیفیت خدمات (QoS)، پیشگیری از نفوذ، آگاهی از برنامه و بازرسی SSL ارایه شده است. ویژگی های امنیتی چندگانه در قالب یک پلت فرم برای محافظت از شبکه، وب، ایمیل، برنامه ها ارایه شده است که کاربران را در برابر حملات، ویروس ها، تروجان ها، نرم افزارهای جاسوسی و هرزنامه ها محافظت می‌کند. فن آوری های پیشرفته مانند بازرسی عمیق محتوا (DCI) به شما این امکان را می‌دهد که بصورت هوشمندانه ترافیک را مدیریت، برنامه های کاربردی اینترنت را کنترل و با تهدیدات مداوم مقابله کنید. UserGate UTM یکی از سریع ترین و قابل اطمینان ترین محصولات امنیتی دروازه در بازار است.

UserGate UTM به عنوان یک دروازه امنیتی وب کار می‌کند. این دستگاه به دو صورت سخت افزاری و نرم افزاری ارایه شده است.

UserGate UTM بر اساس حساب کاربر و سیاست های قابل اجرای سازمان کار می‌کند. این محصول به مدیران اجازه می‌دهد تا جریان ترافیک را کنترل و مدیریت کنند و صفحات وب را که توسط کارکنان بازدید می‌شود، ردیابی کنند. برای اعطا یا محدود کردن دسترسی به وب سایت‌ها، کنترل دانلود یا استفاده از برنامه، تعیین میزان ترافیک و حفظ آمار می‌توان سیاست‌های متعددی اعمال کرد.

نرم افزار مانیتورینگ

NetCrunch یک سیستم جامع مانیتورینگ بدون Agent می‌باشد که قادر به مانیتور کردن هزاران نود شبکه (سویچ، روتر، فایروال، یوپی‌اس، پرینتر، سنسورها و ...) می‌باشد. این سیستم بر روی ویندوز نصب شده و دارای کنسول وب، موبایل (iOS, Android, Blackberry) و دسکتاپ است. NetCrunch، به صورت موثر داده های شبکه را سازماندهی کرده، به صورت خودکار شبکه را پویش کرده و نماها و نقشه‌های (منطقی و فیزیکی) شبکه را ایجاد می‌کند. این نرم افزار، تمامی‌سیستم عاملهای مرسوم از قبیل ویندوز، لینوکس ، VMware ESX/ESXi ، Mac OS X و BSD را پشتیبانی می‌کند. همچنین انواع ترافیک‌های مرسوم شبکه مانند IPFix, NetFlow و ... در این سیستم قابل نظارت هستند. در مورد اکثر نرم‌افزارهای مرسوم مانند MS SQL و MS Exchange ، این نرم افزار بسته‌های نظارتی از پیش تعیین شده دارد که باعث سهولت، دقت و سرعت در تعریف و نظارت این نرم‌افزارها می‌شود.

محصولات Sangor

Sangfor ارایه کننده محصولات WAN Optimization ، امنیت شبکه و مجازی سازی می باشد.

WAN Optimization: محصولات WAN Optimization Sangfor ، ترافیک WAN را به صورت موثر فشرده کرده و در نتیجه، ۷۰٪ ترافیک زاید حذف شده، Packet loss به زیر ۱٪ رسیده وبرنامه ها ۳ تا ۱۰ برابر سریعتر اجرا شده و هزینه پهنای باند به حداقل نصف کاهش می‌یابد.

محصولات امنیتی عبارتند از:

Internet Access Management: برای مدیریت و کنترل دسترسی کاربران به اینترنت. این محصول دارای قابلیت اینترنت اکانتینگ بوده و قادر است سیاستهای کنترل پهنای باند به ازای کاربر و یا برنامه را اعمال کند. کنترل حجم و زمان استفاده شناور از دیگر قابلیتهای این محصول است.

NGAF Firewall : فایروال نسل بعد که موفق به کسب نشانهای جهانی از جمله NSS شده است.

SSL VPN : ایجاد دسترسی از راه دور به منابع شبکه سازمان

در زمینه مجازی سازی، Sangfor محصولاتی جهت انتشار برنامه و انتشار ایستگاه کاری (VDI) ارایه می‌کند.

ایمیل سرور MailEnable

MailEnable محصول استرالیا از سال ۲۰۰۲ در حوزه ایمیل سرور فعالیت دارد. MailEnable بر پایه تکنولوژی Net. طراحی شده و از تمامی پروتکلهای استاندارد ایمیل مانند SMTP,POP3, IMPA به صورت SSL/TLS پشتیبانی می‌کند. این محصول همچنین دارای List Server و آنتی ویروس و آنتی اسپم می‌باشد. MailEnable برای کاربران، دارای وبمیل پیشرفته مخصوص پی سی و موبایل بوده و از ActiveSync به صورت کامل پشتیبانی می‌کند. قابلیتهای کار گروهی و Collaboration با استفاده از پروتکلهای MAPI, CalDAV, CardDAV, SyncML و Exchange ActiveSync پیاده سازی شده است. از نقطه نظر مدیریت، تمامی عملیات مدیریتی از طریق کنسول MMC و کنسول تحت وب و همچنین PowerShell قابل انجام است.

به دلیل پاسخگویی تعداد کاربران زیاد و همچنین امکانات و ویژگیهای کامل، MailEnable مناسبترین انتخاب برای ISP ها و ایمیل سرورهای بزرگ است.

