رایان سامانه آرکا

arka
رایان سامانه آرکا

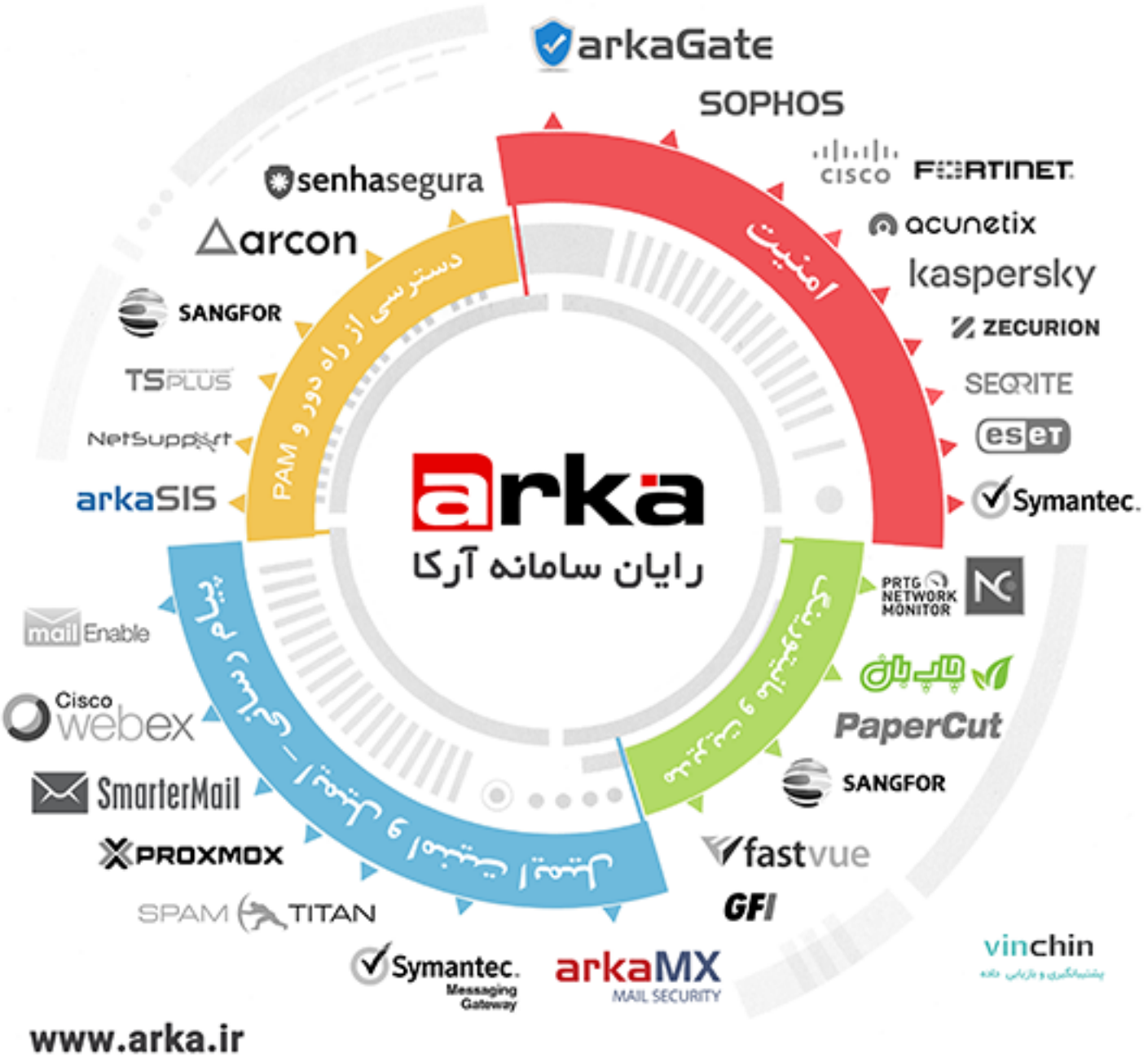
arkaGate | SOPHOS | arcon

سخن مدیر عامل

بهره مندی مشتریان ایرانی از آخرین فناوری ها و محصولات بروز در حوزه فناوری اطلاعات به خصوص در شاخه امنیت، یکی از اهداف شرکت رایان سامانه آرکا بوده است. در این راستا، این مجموعه از سال ۱۳۸۳ تاسیس یافته و با ارایه خدمات فنی و همچنین اخذ نمایندگی های محصولات شناخته شده در حوزه امنیت، مدیریت شبکه و ایمیل سرو به ارایه خدمات به مشتریان ایرانی پرداخته است. جهت ارایه خدمات فروش و پس از فروش عالی، این شرکت در تمامی استانهای کشور دارای نمایندگی است. و افتخار همکاری با بیش از ۲۵۰۰ مشتری را داریم.

به لطف متخصصان خبره کشور، این شرکت محصولاتی در زمینه های امنیت و مدیریت تولید کرده و پس از تست و ارزیابی و کسب مجوزهای لازم به خصوص از سازمان افتا، به مشتریان خود ارائه کرده است. از جمله محصولات تولیدی این شرکت می توان به مواردی مانند آرکاگیت که یک فایروال بومی با امکانات کامل و اینترنت اکانتینگ کامل است اشاره کرد. همچنین، چاپبان، نرم افزاری برای مدیریت چاپ در شبکه و ArkaSIS برای جداسازی اینترنت از اینترانت، از دیگر محصولات تولیدی شرکت رایان سامانه آرکا است.

محصولات و راهکارهای رایان سامانه آرکا



راهکارها و خدمات

ارایه راهکارهای جامع امنیتی

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

مانیتورینگ و آنالیز شبکه و امنیت شبکه ، تست

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.

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.

مرکز عملیات امنیت

مرکز عملیات امنیت شبکه، (SOC) مجموعه ای از خدمات و مکانی است جهت مانیتورینگ ۷*۲۴ سرویس ها و ارتباطات شبکه به منظور کشف تهدیدات و رخدادهای امنیتی مرتبط با دارایی های اطلاعاتی سازمان و پاسخ گویی بلادرنگ 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.

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، یك 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 می دهد.

تست نفوذ

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.

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 .

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.

راهکارهای جامع مجازی سازی و پشتیبان

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.

راهکارهای VDI و انتشار برنامه

در راهکار VDI ، برنامه های کاربردی/ سیستم عامل بر روي يك يا 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 اقتصادي از مزایای متعددی مانند عدم نیاز به خرید مجوز نرم افزارها، نگهداری آسان برنامه ها امنیت فوق العاده و ... برخوردار است.

ارزیابی آسیب

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.

برگزار کننده دوره های آموزش

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

راهکارهای جامع مدیریت و سهمیه بندی منابع

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 می کند.

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

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 امنیتي چند لایه، شبکه ها و اجزای آن را در مقابل خطرات و تهدیدهای اینترنتی و تهدیدات داخلی محافظت می‌کند. این طرح شامل آنتي ویروس، دستگاههای مدیریت تهدید یکپارچه UTM، فایروالWAF و مدیریت وصله و امنیت نقاط انتهایی Endpoint Security (DLP) می‌باشد.

PAM مدیریت دسترسی ادمین

لزوم استفاده از PAM

افزایش تهدیدات امنیتی پیچیده و هدفمند توسط مهاجمان خارجی و خودی های مخرب ، محافظت صحیح از اطلاعات مهم و حساس را برای سازمان ها بسیار دشوار کرده است. وظیفه حفاظت از این دارایی ها به مراتب سخت تر شده است چرا که محیط های فناوری اطلاعات پیچیده تر شده و به طور گسترده در نقاط جغرافیایی و ابر توزیع شده اند. متجاوزان، حساب های ممتاز را به سرقت برده و از زیرساخت های کل شرکت سو استفاده کرده اند. متأسفانه ، بسیاری از مدیران فناوری اطلاعات درک کاملی از نحوه عملکرد حسابهای ممتاز و همچنین خطرات مرتبط با سازش و سو استفاده از آنها ندارند. این امر باعث می شود که آنها و سازمان هایشان در برابر آسیب های احتمالی پولی و اعتباری بسیار آسیب پذیرتر باشند. مدیریت دسترسی ممتاز Previldge Access Management-PAM راهکاری برای مقابله با این مسئله است.

senhasegura

محصول سنهاسگورا

گزارش گیری Senhasegura

این امکان را می دهد تا SIEM های مختلف بتوانند به این راهکار متصل شده و اطلاعات و رخدادهای ثبت شده را از این راهکار خوانده و در سیستم خود ذخیره نمایند لذا هر SIEM که قابلیت خواندن اطلاعات از راهکارهای دیگر را داشته باشد می تواند با Senhasegura همسو شود.

