شرکت کامپیوتری
علم و صنعت

تلفن: ۰۲۱۸۴۳۳۶ – داخلی ۴۴۰
ایمیل: CyberSecurity [AT] elmosanat.com
نشانی وب سایت: www.elmosanat.com
نشانی دفتر مرکزی: تهران، خیابان فاطمی، خیابان پروین اعتصامی، پلاک ۳

شرکت علم و صنعت

ارائـه کننده راهکارهـای نوین امنیـت فناوری اطلاعات

راهکارها و خدمات امنیت فناوری اطلاعات علم و صنعت >

با گسترش استفاده از راهکارهای مبتنی بر فناوری اطلاعات در سازمانها و صنایع گوناگون و پیرو آن پیچیدگی روز افزون تهدید ها با اهداف مختلف، حفاظت از زیرساخت های پردازش و تبادل داده و نیز پیشگیری از حمله های داخلی و خارجی به چالشی مداوم مبدل شده است. مهم ترین عامل موفقیت در مقابله با حملات سایبری و پیشگیری از وقوع رخدادهای امنیتی، بکارگیری دانش و فناوری روز و نیز بهره‌مندی از تجربه کارشناسان امنیت فناوری اطلاعات می باشد.

هدف اصلی ما در خدمت رسانی و پاسخگویی به طیف وسیع درخواستهای مشتریان، ارائه و انتقال صحیح خدمات و محصولات نوین امنیت داده، امنیت زیرساخت شبکه و نقاط پایانی و نیز آگاهی رسانی در خصوص پیشگیری و مقابله با چالشهای امنیتی می باشد.

فهرست

۵۰ نماینده فعال در کشور

سرعت و سهولت در ارائه خدمات و محصولات به مشتریان سراسر کشور

Lorem

گروه پشتیبانی متمرکز

افزایش کیفیت در پاسخگویی به درخواستها

علم و صنعت با بهره مندی از گسترده ترین شبکه فروش و خدمات پشتیبانی و پس از فروش، سادگی دسترسی به راهکارهای نوین امنیت فناوری اطلاعات را برای مشتریان سراسر کشور فراهم نموده است.

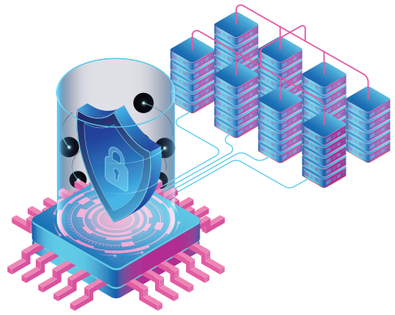
راهکار های علم وصنعت

مهم ترین عامل موثر در حفظ امنیت دارایی‌های اطلاعاتی و نیز پیشگیری از اختلال عملکرد سرویسهای سازمانی، واکنش هماهنگ و یکپارچه راهکارهای حفاظتی می باشد. راهکارهای حفاظتی علم و صنعت ترکیبی هماهنگ از محصولات و خدمات ویژه منطبق با استانداردهای امنیت فناوری اطلاعات بوده که علاوه بر کاهش هزینه های اجرایی و نگهداری، امکانات امنیتی فراگیر را در اختیار شما قرار می دهد.

راهکار امنیت نقاط پایانی

حفاظت از ایستگاه های کاری و سرورها در برابرانواع تهدید ها

- مقابله با انواع بدافزار در سراسر شبکه
- پیاده سازی فناوری های امنیتی پیشرفته جهت شناسایی و دفع تهدیدها
- پوشش کامل امنیتی برای حفاظت از سیستمهای حساس و آسیب پذیر
- شناسایی مستمر و رفع نقاط ضعف و آسیب‌پذیر
- آگاهی رسانی و انتقال دانش مقابله با انواع بدافزار
- برنامه ریزی و آمادگی برای مقابله با حملات سایبری



راهکار امنیت پیشرفته

واکنش هماهنگ در برابر تهدیدهای داخلی و خارجی

- شناسایی نقاط ضعف و انتخاب کارآمدترین راهکارهای مقابله با تهدید ها
- کنترل سطح دسترسی به سرویسها و منابع شبکه
- راه اندازی راهکارهای امنیتی سازگار با چرخش کار سازمان
- پیاده سازی روشهای عبور از بحرانهای امنیتی
- برقراری امنیت در لایه های مختلف شبکه
- آموزش راهبران و کاربران برای مقابله با تهدید ها

