PERSIA
SYS. Middle East
خاورمیانه
پرشیا سیس

ارائـه خدمـات بـا یک لبخنـد

روند شکل‌گیری پرشیاسیس خاورمیانه

هسته اولیه شرکت پرشیاسیس خاورمیانه از سال ۱۳۸۸ با همکاری جمعی از مدیران با تجربه و متخصصان حوزه فناوری اطلاعات شکل گرفت و فعالیت رسمی خود را از همان سال با تاسیس رسمی شرکت آغاز نمود. ساختار مدیریتی پرشیاسیس با تکیه بر دانش و تجربه کاری تجمیعی بالغ بر ۸۵ ساله هیئت اجرایی خود بنا نهاده شده است تا نیروی لازم جهت بهره‌گیری از توان علمی و تخصصی کارشناسان خبره این شرکت را فراهم آورده و با چالش همیشگی شرکت‌های دانش بنیان (وابستگی به بدنه کارشناسی به دلیل وسعت حوزه فناوری اطلاعات و ارتباطات و تخصصی و دانش محور بودن این حوزه) فائق آید.

چشم انداز پرشیاسیس : توزیع کننده برتر محصولات و خدمات مورد نیاز جامعه هدف در حوزه فناوری اطلاعات و ارتباطات در سطح کشور

ماموریت پرشیاسیس خاورمیانه

پرشیاسیس برای دستیابی به چشم‌انداز خود، جامعه هدف خود را عموم مردم، کسب و کارهای متوسط و بزرگ (سازمان‌ها و شرکت‌ها) تعیین نموده و ماموریت خود را بدین شرح تدوین نموده است:

۱- شناسایی نیازهای جامعه هدف و بررسی و امکان سنجی برآورده‌سازی آنها با استفاده از محصولات و خدمات موجود فناوری اطلاعات و ارتباطات

۲- شناسایی منابع قابل دسترس، مطمئن، مناسب و منطبق با نیازهای جامعه هدف به منظور فراهم آوردن امکانات لازم و معرفی آنها در بازار

۳- گسترش شبکه توزیع، فروش و خدمات پس از فروش، با شناسایی همکاران قابل اعتماد و توانمند، ارائه آموزش‌های لازم و تشویق آنان به ارزش‌آفرینی در زنجیره توزیع و در نهایت فراهم‌سازی انگیزه‌های لازم جهت همکاری

٤- سرمایه‌گذاری بر روی منابع انسانی (به عنوان اصل اساسی پیشرفت شرکت) با کشف استعدادهای جوان، تربیت و آموزش مستمر و ارتقاء توان تخصصی نیروی کارشناسی موجود به منظور پاسخگویی با نیاز جامعه هدف

۵- سرمایه‌گذاری مادی و معنوی بر روی پروژه‌های تعریف شده به منظور آگاه‌سازی، فرهنگ‌سازی و در دسترس قرار دادن عملیاتی خدمات برای مخاطبین

ارزش‌های سازمانی پرشیاسیس

۱- نوآوری و خلاقیت در درک نیاز مشتریان و تأمین خدمات و محصولات مورد نیاز بازار

۲- مشتری‌گرایی و مشتری مداری، با بکارگیری روش‌های نوین پشتیبانی و ارزش‌آفرینی برای مشتریان

۳- ارج نهادن بر سرمایه‌های انسانی، تقویت روحیه کار گـروهی و شایسته سالاری با هدف پویایی سازمانی و فراهم‌سازی بستر بروز خلاقیت‌های فردی

٤- مسئولیت‌پذیری و پایبندی به تعهدات نسبت به مشتریان و کارکنان

۵- تمرکز بر کارایی و اثربخشی به منظور توسعه بهره‌وری سازمـانی

٦- گسترش مشارکت‌هـا به منظور تقویت روحیه همگرایی در بـازار


PERSIASYS. Middle East
ABILITIES

توانمندی‌های پرشیاسیس خاورمیانه

۱- ارائـه راهکارهـا، محصولات و خدمات با محوریت امنیت داده‌ها و نظارت و مدیریت بر شبکه‌های رایانـه‌ای

۲- مشـاوره و تأمین نرم افـزارهای تخصصی اصلی (Original)

۳- تأمین تجهیزات سخت‌افـزاری شبکـه و مراکز داده نظیر UPS، انـواع سرور، ایستگاه‌هـای کاری و اتـاقک سرور قابل حمل

٤- طراحی و پیـاده‌سازی سرویس‌هـای جامع سازمانی براسـاس راه حل‌های استـاندارد شرکت Microsoft

۵- صـدور گواهینـامه‌هـای امنیتـی SSL جهت وب سایت‌هـا و پورتال‌های سازمانی

٦- تأمین سخت‌افزارهای استـاندارد سازمان‌ها و شرکت‌ها نظیر انواع Laptop ،PC، چاپگـر و ...

با توجه به پیشرفت‌های مداوم و سریع تکنولوژی و روند رو به رشد استفاده از آن در سازمان‌ها، امنیت اطلاعات و نگهداری از آنها، بزرگترین چالش در عصر فناوری اطلاعات محسوب شده و حفاظت از اطلاعات در مقابل دسترسی‌های غیرمجاز، تغییرات، خرابکاری و افشاء، امری ضروری و اجتناب‌ناپذیر به شمار می‌رود. امروزه به امنیت اطلاعات در سیستم‌های کامپیوتری باید به عنوان یک فرایند نگاه کرد. از این رو امنیت دارایی‌های اطلاعاتی، برای تمامی سازمان‌ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش می‌باشد.

در همین راستا، شرکت پرشیاسیس خاورمیانه با داشتن سال‌ها تجربه در ارائه مشاوره، خدمات و محصولات در لایه‌های مختلف شبکه، آماده رفع نیازهای سازمان‌ها می‌باشد.

- لایه ۱ (Physical Layer)

در این لایه نوع اتصال و روش برقراری ارتباط مطرح است. همانطور که می دانید سخت‌افزارهای مختلف بر اساس نوع عملکرد و ساختار آن دارای مدل‌های ارتباطی متفاوتی هستند. این لایه در واقع تعیین میکند که ما اطلاعات خود را قرار است به چه شکل و از طریق چه رسانه‌ای انتقال دهیم، برای مثال رسانه ما کابل فلزی است یا تجهیزات بی‌سیم؟
انواع تجهیزات پسیو شبکه مانند فیبرها، کابل‌ها، سوکت‌ها، پچ پنل و .... در این لایه قرار می‌گیرند.

- لایه ۲ (Data Link Layer)

در این لایه اطلاعات هویتی دستگاه‌های در ارتباط با شبکه به منظور تعیین مقصد پاسخ درخواست مورد استفاده قرار می‌گیرد.
انواع سوییچ‌های لایه ۲ و اکسس پوینت‌های شبکه در این لایه می‌باشد.