تحلیل رفتار وقایع و اتفاقات ماژول BehavioراهکارSenhasegura بر پایه هوش مصنوعی پیشرفته این شرکت امکان تحلیل رفتار کاربران را برای تشخیص رفتارهای ناهنجار را به سازمان می دهد.

نظارت و مانیتورینگ

تمامی پروتکل های مطرح شده به همراه Web Application ها به طور کامل پشتیبانی می شود. و به طور کلی بیش از ۱۰۰ برنامه و سرویس مانند IBM Applications, SANS Application))را پشتیبانی می نماید.

سطوح دسترسی کاربران

کنترل سطح دسترسی کابران ادمین برای جلوگیری از تغییرات و خراب کاری های ناخواسته.

arcon

محصول آرکون PAM

امروزه با گسترش زیرساخت‌های شبکه، افزایش تجهیزات فعال و برون سپاری و پیمانکاری بخش‌های عظیمی‌از 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 BeyondTrust ، CyberArk و Dell در این حوزه را دارا می‌باشد. با توجه به پیاده سازی و استفاده در بسیاری از موسسات مالی و اعتباری و وزارت‌خانه های 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 بومی‌را توسط بخش تحقیق و توسعه این شرکت جهت ایجاد اتصال‌گر اختصاصی دارا می باشد.

ویزگیها و امکانات:

- مدیریت و کنترل سطوح دسترسی کاربران ارشد، برنامه ها و سیستم های عامل
- جلوگیری از اعمال سهوی یا عمدی دستورات مخرب با دسترسی سطح بالا بر روی سیستم های حیاتی
- مدیریت دسترسی برای کاربران از راه دور
- محافظت در برابر تهدیدات امنیتی ناشی از دسترسی در سطوح بالا
- احراز هویت یکپارچه و دو عاملی

DLP جلوگیری از نشت داده

لزوم استفاده از راهکارهای جلوگیری از نشت داده‌ها یا DLP

نقض داده‌ها یک پدیده رایج در دنیای داده است و می تواند تهدیدی جدی برای سازمان ها باشد. هنگامی که نقض داده رخ می دهد، شهرت یک شرکت یا سازمان در خطر است و ممکن است اعتبار و مزیت رقابتی شما را از بین ببرد. هزینه های چنین حوادثی می تواند بسیار زیاد باشد. طبق گزارش IBM Cost of a Data Breach که در ارتباط با مؤسسه Ponemon منتشر شد، در سال ۲۰۲۱ میانگین هزینه نقض داده به ۴/۲۴ میلیون دلار در هر حادثه رسید. تهدیدهای داخلی در حال افزایش هستند و اگر شرکتی از راه حل DLP استفاده نکند و سیاست های امنیتی نامشخصی داشته باشد، خطر از دست دادن داده ها افزایش می یابد.

safetica

نرم‌افزار Safetica

نرم افزار Safetica تنها راه‌حل امنیت داده تخصصی است که برای سازمان‌ها و شرکت‌ها در مقیاس‌های مختلف طراحی شده است. داده‌های ارزشمند خود را در کمترین زمان ایمن کنید. با تجزیه و تحلیل رفتار کل‌نگر از پیشگیری نشت داده فراتر بروید تا تهدیدات داخلی را حتی زودتر شناسایی کنید و قبل از تبدیل شدن آن‌ها به حادثه پاسخ دهید. برای بهینه‌سازی هزینه‌ها، از اطلاعات کسب‌شده در مورد فضای کاری شرکت، دارایی‌های دیجیتال و عملیات استفاده کنید.

کشف جریان داده و تشخیص ریسک

نرم افزار Safetica هر گونه تلاش برای افشای عمدی یا غیرعمدی داده‌ها را بررسی و ثبت می کند، مهم نیست که اطلاعات حساس در کجا ذخیره شده است یا چه کسی به آن دسترسی داشته است. تجزیه و تحلیل ریسکSafetica به شما کمک می‌کند تا نحوه لو رفتن یا سرقت داده‌های شما را شناسایی و بررسی کنید.

انطباق با مقررات

نرم افزار Safetica به شما کمک می‌کند نقض مقررات را شناسایی و از آن جلوگیری کنید و حوادث را برای مطابقت با مقررات و استانداردهای حفاظت از داده مانند GDPR، HIPAA، SOX، ISO/IEC ۲۷۰۰۱ PCI-DSS، GLBA یا CCPA بررسی کنید.

حفاظت از داده‌ها و راهنمایی کارکنان

هر کسی ممکن است اشتباهی مرتکب شود که می تواند کسب‌وکار شما را در معرض خطر قرار دهد. با نرم‌افزار Safetica می‌توانید ریسک‌های داخلی را تجزیه و تحلیل کنید، تهدیدها را شناسایی کرده و به سرعت آن‌ها را کاهش دهید. اعلان‌های مربوط به نحوه برخورد با داده‌های حساس می‌تواند به افزایش آگاهی در مورد امنیت داده‌ها و آموزش کارکنان کمک کند.

رایان سامانه آرکا، نماینده رسمی Safetica

رایان سامانه آرکا، نماینده انحصاری Safetica در ایران است. ما همراه شما هستیم تا داده‌های شما را به وسیله نرم افزار Safetica ایمن کنیم و شما را از آنچه در سازمان یا شرکت شما می گذرد مطلع کنیم.

ANTI-VIRUS آنتی ویروس شبکه

ضرورت استفاده از آنتی ویروس سازمانی

حملات سایبری همواره در حال توسعه هستند. همانطور که امنیت سیستم عامل‌ها و مرورگرهای وب توسعه یافته و پیشرفت قابل ملاحظه ای کرده‌اند، مجرمان سایبری نیز انواع جدیدی از حملات سایبری را طراحی کرده‌اند. بدافزارهای جدید معمولا از آسیب پذیری‌های کشف نشده در شبکهِ هدف استفاده می‌کنند و اگر سازمان‌ها مجهز به یک آنتی ویروسِ شبکه قدرتمند نباشند، به راحتی به شبکه آنها نفوذ شده و آلوده می‌شوند. در این راستا شرکت رایان سامانه آرکا اقدام به ارائه بهترین آنتی ویروس ها در سطح جهان کرده است.

Symantec

SEP (Symantec Endpoint Protection) حفاظت برتر و چند لایه براي جلوگیری از تهدیدات، بدون در نظر گرفتن چگونگی حمله به Endpoint را ارائه میدهد SEP.
با زیرساختهای امنیتی موجود سازمان ادغام میشود تا پاسخ های هماهنگ شده ای را که به سرعت تهدیدات را متوقف میسازد، ارائه دهد. عامل واحد و سبک وزنSEP ، عملکردی بالا، بدون به خطر انداختن بهره وری، ارائه میکند، بنابراین شما میتوانید در کسب و کار خود تمرکز کنید.

- مجهز به هوش مصنوعی بالا براي شناسایی
- تهدیدات ناشناخته
- مدیریت آسان و متمرکز
- مجهز به سندباکس و فناوری فریب برای به تله انداختن بدافزارها
- مجهز به فناوری تشخیص بدون امضاء مانند یادگیری ماشین، نظارت بر فعالیت برنامه و ...
- گزارش دهی جامع

محصولات معروف سیمانتک از قبیل:

Endpoint Security,Advanced Threat Protection,Information Protection,Email Security,Network Security,Cloud Security,Cyber Security Services

kaspersky

این محصول، یک راه حل کامل امنیتی ارائه میدهد که توسط کارشناسان برجسته امنیتی جهان طراحی شده است .عمیق ترین، آینده نگرترین حافظت، عملکرد موثر و مدیریت سرراست از طریق لایه های مترقی برای ایجاد امنیت کامل در تجارت شما ایجاد میشود.
کلیه مؤلفه ها به صورت داخلی طراحی و ساخته شده اند تا در یک قالب امنیتی منسجم متناسب با نیازهای تجاری شما ساخته شوند. نتیجه، یک راه حل استوار و یکپارچه بدون درز، بدون مشکلات سازگاری و بار کاری اضافی در سیستم شماست.

