رَسیس

مراقب دنیای دیجیتال شما

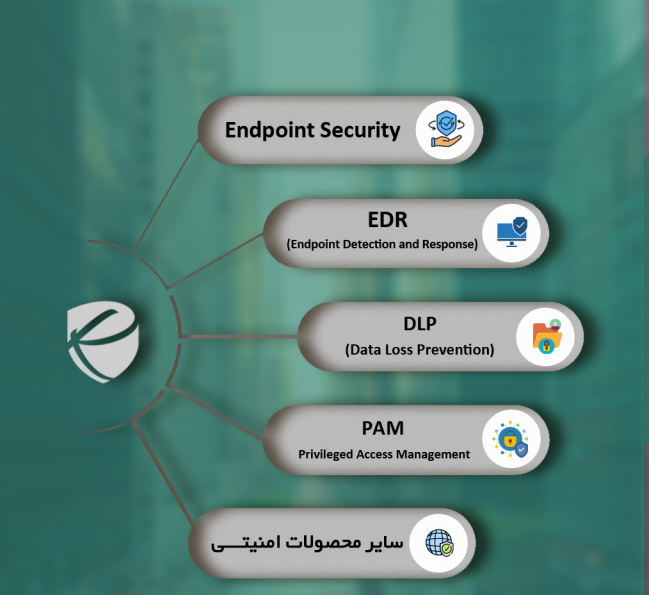
کمپانی پروفایل

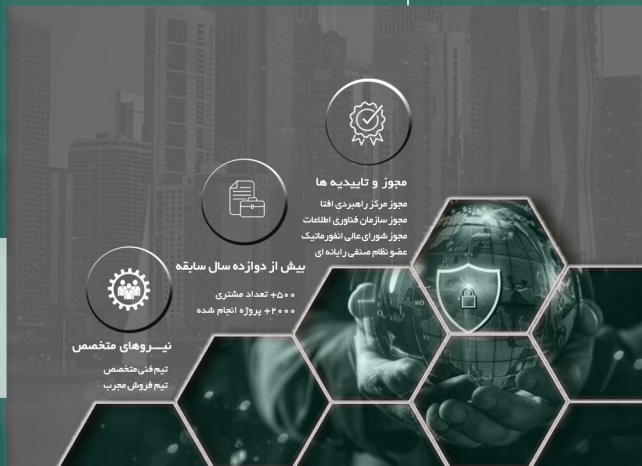
www.rasiss.com

درباره شرکت رَسیس

شرکت رَسیس پردازش پارس در سال ۱۳۹۱ تأسیس و از همان ابتدا به طور تخصصی بر روی امنیت کامپیوترهای شخصی و شبکه های کامپیوتری متمرکز شد. در سالهای ابتدایی علاوه بر امنیت شبکه های سازمانی، بخش مهمی از کار این شرکت به فروش و خدمات پس از فروش محصولاتی متنوع از آنتی ویروسهای خانگی اختصاص یافت. این شرکت از سال ۱۳۹۴ با تمرکز بر محصولات و خدمات امنیت شبکه سازمانی فعالیت خود را گسترش داد. از سال ۱۳۹۷، با رویکرد جدید ارائه خدمات مشاوره‌ای و پشتیبانی در حوزه امنیت اطلاعات، توانست رضایت حداکثری مشتریان را جلب کند.تفاوت اصلی رَسیس ارائه خدمات بر مبنای اصول امنیتی به‌جای وابستگی صرف به محصولات است و خدمات آن تمام نیازهای امنیت شبکه سازمانی را پوشش می‌دهد.

رَسیس
مراقب دنیای دیجیتال شما





مشهد، خیابان سلمان فارسی، مقابل سلمان ۷، پلاک ۳۳ (ساختمان آبشار)، طبقه سوم، واحد ۶