- لایه ۳ (Network Layer)

این لایه چگونگی رسیدن داده‌ها به مقصد با وظایفی از قبیل آدرس‌دهی، مسیریابی و پروتکل‌های منطقی را عهده‌دار است که شامل انواع روترها، سوییچ‌های لایه۳، فایروال، UTM و ... می‌باشد.

- لایه ٤ (Transport Layer)

این لایه پشتیبانی کنترل جریان داده‌ها و بررسی خطا و بازیابی اطلاعات بین دستگاه‌های متفاوت را برعهده دارد. از جمله مواردی که در این لایه می‌توان به آن اشاره نمود UTM ها و SSL Certificate ها برای برقراری ارتباط امن در بستر شبکه هستند.

- لایه ۵ (Session Layer)

این لایه وظیفه ترکیب و اعلام درخواست به سرویس مورد نظر را برعهده دارد. به عنوان مثال درخواست برقراری ارتباط با سرویس http و یا https بر عهده این لایه می‌باشد. از جمله تجهیزات فعال در این لایه دستگاه‌های فایروال و UTM می‌باشند.

- لایه ٦ (Presentation Layer)

وظیفه اصلی این لایه قالب بندی اطلاعات است. معمولا فعالیت‌هایی نظیر رمزنگاری و فشرده‌سازی از وظایف اصلی این لایه محسوب می‌شود. محصولات دارای خدمات رمزنگاری مانند DRM ها در این لایه قرار می‌گیرند.

- لایه ۷ (Application Layer)

نرم‌افزارهای کاربردی از طریق این لایه با شبکه ارتباط برقرار می‌کنند. می‌توان گفت که این لایه رابط بین کاربر و شبکه است. محصولاتی مانند آنتی‌ویروس، مانیتورینگ، فایروال، DLP، UTM و .... در این لایه فعالیت دارند.

شرکت پرشیاسیس خـاورمیانه آمادگی ارائـه مشاوره، فروش، پیکره‌بندی و خدمات انواع محصولات مختلف در این لایه‌ها را داشته و در این راستا با اخذ نمایندگی محصولاتی مانند Kaspersky، ESET، Symantec، Padvish، Sophos، Fortinet، Juniper، OwnerGuard، Falcongaze، Safetica، SSL، HP، EMC، IBM و ... اقدام به ارائه خدمات به سازمان‌ها نموده است.

SERVICES

خدمات شرکت پرشیاسیس خاورمیانه

مشـاوره، طـراحی و نظارت :

مشاوره، طراحی و نظارت ۳ اصل مهم در پیاده‌سازی پروژه‌های IT می‌باشند. همواره در پروژه‌هـا، تیم‌های نظارتی و مشـاورین پویا در جهت‌دهـی صحیح رونـد طراحی، اجرا و بهـره‌بـرداری از یک پروژه نقش بسزایی دارند. کسب اطمینان از تأمین نیازمندی‌ها و الزامات پروژه از یک سو و اجرای دقیق و صحیح آنها در موعد مقرر و همچنین منطبق با دستـورالعمل و استـانداردهای بروز و متعارف جهانی، اهمیت استفاده از مشـاوره، طراحی و نظارت بر پروژه‌های IT را بیان می‌کنند. شرکت پرشیاسیس خـاورمیانه با نیـازسنجی دقیق، بررسی زیرساخت‌هـا، شنـاخت استراتـژی، هزینـه منطقی و منـاسب، طراحی و آنالیز سخت‌افزاری، برنـامه‌ریزی زمانی و پیش‌بینی نیـازهای آتی سازمان‌هـا، اقدام به ارائـه خدمات در این زمینه می‌نماید.

نصب و راه‌اندازی شبکه‌های کامپیوتری و دیتا سنتر:

با توجه به اینکه امروزه شبکه‌های کامپیوتری زیر ساخت لازم برای استفاده از منابع فیزیکی و منطقی را در یک سازمان فراهم می‌نمایند و در بسیاری از سازمان‌ها ارتباطات دیتا، صدا، تصویر و... بر روی این بستر ارائه می‌گردد لذا طراحی، نصب و راه اندازی شبکه‌های کامپیوتری و دیتا سنتر می‌بایست با در نظر گرفتن شرایط و سیاست‌های سازمان، انجام گردد. در طراحی و پیاده‌سازی شبکه و دیتا سنتر باید مواردی مانند سرویس‌ها و خدمات مورد نیاز سازمان، پروتکل‌ها و فاکتورهای امنیتی، سرعت شبکه، نیازسنجی برای چند سال آینده و... در نظر گرفته شود. شرکت پرشیاسیس خاورمیانه با داشتن متخصصین مجرب و با تکیه بر دانش بروز و تجربه متخصصین خود توانسته است نیازهای مشتریان را در این زمینه برآورده سازد.

پشتیبـانـی و نگهـداری شبکه:

با توجه به رشد و نفوذ فناوری اطلاعات در تمامی حوزه های کسب و کار، پشتیبانی و نگهداری شبکه‌هـای کامپیوتری در حال حاضر اصلی‌ترین نیاز شرکت‌ها، موسسات، سازمان‌ها و ... در حوزه فناوری اطلاعات می‌بـاشد.

شرکت پرشیـاسیس خاورمیـانه با داشتن تجربه طولانی در این زمینـه، بهتـرین خدمـات پشتیبـانی و نگهـداری در دو بخش سخت‌افزار شبکه شامل سیستم‌های کامپیوتری، UPS، سرورها،... و نرم‌افزار شبکه شامل نگهداری از نرم‌فزارهـا، تهیه نسخه پشتیبان، رفع ایرادات سیستم عـامل و نـرم‌افـزاری و... را به سازمان‌ها و شرکت‌هـا ارائـه می نماید.


S O L U T I O N S
راهکارهای شرکت پرشیاسیس خاورمیانه

راهکارهای مایکروسافت (مدیریت یکپارچه کلاینت‌ها و کاربران و اعمال سیاست‌های سازمان بر آنها):

اکتیو دایرکتوری از دستاوردهای بسیار شگفت‌انگیز شرکت مایکروسافت می‌باشد که با استفاده از دامین کنترلر می تواند تمامی منابع موجود در یک شبکه را به صورت کاملاً متمرکز و یکپارچه مدیریت نماید. سرویس اکتیو دایرکتوری بر اساس یک پایگاه داده متمرکز که توانایی توزیع پذیری بسیار شناوری دارد، به عنوان یک سرویس‌دهنده بر پایه ویندوزهای سرور مایکروسافت تهیه شده است. اگر در داخل شبکه از این سرویس استفاده نگردد، برای مدیریت تمامی منابع باید از مدیریت تک به تک سرویس‌ها استفاده نمود که این امر موجب اتلاف وقت، به حداکثر رساندن هزینه‌ها و کاهش امنیت خواهد شد. اکتیو دایرکتوری به گونه‌ای ساخت یافته طراحی گردیده که می‌تواند تعداد بسیار زیادی از عملیات‌های خواندن، نوشتن و به روز رسانی‌ها را به صورتی کاملاً یکپارچه انجام دهد. از دیگر تعریف‌هایی که می‌توان از سرویس اکتیو دایرکتوری عنوان نمود، این است که اطلاعات ذخیره شده در این سرویس به صورت سلسله مراتبی، قابل بازگشت و تمدیدپذیر است.