محصولات معروف کسپرسکی از قبیل:

Kaspersky Endpoint Security for Business SELECT,
Kaspersky Endpoint Security for Business ADVANCED,
Kaspersky TOTAL Security for Business

eset

راه حل های محافظت از نقطه پایانی ESET چندین لایه دفاعی را فراهم می کند تا نه تنها از بدافزار جلوگیری کند بلکه در صورت بروز در سازمان ، آن را تشخیص دهد. هنگامی که حمله یا نقض داده رخ می دهد سازمان ها معمولاً از به خطر افتادن دفاعیات خود تعجب می کنند و یا اینکه از حمله کاملاً بی اطلاع هستند.

تهدیدهای جدید ، بدافزار بدون پرونده ، به طور انحصاری در حافظه رایانه وجود دارد ، و این امکان را برای حفاظت مبتنی بر اسکن پرونده ، برای شناسایی آنها غیر ممکن می کند.

محصولات معروف ESET از قبیل:

ESET PROTECT Entry, ESET PROTECT Advanced, ESET PROTECT Complete

CHOMAR آنتی ویروس و آنتی اسپایور

CHOMAR Endpoint Security

برای کمک به شما در استفاده از دستگاه‌های خود با سرعت بالا طراحی شده است و در عین حال امنیت شما را در دنیای دیجیتال تضمین می کند.CHOMAR Endpoint Security خطراتی را که ممکن است توسط انواع ویروس ها، نرم افزارهای جاسوسی، تروجان ها، کرم ها، ابزارهای تبلیغاتی مزاحم، روت کیت ها و سایر تهدیدات ایجاد شود حذف می کند بطوریکه شما کارهای روزانه خود را بدون خسته کردن و پایین آمدن عملکرد دستگاه خود انجام می دهید. این آنتی ویروس با حفاظت اکتشافی خود از دستگاه شما محافظت کامل می کند. CHOMAR Endpoint Security برای استفاده در ایستگاه های کاری در محیط کسب و کار طراحی شده است. علاوه بر آن می توانید به راحتی چندین ایستگاه کاری مشتری را مدیریت کنید، خط مشی های خود را اعمال کنید و آنها را از راه دور از هر کامپیوتر شبکه پیکربندی کنید.

حفاظت اکتشافی

از بدافزارهای جدید و شناخته شده محافظت می کند.

محافظت از زمان واقعی

تهدیدات را بی درنگ بدون حتی یک تغییر درکامپیوتر شما شناسایی می کند.

آنتی ویروس و آنتی اسپایور

از کامپیوتر شما در برابر ویروس ها، نرم افزارهای جاسوسی و سایر مخرب ها محافظت می کند.

مصرف کم منابع

از منابع سیستم شما به نحو احسن استفاده می کند و از رایانه شما بدون کاهش سرعت آن محافظت می کند.

حفاظت از اینترنت

از دسترسی به وب سایت های مضر و مخرب جلوگیری می کند و به طور اتوماتیک فایل های دانلود شده از اینترنت را اسکن می کند.

حفاظت از ایمیل

از ایمیل های ناخواسته و مخرب به صندوق ورودی شما جلوگیری می کند و فایل های پیوست را به طور خودکار اسکن می کند.

مدیریت از راه دور CHOMAR

با مدیریت از راه دور CHOMAR می توانید به راحتی چندین کلاینت و ایستگاه کاری را مدیریت کنید.

اسکن هوشمند

در یک مرحله اسکن به صورت یکپارچه از کامپیوتر شما محافظت می کند.

ENDPOINT SECURITY (ANDROID)

CHOMAR Endpoint Security به گونه ای طراحی شده است ک توانایی استفاده از دستگاه های خود با بالاترین عملکرد را به شما می دهد و در عین حال این اطمینان را نیز به شما میدهد که دستگاه های تلفن همراه مورد استفاده در سازمان شما در دنیای دیجیتال ایمن هستند. CHOMAR Endpoint Security خطراتی را که می تواند توسط تهدیدات موبایل مانند ویروس ها، اسپایورها، تروجان ها، کرم ها، ابزارهای تبلیغاتی مزاحم ایجاد شود را، بدون خسته کردن دستگاه شما و بدون اینکه عملکرد دستگاه شما پایین بیاید، از بین می برد. CHOMAR Remote Administrator می تواند دستگاه های کلاینت شما را از طریق پنل مدیریت، کنترل کند، موقعیت مکانی دستگاه شما را به روز کند و آن را روی نقشه نمایش دهد. شما در پنل مدیریت می توانید مشاهده کنید، تنظیمات کارخانه را ریست کنید و موقعیت مکانی فوری را برای کاربران شناخته شده ، از طریق پیامک ارسال کنید.

FIREWALL فایروال های شبکه

لزوم استفاده از فایروال ها

فایروال ها به عنوان لبه اصلی محافظت از شبکه یکی از مهم ترین عنصر های امنیتی یک سازمان یا شرکت می باشد. فایروال ها یا در اصل UTM ها خود دارای لایه های مختلفی برای محافظت از شبکه میباشند این لایه ها شامل انتی ویروس ،آنتی اسپم،سیستم تشخیص نفوذ،سیستم جلوگیری از نفوذ،فایروال ، و... میباشد.

فایروال سیستمی است که شبکه و یا کامپیوتر شخصی شما را در مقابل نفوذ مهاجمین، دسترسی‌های غیرمجاز، ترافیک‌های مخرب و حملات هکرها محافظت کند. نحوه عملکرد فایروال‌ها به اینگونه است که بسته‌ها را بین شبکه‌ها رد و بدل و مسیریابی (Route) می‌کنند. فایروال هم ترافیک ورودی به شبکه و هم ترافیک خروجی از آن را کنترل و مدیریت کرده و با توجه به قوانینی که در آنها تعریف می‌شود به شخص یا کاربر خاصی اجازه ورود و دسترسی به یک سیستم خاص را می‌دهد. مثلا شما می‌توانید برای فایروال خود که از یک شبکه بانکی محافظت می‌کند با استفاده از قوانینی که در آن تعریف می‌کنید بخواهید که به کاربر X در ساعت Y اجازه دسترسی به کامپیوتر Z را که درون شبکه داخلی شما قرار دارد را بدهد. قوانینی که در یک فایروال قرار دارد بر اساس نیازهای امنیتی یک سازمان و شرکت تعیین می‌شود. ترافیکی می‌تواند اجازه ورود و خروج را داشته باشد که منطبق بر سیاست‌های امنیتی فایروال باشد و بقیه ترافیک غیر مجاز است.

SOPHOS

سوفوس، بهترین فایروال در جهان از لحاظ محافظت از شبکه و همچنین امکان تشخیص تهدیدات و علی الخصوص سرعت عکس العمل به آنها میباشد. فایروال Sophos XG رویکرد جدید و تازه ای برای مدیریت، پاسخ به تهدیدات و مانیتورکردن هر آنچه که در شبکه شما اتفاق می افتد را به ارمغان می آورد. سوفوس به دو صورت مجازی و دستگاه فیزیکی ارایه می شود.

فایروال Sophos XG

آخرین فناوری پیشرفته برای محافظت از شبکه خود در برابر باج افزارها. و تهدیدهای پیشرفته از جمله IPS دارای رتبه بالا ، محافظت از تهدیدات پیشرفته ، Cloud Sandboxing و تحلیل تهدیدات کامل با هوش مصنوعی، Dual AV ، کنترل وب و کنترل برنامه ها ، محافظت از ایمیل و یک WAF کامل فراهم می کند و البته تنظیم و مدیریت آن آسان است.

ویژگی ها

- جلوگیری از حملات ساعت صفر - پشتیبانی از SD-WAN - پشتیبانی از انواع پروتکل های تانلینگ - سیستم جلوگیری از نفوذ قدرتمند

ArkaGate

آرکاگیت (ArkaGate) ، يك سخت افزار مدیریت یکپارچه تهدیدات (UTM) و ساخت شرکت "رایان سامانه آرکا " مي‌باشد. این محصول با به کارگیري فن‌آوری‌های پیشرفته امنیتی، شبکه‌هاي کامپیوتري را در مقابل انواع تهدیدات امنیتی، محافظت می‌کند. آرکاگیت، تمامی امکانات امنیتی شامل: فایروال، VPN ، آنتی ویروس، آنتی اسپم، فیلترینگ وب (براساس نام‌سایت، IP و موضوع)، مقابله با تهدید شامل (IPS/IDS) ، مدیریت پهنای باند و حسابرسي اینترنت را در قالب یک دروازه امنیتی کاملا قابل اعتماد ارائه می‌نماید. مدیریت تحت وب قدرتمند و آسان در این محصول، امکان نصب و راه اندازی آن را در سریع ترین زمان ممکن امکان پذیر ساخته است.