۰۵۱-۳۸۴۷ ۸۱۳۰-۵

info@rasiss.com

1 EndPoint Security

حفـــاظت از اندپوینت‌ها

حفاظت از اندپوینت‌ها (Endpoint Protection) در شبکه‌ها به‌عنوان یکی از ارکان اساسی امنیت سایبری و زیرساخت‌های دیجیتال هر سازمان محسوب می‌شود. اندپوینت‌ها به هر دستگاه یا وسیله‌ای اطلاق می‌شود که به شبکه متصل است، مانند کامپیوترها، لپ‌تاپ‌ها، تلفن‌های هوشمند، تبلت‌ها، پرینترها و دستگاه‌های اینترنت اشیاء (IoT). این دستگاه‌ها به‌عنوان نقطه ورود اطلاعات و داده‌ها در شبکه، می‌توانند هدف حملات سایبری مختلفی مانند ویروس‌ها، بدافزارها، حملات فیشینگ، و حملات مبتنی بر نقص‌های نرم‌افزاری قرار گیرند. با توجه به این‌که اندپوینت‌ها به طور مستقیم به منابع حیاتی اطلاعاتی دسترسی دارند، حفاظت از آن‌ها نه‌تنها از سرقت داده‌ها جلوگیری می‌کند بلکه از انتشار تهدیدات به سایر قسمت‌های شبکه نیز پیشگیری می‌کند. حملات سایبری معمولاً از طریق آسیب‌پذیری‌های موجود در این دستگاه‌ها آغاز می‌شود و پس از ورود، می‌تواند به سرعت گسترش یابد و آسیب‌های زیادی به زیرساخت‌های شبکه وارد کند. برای حفظ امنیت اندپوینت‌ها، پیاده‌سازی لایه‌های امنیتی متعدد ضروری است.

مخاطبین

این راهکار به‌ویژه برای سازمان‌ها و شرکت‌هایی طراحی شده است که نیاز به حفاظت از دستگاه‌ها و سیستم‌های متصل به شبکه خود دارند. تمامی دستگاه‌هایی که به شبکه‌های داخلی و خارجی متصل هستند، اعم از کامپیوترها، موبایل‌ها، تبلت‌ها، و دستگاه‌های اینترنت اشیاء (IoT)، باید تحت پوشش این راهکار امنیتی قرار گیرند. نظارت مستمر بر دستگاه‌ها و سیستم‌ها است. با پیاده‌سازی این راهبردها، سازمان‌ها قادر خواهند بود از دستگاه‌های خود در برابر حملات سایبری و تهدیدات در حال ظهور به‌طور مؤثر محافظت کنند.

الزامات امنیتی دستگاه‌ها

الزامات این راهکار شامل کنترل‌های ضروری برای کاهش آسیب‌پذیری‌ها و تهدیدات امنیتی در دستگاه های متصل به شبکه است. این اقدامات باید به‌صورت منظم و در راستای شناسایی و مقابله با تهدیدات جدید به‌روزرسانی شوند. هدف این بخش، ایجاد چارچوبی برای بهبود مستمر امنیت اندپوینت‌ها در سازمان‌ها است تا از حملات احتمالی به‌ویژه از طریق دستگاه‌های خارجی و غیرمجاز جلوگیری شود. همچنین، سطح امنیتی هر سازمان با توجه به ارزیابی‌های ریسک‌پذیری و نیازهای خاص آن تعیین و در برنامه‌های عملیاتی گنجانده خواهد شد.

راهبردها و اقدامات پیشگیرانه

این بخش به تشریح روش‌های پیشگیرانه برای تقویت امنیت اندپوینت‌ها و مقابله با تهدیدات جدید می پردازد. این اقدامات شامل اعمال سیاست‌های دسترسی رمزنگاری داده‌ها، استفاده از آنتی‌ویروس‌ها و فایروال‌ها، و نظارت مستمر بر دستگاه‌ها و سیستم‌ها است. با پیاده‌سازی این راهبردها، سازمان‌ها قادر خواهند بود از دستگاه‌های خود در برابر حملات سایبری و تهدیدات در حال ظهور به‌طور مؤثر محافظت کنند.

برنـــدها

kaspersky

محصولات کسپرسکی با رویکردی یکپارچه و مدرن، امنیت را در تمام سطوح کسب وکار تضمین می‌کنند. این محصولات شامل ابزارهایی برای حفاظت از دستگاه های مختلف، امنیت شبکه، مدیریت تهدیدات و حفاظت از داده‌های حساس هستند. از سوی دیگر، محصولات این کمپانی به سازمان‌ها این امکان را می دهد که با استفاده از خدمات مدیریتی، امنیت سایبری خود را به صورت مداوم زیر نظر داشته باشند و در صورت بروز هر گونه مشکل، سریعاً اقدام کنند.