راهکارهای مجازی سازی:

مجازی‌سازی یک تکنولوژی نوظهور در دنیای IT است، که به طور روزافزونی مورد استقبال سازمان‌ها در سرتاسر جهان واقع شده است. بهره‌گیری از مجازی‌سازی، انقلابی در زیرساخت سخت افزاری سازمان‌ها پدید آورده است و عملاً معماری جدیدی بر اساس آن بنیان گذاشته شده است. در واقع مجازی سازی به نوعی راهکار، برای استفاده حداکثری از منابع سخت‌افزاری است. با بهره‌گیری از این راهکار نه تنها در استفاده از سخت افـزار صرفه جویی می‌شود و هزینه‌هـای کمتری را متحمل می‌شوید، بلکه وابستگی محیط عملیاتی به سخت‌افزار کم شده و جابه جایی و به روزرسانی سیستم ها نیز به راحتی انجام می‌گردد. بنابراین مدیریت آسان‌تر و پشتیبانی ساده‌تر از برترین ویژگی‌های این راهکار است. برای مجازی سازی، محصولات متنوعی از شرکت‌های مختلف وجود دارد. اما معتبرترین آنها تولید سه شرکت VMware, Microsoft, Citrix می‌باشد.

"مجـــــازی‌ســـــازی" در بخش‌هـــای سرورهـــا، سیستـم‌هـــای کـاربـــران و برنـامـه‌هـــــای کـــاربـردی قـــابل اجـــرا مـی‌بـــاشـد

راهکـارهای پشتیبـان گیـری:

پر اهمیت‌ترین بخش هر سازمان، اطلاعات و سیستم‌های آن سازمان می‌باشند. همواره حفـاظت از اطلاعـات و سیستم‌هـا به دلیل رشد روز افزون آنهـا در سازمان و پیچیدگی خاص خود، سخت و طاقت فـرسا است. قابل ذکر است یکی از هزاران مشکل اساسی و ریسک‌های بزرگـی که سـازمان‌هـا با آن مواجه هستند، خطرات ناشی از انهدام داده‌ها می‌باشد. برای این منظـور هر سازمـان نیاز به روش‌ها و استانداردهایی دارد تا بتواند در زمان از بین رفتن اطلاعات در حداقل زمـان ممکن آن را بازیابی کـرده و سازمان را در مسیر عادی خود قرار دهـد. در راستـای تهیه نسخه پشتیبان از اطلاعات سرور و شبکه، برخی تکنولوژی‌ها در این زمینه می‌توانند در حداقل زمان، اطلاعات از بین رفته را بازیـابی کنند.

حفـــاظت از اطلاعـــــات و سیستـم‌هـــا بـه دلیل رشـــد روز افـــزون آنهـا در سازمـــان و پیچیدگـی خـــاص خـود سخـت و طـاقـت فرســـا است

برای یک سازمان بهترین سیستم تهیه نسخه پشتیبان و بازیابی اطلاعـات بایـد دارای خصوصیـات ذیل باشد:

- بازیابی اطلاعات هارد سرور در کمترین زمان ممکن
- نگهداری نسخه‌های زمانی مختلف از داده‌ها
- ایجاد زمانبندی برای گرفتن نسخه پشتیبان، طبق سیاست‌های امنیتی
- آرشیو کردن اطلاعات و نگهداری آنها در فضای کاری، بیرون از سایت یا بیرون از فضای کاری
- پشتیبان‌گیری در کمترین زمان ممکن
- تهیه نسخه‌های پشتیبان از سیستم عامل‌های مختلف و برنامه‌های کاربردی
- امکان پشتیبان‌گیری متمرکز و خودکار

راهکارهای مانیتورینگ:

مانیتورینگ شبکه و دیتا سنتر جزو استانداردهای اولیه و یکی از مهمترین فعالیت‌هایی است که مدیران شبکه باید به آن بپردازند. با استفاده از مکانیزم مانیتورینگ علاوه بر پیشگیری از بروز خطا و اشکال در ساختار شبکه، صرفه جویی هزینه و زمانی مناسبی نیز در امر مدیریت شبکه انجام خواهد شد.

مانیتورینگ شبکه و زیرساخت را به ۵ دسته‌بندی کلی تقسیم می‌کنند:

۱- مانیتورینگ شرایط محیطی.
در این دسته‌بندی، شرایط محیطی اتاق سرور و تجهیزاتی مانند سیستم سرمایشی و سیستم اطفاء حریق مانیتور می شوند.

۲- مانیتورینگ تجهیزات اکتیو شبکه.
در این دسته‌بندی، کلیه تجهیزات اکتیو شبکه مانند سوئیچ‌ها، روترها و فایروال‌ها مانیتور شده و علاوه بر بررسی سخت‌افزاری شبکه، نظارت بر عملکرد پورت‌ها و همچنین کنترل اطلاعات ارسالی و دریافتی نیز مورد ارزیابی و مانیتورینگ قرار می‌گیرد.

۳- مانیتورینگ تجهیزات ذخیره‌سازی و سرورهای فیزیکی.
در این دسته، عملکرد دستگاه‌های ذخیره‌سازی مانند NAS و SAN و همچنین سرورهای فیزیکی از حیث ارتباط شبکه‌ای، دیسک‌ها، حافظه و Raid آنها مانیتور می‌شوند.

۴- مانیتورینگ سرورهای مجازی.
در این دسته، ماشین‌های مجازی، ارتباط آنها با Hypervisor، خود Hypervisor و سرورهای مدیریتی مانند vCenter مورد ارزیابی و مانیتورینگ قرار می‌گیرند.

۵- مانیتورینگ سرویس‌ها.
در این دسته‌بندی، شما از سلامت و درستی عملکرد سرویس‌های موجود در شبکه مانند DHCP، DNS، Active Directory، سرویس‌های بکاپ و سرویس های بانک اطلاعاتی آگاهی یافته و مدیریت ساده‌تری روی سرویس‌ها خواهید داشت.

راه‌انـدازی و پشتیبـانـی VOIP:

انتقال صدا بر روی بستر شبکه و یا اینترنت (VOIP) یکی از پروتکل‌های روز دنیا می‌باشد که با داشتن مزایا و ویژگی‌های خاص خود توانسته است بخش مهمی از زیر ساخت ارتباط صوتی را در دنیای امروز به خود اختصاص دهد. این تکنولوژی که به نام IP Telephony نیز شناخته می شود این امکان را فراهم می‌آورد تا به جای استفاده از زیر ساخت‌های سنتی تلفن، به راحتی بتوانید کلیه تماس‌های صوتی، فکس، SMS و حتی تماس‌های تصویری خود را بر روی بستر شبکه و اینترنت برقرار نمـایید و با ایجاد ارتباط بین دفـاتر مختلف خود در سراسر دنیا، هزینه های تماس خود را به شکل چشم‌گیری کاهش دهید.