ویژگی ها

• دیواره آتش • کنترل کاربران • مدیریت پهنای باند • امنیت ایمیل ها • آنتی اسپم قوی • گزارش گیری کامل از فعالیت کاربران • کنترل مصرف کاربران

SANGFOR

سنگفور

به عنوان فروشنده پیشرو در آسیا و برند برجسته در چین برای بازار مدیریت شبکه ، Sangfor IAM در ربع جادویی گارتنر/ Gartner Magic Quadrant به مدت چهار سال در رده ثبت شده است.مدیریت رفتاری حرفه ای کنترل نرم افزار کاربردی، کنترل ترافیك، کنترل اطلاعات، کنترل hotspot غیر قانونی، تحلیل رفتار ،مدیریت شبکه بی سیم/ وایرلس و سایر ویژگی ها را دارا می باشد که واقعا مدیریت رفتاری اینترنت یکپارچه همه کلاینت ها را در کل شبکه کسب می کند.

به طور موثر از فعالیت‌های غیر مرتبط کارکنان جلوگیری می‌کند. به حداکثر رساندن پهنای باند جلوگیری از نشت و ریسك‌های نظارتی ، حفاظت از امنیت داده‌های اینترنت مدیریت visual و کنترل جامع APs بی سیم/ وایرلس عمدتا به عنوان دستگاه مستقر در دروازه اینترنت برای مدیریت رفتاری اینترنت بکار می‌رود و می‌تواند از محیط ۱۰گیگابایت در هر ثانیه پشتیبانی کند،شبکه های سیمی و بی سیم یکپارچه فراهم کند و می تواند در سایر سناریوها برای امنیت شبکه بکار رود. Sangfor IAM به بیش از ۲۰۰۰۰مشتری در هر صنعتی خدمت رسانی می‌کند.

MAIL SERVER ایمیل سرور

شرکت رایان سامانه آرکا پیشرو در ارایه راهکارهای ایمیل و امنیت ایمیل در ایران است که از سال ۸۳ تاکنون توانسته است بیش از ۳۰۰ پروژه ایمیل را در کشور نصب، راه اندازی و نگهداری کند و به بسیاری از دانشگاههای بزرگ، سازمانها، وزارتخانه ها، شرکت های بزرگ و کوچک، خدمات ایمیل ارائه داده است.

این شرکت موفق به ارایه ایمیل سرور ابری با بستری نو و مدرن شده است. از مهمترین مزایای ایمیل ابری، می توان به مواردی مانند پایداری بالا، نگهداری آسان، هزینه تمام شده پایین و امنیت بالا اشاره کرد.

امنیت ایمیل سرور

- ArkaMX اولین آنتی اسپم بومی کشور - امنیت ایمیل سرور Symantec Messaging Gateway-SMG - دروازه امنیتی ایمیل سرور ProMox - آنتی اسپم SpamTitan
- نرم افزار GFI MailEssentials

ایمیل سرور

- ایمیل سرور ابری آرکا Arka CloudMail - ایمیل سرور MailEnable - ایمیل سرور SmarterMail - ایمیل سرور کریو کانکت Kerio Connect

با استفاده از یک مرورگر وب ، تلفن همراه یا دستگاه رایانه لوحی جلسه را راه اندازی کنید یا به آن بپیوندید. به شرکت کنندگان این امکان را بدهید تا بدون توجه به موقعیت مکانی ، از طریق تلفن یا صوتی یکپارچه در رایانه خود متصل شوند.

نرم MailEnable بر پایه تکنولوژی .Net طراحی شده و از تمامی پروتکلهای استاندارد ایمیل مانند IMPA ,SMTP,POP۳ 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.

SmarterMail یک ایمیل، چت گروهی و سرورهمکاری تیمی با امکانات کامل است که بهترین گزینه برای Microsoft Exchange است.

این برنامه برای تأمین عملکرد مورد نیاز مشاغل ، بدون از بین بردن دسترسی مطمئن و معتبر برای تجارت و ارتباطات شخصی ، طراحی شده است.

MAIL SECURITY امنیت ایمیل

ایمیل یکی از ابزارهای ارتباطی حیاتی شرکتهای امروزی است. که مزایای زیادی مانند افزایش بهره وری، کارایی و صرفه جویی در هزینه ها را به ارمغان می‌آورد. متاسفانه در کنار مزایای بسیار، ارتباطات ایمیلی با تهدیدهای مهمی‌گره خورده است که علاوه بر توانایی تخریب شبکه شما، ممکن است. پیامدهای جدی حقوقی و مالی برای شما و تجارت شما به همراه داشته باشد. اقدام ساده باز کردن ایمیل و یا کلیک بر روی یک لینک می‌تواند ویروس ها را آزاد کند. که علاوه بر تخریب ساختارهای داخلی شبکه شما، می‌تواند پیامدهای ویرانگری را برای کلاینت ها بهمراه داشته باشد.

محصولات امنیت ایمیل رایان سامانه آرکا، با مدیریت ترافیک ایمیل سازمان و با مسدود کردن نامه های ناخواسته، ویروس ها و بدافزارها، سازمان را در برابر تهدیدات محافظت می‌کند.

Symantec

امنیت ایمیل سرور SMG شرکتها/سازمان ها را قادر میسازد تا زیرساخت های ایمیل خود را با روشهایی مانند: محافظت آنتی اسپم و ضد بدافزار بلادرنگ موثر و دقیق، محافظت در برابر حملات هدفمند، فیلتر کردن پیشرفته محتوا، DLP و رمزگذاری ایمیل ایمن سازند.

مدیریت این محصول ساده بوده و بیش از ۹۹ درصد اسپم ها را با کمتر از یک در یک میلیون مثبت کاذب(خطا) به دام میاندازد.

با استفاده از امنیت ایمیل سرور SMG ، سازمان ها میتوانند به طور موثر تهدیدهای جدید پیام رسانی را خنثی کرده، اختلال در شبکه را به حداقل رسانده و بهره وری کارمندان و اعتبار شرکت/سازمان را حفظ کنند.

PROXMOX

امنیت ایمیل Proxmox Mail Gateway یکی از پیشروان راه حل امنیت ایمیل است که از ایمیل سرور شما در برابر تهدیدات ایمیل در لحظه محافظت می کند. سازمانهای بزرگ و کوچک می توانند در ساختار شبکه ای خود در عرض فقط چند دقیقه پلتفرم ضد هرزنامه و ضد ویروس را پیاده سازی و استقرار دهید. استقرار Proxmox Mail Gateway با ویژگی های کامل بین فایروال و ایمیل سرور داخلی شما امکان کنترل همه ترافیک ایمیل های ورودی و خروجی را فراهم می کند.

امنیت ایمیل Proxmox Mail Gateway می تواند دامنه های نامحدود ایمیل سرور را با چندین سرور ایمیل داخلی و میلیون ها ایمیل در روز مدیریت کند. با مجموعه ای از ویژگی های جامع،کلاس سازمانی و با پنل مدیریتی قدرتمند که تحت وب می باشد، متخصصان و مدیران شبکه می توانند کلیه پیام ها را کنترل کرده،هرزنامه ها و ویروس ها را شناسایی و مسدود کنند.

SpamTitan

اسپم تایتان راه حل فوق العاده ساده برای تنظیم و مدیریت ایمیل است. ازجمله ویژگیهای آن می‌توان به مواردی مانند دقت ۹۹.۹۷٪ شناسایی هرزنامه،. مسدود کردن ویروس و بدافزار، کنترل احراز هویت،. اسکن خروجی و همچنین ساختارهای گزارشگری قوی، اشاره کرد.

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.

مدیریت منابع مصرفی(با محصولات بومی)

کنترل میزان مصرف منابع علاوه بر صرفه جویی مالی در هر سازمان، فعالیتی اجتماعی نیز محسوب می شود که از فواید آن همه مردم جهان بهره مند می شوند. شرکت رایان سامانه آرکا، به عنوان پیشرو در ارایه راهکارهای نظارت و مدیریت بر مصرف منابع از سال ۱۳۸۰ با ارایه محصولات شناخته شده جهانی خدمات مربوطه را به بیش از ۲۰۰ سازمان و شرکت بزرگ ارایه کرده است. با در نظر گرفتن نیاز مبرم کشور به محصولات مدیریتی، این شرکت اقدام به طراحی و توسعه نرم افزار های مربوطه نموده است.