SANGFOR

راهکارهای امنیتی سنگفور با تمرکز بر فناوری‌های پیشرفته، از جمله فایروال های هوشمند، آنتی‌ویروس‌های قدرتمند، و سیستم‌های تشخیص تهدید مبتنی بر هوش مصنوعی، شناخته می‌شوند. این راهکارها با شناسایی و خنثی‌سازی تهدیدات سایبری، به سازمان‌ها امکان می‌دهند امنیت شبکه‌ها و داده‌های خود را به‌بالاترین سطح ارتقا دهند و از حملات پیچیده سایبری به‌طور مؤثر محافظت کنند.

Bitdefender

راهکار امنیتی بیت‌دیفندر شامل ابزارهای امنیتی قدرتمند است که با موتور منحصر به‌فرد خود برای مدیریت یکپارچه ایستگاه‌های کاری و سرورها طراحی شده است. این ابزارها به سازمان‌ها امکان حفاظت کامل در برابر تهدیدات دیجیتال را می‌دهند.

Trellix

ترلیکس آنتی ویروس قدرتمندی است که با استفاده از تکنولوژی‌های نوین، اطلاعات سازمان را در برابر انواع ویروس‌ها، بدافزارها، حملات شبکه‌ای و تهدیدات سایبری محافظت می‌کند. این نرم‌افزار با تحلیل‌های ایستا و پویا، بررسی دقیق پیشینه و پویش‌های رفتارشناسانه، علاوه بر شناسایی و کشف بهره‌جویان بالقوه، به شناسایی تهدیدات جدید و ناشناخته می‌پردازد و با ارائه راهکارهای امنیتی جامع، سازمان‌ها را در برابر تهدیدات نوظهور و پیچیده ایمن می‌سازد.

eset

راهکارهای امنیتی ESET شامل محصولات و خدماتی هستند که هر کدام برای بخش خاصی از نیازهای امنیتی سازمانی تهیه شده‌اند. از مزایای استفاده از راهکارهای ESET Business برای سازمان‌ها و کسب و کارها می‌توان به محافظت چندلایه اشاره کرد که ترکیب فناوری‌های مختلف برای محافظت جامع است.

2 EDR
(Endpoint Detection and Response)

راهکار جامع شناسایی و پاسخ به تهدیدات پیشرفته

راهکارهای پیشرفته EDR بعنوان نسل جدید حفاظت از اندپوینت‌ها، بر شناسایی، تحلیل، و پاسخ سریع به تهدیدات پیچیده سایبری تمرکز دارند. این فناوری با استفاده از جمع‌آوری و تحلیل داده‌های رفتاری دستگاه‌ها، توانایی شناسایی حملات ناشناخته و اقدامات مخرب را در زمان واقعی فراهم می‌کند. سیستم‌های EDR قابلیت‌هایی مانند تشخیص تهدیدات پیشرفته، تحلیل رفتارشناسانه، و پاسخ خودکار به رخدادها را ارائه می‌دهند. این راهکار نه‌تنها به سازمان‌ها در مدیریت ریسک‌های امنیتی کمک می‌کند، بلکه از طریق ارائه دیدگاه جامع به تیم های امنیتی امکان بررسی دقیق‌تر و کاهش زمان واکنش را می‌دهد. با EDR، سازمان‌ها می توانند امنیت زیرساخت‌های خود را به سطحی جدید ارتقا داده و در برابر تهدیدات نوظهور ایمن بمانند.

قابلیت‌های پیشرفته راهکار EDR

- ☑ **شناسایی پیشرفته تهدیدات:**
  تشخیص تهدیدات سایبری پیچیده با استفاده از تحلیل‌های رفتارشناسانه و الگوریتم‌های هوش مصنوعی.
- ☑ **تحلیل و بررسی جامع:**
  جمع‌آوری و تحلیل داده‌های رفتاری از تمامی اندپوینت‌ها برای شناسایی الگوهای غیرعادی و فعالیت‌های مشکوک.
- ☑ **پاسخ خودکار به تهدیدات:**
  ارائه قابلیت‌های واکنش سریع و خودکار برای قرنطینه، حذف یا محدودسازی دسترسی به فایل‌ها و فرآیندهای مخرب.
- ☑ **داشبورد مدیریتی پیشرفته:**
  مشاهده لحظه‌ای وضعیت امنیتی اندپوینت‌ها و تحلیل وضعیت سازمان از طریق داشبورد کاربرپسند.
- ☑ **ایجاد گزارش‌های دقیق:**
  امکان تولید گزارش‌های سفارشی در قالب‌های PDF، Excel و Word برای تحلیل و ارائه مستندات.
- ☑ **مدیریت متمرکز:**
  کنترل و نظارت بر تمامی اندپوینت‌ها از یک پلتفرم واحد با امکان پیکربندی آسان.
  پشتیبانی از احراز هویت با Active Directory و دیگر پروتکل‌های امنیتی.