در VoIP محدودیت های سیستم‌های تلفن قدیمی وجود نـدارد و شما می‌توانید به راحتی داخلی خود را با خود به هر جایی ببرید و در هر مکـان و لحظـه‌ای و با استفـاده از هر نـوع اینترنتی، از داخلی خود استفـاده نمایید.

ضـد حملـــه هدفمنـــد:

حملات هدفمند، فرایندهای بلند مدت هستند که امنیت را به خطر انداخته و کنترل مهاجم غیر مجاز را بر شبکه و اطلاعات سازمان برقرار می‌کنند.

ضد حمله هدفمند، راهکار امنیتی می‌باشد کـه با ارائه مدیریت پیشرفته تهدیدات و دفاع و رسیدگی به تمام مراحل مقابله با حملات هدفمند که توسط آنتی ویروس‌های عادی قابل شناسایی نیستند، تداوم کسب و کار و اطلاعات سازمان را محافظت و تضمین می کند. این پلتفرم به صورت پیش فرض دارای ویژگیها و تکنولوژی‌هـای محافظت چند لایه می‌باشد، و این در حالی است که قابلیت ادغام و یکپارچه شدن با مجموعه گسترده‌ای از محصولات و سرویس‌های دیگر را دارد تا یک سیستم جامع اختصاصی برای تشخیص، پاسخ و پیش بینی تهدیدات را تشکیل بدهد.

ارزیـابـی امنیتـی و تست نفـوذ پذیـری:

با افزایش روز افزون استفاده از کامپیوتر و اینترنت در زندگی انسان نیاز به امنیت اطلاعات به امری بدیهی و بسیار مهم برای شرکت‌ها و سازمان‌ها بدل شده است. به منظور افزایش امنیت شبکه، نیاز است تا پیش از هکرها، نقاط ضعیف و آسیب‌پذیر شبکه را شناسایی و نسبت به رفع این نقایص اقدام گردد. از طریق ارزیابی امنیتی و تست نفوذپذیری این امکان برای سازمان‌ها فراهم می گردد که ضمن حفظ اطلاعات محرمانه، از نقاط آسیب‌پذیر شبکه خود اطلاع یافته و نسبت به رفع آن اقدام کنند.

PRODUCTS

محصولات شرکت پرشیاسیس خاورمیانه


- آنتی ویروس‌ها
- مدیریت تهدیدات (UTM)
- پیشگیری از حملات هدفمند و تهدیدات پیشرفته(ATA)
- جلوگیری از نشت اطلاعات(DLP)
- مدیریت حقوق مالکیت داده‌های دیجیتال(DRM)
- NeuShield
- GreyCortex Mendel
- تجهیزات ذخیره‌سازی
- SSL
- اتاقک سرور قابل حمل (Portable)