راهکار امنیت جامع

شکار تهدید های پیشرفته و واکنش دفاعی خودکار

- ارزیابی مستمر وضعیت امنیت شبکه و رفع آسیب‌پذیری ها
- تهیه نقشه راه امنیت و طراحی مراحل و استراتژی دفاعی
- پیاده سازی سامانه رصد و واکنش خودکار در برابر حملات
- پالایش رخدادها بمنظور شناسایی و پیشگیری از حملات روز صفر
- پوشش امنیتی بسترها و زیرساخت مجازی

راهکار پیشگیری از نشت اطلاعات

امنیت دارایی های اطلاعاتی ارزشمند و حیاتی

- شناسایی و دسته بندی اطلاعات حساس
- کنترل راه های تبادل اطلاعات
- طراحی سیاست های حفاظت از اطلاعات مهم سازمانی
- پیاده سازی و راه اندازی سامانه پیشگیری از نشت اطلاعات
- بررسی رفتار کاربران و پیشگیری از سرقت و یا تغییر اطلاعات
- کنترل سطح دسترسی برنامه ها به اطلاعات حساس

راهکار امنیت نقاط پایانی

ایستگاه های کاری، سرورها و سایر دستگاه هایی که در ارتباط با یکدیگر بعنوان نقاط پایانی اجزای یک شبکه را تشکیل می دهند، به دلیل در اختیار داشتن منابع مهم از جمله سرویسها و دارایی های اطلاعاتی سازمان، همواره از جمله اهداف اصلی سوء استفاده و نفوذ محسوب می شوند.

چالشهای گوناگونی برای حفاظت از نقاط پایانی و حفظ تداوم عملکرد صحیح آنها مطرح می باشد که در صورت عدم توجه و رسیدگی به هر یک از آنها، تدابیر حفاظتی و دفاعی اندیشیده شده بمنظور حفظ امنیت شبکه را کم اثر کرده و امکان نفوذ انواع تهدیدها از جمله بدافزارها را فراهم می سازد.

راهکار امنیت نقاط پایانی علم و صنعت، خدمات و محصولات مورد نیاز جهت رفع چالشهای فوق را درقالب راهکاری یکپارچه بمنظور حفاظت از نقاط پایانی برای شما فراهم نموده است.

- ارزیابی ابتدایی بمنظور سنجش نیازمندیها و شناسایی نقاط ضعف و آسیب پذیر
- بازنگری طراحی امنیت بر مبنای استانداردهای معتبر
- راه اندازی و نگهداری سامانه های مدیریت نصب اصلاحیه و آسیب پذیری
- ارزیابی دوره ای وضعیت امنیت نقاط پایاتی و کنترل عملکرد محصولات امنیتی
- خدمات مشاوره بمنظور انتخاب محصولات امنیتی سازگار و فناوریهای کارآمد
- پیکربندی زیرساختها و سرویسهای مرتبط با نقاط پایانی
- پیاده سازی، راه اندازی و نگهداری سامانه یکپارچه ضدبدافزار
- خدمات پشتیبانی نامحدود

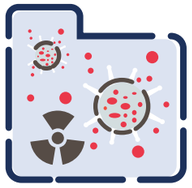
چالشهای امنیتی در لایه نقاط پایانی

مشکل به روز رسانی

سوء استفاده از نقاط آسیب پذیری ها

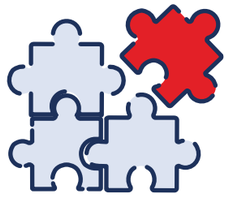
طراحی ناکارآمد سطوح امنیت

سهولت نفوذ تهدیدها و دسترسی آسان به نقاط آسیب پذیر



حملات بدافزارها

فعالیت مخرب انواع ویروس، باج افزار، جاسوس افزار و تهدیدهای پیشرفته و ماندگار



ناسازگاری محصولات امنیتی

کندی عملکرد نرم افزارها و تاثیر منفی بر سرعت کار

راهکار امنیت پیشرفته

برای حفاظت کامل از تمام اجزای یک شبکه که متشکل از نقاط پایانی، سرورها و سرویس ها، بستر مجازی و زیرساخت ارتباطی می باشد، شناسایی نقاط آسیب پذیر و حیاتی بمنظور طراحی ساختار یکپارچه امنیت بر اساس استاندارد های معتبر و فناوری های نوین، گامی کلیدی محسوب می شوند.