برندها

kaspersky

Kaspersky EDR Optimum :

- شناسایی و پاسخ به تهدیدات به صورت خودکار

Kaspersky EDR Expert :

- تشخیص و پاسخ به تهدیدات چند لایه
- آنالیز Eventهای شبکه تحت Engineهایی نظیر MITRE ATT&CK، Virus Total، YARA و ...
- قابلیت نظارت کامل بر ترافیک شبکه و اندپوینت ها

Bitdefender

GravityZone Enterprise:

- تشخیص تهدیدات پیشرفته با تحلیل رفتار
- پاسخ خودکار و بازگردانی سیستم به حالت قبل از حمله
- شناسایی و پاسخ‌دهی به تهدیدات پیچیده در زمان واقعی
- مدیریت متمرکز و ساده برای شبکه‌های بزرگ

SANGFOR

Sangfor Endpoint Secure :

- محافظت بسیار قدرتمند در برابر حملات Ransomware
- امکان تهیه فایل پشتیبان و بازیابی اطلاعات در برابر حملات

Sangfor NG-EDR (Next-Gen EDR) :

- تشخیص تهدیدات پیشرفته با استفاده از هوش مصنوعی
- تحلیل عمیق رفتار و شناسایی تهدیدات ناشناخته

3 DLP (Data Loss Prevention)

جلوگیـــری از نشـــت اطلاعـــات

DLP یک راهکار امنیتی پیشرفته است که با هدف حفاظت از اطلاعات حساس سازمان‌ها طراحی شده است. این فناوری از نشت داده‌ها و دسترسی غیرمجاز به اطلاعات حیاتی جلوگیری می کند. DLP با شناسایی، مانیتورینگ و کنترل جریان داده‌ها، از انتقال اطلاعات به مکان‌های غیرمجاز جلوگیری می‌کند و در برابر تهدیدات داخلی و خارجی محافظت می‌نماید. این سیستم‌ها توانایی شناسایی داده‌های حساس مانند اطلاعات شخصی، مالی، یا محرمانه را دارند و با اعمال سیاست‌های امنیتی خاص، دسترسی و اشتراک‌گذاری آن‌ها را محدود می‌کنند. DLP معمولاً در سه حوزه پیاده‌سازی می‌شود: شبکه (برای نظارت بر داده‌های در حال انتقال)، نقاط انتهایی (برای کنترل داده‌های روی دستگاه‌ها)، و داده‌های ذخیره‌شده (برای محافظت از اطلاعات در دیتابیس‌ها و سرورها). این راهکار نقشی کلیدی در تطبیق با مقررات حفظ حریم خصوصی مانند GDPR و جلوگیری از خسارات ناشی از نشت اطلاعات دارد.

برنـــدها

Trellix

Trellix DLP راه‌حلی پیشرفته برای شناسایی و محافظت از داده‌های حساس است که با اسکن شبکه و ذخیره‌سازی‌های ابری، مکان داده‌ها و مالکیت محتوا را شناسایی می‌کند. این محصول با تحلیل چندبرداری و طبقه‌بندی دقیق، از داده‌های ساختاریافته و غیرساختاریافته محافظت کرده و از طریق ePolicy Orchestrator مدیریت سیاست های امنیتی را تسهیل می‌کند.

ZECURION

زکوریون راه‌حلی مقرون‌به‌صرفه برای حفاظت از اطلاعات حساس و پیشگیری از نشت داده‌ها است. این سیستم با تحلیل رفتار کاربران و شناسایی تهدیدات، در رعایت مقررات امنیتی مانند GDPR کمک می‌کند. Zecurion DLP با کنترل کانال‌های انتقال داده و مدیریت سیاست‌ها از طریق کنسول وب، امنیت اطلاعات را تضمین کرده و امکان انجام تحقیقات قانونی را فراهم می‌سازد.

safetica

این برند محصول جمهوری چک، راهکاری جامع برای محافظت از داده‌های حساس و کاهش ریسک‌های ناشی از خطاهای انسانی یا تهدیدات داخلی است. این نرم‌افزار با نصب آسان بر روی سرورهای موجود، از کانال‌هایی مانند ایمیل و ذخیره‌سازی ابری پشتیبانی می کند و با قوانین امنیتی مانند GDPR سازگار است.