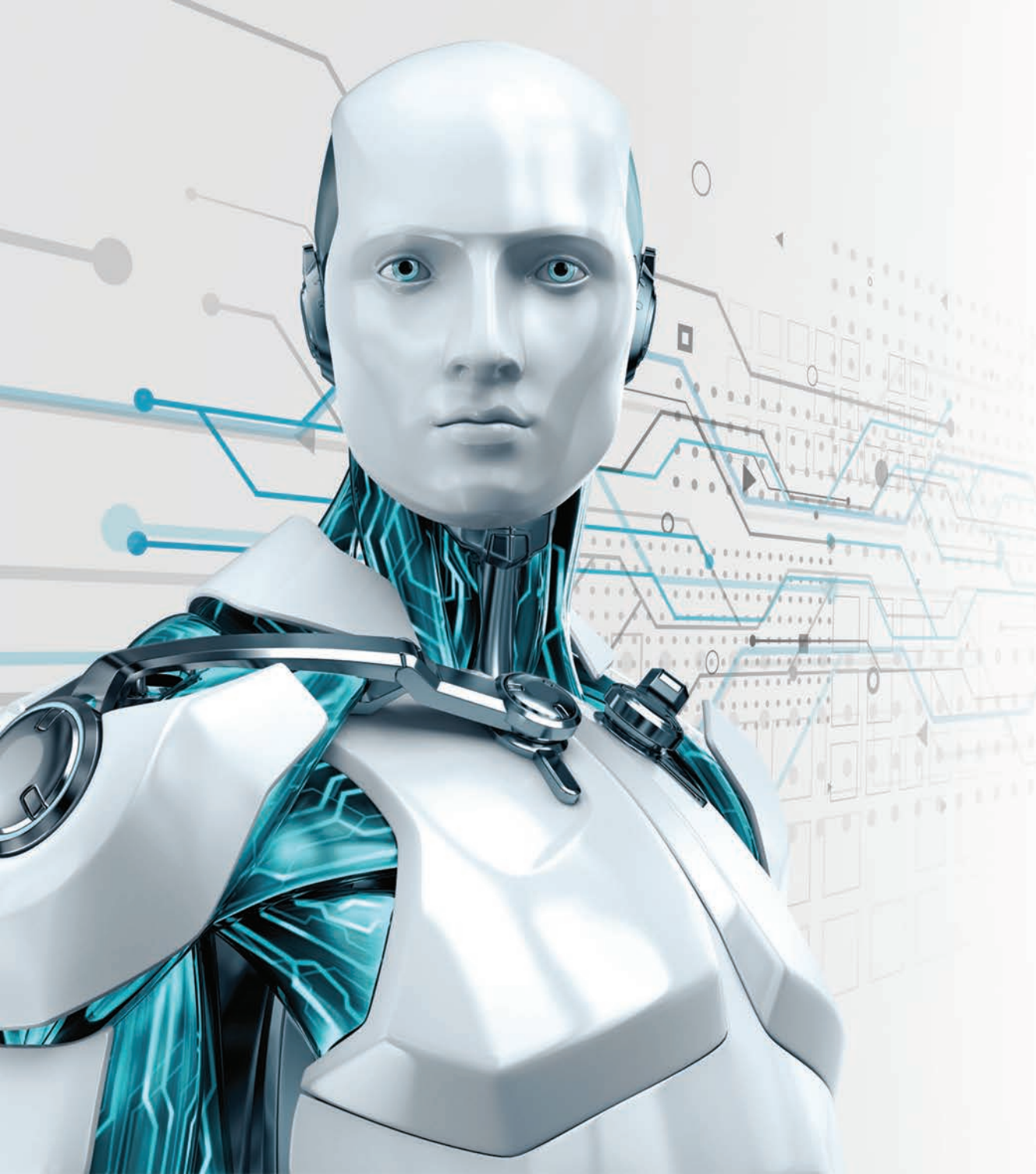
آنتی ویـروس‌ها
Anti Virus

kaspersky

کمپانی کسپرسکی یک شرکت بین‌المللی است که بیش از ۳۹۰۰ کارمند در ۳۱ کشور را در استخدام خود داشته و دفتر مرکزی آن در مسکو واقع است. این شرکت در حال حاضر در بیش از ۲۰۰ کشور جهان فعالیت داشته و محصولات و فناوری‌های آن افزون بر ۴۰۰ میلیون کاربر را در برگرفته است. وقتی موضوع حفاظت مطمئن در برابر ویروس‌ها و حملات هکرها و ارسال کنندگان هرزنامه به میان می‌آید، کمپانی کسپرسکی برای تمام مشتری‌ها راه‌حل‌هایی دارد. این شرکت، گستره‌ای فراگیر از محصولات خود را برای محافظت از کاربران خانگی و شبکه‌های سازمانی در مقابل سیستم‌های بدافزاری پیچیده و چند منظوره‌ای که امروزه در همه جای اینترنت پخش هستند، ارائه کرده است.

Symantec

کمپانی سیمانتک در سال ۱۹۸۲ توسط گروهی از دانشمندان پیشتاز صنعت رایانه، پایه‌گذاری شده است. این شرکت با بیش از ۱۱۰۰۰ کارمند در بیش از ۳۵ کشور مختلف، از بزرگترین کمپانی‌های جهان به شمار می‌رود. سیمانتک ارائـه کننده محصولات امنیتی، مدیریتی و پشتیبـان‌گیری، به مشتریان خود از شرکتهای کوچک تا بزرگترین شرکت‌هـای جهانی کمک می‌کند تا امنیت و مدیریت اطلاعات خود را هرچه کامل‌تر و کارآمدتر محقق سازند. شرکت سیمانتک بعنوان قدیمی‌ترین و با سابقه دارترین شرکت امنیتی جهان به شمار می‌آید که در آمریکا واقع شده است.



کمپانی ESET یک شرکت تولیدکننده نرم‌افزارهای امنیتی است که با بیش از ۱۵۰۰ کارمند، دفتر مرکزی آن در کشور اسلواکی می‌باشد. شرکت ESET رکورد طولانی ترین دریافت کننده متوالی جوایز VB100 برای شناسایی بدافزارها را داراست که در بین ارائه‌کنندگان محصولات امنیتی منحصر به فرد می‌باشد.

ESET به بیش از ۱۱۰ میلیون کاربر در بیش از ۲۰۰ کشور کمک می‌کند تا از تکنولوژی امن لذت ببرند. ۳ دلیل اصلی برای انتخاب راهکارهای سازمانی ESET، راحت و موثر بودن ، سبک و سریع بودن و مدیریت ساده آن می‌باشد.

Padvish

یک آنتی‌ویروس و ضد باجگیر ایرانی است که تمام مراحل طراحی و پیاده سازی آن توسط تیم مجرب داخلی صورت گرفته و قابلیت شناسایی و مقابله با بدافزارهای رایج را دارد.
این محصول به پشتوانه تکنولوژی شبکه ابر کاربران و تیم تحلیل بدافزار قوی، قادر به شناسایی جدیدترین بدافزارها در کمترین زمان ممکن می‌باشد.

مدیریت یکپارچه تهدیدات:

در سال‌های اخیر همگام با روند رو به پیشرفت استفاده از شبکه‌های کامپیوتری و استقرار منابع دیجیتال سازمانی در سطح این شبکه‌ها و در نتیجه وابستگی روزافزون کسب و کار سازمانی، مبحث امنیت درگاه و ارتباطات شبکه‌ای و تجمیع راهکارهای مرتبط در یک یا چند سیستم جامع، اهمیت روزافزونی یافته است.

یکی از راهکارهای بسیار کارآمد در این زمینه که مورد استقبال چشمگیر راهبران و مدیران شبکه قرار گرفته، استفاده از UTM می‌باشد. از نظر تئوری، UTM یا Unified Threat Management نتیجه تکامل فایروال‌های سنتی به یک محصول امنیتی فراگیر که قادر به انجام وظایف امنیتی متعدد در داخل یک دستگاه است، می‌باشد.

به بیانی دیگر، UTM سیستمی سخت‌افزاری مشتمل بر نرم‌افزارهای امنیتی مورد نیاز یک شبکه به صورت مجتمع می‌باشد که هدف نهایی استفاده از آن، ارائه مجموعه‌ای جامع از ویژگی‌های امنیتی در یک محصول با مدیریت مجتمع از طریق یک کنسول واحد است.
استفاده از یك دستگاه UTM، مدیریت استراتژیک امنیتی سازمان‌ها را بسیار آسان کرده و به دلیل وجود مدیریت واحد روی یک دستگاه، پشتیبانی یک منبع و همچنین نیاز به یک راه‌اندازی و نگهداری، بسیار مقرون به صرفه خواهد بود.

SOPHOS

شرکت SOPHOS که یکی از برندهای مطرح در زمینه محصولات و خدمات مرتبط با امنیت شبکه و داده‌ها می‌باشد، با سرمایه‌گذاری گسترده در زمینه UTMها و به مالکیت در آوردن دو برند مشهور Astaro و Cyberoam و در نتیجه استفاده از فناوری‌های این دو شرکت، UTMهای SOPHOS را با طیف گسترده‌ای از توانایی‌های فنی و امکانات متنوع به عنوان یکی از قابل اطمینان‌ترین برندهای این حوزه در سطح جهانی عرضه نموده است.

Sophos XG

Sophos XG از طریق کنسول مدیریتی جدید خود، دید گسترده و تصویری بی‌نظیر را از شبکه، کاربران و برنامه‌های کاربردی ارائه می‌دهد. سوفوس XG مدل یکپارچه جدیدی را ارائه کرده و شما را قادر می سازد قواعد کاربر، برنامه و شبکه را بصورت متمرکز در یک محل مدیریت کنید. سوفوس XG از مدیریت دیواره آتش تا نحوه گزارش‌دهی آن و ارتباط دیواره آتش با سایر سامانه‌های امنیتی، دید کامل و حفاظت جامع در برابر تهدیدات پیچیده امروزی را در اختیار مدیران شبکه قرار می‌دهد.

Sophos SG

UTMهای SOPHOS در سالیان گذشته همواره در رتبه‌بندی معتبر Gartner در رده Leaders جای گرفته و ضمن قرارگیری در کنار برندهای مطرحUTM، امکانات متنوع و متعددی نظیر امنیت درگاه اینترنت، پست الکترونیک، نرم‌افزارهای کاربردی تحت وب و گزارش‌دهی را در قالب تنها یک راه حل و بدون نیاز به استفاده از زیرساخت‌های متعدد و هزینه‌های اضافی گزاف در اختیار کاربران قرار داده است. همچنین، با ارائه نسل جدید این تجهیزات (سریSG) علاوه بر افزایش چشمگیر سرعت و توان سیستم، امکانات امنیتی متنوع و متعددی نیز به کاربران عرضه شده است.