چاپ بان

نرم افزار چاپ بان ، نرم افزار مدیریت و نظارت پرینت
نرم افزاری پیشرفته برای مدیریت، نظارت و سهمیه بندی چاپ در شبکه های سازمانی می‌باشد. این محصول توسط شرکت رایان سامانه آرکا که پیشرو در زمینه مدیریت چاپ است، توسعه داده شده است.

- کنترل، نظارت و سهمیه بندی پرینت در شبکه
- صرفه جویی در منابع مصرفی (کاغذ ، تونر و غیره)
- نصب، مدیریت و نگهداری بسیار آسان
- دارای کنسول تحت وب برای کاربران و مدیران
- قابلیت یکپارچگی با اکتیودایرکتوری و اعمال سیاستهای سهمیه بندی بر اساس کاربر، گروه کامپیوتر و چاپگر
- اعلام تاریخچه استفاده از منابع مصرفی
- مدیریت کامل و متمرکز کاربران و تمامی پرینترهای شبکه
- ایجاد گزارشهای مختلف، فیلترهای پیشرفته، گراف مصرف و ...

ArkaGate

آرکاگیت (ArkaGate) ، یك سخت افزار مدیریت یکپارچه تهدیدات (UTM) ساخت شرکت "رایان سامانه آرکا" می‌باشد. این محصول با به کارگیري فن‌آوری‌های پیشرفته امنیتی، علاوه بر اینکه شبکه‌های کامپیوتری را در مقابل انواع تهدیدات امنیتی، محافظت می‌کند، با مدیریت دسترسی کاربران به اینترنت هزینه های سازمان را کاهش می دهد.

آرکاگیت دارای امکانات کامل اکانتینگ اینترنت است:

- کپتیو پرتال قابل سفارشی سازی
- قابلیت اعمال قوانین پهنای باند بر اساسIP، کاربر/گروه، سایت مقصد، زمان، ترافیک ورودی و خروجی سرویس
- قابلیت تعیین تعداد اتصالات هر کاربر
- قابلیت تعیین دسترسی کاربران به اینترنت بر اساس زمان، حجم یا بصورت تلفیقی
- قابلیت تعیین سهمیه مصرف بصورت روزانه، هفتگی، ماهانه یا تنظیم شده توسط مدیر

راهکارهای Monitoring

نرم‌افزار نظارت بر شبکه، دستگاه‌ها، ترافیک و سرورها را در شبکه‌های شرکتی یا آموزشی زیر نظر دارد و در صورت بروز مشکل به مدیران شبکه اطلاع می‌دهد.
این یک سلاح کلیدی در جعبه ابزار یک مدیر شبکه برای عیب‌یابی مشکلات شبکه است.
نرم افزار نظارت بر شبکه می تواند ترافیک شبکه و استفاده از پهنای باند را زیر نظر داشته باشد. می‌تواند بررسی کند که آیا اجزای مهم شبکه، مانند سوئیچ‌ها، روترها و سرورها فعال یا غیرفعال هستند. مدیران شبکه عموماً می‌توانند آستانه‌هایی را برای عملکرد قابل قبول تعیین کنند و اگر نرم‌افزار سرعت پایین، نرخ خطای بالا، دستگاه‌های در دسترس یا زمان پاسخ آهسته را بیابد، می‌تواند هشدارها را از طریق ایمیل یا پیام متنی برای مدیران ارسال کند.

ManageEngine
Powering IT ahead

نرم افزار OpManager

نرم افزار ManageEngine OpManager نرم افزار مدیریت شبکه ای کامل و End- to-End، مناسب شبکه‌های ناهمگون و بزرگ IT، متشکل از تولیدکنندگان مختلف است. این نرم افزار قابلیت های پیشرفته مدیریت کارآیی و خطا را در میان منابع حساس IT از قبیل تجهیزات شبکه فراهم می‌کند.

نرم افزار OpManager ویژگی های پیشرفته در مدیریت کارایی و اشکالات روی منابع مهم فناوری اطلاعات سازمان مانند سرورهای فیزیکی و مجازی، کنترل کننده دامنه، روتر ها، سوئیچ ها، ارتباط WAN، Firewall و دیگر تجهیزات زیر ساخت فناوری و اطلاعات ارائه می‌دهد.

PRTG NETWORK MONITOR

راه حل نظارت برای تمام حوزه های IT

فناوری اطلاعات حوزه های مختلفی دارد که هر کدام نیازمندی های نظارتی خاص خود را دارند:

شبکه، زیرساخت، سخت افزار و برنامه ها تنها چند نمونه هستند.

PRTG همه چیزهایی را که برای نظارت بر تمام حوزه های IT خود نیاز دارید را برای شما فراهم می‌کند.

NETCRUNCH
Monitoring Platform

NetCrunch یک سیستم جامع مانیتورینگ بدون Agent میباشد که قادر به مانیتور کردن هزاران نود شبکه (سویچ، روتر، فایروال، یوپیاس، پرینتر، سنسورها و ...) است. این سیستم بر روی ویندوز نصب شده و دارای کنسول وب، موبایل (Android, iOS) و دسکتاپ است.

SIEM

حملات سایبری امروزی بیش از هر زمان دیگری پیشرفته‌تر شده‌اند و تاکتیک‌های پیشگیرانه رایج استفاده از فایروال‌ها و نرم‌افزارهای آنتی ویروس کافی نیستند. حملات دیگر به سادگی توسط دستگاه های لبه ای که حملات دریافتی از ابر را مسدود می‌کنند متوقف نمی‌شوند، زیرا حملات می‌توانند از داخل شبکه شما انجام شوند. بدافزارها اکنون در ایمیل‌ها، تبلیغات بنری، وب‌سایت‌های جعلی و غیره پیوست شده است و می‌تواند از طریق یک دستگاه داخلی به شبکه شما دسترسی پیدا کند.

سیستم‌های تشخیص نفوذ و پیشگیری(IDS/IPS) به تنهایی قادر به شناسایی یا جلوگیری از بدافزار مانند این نیستند، به همین دلیل است که SIEM بسیار ضروری است.

علاوه بر این، راه‌حل‌های SIEM می‌توانند داده‌ها را از سراسر شبکه شما جمع‌آوری کنند و این داده‌ها را با هم تجزیه و تحلیل کنند تا موارد مثبت **کاذب را محدود کنند. با یک راه حل SIEM شما یک محصول قابل اعتماد دارید که حملات داخل و خارج را شناسایی می کند و تهدیدها را به طور دقیق و بدون ایجاد نتایج کاذب گزارش می کند.**

splunk>

نرم افزار Splunk

نرم‌افزار Splunk دارای سیستم امنیت مبتنی بر تجزیه و تحلیل هوشمند بوده که شامل فرآیند کشف و شناسایی روابط در کلیه داده‌های مرتبط با حوزه امنیت شامل داده‌های زیرساخت‌های IT، محصولات مختلف امنیتی و تمامی داده‌های ماشینی بوده و هدف آن انطباق سریع با تغییرات در تهدیدات و رویارویی با تهدیدات پیشرفته می‌باشد بدین ترتیب که تهدیدات را در کسری از ثانیه شناسایی، تجزیه و تحلیل و در نهایت به آنها پاسخ خواهد داد.

ویژگی‌های کلیدی:

- شناسایی، بررسی و گزارش بلادرنگ موارد کلاهبرداری و سوء استفاده
- افزایش اثربخشی فرآیندها و پرسنل SOC
- دارای قابلیت پیاده‌سازی به صورت Cloud،On-Premise و ترکیبی از این دو حالت
- قابلیت مقیاس‌پذیری و چابکی

solarwinds

SolarWinds Log and Event Manager محصولی برای اطلاعات امنیتی و مدیریت رویداد (SIEM) است. محصول SolarWinds SIEM سوابق گزارش رویدادهای امنیتی را از کنترل‌های امنیتی سازمان، سیستم‌عامل‌ها، برنامه‌ها و نرم‌افزارهای دیگر جمع‌آوری می‌کند. همانطور که گزارش‌ها جمع‌آوری می‌شوند، SolarWinds Log و Event Manager آن‌ها را برای شناسایی فعالیت‌های مخرب بالقوه، مانند حملات یا عفونت‌های بدافزار، تجزیه و تحلیل می‌کند. این به مدیران هشدار می‌دهد تا بتوانند به صورت دستی به یک حادثه پاسخ دهند، یا محصول می‌تواند به طور خودکار حملات را از طریق تعاملات مختلف با سایر کنترل‌های امنیتی سازمانی متوقف کند.