رجاء

سامانه بومی DLP-RAJA برای پوشش حداکثری امنیت در نقاط انتهایی شبکه طراحی شده است. این سامانه با بهره‌گیری از رویکردهای پیشگیری از نشت داده (DLP/DRM)، به‌عنوان یک راهکار جامع و یکپارچه، وظیفه حفاظت از اطلاعات سازمانی و جلوگیری از نشت آن‌ها را بر عهده دارد.

4 PAM
(Privileged Access Management)

کلیـــد امنیت حساب‌های حیاتـــی

مدیریت دسترسی ممتاز (PAM یا Privileged Access Management) یک راهکار امنیتی پیشرفته است که برای کنترل، نظارت، و حفاظت از دسترسی به حساب‌های کاربری ممتاز در سازمان‌ها طراحی شده است. حساب‌های ممتاز شامل کاربران، سرویس‌ها و برنامه‌هایی هستند که دسترسی به منابع حیاتی و حساس سازمانی را دارند، مانند سرورها، دیتابیس‌ها، و سیستم‌های مدیریتی.PAM با استفاده از روش‌هایی مثل محدود کردن دسترسی به حداقل نیاز، احراز هویت چندعاملی (MFA)، و ارائه دسترسی موقت یا بر اساس نیاز (just-in-time access) ریسک سو،استفاده از این حساب‌ها را کاهش می‌دهد. همچنین، راهکارهای PAM قابلیت ضبط و نظارت کامل بر جلسات کاربران ممتاز را فراهم می‌کنند تا فعالیت‌های مشکوک به‌سرعت شناسایی شوند.یکی از اجزای کلیدی PAM، مدیریت چرخه عمر رمزهای عبور حساب‌های ممتاز است که شامل تغییر خودکار و رمزنگاری آن‌ها می‌شود. PAM همچنین از فناوری‌های مدیریت هویت و دسترسی (IAM) بهره می برد تا ارتباط میان کاربران و منابع بهینه و امن باشد. در نهایت، این سیستم به سازمان‌ها کمک می‌کند تا با استانداردهای امنیتی مانند GDPR و ISO ۲۷۰۰۱ مطابقت داشته باشند و امنیت زیرساخت های حیاتی خود را تضمین کنند.

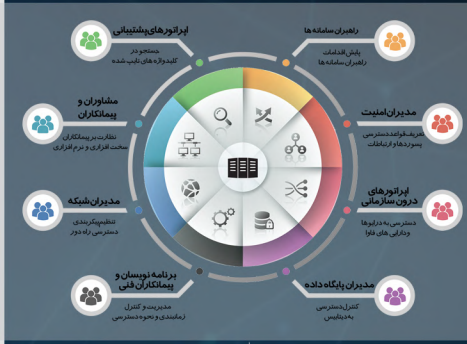
AI-Based PAM+

UBA+

PAM

سامانه مدیریت دستـــرسی های ویـــژه

نظارت و کنترل بر دسترسی های راه دور کاربران مجاز و پیمانکاران به تجهیزات مستقر در مراکز داده و منابع حساس شبکه سازمان اعم از سرورها ، تجهیزات شبکه ای و امنیتی از نگرانی های جدی مدیران سازمانی محسوب می گردد. این کاربران با استفاده از پروتکل های مختلف دسترسی راه دور نظیرRDP،HTTP/S ،SSH ،VNC به تجهیزات حساس سازمانی متصل می شوند. این در حالیست که معمولا این پروتکل ها فاقد امکانات کیفی ثبت رخداد و رویدادنگاری بوده و لذا مدیر امنیت سازمان، نظارت لازم را بر اینگونه دسترسی ها نخواهد داشت.