در پیاده سازی راهکارهای پیشرفته امنیت، علاوه بر لزوم پیش بینی انواع چالشهایی که بطور خاص زیرساخت فناوری اطلاعات را تهدید می کنند، باید تعامل و هماهنگی بین راهکار های حفاظتی برقرار گردد؛ تا سامانه‌های دفاعی بطور هماهنگ قادر به شناسایی حملات و نیز واکنش در برابر رخداد ها باشند.

بهره مندی از دانش و مهارت متخصصان مجرب و با سابقه، عامل اصلی موفقیت ما در طراحی، پیاده سازی و نگهداری پروژه های بزرگ راهکارهای نوین امنیتی می باشد.

حملات پیشرفته

اختلال وسیع در سامانه ها و چرخش کار

نقاط ضعف قابل شناسایی

نفوذ به سرویسها و منابع حیاتی شبکه

دسترسی های غیر مجاز

ورود نفوذگران بمنظور شناسایی آسیب پذیریها

به خطر افتادن اطلاعات حساس

باجگیری و یا تخریب داده ها توسط نفوذگران

محصولات امنیتی ضعیف

انتشار وسیع بدافزار در سطح شبکه

ایمیلها و وب سایت های جعلی

فریب کاربران برای اجرای کد مخرب و یا سرقت اطلاعات

توقف سرویس ها و چرخش کار

ضرر و زیان مالی و اعتباری همراه با خسارتهای وسیع

ضعف در دانش و تجربه

آماده نبودن نیروها جهت واکنش هماهنگ در برابر تهدید ها

سیاست های دفاعی ناکارآمد

فقدان برنامه مشخص برای مقابله با رخدادهای امنیتی

- ارزیابی امنیت نقاط پایانی، سرویسها، شبکه داخلی، بستر ارتباطی و زیر ساخت مجازی
- طراحی و بازنگری ساختار امنیت شبکه بر مبنای استانداردهاو سیاستهای سازمانی
- نصب و راه اندازی و پیکربندی سامانه مدیریت جامع تهدید ها
- پیاده سازی راهکار جامع مدیریت سطح دسترسی
- نصب و راه اندازی ضدهرزنامه
- مستند سازی پیکربندی های اعمال شده در محصولات
- برگزاری دوره های آموزشی و آگاه سازی
- ارائه خدمات مشاوره بمنظور انتخاب محصولات امنیتی مورد نیاز
- نصب و راه اندازی راهکار مدیریت آسیب پذیری
- نصب و راه اندازی راهکار مدیریت متمرکز پشتیبانی اطلاعات
- پیاده سازی سامانه یکپارچه ضدبدافزار
- پیاده سازی راهکار مدیریت نصب اصلاحیه
- بررسی دوره ای عملکرد محصولات امنیتی و وضعیت امنیت زیرساخت فناوری اطلاعات
- واکنش به رخدادها و خدمات پشتیبانی نامحدود

راهکار امنیت جامع

راهکار امنیت جامع بر مبنای شناخت صحیح چالشهای حفاظتی، نیازهای مطرح شده در برقراری امنیت را پوشش داده و با ایجاد یکپارچگی بین محصولات امنیتی، امکان واکنش سریع و خودکار در برابر تهدیدهای پیشرفته و پیچیده را فراهم می‌سازد.

مهمترین عامل در حفظ یکپارچگی و هماهنگی در واکنش به تهدیدها استفاده از فناوریهای پیشرفته از جمله یادگیری ماشین و هوش مصنوعی در مرکز عملیات امنیت می باشد که علاوه بر کاهش بار کاری و سرعت بخشیدن به پردازش انبوه رخدادهای دریافت شده از محصولات حفاظتی، از وقوع خطای انسانی نیز پیشگیری می نماید.