ویژگی های کلیدی:

- جمع آوری و عادی سازی لاگ متمرکز
- شناسایی و پاسخ خودکار تهدید
- ابزارهای گزارش انطباق یکپارچه
- داشبورد و رابط کاربری بصری
- نظارت بر یکپارچگی فایل داخلی
- صدور مجوز ساده و مقرون به صرف

VDI مجازی سازی و جداسازی اینترنت از اینترانت

استقرار برنامه های کاربردی کاربران، می تواند بسیار وقت گیر و پرهزینه برای ارگانها و سازمان ها باشد این برنامه ها احتیاج دارند که بصورت مداوم برای کاربران جدید و دستگاههای جدید راه اندازی شوند همین امر می تواند بخش IT را درگیر مسائل مختلف روزمره برای ارتباط کاربر با این برنامه ها نماید. در دسترس بودن برنامه های کاربردی در سایه امنیت یکی از دغدغه های مدیران است، مجازی سازی به عنوان یک راه حل برای تسهیل این ارتباط و کاهش هزینه ها در حال حاضر بسیار مورد توجه قرار گرفته است که به سرعت به نیازهای کسب و کار شما پاسخ درست می دهد. ساختار های سلسله مراتبی و عدم مدیریت مرکزی در زیرساخت های سنتی موضوعی بود که برطرف کردن آن و پیاده سازی مدیریت مرکزی هزینه های گزاف را می طلبید. در نتیجه نرم افزارهای سازمانی از سرورهای فیزیکی به ماشین های مجازی انتقال داده شدند.

هرچند که این پراکندگی به نگهداری سریع برنامه ها کمک میکرد و با جداسازی هر یک از سیستم ها از یکدیگر بر روی شبکه باعث افزایش امنیت میشد، هزینه مصرف برق را نیز افزایش می داد و نیازمند تلاشهای مدیریتی بیشتر و پیگیری های دقیقتری نیز بود.

در نهایت باید گفت که مجازی سازی یک نقطه میانی در بین محیط های متمرکز و غیر متمکز است. به زودی شما مجبور خواهید بود تا برای هر برنامه یک قطعه سخت افزار جداگانه تهیه کنید. اگر هر یک از برنامه ها دارای محیط عملکرد جداگانه ای روی یک قطعه سخت افزاری باشد، شما قادر خواهید بود هم از مزایای امنیت و ثبات بهره ببرید و هم از منابع سخت افزاری آن.همچنین، ماشین های مجازی از میزبان مستقل هستند.

VDI مجازی سازی و جداسازی اینترنت از اینترانت

Horizon View نام نرم افزاری است که برای این منظور ساخته شده است که شما دسکتاپ و یا نرم افزار های خود را به صورت مجازی در اختیار داشته باشید و از آن در هر مکان و زمانی و با هر دستگاهی از آن استفاده کنید. رکت VMware در سال ۲۰۱۶ با ارائه نسخه ۷ نرم‌افزار VMware Horizon، تحول بزرگی را در مجازی سازی دسکتاپ یا به عبارتی VDI ایجاد نموده است. VMware Horizon ۷ (مجازی‌سازی دسکتاپ) با ارائه بهترین شرایط Cloud و Mobile، به طور اساسی VDI را تغییر داده و مزایایی همچون سادگی، امنیت، سرعت و Scale را با هزینه کمتری برای کاربران ارائه نموده است. علاوه بر آن Horizon ۷، قابلیت عملکرد را تا ۳۰ برابر سریع‌تر و در عین حال هزینه‌ها را نیز نسبت به راهکارهای سنتی تا ۵۰ درصد کاهش می‌دهد.

امروزه End Userها می‌توانند جهت انجام امور از انواع تجهیزات جدید بهره گیرند و به برنامه‌های Windows و Linux در کنار برنامه‌های اندروید یا iOS که بیش از همیشه قابلیت سیار بودن را دارند، دسترسی یابند.

سیتریکس برنامه ای است برای پیاده سازی تکنولوژی مجازی سازی. برنامه ای همچون vmWare با ویژگی های مختلف که با توجه به زیرساخت شبکه شما پیاده سازی می شود. شرکت سیتریکس یکی از شرکت های پرآوازه و قدیمی در این صنعت شناخته می شود، که کار خودش را از سال ۱۹۸۹ آغاز کرده است. ولی به دلیل ناشناخته بودن محصولات این کمپانی در کشور ما، بر این باور غلط هستیم و نگرانی هایی در خصوص استفاده از محصولات این شرکت داریم. در حالی که شرکت سیتریکس با ارائه محصولاتی نظیر XenServer و XenDesktop یکی از محبوب ترین و قویترین محصولات در عرصه تکنولوژی مجازی سازی به شمار می آید.

سیتریکس را انتخاب کنیم یا VmWare؟

پاسخ به این سوال و مقایسه این دو کمپانی مثل این می ماند که بگوییم ویندوز بهتر است یا لینوکس. در صورتی که هر دوی این سیستم عامل ها کارایی مخصوص به خود را دارند، که دیگری نمی تواند از عهده آن بربیاید. سیتریکس یا VmWare هم دقیقا به همین شکل است. پس بهترین جواب به این سوال این است که بگوییم با کارشناسان ما تماس بگیرید

VDI مجازی سازی و جداسازی اینترنت از اینترانت

PROXMOX

Proxmox VE یک راه حل کامل منبع باز برای مجازی سازی سازمانی است که hypervisor های KVM و کانتینرهای (LXC)، عملکردهای شبکه و فضای ذخیره سازی مبتنی بر نرم افزار را در قالب یک سیستم عامل کاملاً یکپارچه ارایه می‌کند. با رابط کاربری مرکزی می‌توانید به راحتی ماشین های مجازی و کانتینرها را اجرا کنید، منابع ذخیره سازی مبتنی بر نرم افزار و شبکه را مدیریت کنید، خوشه های دسترسی بالا(HA) و چندین ابزار خارج از جعبه مانند پشتیبانگیری/ بازیابی، انتقال زنده، تکثیر ذخیره سازی یا فایروال یکپارچه را مدیریت کنید.

Proxmox VE شما را قادر می‌سازد حتی برنامه های کاربردی پرتقاضای لینوکس و ویندوز را مجازی سازی کنید.

Proxmox VE با ترکیب دو فناوری مجازی سازی در یک سیستم عامل، حداکثر انعطاف پذیری را در مرکز داده شما ایجاد می‌کند. این امر شامل پشتیبانی از قابلیت دسترسی بالا (HA) و – به لطف طراحی منحصر به فرد چندگانه – عدم نیاز به یک سرور مدیریت اضافی است. بنابراین در منابع صرفه جویی کرده و به HA بدون یک نقطه خرابی (SPOF) دست می‌یابید.

Parallels

Parallels RAS یک راهکار جامع برای پیاده سازی Virtual Desktop Infrastructure است. روش کار بدینصورت است که برنامه های مورد نظر در سرور نصب شده و کاربران بدون اینکه متوجه شوند از طریق این نرم افزار به سرور وصل شده و برنامه های کاربردی خود را اجرا می کنند.کاربران قادرند با هر نوع سیستم عامل (موبایل، ویندوز و لینوکس) و با کمترین امکانات سخت افزاری، و در هر جلسه مختص خود به نرم افزار متصل شده و کارهای روزانه خود را انجام دهند.

لازم به ذکر است، همه تغییرات و رویداد ها برای امنیت بیشتر ثبت میشود.

این نرم افزار برای سازمان هایی که سالانه هزینه گزافی برای تامین و نگهداری سیستم های کامپیوتری خود پرداخت میکنند، بسیار مناسب می باشد. علاوه بر آن کاربر کارهای خود را بر روی سرور با سرعت بیشتری انجام داده و این امر باعث افزایش میزان رضایت کاربر همچنین افزایش بهره وری سازمان می‌گردد. چرا RAS Parallels ؟تجربه کاربری فوق العاده

نرم افزار Parallels RAS کاربران را قادر می سازد تا از طریق هر سیستم عامل (Parallels Clients برای ویندوز ، iOS / iPadOS ، Linux ، MAC OS ، Chrome OS ، Android و مرورگر HTML۵) روی برنامه ها و دسک تاپ ها کار کنند. ورود (لاگین) بسیار سریع ، بازیابی سریع پرونده و پاسخ سریع برنامه ، علاوه بر انجام چند وظیفه ای بدون دردسر .