شرکت Fortinet در سال ۲۰۰۰ و در کشور آمریکا تأسیس شد. دیدگاه شرکت Fortinet از ابتدا، ارائه امنیت گسترده با کارایی بالا در زیرساخت فناوری اطلاعات بوده است. Fortinet با ارائه محصولات سطح بالا در حوزه امنیت، توانسته است یکی از شرکت‌های سرآمد در این زمینه باشد.

این شرکت در زمینه امنیت شبکه، محتوای ارزشمند و همچنین محصولات رده بالای امنیتی را به اشتراک می‌گذارد که اطلاعات را بصورت کاملاً ایمن نگه‌داری می‌کنند. امنیت یکپارچه و منحصر به فرد این شرکت ترکیبی از پردازنده‌های امنیتی، یک سیستم عامل بصری و هوش مصنوعی شناسایی تهدید است تا برای شما امنیت ثابت، عملکرد استثنایی، دید بهتر و کنترل را با مدیریت آسان‌تر فراهم سازد.

Fortinet شرکتی با رویکرد معماری امنیتی است که فناوری‌های امنیتی موجود در سراسر شبکه شامل سیستم پردازش ابری، اندپوینت‌ها، ایمیل‌ها، برنامه‌های کاربردی وب و نقاط دسترسی شبکه را بطور ایمن و یکپارچه طراحی و عرضه می‌کند.

جلوگیری از نشت اطلاعات(DLP)

هر سازمان یا شرکت، داده‌های محرمانه و مهمی را در سطح شبکه خود تولید، ذخیره و منتقل می‌کند که افشاء یا سرقت این اطلاعات محرمانه می تواند تداوم کسب و کار و حتی موجودیت شرکت را با مخاطره روبرو نماید.

اشتباهات و یا غرض ورزی نیروی انسانی از اصلی‌ترین عوامل نشت و سرقت اطلاعات در سازمان‌ها هستند که می‌توانند خسارات جبـران ناپذیری به سازمان یا شرکت وارد آورند که نمونه‌های آن متأسفانه در کشور ما در حوزه‌های مختلف پرداخت، بانک و اپراتورها اتفاق افتاده و موجب وارد آمدن خسارات سنگینی به این شرکت‌ها شده است.

از این رو کنترل و نظارت بر عملکرد و مکاتبات نیروهای انسانی می‌تواند از بروز رخدادهای امنیتی بزرگ جلوگیری به عمل آورد، مثلاً عدم اجازه ارسال اطلاعات محرمانه به خارج از سازمان و یا شناسایی افراد ناراضی در سازمان که به دنبال شغل جدید می‌گردند، می‌تواند از بروز رخدادهای امنیتی جلوگیری نماید.

falcongaze™

شرکت Falcongaze فعالیت رسمی خود را از سال ۲۰۰۷ میلادی آغاز نموده است. این شرکت ارائه دهنده راهکار جامع کنترل مداوم و جلوگیری از سرقت و افشای ناخواسته اطلاعات حساس سازمانی است که به منظور نظارت بر فعالیت‌های شبکه کارکنان طراحی شده است. محصول تولید شده شرکت Falcongaze یک پلتفرم مدیریت امنیت اطلاعات و مخاطرات عملیاتی است که Secure Tower نامگذاری شده است، این محصول ترکیبی از چندین مفهوم امنیتی است که تجربه کاربری بهتر و مؤثرتری به نسبت استفاده از چندین سیستم مختلف ارائه می‌دهد.

ویژگی های منحصربفرد Secure Tower در کنترل و محافظت از اطلاعات محرمانه سازمان و نظارت دقیق و کامل از همه فعالیت‌های کاربران در کنار سادگی استفاده و کاربر پسند بودن آن، باعث شده سازمان بتواند به راحتی مخاطرات داخلی خود را کنترل نماید.

safetica

پرسنل شرکت که جزو پایه‌های اصلی سازمان به شمار می‌آیند، در عین حال می‌توانند به عنوان تهدیدی جدی برای سازمان محسوب شوند. برخی از کارمندان تظاهر به کارکردن در سازمان می‌کنند در حالیکه صرفا در حال اتلاف منابع سازمان بوده و اغلب اوقات خود را در جهت وبگردی، چت کردن، بازی کردن و یا سایر فعالیت‌هایی که در راستای منافع سازمان نیست، می‌گذرانند. گاهی اوقات، اطلاعات ارزشمند و محرمانه سازمان، به صورت عمد و یا غیر عمد از طریق ابزارهای جانبی ذخیره‌ساز 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 ذی ربط سازمان می‌توانند کارمندان مضر را قبل از اینکه به سازمان آسیب جدی وارد آورند، شناسایی کرده و مسئولیت‌پذیری را در سازمان گسترش دهند. این نرم‌افزار، همچنین از خروج اطلاعات شرکت جلوگیری می‌کند.

پیشگیری از حملات هدفمند و تهدیدات پیشرفته:

حملات هدفمند، فرآیندهایی بلندمدت هستند که امنیت سازمان‌ها را به خطر انداخته و کنترل مهاجم غیر مجاز را بر شبکه و اطلاعات قربانی این نوع حملات میسر ساخته و به مهاجم کمک می‌کنند تا از تکنیک‌های امنیتی سنتی گذر کنند.

اصولا این حملات مدت‌ها بعد از نفوذ به شبکه شناسایی می‌گردند که این موضوع به معنای خسارت‌های جبران‌ناپذیر می‌باشد. مقابله با این نوع حملات با راهکارهای سنتی موجود امکان‌پذیر نمی‌باشد.

در این راستا شرکت‌های Kaspersky و ESET اقدام به عرضه پلتفرم ضد حملات هدفمند (ATA & EDR) نموده‌اند.

مدیریت حقوق مالکیت داده‌های دیجیتال(DRM)

با رشد روز افزون تکنولوژی‌های ارتباطی، سرعت انتشار اطلاعات به طور قابل ملاحظه‌ای در حال افزایش است که همین امر سبب مشکل شدن کنترل نحوه انتشار و توزیع داده‌های دیجیتالی بر روی شبکه جهانی گشته و روند پیگیری مسیرهای نشر اطلاعات را با مشکل مواجه می‌کند.
از سویی دیگر در سیستم‌های نظامی، سازمان‌ها و شرکت‌ها شاهد خروج و استفاده غیرقانونی اطلاعات محرمانه از داخل و یا خارج از محیط سازمانی هستیم. به طور قطع در این گونه موارد لطمات ایجاد شده، جبران‌ناپذیر بوده و حتی می‌تواند امنیت ملی یک کشور را به خطر بیاندازد.