چالشهای مهم در برقراری امنیت

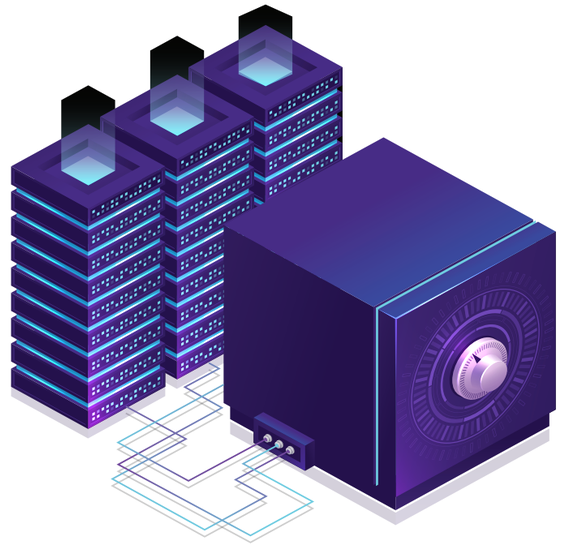
- انبوه هشدارهای امنیتی که بطور مداوم توسط محصولات حفاظتی مخابره می شوند و نیازمند بررسی دقیق در زمان مناسب می باشند.
- تعدد و گوناگونی ابزارهای حفاظتی که برای پوشش دهی نیازهای مختلف بطور همزمان مورد استفاده قرار میگیرند.
- طولانی بودن فرایند تحلیل رخدادها به دلیل وابستگی به اطلاعات و تجربه نیروی متخصص و با در نظر گرفتن ضریب احتمال خطای انسانی.
- در دسترس نبودن منابع لازم برای واکنش در زمان رخداد شامل نیروی انسانی، منابع اطلاعاتی و تجهیزات.

راهکار امنیت جامع علم و صنعت با رفع چالشها و تنگناها و نیز سرعت بخشیدن به عملیات پردازش رخدادها، برقراری امنیت در سراسر شبکه را برای شما تامین می کند.

- ارزیابی امنیت نقاط پایانی، سرورها و سرویسها، زیرساخت مجازی و زیرساخت شبکه
- طراحی ساختار امنیت شبکه بر مبنای استانداردهای معتبر و سیاستهای سازمانی
- نصب و راه اندازی سامانه مدیریت جامع تهدید ها
- پیاده سازی راهکار مدیریت دسترسی به شبکه
- پیاده سازی سامانه مدیریت دسترسی به سرویسها
- راه اندازی سامانه یکپارچه ضدبدافزار
- نصب و راه اندازی سامانه ضدهرزنامه
- برگزاری دوره های آموزشی و آگاه سازی
- ارائه مشاوره و تولید نقشه راه امنیت بر اساس نتایج نیاز ارزیابی های صورت گرفته
- نصب و راه اندازی راهکار مدیریت آسیب پذیری
- پیاده سازی راهکار مدیریت پشتیبانی اطلاعات
- راه اندازی راهکار نصب و گسترش اصلاحیه ها
- مقاوم سازی نقاط پایانی، سرویسها و تجهیزات ارتباطی
- مستند سازی پیکربندی های اعمال شده در محصولات
- بررسی مستمر عملکرد محصولات امنیتی و وضعیت امنیت سایبری
- واکنش و تحلیل رخدادها و خدمات و پشتیبانی نامحدود

راهکار پیشگیری از نشت اطلاعات

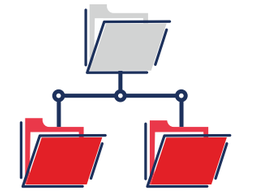
خروج و تغییر غیر مجاز اطلاعات از جمله تهدیدهای موثر در افزایش ریسک از دست دادن دارایی های اطلاعاتی محسوب می شوند. عواملی مانند جاسوسی های برنامه ریزی شده با هدف تخریب کسب و کار و یا ایجاد اختلال در چرخه کاری و همچنین ضعفهای طراحی امنیت مانند عدم طبقه بندی اطلاعات و اعمال سیاستهای حفاظتی درون سازمانی، دلایل اصلی خسارتهای ناشی از نشت اطلاعات می باشند.



گامهای مهم درپیشگیری از نشت اطلاعات

- تفکیک اطلاعات بر اساس طبقه بندی های سازمانی
- پایش دسترسی کاربران به داده های حساس
- پایش انتقال داده از طریق وب و ایمیل
- تحلیل رفتارهای سازمانی در زمان تبادل اطلاعات
- اطمینان از امنیت محل قرارگیری اطلاعات
- پایش محتوای فایل های در حال تبادل
- کنترل وسایل ذخیره سازی قابل حمل
- رمزنگاری داده های مهم در زمان انتقال

امکاناتی مانند شناسایی الگوی داده، دسته بندی اطلاعات سازمانی، قواعد پیشگیرانه سازگار با چرخه کاری و نیز تولید هشدار و گزارش‌های کارآمد بمنظور اطلاع از وضعیت تبادل اطلاعات، از جمله عوامل راهبردی در اعمال سیاستهای سازمانی بمنظور پیشگیری از نشت و سرقت اطلاعات می باشند.