برخی امکانات سامانه RAJA-PAM عبارتست از :

- مشاهده اتصالات در حال انجام شامل صفحه نمایش ، صفحه کیبورد ، کـــلیپبورد و انتقال فایل
- نوع دسترسی مانند صفحه نمایش اطلاعات کیبورد ، کلیپبورد یا انتقال فـــایل
- مشاهده وضعیت سامانه به منظور بررسی بار و اطلاعات لحظه ای سامانه
- دسترسی به اطلاعات ثبت شده کاربران با اتصالات خاص
- ایـــجاد کاربران «حساس» با اختیارات قابل تعریف
- دریـــافت کامل تعامل کـــاربر به صورت فـــایل ویدیو

فایروال و ســـرور

Firewall :

فایروال به‌عنوان یک سد امنیتی قدرتمند، ترافیک ورودی و خروجی شبکه را بر اساس سیاست‌های تعریف‌شده کنترل و مدیریت می‌کند. این ابزار با شناسایی و مسدود کردن نفوذهای غیرمجاز، بدافزارها و حملات سایبری، از داده‌ها و زیرساخت‌های حیاتی سازمان محافظت می‌کند. فایروال‌ها در انواع سخت‌افزاری و نرم‌افزاری ارائه می‌شوند و از تکنیک‌هایی مانند تحلیل عمیق بسته‌ها (DPI) برای ایجاد امنیت پیشرفته استفاده می‌کنند. این فناوری علاوه بر حفاظت اولیه، با ارائه قابلیت‌هایی همچون مدیریت یکپارچه تهدیدات (UTM) به ارتقای امنیت شبکه کمک می‌کند. فایروال‌ها یکی از ارکان اصلی امنیت سایبری در سازمان‌ها به‌شمار می‌روند.

FORTINET SANGFOR

Server :

سرور به‌عنوان یک سیستم قدرتمند و مرکزی، نقش حیاتی در مدیریت و ارائه خدمات دیجیتال ایفا می‌کند. این دستگاه با پردازش حجم بالایی از داده‌ها، ذخیره‌سازی اطلاعات و پاسخگویی به درخواست‌های کاربران، زیرساخت‌های شبکه‌ای را به بهره‌وری می‌رساند. سرورها در انواع مختلف، از جمله فیزیکی، مجازی و ابری، ارائه می‌شوند و با ویژگی‌هایی نظیر مقیاس‌پذیری، پایداری و امنیت بالا طراحی شده‌اند. از مدیریت دیتابیس‌ها و میزبانی وب گرفته تا اجرای برنامه‌های پیچیده، سرور بخش کلیدی در عملکرد روان و کارآمد سازمان ها است. انتخاب و مدیریت صحیح سرور، پایه‌ای برای دستیابی

Hewlett Packard Enterprise

ذخیره‌ساز، روتر، سوئیچ و جداساز اینترنت

Storage :

ذخیره‌ساز یا استوریج، راهکاری پیشرفته برای ذخیره، مدیریت و بازیابی داده‌های حیاتی سازمان‌ها است. این سیستم‌ها با ارائه ظرفیت بالا، امنیت، و پایداری، به کاربران اجازه می‌دهند اطلاعات را به صورت متمرکز یا توزیع‌شده ذخیره کنند. استوریج‌ها در انواع NAS، SAN و DAS ارائه می‌شوند و نقش کلیدی در پشتیبان‌گیری، آرشیو داده‌ها و تداوم کسب‌وکار ایفا می‌کنند. انتخاب یک ذخیره‌ساز مناسب، تضمین‌کننده عملکرد بهینه و امنیت اطلاعات سازمان است.

QSAN

Switch & Router :

سوییچ و روتر دو دستگاه اساسی در شبکه‌های کامپیوتری هستند که هرکدام نقش مهمی در انتقال داده‌ها ایفا می‌کنند. سوییچ وظیفه مدیریت ترافیک داخلی شبکه را بر عهده دارد و با مسیریابی بسته‌ها بین دستگاه‌های مختلف شبکه، ارتباطات سریع و موثر را ممکن می‌سازد. روتر نیز برای اتصال شبکه‌های مختلف به یکدیگر استفاده می‌شود و داده‌ها را از یک شبکه به شبکه دیگر مسیریابی می‌کند. این دستگاه‌ها به‌طور مشترک به بهبود عملکرد، سرعت و امنیت شبکه کمک می‌کنند و زیرساخت‌های ارتباطی را برای انتقال اطلاعات بهینه می‌سازند.