مالکین و تولید کنندگان اطلاعات، به منظور نظارت و کنترل بر اطلاعات خود نیازهای گوناگونی دارند که عبارتند از:

- نظارت وکنترل بر نحوه کاربرد، انتشار و استفاده از اطلاعات
- تضمین مالکیت اطلاعات پس از واگذاری
- جلوگیری از سرقت‌های داخل سازمانی
- مصونیت در مقابل نفوذهای اینترنتی

OwnerGuard

OwnerGuard DRM برای اولین بار در سال ۲۰۰٤ توسط متخصصین ایرانی عرضه شد و توانست انقلابی را در عرصه DRM و فناوری حفاظت و مالکیت اطلاعات پدید آورد. این تکنولوژی کلیه نقاط ضعف سیستم‌های فعلی را برطرف نموده و تمامی نیازهای مالکین، توزیع کنندگان و کاربران اطلاعات را تحت پوشش قرار می‌دهد.
Armjisoft OwnerGuard می‌تواند بدون نیاز به ایجاد تغییرات در ساختار نـرم‌افزارها و فرمت‌های استاندارد ذخیره‌سازی داده‌ها، سیستم‌های جـامع مدیریت و حفاظت از حقوق مالکیت اطلاعات را پیـاده‌سازی کند.

NeuShield

با هجـوم باج افزارهـا و سایـر حملات سـایبری، محـافظت از داده‌هـا برای شرکت‌هـا سخت‌تـر می‌شود.

NeuShield با ارائه حفاظت از داده‌ها، رویکرد کاملاً متفاوتی نسبت به امنیت سنتی اتخاذ کرده است. به جای تلاش برای شناسایی و مسدود کردن تهدیدات به صورت یکجا، یک رویکرد جدید، ثبت اختراع نموده، که از One-Click Restore، Mirror Shielding و Data Engrams استفاده کرده تا از داده‌های مهم محافظت و از تهدیدات در مقابل تغییر آن جلوگیری کند.

این رویکرد جدید، امکان می دهد تا داده‌ها را از هرگونه تهدید ناشناخته یا روز صفر بازیابی کنیم. از آنجا که این نرم‌افزار به جای تلاش برای یافتن تهدیدات خاص، از داده‌ها محافظت می‌کند، می‌تواند بدون نیاز به بروزرسانی مداوم و بدون امضاء، این کار را انجام دهد.

قابلیت‌های نرم‌افزار NeuShield:

• Mirror Shielding (آینه محافظ): از داده‌ها در برابر باج افزار، حملات هدفمند، تهدیدات روز صفر و ناشناخته که سعی در رمزگذاری یا قفل کردن پرونده‌ها را دارند، محافظت می‌کند.

• Boot Protection (محافظت از بوت): مانع باج افزارهایی که بوت سیستم را غیرفعال می‌کنند، می‌شود.

• Disk Wipe Protection (محافظت از پاک کردن دیسک): جلوگیری از پاک شدن یا از بین بردن داده‌های موجود بر روی دیسک سخت در برابر پاک کننده‌ها (Wipers)

• My Documents and Desktop Folder Protection (محافظت از پوشه‌های اسناد و دسکتاپ)

• Cloud Management (مدیریت ابری): کلاینت‌های نرم‌افزار را از کلود مدیریت می‌کند.

• One-Click Restore (بازیابی با یک کلیک): پرونده‌ها و تنظیمات سیستم عامل را به حالت خوب شناخته شده، باز می‌گرداند.

• Cloud Drive Protection (محافظت از داده‌های ابری): حفاظت یکپارچه برای پرونده‌ها در Microsoft OneDrive ، Dropbox ، Google Drive و Box.com

• Revision History using Data Engrams (تاریخچه ویرایش‌ها با استفاده از تغییرات داده‌ها): چندین نسخه از پرونده‌های محافظت شده را ذخیره می‌کند.

• File Lockdown (قفل کردن پرونده): دسترسی ایمن به پرونده‌ها را حتی قبل از تمیز کردن سیستم از آلودگی، امکان‌پذیر می‌کند.

• Customized Folder Protection (حفاظت از پوشه سفارشی): از پرونده‌ها در هر پوشه محلی که تعیین کرده‌اید محافظت می‌کند.

• Large File Support (پشتیبانی از فایل‌های بزرگ): می‌تواند از پرونده‌ها تا حجم ۵۱۲ گیگابایت محافظت کند.

• Pictures, Music and Videos Folder Protection (محافظت از پوشه تصاویر، موسیقی و فیلم‌ها)

• ادغام با Kaseya VSA برای مدیریت و نظارت از راه دور

GREYCORTEX
MENDEL

Mendel از هوش مصنوعی پیشرفته، یادگیری ماشین و تجزیه و تحلیل داده‌ها استفاده کرده و به عنوان یک فناوری، جهت کمک به کاربران ایجاد گردید. از جمله قابلیت‌های این نرم‌افزار، تشخیص قدرتمند برای پاسخ سریع به تهدیدهای ناشناخته پیشرفته، دید کامل شبکه به لایه ۷ برای هر دستگاه، حتی IoT / BYOD، قابلیت ادغام با زیرساخت‌های موجود مانند SIEM و فایروال‌ها و نظارت بر ترافیک شبکه SCADA می‌باشد.
ابزارهای امنیتی فعلی شبکه به دلیل عدم تشخیص تهدیدهای پیشرفته، عدم دید و عدم ادغام، شبکه ها را آسیب‌پذیر می‌کنند. این بدان معناست که تهدیدها در شبکه پنهان می‌شوند، دستگاه‌های آلوده و تنظیمات غلط، بدون توجه به نظر می‌رسند و هنگامی که حمله شناسایی می‌شود، تحلیلگران برای توقف آن، باید بین سیستم عامل‌های مختلف جابجا شوند.

محصول MENDEL، راه حل تحلیل ترافیک شبکه، ترکیبی از تکنیک های پیشرفته تشخیص با دید کامل شبکه و قابل ادغام با ابزارهای زیرساخت‌های امنیتی برای شناسایی تهدیدات (پیشرفته و ناشناخته)، تجسم ارتباطات و پاسخ سریع و مؤثر است.
یکی از قابلیت‌های این محصول، مشاهده عمیق شبکه می‌باشد. بسیاری از ابزارهای امنیتی شبکه، به شما نشان نمی‌دهند چه چیزی در شبکه شما پنهان است. MENDEL اطلاعات لازم را در اختیار تیم‌های امنیتی قرار می‌دهد، تا دقیقاً بتوانند دستگاه‌های درون شبکه و ارتباطات آن‌ها را در زمان واقعی پیدا کنند. همچنین امکان تجزیه و تحلیل آسان ریشه‌ای، شکار سریعتر تهدید و عیب‌یابی مؤثر شبکه را فراهم می‌آورد.
هنگام وقوع حملات، داده‌های ارزشمند با یک تاخیر جزئی از دست می‌روند، در صورت استفاده از MENDEL که در ابتدا با ابزارهای امنیتی در شبکه شما یکپارچه شده، می‌توانید به حملات پاسخ دهید، تحقیقات انجام دهید و حوادث را از یک رابط واحد مدیریت کنید.