روشهای ناامن انتقال داده در شبکه داخلی

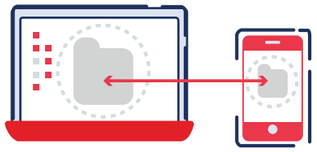
دسترسی نفوذگران به منابع اطلاعاتی سازمان

عدم کنترل رفتار و فعالیتهای کارمندان

محل نا امن قرارگیری اطلاعات حساس

جاسوس افزارها و حملات پیشرفته

تبادل ناامن داده در اینترنت و شبکه های خارج سازمان



استفاده از تجهیزات شخصی برای مصارف سازمانی

راهکار پیشگیری از نشت اطلاعات آمیخته ای از فناوری های حفاظتی است که بر اساس سیاستهای امنیتی سازمان، دارایی‌های اطلاعاتی شما را حفظ و از سرقت و یا تغییر غیر مجاز آنها پیشگیری می کند.

- ارائه خدمات مشاوره و طراحی سیاستهای حفاظت از دارایی های اطلاعاتی
- نصب و راه اندازی سامانه مدیریت دسترسی به اینترنت
- مقاوم سازی نقاط پایانی، سرویسها و تجهیزات ارتباطی در برابر تهدید ها
- شناسایی الگوی تبادل داده های سازمانی و اعمال سیایتهای امنیتی مناسب
- ارزیابی امنیت نقاط پایانی، سرورها و سرویسها، زیرساخت مجازی و زیرساخت شبکه
- طراحی و راه اندازی راهکار پیشگیری از نشت اطلاعات
- پیاده سازی سامانه پشتیبانی اطلاعات
- پیاده سازی و راه اندازی راهکار نصب و گسترش اصلاحیه
- مستند سازی پیکربندی های اعمال شده در محصولات
- برگزاری دوره های آموزشی و آگاه سازی

خدمات امنیت سایبری علم و صنعت

توسعه و گسترش امنیت فناوری اطلاعات باعث پدید آمدن زیر شاخه های وسیع آن شده و این امر پیچیدگی هایی را در انتخاب نوع خدمات برای کاربران پدید آورده است. بسته های خدمات امنیت سایبری علم و صنعت با هدف رفع این پیچیدگیها، دستیابی کاربران به خدمات امنیت فناوری اطلاعات بر اساس نیازهای سازمانی مد نظر را آسان نموده است.

ارزیابی

شناسایی و رفع نگرانی های حفاظتی

- بررسی صحت تنظیمات و عملکرد محصولات امنیتی
- اطمینان از مقاوم بودن سرورها و سرویسها در برابر تهدید های سایبری
- رفع نقاط آسیب پذیر در زیرساخت ارتباطی و پیشگیری از حملات
- تامین امنیت زیرساخت مجازی و اطمینان از عملکرد سرویسهای مبتنی بر این زیرساخت

نصب و راه اندازی

اطمینان از عملکرد صحیح محصولات امنیتی

- طراحی سامانه های حفاظتی بر اساس نیازهای سازمانی
- اطمینان از پوشش سراسری راهکارهای امنیتی در سراسر شبکه
- پایش مستمر اجزای شبکه و شناسایی نقاط ضعف و آسیب پذیر
- طراحی روشهای استاندارد بازگشت از بحران
- اعمال سیاستهای پیشگیری از نشت اطلاعات

مشاوره

بهره مندی از دانش و تجربه متخصصان

- طراحی معماری زیرساخت شبکه بر اساس استانداردهای امنیتی
- بازنگری طراحی امنیت و ایجاد سازگاری در تبادل امن اطلاعات سازمانی
- بررسی نیازمندیها و امکانسنجی پیاده سازی راهکارهای حفاظتی
- طراحی و تولید نقشه جامع امنیت بر مبنای مدل کسب و کار و دورنمای آینده سازمان
- نظارت بر عملکرد پیمانکاران و تحویل گیری سرویسهای امنیت فناوری اطلاعات