TSPLUS SECURE REMOTE ACCESS

نرم افزار مجازی سازی TSplus ابزاری است کاربردی در سیستم عامل های که کاربران می توانند با استفاده از این نرم افزار برنامه های در سیستم عامل و دسکتاپ را مجازی کنند . در نرم افزار TSPlus متمرکز سازی دیتاها در دیتاسنتر ها و مجازی سازی سرور ها و برنامه ها از اهم فعالیتهای بخش فن آوری اطلاعات تمامی کمپانی ها شده است، از این رو بهره گیری از آخرین Technologyها و Standardهای معتبر در زمینه های مجازی سازی Server ها و برنامه ها اهمیت ویژه ای در موفقیت این گونه پروژه ها دارد و به شما امکان می‌دهد تا بتوانید از طریق پروتکل RDP از روی هر دستگاهی به برنامه‌ها و دسکتاپ های مجازی دسترسی داشته باشید برای اینکه با این تکنولوژی بیشتر آشنا شوید می بایست ابتدا به انواع مجازی سازی ها اشاره کنیم مجازی سازی برنامه های کاربردی ، مجازی سازی Server ها و مجازی سازی Desktop کاربران که نرم افزار TSPlus آن ها را پشتیبانی می کند .

شما می توانید بدون نیاز به CALS با این برنامه به راحتی کار کنید.

با استفاده از گزینه AdminTool فرآیند مدیریت سرور برای کاربران گسترده تر خواهد شد و همچنین نرم افزار TSplus انتقال فایل ها بین کامپیوتر و سرور های TSplus را سریع تر انجام می دهد.

Backup پشتیبان گیری و بازیابی اطلاعات

امروزه با رشد سریع داده ها در دنیای مدرن و نیاز بالای SLA تجاری ، حفاظت از داده ها بیشتر و بیشتر مورد توجه بیشتر صنایع، به ویژه شرکت های IT قرار می گیرد. شما به عنوان فرد مسئول در سازمان باید یک استراتژی و خط مشی مناسب برای بکاپ‌گیری تان طراحی کنید. هر چه که زمان میگذرد، افراد و شرکتها با حجم بالا و غیر قابل کنترلی از اطلاعات روبرو میشوند، که منظم‌سازی و دسته‌بندی آنها روز به روز سخت تر شده و مهمتر اینکه بدون حمایت لازم رها شده‌اند. با این تفاسیر مهمترین نکته در پشتیبان‌گیری، برنامه‌ریزی برای یک استراتژی صحیح و کارآمد است، تا در گذر زمان و با بالا رفتن حجم اطلاعات، کارایی لازم را داشته باشد.

SEP
Backup & Disaster Recovery

امروزه با رشد سریع داده ها در دنیای مدرن و نیاز بالای SLA تجاری حفاظت از داده ها بیشتر و بیشتر مورد توجه بیشتر صنایع، به ویژه شرکت های IT قرار می گیرد.
شما بعنوان فرد مسئول در سازمان باید یک استراتژی و خط مشی مناسب برای بکاپ‌گیری تان طراحی کنید. هر چه که زمان میگذرد، افراد و شرکتها با حجم بالا و غیر قابل کنترلی از اطلاعات روبرو میشوند، که منظم‌سازی و دسته‌بندی آنها روز به روز سخت تر شده و مهمتر اینکه بدون حمایت لازم رها شده‌اند. با این تفاسیر مهمترین نکته در پشتیبان‌گیری، برنامه‌ریزی برای یک استراتژی صحیح و کارآمد است، تا در گذر زمان و با بالا رفتن حجم اطلاعات، کارایی لازم را داشته باشد.

vinchin

نرم افزار Vinchin Backup & Recovery یک راه حل پشتیبان گیری با کاربردی آسان، قابل اعتماد و مقرون به صرفه است که برای محافظت از انواع محیط های مجازی از جمله VMware ، Hyper-V ، XenServer ، Sangfor ، OpenStack ، XCP ng ، OLVM ، RHV / oVirt و Huawei FusionCompute طراحی شده است.
Vinchin Backup & Recovery توسط برترین فروشندگان مجازی سازی جهان مورد تایید قرار گرفته و گواهینامه هایی از جمله VMware Ready ، Citrix Ready ، Redhat Certified Technology و غیره را به دست آورده است. شرکت ها می توانند از مزایای کامل نرم افزار پشتیبان Vinchin برای محافظت از محیط مجازی سازی خود و کاهش ریسک پروژه بهره مند شوند.

VERITAS

وریتاس دارای ساختاری هدفمند و قوی جهت بکاپ گیری از تمامی داده های دیتاسنتر هم بصورت Local و هم بصورت Remote می باشد.
این محصول با بهره گیری از تکنولوژی روز دنیا و بصورت کاملا ساده از انتهایی ترین منابع موجود در شبکه بکاپ گرفته تا در هر زمان و هر وضعیت شبکه ای توان Restore کردن را دارا باشد. با استفاده از این قابلیت می توان backup ها را روی سیستمی دیگر با مشخصات سخت‌افزاری متفاوت، بازیابی نمود.

مدیریت آسیب پذیری

آسیب پذیری‌های شبکه، نمایان‌گر حفره‌های امنیتی هستند که هکر با سوءاستفاده از آن‌ها می‌تواند به داراهایی شبکه آسیب بزند، حمله DDoS انجام دهد و یا اطلاعات حساس شرکت را سرقت کند. مهاجمین دائما به دنبال آسیب‌پذیری‌های جدید یا آسیب پذیری‌های قدیمی‌هستند که هنوز رفع نشده‌اند تا بتوانند آن‌ها را اکسپلویت کنند. وجود یک فریم‌ورک مدیریت آسیب پذیری در مکان‌هایی که امنیت اهمیت دارد، ضروری است زیرا باید به طور منظم آسیب‌پذیری‌های جدید اسکن شوند و از نقایض امنیتی جلوگیری شود. بدون داشتن یک سیستم مدیریت Patch و تست آسیب پذیری، شکاف‌های امنیتی قدیمی که رفع نشده‌اند، می‌توانند برای مدتی زیادی در شبکه باقی بمانند. این موضوع، شانس بیشتری به مهاجمان می‌دهد تا آسیب‌پذیری‌ها را اکسپلویت کنند و از آن‌ها برای انجام حملات خود استفاده کنند.

ManageEngine Desktop Central

نرم‌افزار ManageEngine Desktop Central

Desktop Central یک راه حل UEM است که به مدیریت سرورها، دسکتاپ ها و دستگاه های تلفن همراه از کنسول واحد کمک می کند. این چرخه مدیریت کامل دسکتاپ و دستگاه تلفن همراه را از ابتدا تا انتها خودکار می‌کند تا به کسب‌وکارها کمک کند هزینه‌های زیرساخت فناوری اطلاعات خود را کاهش دهند، به موفقیت عملیاتی برسند، بهره‌وری را بهبود بخشند، و با آسیب‌پذیری‌های شبکه مبارزه کنند.

Desktop Central با ماژول Patch Management خود این امکان را برای مدیران سیستم فراهم می کند تا به تهدیدات رایانه در زمان سریع پاسخ دهند. همه اینها مطابق با چرخه حیات مدیریت وصله و با نگاهی تازه به امنیت شبکه است. مدیران می‌توانند از Desktop Central برای اسکن شبکه، شناسایی وصله‌های گمشده، دانلود وصله‌های گمشده و استقرار آنها در رایانه‌هایی با استفاده از سیستم‌عامل‌های Windows و MaC استفاده کنند.

acunetix

Acunetix

Acunetix به عنوان اولین شرکتی که اسکنر آسیب پذیری وب را به صورت کاملاً اختصاصی و کاملاً خودکار ساخته است، تجربه بی‌نظیری را در این زمینه نشان داده و یک راه حل قابل اعتماد جامع برای همه نیازهای امنیتی برنامه وب شما ارائه می‌دهد.

Acunetix به طور خودکار تمام آسیب‌پذیری‌ها را بر اساس تأثیر بالقوه آنها ارزیابی می کند. هنگام ارزیابی، Acunetix به طور خودکار اهمیت مورد پیکربندی دارایی اسکن شده را در نظر می گیرد.