Fastvue Reporter

نرم‌افزار TMG Reporter محصول شرکت Fastvue تنها راه‌حل کامل جهت گزارش‌گیری و مانیتورینگ از Forefront TMG در دنیا است. این محصول راهکاری ساده برای بررسی و مرور دقیق عملکرد کاربران به همراه گزارش‌های کامل است. TMG Reporter به صورت RealTime اطلاعات سازمان مانند فعالیت‌های کاربران و برنامه‌های کاربردی را نشان می‌دهد. سیستم هشدار دهنده همچنین بروز اتفاقات معین را به مدیر شبکه گزارش داده و نیازی به مراقبت دائمی‌از آن نمی‌باشد. این نرم‌افزار همچنین گزارش کامل از سایتهای مرور شده توسط کاربران را در اختیار مدیر شبکه قرار می‌دهد تا از طریق این گزارشات، قادر به تشخیص فعالیت‌های مفید از غیرمفید کاربران باشند. فست ویو همچنین محصولاتی برای گزارشگیری از Sophos و Barracuda و SonicWall ارایه می کند.

Safetica – نرم افزار DLP

پرسنل شرکت که جزو پایه‌های اصلی سازمان به شمار می‌آید، در عین حال می‌تواند به عنوان تهدیدی جدی برای سازمان محسوب شود. برخی از کارمندان تظاهر به کارکردن در سازمان می‌کنند در حالیکه صرفا در حال اتلاف منابع سازمان بوده و اغلب اوقات خود را صرف وبگردی ، چت کردن، بازی کردن و یا سایر فعایتهایی می کنند که در راستای منافع سازمان نیست. گاهی اوقات اطلاعات ارزشمند و محرمانه سازمان به صورت عمد و یا غیر عمد از طریق ابزارهای جانبی ذخیره ساز مانند USB, CD/DVD و یا از طریق ایمیل، وب، چت و... از شرکت خارج می‌شود. Safetica نرم افزاری قدرتمند برای حل کلیه مشکلات داخلی ناشی از کارمندان و نقاط ضعف شبکه می‌باشد. مدیران ذیربط سازمان می‌توانند کارمندان مضر را قبل از اینکه به سازمان آسیب جدی وارد آورند، شناسایی کرده و مسئولیت پذیری را در

PrintWatch

نرم افزار PrintWatch قدرتمندترین و با سابقه‌ترین محصول در زمینه مدیریت و سهمیه‌بندی پرینت است. این نرم‌افزار قابلیت‌های بسیاری از جمله اعمال سیاست‌های سهمیه‌بندی و کنترل و گزارشگیری مصرف پرینت بر اساس کاربر و گروه را در اختیار مدیر شبکه قرار می‌دهد

پیپرکات- نرم افزار مدیریت پرینت

نرم افزار Papercut قدرتمندترین و با سابقه‌ترین محصول در زمینه مدیریت و سهمیه‌بندی پرینت است. این نرم‌افزار محصول کشور استرالیا بوده و قابلیت‌های بسیاری از جمله اعمال سیاست‌های سهمیه‌بندی و کنترل و گزارشگیری مصرف پرینت بر اساس کاربر و گروه را در اختیار مدیر شبکه قرار می‌دهد که در نهایت منجر به کاهش هزینه های چاپ، اتلاف کاغذ و حفظ محیط زیست می‌شود. این نرم افزار مدیر شبکه را قادر می‌سازد تا محتوای فایلهای چاپ شده توسط کاربران را مشاهده کند. Papercut از تمامی‌سیستم عاملهای مرسوم ویندوز، لینوکس و مکینتاش و همچنین از تمامی‌پرینترهای موجود (شبکه یا به اشتراک گذاری شده) پشتیبانی کرده و قابلیت یکپارچگی با تمامی LDAP ها از جمله اکتیودایرکتوری را داراست.

سازمان گسترش دهند. همچنین این نرم افزار از خروج اطلاعات شرکت جلوگیری می کند.

SpamTitan امنیت ایمیل سرور

SpamTitan یک راهکار جامع برای امنیت ایمیل می‌باشد که از ایمیل سرور در برابر تهدیدات مختلف مانند اسپم (هرزنامه)،ویروس‌ها، تروجان‌ها، فیشینگ و محتوای ناخواسته محافظت به عمل می‌آورد. جوایز و نشان های متعدد و پی در پی این کمپانی بزرگ ایرلندی بیانگر قدرت و دانش آنها در این زمینه می باشد. SpamTitan به لطف استفاده از آنالیز چند لایه ضد اسپم توانسته است دقت تشخیص خود را به بیشتر از ۹۸٪ برساند و همچنین میزان خطای کمتر از ۳٪ داشته باشد. با توجه به چنین ویژگی ها و مزایای منحصر به فرد می توان این ضد اسپم را به آسانی یکی از بهترین های دنیا در این زمینه بنامیم.

BSplitter – مدیریت پهنای باند

Bandwidth Splitter یک نرم افزار قدرتمند برای مدیریت پهنای باند و سهمیه بندی اینترنت می‌باشد که به شکل افزودنی به ForeFront TMG و یا ISA اضافه شده و می تواند سیاستهای تعیین پهنای باند بر اساس IP، کاربر و گروه را اعمال کند. این برنامه همچنین می‌تواند حجم دانلود و آپلود هر کاربر را کنترل کند. ForeFront TMG و ISA فاقد چنین امکاناتی است. با استفاده از BSplitter امکانات مربوط به کنترل پهنای باند به آنها اضافه شده ومدیران شبکه از طریق کنسول ISA یا ForeFront می توانند قواعد مربوط به پهنای باند را اعمال کنند. از جمله مزایای این نرم افزار، عدم نیاز به نصب برنامه در سمت کاربران می‌باشد.

.