نظارت بر شبکه تحت کنترل شما
(رویکرد ایده‌آل برای محیط‌های SCADA)

حملات پیشرفته علیه سیستم‌های کنترل صنعتی معمول، خطرناک و دارای پیامدهای جدی است. بسیاری از ابزارهای امنیتی موجود با این سیستم‌های صنعتی کار نمی‌کنند و بسیاری از ابزارهای امنیتی SCADA خطرات دستگاه‌های غیر SCADA متصل را تشخیص نمی‌دهند.

MENDEL بصورت غیرفعال، نظارت بر ترافیک شبکه SCADA، ارائه دید عمیق، کشف تمام دستگاه‌های متصل و شناسایی دستگاه‌ها یا خدماتی که قبلا فعال بوده یا تازه دیده شده‌اند را، برعهده دارد.

MENDEL کمک می‌کند تا تهدیدهای شناخته شده، رفتارهای غیر عادی و تنظیمات غلط، از جمله تهدیدهای خاص SCADA را برای محافظت از شبکه صنعتی خود در برابر اختلال در عملکرد، بکار گیرید.

تجهیـزات ذخیـره‌سـازی:

SAN: شبکه‌ای از استوریج‌ها با دسترسی Block level برای سرور در دیتاسنتر است، یعنی می‌توان بدون واسطه و مستقیم به بلاک‌های هارد دیسک دسترسی پیدا کرد که این روش سرعت بالایی دارد. در SAN تنها ارسال اطلاعات بین سرورها و دستگاه‌های ذخیره ساز صورت می‌پذیرد، یعنی فقط خواندن و نوشتن اطلاعات انجام می‌شود و سرویس‌هایی مانند وب و یا ایمیل در آن ارائه نمی‌شود. در سازمان‌های بزرگ با تعداد زیادی سرور، کارایی و انعطاف پذیری بیشتری نسبت به DAS ارائه می‌دهد و در عین حال که هزینه سخت افزار آن بیشتر است اما باعث صرفه‌جویی در هزینه می‌شود.

NAS: در این روش ذخیره‌سازی، هارد دیسک‌ها بر روی یک سرور قرار دارد که به آن NAS Storage گفته می‌شود و سپس این هاردها را در شبکه برای دستگاه‌های دیگر به اشتراک می‌گذاریم.

در واقع از طریق پروتکل TCP/IP به استوریج متصل شده و از آن سرویس می‌گیریم. این استوریج‌ها به سادگی، فضایی مرکزی، محلی و قابل دسترس را برای ذخیره‌سازی فایل‌ها و فولدرهای حیاتی برای هر سازمانی، با قیمتی مناسب نسبت به SAN فراهم می‌کنند.

Tape: انواعی از ابزارهای ذخیره‌سازی که در دنیای فناوری اطلاعات استفاده می‌شوند، Tapeها هستند که در زمینه ذخیره‌سازی پیشکسوت بوده و برای تهیه نسخه پشتیبان از داده و اطلاعات، کاربرد دارند. این درایوها گاهی به طور مستقیم روی سرورها نصب می‌شوند. در صورتی که نیاز باشد پس از پر شدن یک Tape، Tape بعدی به صورت خودکار جایگزین شود، باید بر روی دستگاه‌ها Autoloader نصب شود. در صورتی که بخواهیم همزمان از چند درایو برای تهیه پشتیبان از چند دستگاه استفاده کنیم، باید Tape Library استفاده شود.

شرکت پرشیـاسیس خـاورمیانه با داشتن تجربه طولانـی در زمینه تأمین و ارائـه گواهینامه‌های دیجیتال سازمانی، نمایندگی شرکت Certum را در این زمینه دارد.

اتاقک سرور قابل حمل (Portable):

با توجه به اینکه هر شرکت متوسط جهت نگهداری اطلاعات و سرویس دهی، حداقل به سه یا چهار سرور نیاز دارد و نظر به حساس بودن امنیت سرورها و عدم دسترسی افراد غیر مسئول و ایجاد مکانی امن جهت متمرکز نمودن سرورها، هر شرکت در اندازه‌های متوسط و بزرگ باید اقدام به راه‌اندازی اتاق سرور یا دیتاسنتر نماید.

برای راه اندازی اتاق سرور می‌بایست به مباحث کلیدی آن ازجمله استانداردهای ISMS یا همان مدیریت امنیت اطلاعات توجه ویژه داشت.

اتاقک سرور قابل حمل هوشمند، یک محصول بومی با رعایت استانداردهای پایه دیتا سنتر و اتاق سرور، با اشغال فضایی معادل رک و دارای بیش از ۸۰٪ قابلیت‌های دیتا سنتر، طراحی و تولید شده که می‌تواند بهترین گزینه برای تکمیل یا گسترش شبکه سازمانی باشد و جایگزین اتاق سرور (دیتا سنتر) گردد.

مقایسه چشم‌گیر هزینه نصب اتاقک سرور و نکات پدافندی با پیاده‌سازی و راه‌اندازی اتاق سرور (دیتا سنتر)، نقش ارزش آفرین آن را برای عمده کسب و کارهای کوچک و بزرگ ازجمله مجموعه‌های دولتی و خصوصی نمایان می‌نماید.

ویژگی‌های اتاقک سرور:

- ضد ارتعاش، با قابلیت نصب، راه انـدازی و جابجایی در زمانی کوتاه (به ویژه در بحران‌های طبیعی و غیرطبیعی)
- مصرف بهینه انرژی با قابلیت کارکرد، حتی با پنل‌های خورشیدی
- طراحی شده براساس عملکرد کاملاً هوشمند در تمام بخش‌ها با قابلیت کارکرد در دمای ۲۰- الی ۵۰+
- سیستم هوشمند اطفاء حریق مطابق با بالاترین استانداردهای جهانی و محیط زیستی
- یونیت تقسیم، تسهیم و تخصیص برق بومی (سیستم کاملاً هوشمند)
- اشغال حداقل فضا، رعایت استاندارد محفظه با امنیت بالا و نفوذ ناپذیری حداکثری تا IP54
- رعایت استاندارد ISO27001
- دارای پاور ماژول (PDU) و کنترل اتوماتیک برق (ATS) و سیستم برق اضطراری داخلی
- امکان افزایش زمان ذخیره‌سازی تا ۲ ساعت
- دارای سیستم برودت و تنظیم دمای داخلی
- دارای نمایشگر وضعیت عمومی اتاقک سرور، حفاظت تصویری (دوربین مدار بسته) و کنترل از راه دور

من
پرشیاسیس خاورمیانه
هستم

تلفن: ۸۸۶۴۳۶۹۲ | فکس: ۸۸۶۷۳۲۹۵
info@persiasysco.com
www.persiasysco.com