GFI LanGuard

GFI LanGuard یک ابزار کارآمد برای کشف و مدیریت آسیب‌پذیری در سازمان‌ها است، این راهکار امنیتی مجهز به یک کنسول مدیریتی است که از طریق آن می‌توانید انواع تجهیزات شبکه و سیستم عامل‌ها از قبیل ویندوز، مک، لینوکس و حتی ماشین‌های مجازی (Virtual Machine) را برای مانیتور شدن اضافه کنید. GFI LanGuard می‌تواند کل شبکه را به صورت خودکار مانیتور کند و به محض کشف آسیب‌پذیری در هر کدام از آن‌ها به سرعت وارد عمل شده و آن‌ها را برطرف کند.

جوایز و نشان ها


پروانه فعالیت در حوزه خدمات فنی افتا

شماره پروانه: ITO-NAMA-TS-0175

به استناد قوانین «برنامه های پنج‌ساله توسعه جمهوری اسلامی ایران»، «وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات»، «سند راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا)» و در راستای اجرای «مصوبه مورخ ۱۳۸۸/۱۲/۲۴ هیات محترم دولت» و با توجه به احراز صلاحیت به‌عمل آمده به:

شرکت رایان سامانه آرکا

اجازه داده می‌شود به مدت دو سال از تاریخ صدور پروانه تحت نظارت سازمان فناوری اطلاعات ایران با گرایش

نصب و پشتیبانی محصولات فتا

در کشور فعالیت نماید.


پروانه فعالیت در حوزه خدمات عملیاتی افتا

شماره پروانه: ITO-NAMA-OS-0206

به استناد قوانین «برنامه های پنج‌ساله توسعه جمهوری اسلامی ایران»، «وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات»، «سند راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا)» و در راستای اجرای «مصوبه مورخ ۱۳۸۸/۱۲/۲۴ هیات محترم دولت» و با توجه به احراز صلاحیت به‌عمل آمده به:

شرکت رایان سامانه آرکا

اجازه داده می‌شود به مدت دو سال از تاریخ صدور پروانه تحت نظارت سازمان فناوری اطلاعات ایران با گرایش

امن سازی و مقاوم سازی سامانه ها، زیرساخت ها، سرویس ها

در کشور فعالیت نماید.


Uluslararası Standart Sertifikasyon Enstitüsü
International Standards Certification Institute

TS EN ISO 9001 : KALİTE YÖNETİM SİSTEMİ BELGESİ
TS EN ISO 9001 : QUALITY MANAGEMENT SYSTEM CERTIFICATE

Firma Adı / Company Name : Rayan Samaneh Arka
Firma Adresi / Company Adress : Shahid Beheshti street, Abrisham Tower, 6th floor, unit 8, Tabriz, Iran
Belge Kapsamı / Certificate Scope : Bilgisayarların, çevre donanımlarının ve yazılım programlarının perakende ticareti / Retail sale of computers, peripheral equipment and software programs
EA : 29
Sertifika No / Certificate Number : KYS522054200
İlk Belgelendirme / First Certification : 18.06.2022
1. Gözetim Tarihi / 1. Custody Date : 18.06.2023
2. Gözetim Tarihi / 2. Custody Date : 18.06.2024
Belge Süresi / Certification Duration : 3 YIL / YEARS
Belge Bitiş Süresi / Certification Ends Duration : 18.06.2023
Revizyon No/Tarih / Revision Number/ Date : 00 / --

Sertifika • Certificate • Zertifikat • Certificat • Сертификат • πιστοποιητικό • certificaat


International Standards Certification Institute

TS EN ISO/IEC 27001: BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ BELGESİ
TS EN ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT SYSTEM CERTIFICATE

Firma Adı / Company Name : Rayan Samaneh Arka
Firma Adresi / Company Adress : Shahid Beheshti street, Abrisham Tower, 6th floor, unit 8, Tabriz, Iran
Belge Kapsamı / Certificate Scope : Bilgisayarların, çevre donanımlarının ve yazılım programlarının perakende ticareti / Retail sale of computers, peripheral equipment and software programs
EA : 29
Sertifika No / Certificate Number : BTG5222040000
İlk Belgelendirme / First Certification : 18.06.2022
1. Gözetim Tarihi / 1. Custody Date : 18.06.2023
2. Gözetim Tarihi / 2. Custody Date : 18.06.2024
Belge Süresi / Certification Duration : 3 YIL
Belge Bitiş Süresi / Certification Ends Duration : 18.06.2023
Revizyon No/Tarih / Revision Number/ Date : 00 / --

Sertifika • Certificate • Zertifikat • Certificat • Сертификат • πιστοποιητικό • certificaat


سازمان نظام صنفی رایانه ای استان آذربایجان شرقی
مجوز فعالیت

سازمان نظام صنفی رایانه‌ای کشور
استان آذربایجان شرقی

شماره: ۲۹/ص/۱۴۰۰
تاریخ عضویت اولیه: ۱۳۹۹/۰۶/۲۷
تاریخ اعتبار: ۱۴۰۱/۰۶/۲۶

بدینوسیله به شرکت (رایان سامانه آرکا (با مسئولیت محدود)) به مدیریت آقا / خانم آیدین مهدی پور و شناسه ملی ۱۰۳۲۰۴۹۷۸۰۳ با شماره نظام صنفی رایانه‌ای ۱۴۱۰۰۴۹۰ اجازه داده می‌شود که طبق قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹/۱۰/۴ مجلس شورای اسلامی و آیین‌نامه اجرایی شماره ۲۱۱۸۵/ت۶۰۸۹ه‍ـ مورخ ۱۳۸۳/۰۴/۲۴ مصوب دولت جمهوری اسلامی تحت پوشش نظام صنفی رایانه‌ای استان آذربایجان شرقی در زمینه فعالیت خدماتی اطلاعات و ارتباطات در نشانی میدان منصور، برج ابریشم، طبقه ۵، واحد ۷ به فعالیت بپردازد.

صحت این مجوز در سایت Azerbaijansh.irannsr.org قابل مشاهده است.

حسین علی محمدی
رئیس هیات مدیره

شعله نهاوندی
دبیر نظام


ریاست جمهوری
سازمان برنامه و بودجه کشور

شماره: ۵۰۷۱۱۲
تاریخ: ۱۳۹۹/۰۹/۲۵

گواهینامه صلاحیت خدمات انفورماتیکی

جناب آقای آیدین مهدی پور
مدیرعامل محترم شرکت رایان سامانه آرکا
شماره ثبت: ۳۹۹۹۷۶

به استناد آیین‌نامه احراز صلاحیت و رتبه‌بندی شرکت‌های انفورماتیکی و با رعایت مفاد بخشنامه شماره ۱۰۰/۱۰۳۵۵۶ مورخ ۱۳۸۷/۱۱/۰۷ و سایر مقررات مربوطه، و با توجه به احراز شرایط لازم و تایید صلاحیت آن شرکت در سامانه جامع تشخیص صلاحیت عوامل نظام فنی اجرایی به این وسیله صلاحیت آن شرکت برای انجام خدمات فناوری اطلاعات از تاریخ صدور این گواهینامه تا پایان دوره ارزشیابی و حداکثر تا تاریخ ۱۴۰۱/۰۹/۲۵ اعلام می‌گردد.

شناسه ملی شرکت : ۱۰۳۲۰۴۹۷۸۰۳
مقتضی است برای مشاهده جزئیات گواهینامه صادره به پایگاه https://sajar.mporg.ir مراجعه فرمایید.

رعایت قانون برگزاری مناقصات ابلاغیه شماره ۱۳۰۸۹۰ مورخ ۱۳۸۳/۱۱/۱۷ رییس مجلس شورای اسلامی، آیین‌نامه‌های اجرایی مربوطه و ظرفیت کاری مجاز در زمان ارجاع کار توسط آن شرکت ضروری است.

سیدجواد قانع‌فر
رئیس امور نظام فنی اجرایی، مشاورین و پیمانکاران

تماس با ما

Email: info@arka.ir

WhatsApp: +۹۸۹۹۱۹۰۰۳۲۱۹

Telegram: t.me/rayansamanarka

Instagram: rayansamanarka

آدرس : تهران، خیابان شهید بهشتی، خ پاکستان، کوچه ۴ پلاک ۱۱ واحد ۷

تلفن: ۰۲۱۹۱۳۰۰۴۷۶ – ۰۲۱۸۸۸۰۴۹۶۱

دفتر تبریز: چهارراه منصور، برج ابریشم، طبقه ۶، واحد ۸

تلفن: ۰۴۱۳۵۵۹۵۲۳۰