CISCO

Network Segregator :

جداساز اینترنت ابزاری است که ترافیک شبکه را به بخش‌های جداگانه تقسیم کرده و دسترسی به منابع حساس را محدود می‌کند. این فناوری با جلوگیری از انتشار تهدیدات بین بخش‌های مختلف، امنیت شبکه را افزایش می‌دهد و به مدیریت بهتر ریسک‌ها کمک می کند. همچنین، با تفکیک شبکه‌ها، امکان نظارت دقیق‌تر و کنترل بهتر بر ترافیک ورودی و خروجی فراهم می‌شود و از آسیب‌پذیری‌ها در یک بخش جلوگیری می‌کند.

رجاء

خدمـــات رَسیـــس

خدمات قبل از فروش: مشاوره

– بررسی شبکه موجود و ارائه راهکاری های امنیتی در هر دو زمینه نرم افزاری و سخت افزاری

– ارائه اطلاعات کاربردی و عملی در رابطه با محصولات مختلف و مقایسه آنها

– ارائه وبینارهای تخصصی در حوزه امنیت و محصولات مورد استفاده در این زمینه

خدمات فروش: نیازسنجی

– تست و بررسی محصولات مورد نظر به صورت عملی در شبکه موجود

– ارائه بهترین پیشنهاد ممکن بر اساس داده های جمع آوری شده از شبکه موجود و الزامات مورد نظر مدیران شبکه

خدمات پس از فروش: راه های ارتباطی

تیم فنی شرکت رسیس همواره در تلاش است که ارتباطی مستمر را با مشتریان حفظ کند چرا که این ارتباط لازمه ارائه با کیفیت ترین خدمات ممکن می باشد. راه های ارتباطی با تیم فنی و خدمات پس از فروش این شرکت عبارتند از:

- تماسها و پیگیری های دوره ای بر اساس سیستم اتوماسیون داخلی و سی آر ام
- پنل کاربری مشتریان شامل سیستم تیکتینگ با قابلیت ارائه کد رهگیری
- ارائه وبینارهای آموزشی در سه سطح:
  - نصب و راه اندازی (Deployment)
  - پیشرفته (Maintenance & Troubleshooting)
  - اختصاصی (خدمات سطح +A)
- ارائه وبینارهای آشنایی با سایر محصولات و خدمات

اهداف و چشـــم‌انـــداز

ارائه فناوری‌های نوآورانه:
توسعه راهکارهای پیشرفته و مبتنی بر هوش مصنوعی برای مقابله با تهدیدات سایبری آینده.

توسعه شبکه‌های ایمن و پایدار:
ارائه راهکارهایی که امنیت و کارایی را به‌صورت هم‌زمان برای سازمان‌ها تضمین کند.

هم‌راستایی با استانداردهای جهانی:
ارائه محصولات و خدماتی که با الزامات استانداردهای ملی و بین‌المللی هم خوانی داشته باشند.

تقویت آگاهی امنیتی:
تمرکز بر آموزش و توانمندسازی سازمان‌ها برای پیشگیری موثر از تهدیدات سایبری.

ایجاد ارزش برای مشتریان:
تمرکز بر ارائه راهکارهایی که نیازهای امنیتی مشتریان را به بهترین شکل ممکن پوشش دهد.

افزایش اعتماد مشتریان:
ارتقای سطح اعتماد مشتریان از طریق ارائه خدمات قابل اعتماد و پایدار.

مجـــوز و تاییدیه ها

شورای عالی انفورماتیک کشور	سازمان نظام صنفی رایانه‌ای کشور	وزارت ارتباطات و فناوری اطلاعات سازمان فناوری اطلاعات ایران
گواهی احراز صلاحیت از شورای عالی انفورماتیک کشور	گواهی عضویت نظام صنفی رایانه ای کشور	گواهی مرکز مدیریت راهبردی افتا

ارتباط با ما

واحد فروش راهکارهای امنیت شبکه
(داخلی ۱۰۸-۱۰۲)

واحد فروش تجهیزات امنیت شبکه
(داخلی ۱۲۵)

واحد زیرساخت فناوری و عملیات داخلی
(داخلی ۱۲۴-۱۲۱)

واحد پشتیبانی و خدمات فنی
(داخلی ۱۲۰-۱۱۲)

واحد امور مالی و حسابداری
(داخلی ۱۱۱-۱۰۹)

۰۵۱-۳۸۴۷ ۸۱۳۰-۵

info@rasiss.com

www.rasiss.com

رَسیس

مراقب دنیای دیجیتال شما