آگاه سازی و آموزش

دستیابی به اطلاعات و دانش مقابله با رخدادهای امنیتی

- انتقال دانش بمنظور بهره برداری از محصولات و راهکارهای امنیتی
- اعلام هشدار در زمان وقوع رخدادهای فراگیر به همراه راهکار مقابله با تهدید ها
- جلسات آگاه سازی مدیران و راهبران فناوری اطلاعات
- برگزاری دوره های عمومی و اختصاصی آموزش مباحث امنیت

بی تردید آگاهی از سطح امنیت سایبری سازمان، اولین و مهمترین گام در اخذ تصمیم های موثر برای اولویت بندی در بکارگیری راهکارهای حفاظتی و نیز مقاوم سازی زیرساخت فناوری اطلاعات در برابر تهدید ها می باشد. با اطلاع از ریسکهای امنیتی بالقوه و درک صحیح از وضعیت مقاومت زیر ساخت فناوری اطلاعات در برابر حملات، قادر خواهید بود برنامه های حفاظتی را بر اساس اولویتهای امنیتی طرح ریزی و پیاده سازی نمایید.

نکات مهم مورد توجه در ارزیابی امنیت:

- آسیب پذیریها در لایه نقاط پایانی
- باج افزارها، ویروسها، جاسوس‌افزارها
- تهدید های پیچیده و ماندگار
- نفوذ به پایگاه داده و تخریب یا سرقت اطلاعات
- دسترسی کاربران به وب سایتهای مخرب
- دسترسیهای شبکه ای غیر مجاز
- ایمیلهای حاوی کدهای مخرب
- ارتباط شبکه ای ناامن بین شعب
- حملات با هدف از کاراندازی سرویسها
- شنود ارتباطات و سرقت اطلاعات
- جعل نشانی های ارتباطی با هدف ایجاد اختلال
- ناهماهنگی در واکنش به تهدیدها و حملات
- آسیب پذیری سامانه های حساس مانند اتوماسیون
- اجرای نرم افزارهای ناشناس توسط کاربران
- محل ناامن قرارگیری اطلاعات حساس
- دسترسی غیر مجاز به منابع اطلاعاتی محرمانه و حساس

سوالاتی مدیران سازمان برای آگاهی از احتمال برخورد با حملات سایبری باید از خود بپرسند:

- تهدید های سایبری از چه طریقی ممکن است عملکرد و کارایی چرخش کار را تحت تاثیر قرار دهند و بر کدام بخش سازمان تاثیر منفی خواهند گذاشت؟ (زنجیره تامین، ارتباطات عمومی، منابع انسانی و یا عملیات مالی)
- چه نوع اطلاعاتی را از دست خواهیم داد؟ (اطلاعات محرمانه معاملات، اطلاعات مشتریان، منابع تحقیقاتی و یا اطلاعات هویتی اشخاص)
- زیرساخت فناوری اطلاعات سازمان تا چه حد توان مقابله با حملات سایبری را دارد؟
- در حال حاضر هدف چه نوع حملاتی قرار گرفتیم و چه کسانی پشت این تهدید ها هستند؟
- کدام بهروشها را باید برای حفظ سازمان در برابر تهدید های فعلی و آینده بکار بگیریم؟

شناسایی ریسک ها و میزان احتمال وقوع رخداد های امنیتی مهمترین گام در طراحی برنامه های حفاظتی آینده بمنظور رفع ضعف‌های فعلی می باشد. متخصصان امنیت سایبری علم و صنعت شما را در طراحی لایه های حفاظتی همراهی خواهند نمود.

- شناسایی نقاط ضعف سیستمهای عامل و نرم‌افزارهای مورد استفاده در شبکه
- ارزیابی ریسکها و احتمال وقوع رخدادهای امنیتی
- بررسی احتمال سرقت و تخریب دارایی های اطلاعاتی
- بررسی روشهای مورد استفاده برای بازگشت از بحران و بازیابی اطلاعات و سرویسها
- بررسی صحت عملکرد و کارایی تنظیمات محصولات حفاظتی مورد استفاده
- شناسایی دسترسی ها و ارتباطات غیر مجاز
- اطمینان از فعال بودن فناوریهای نوین دفاعی در محصولات امنیتی
- شناسایی راه های نفوذ به شبکه
- مستند سازی تنظیمات و راهکارهای مورد استفاده
- شفاف سازی سطح آمادگی دفاعی سازمان برای مقابله با تهدیدها و حملات

مهمترین هدف ما ارائه فناوریهای نوین حفاظتی و نیز برترین محصولات بین‌المللی به همراه خدمات پشتیبانی با کیفیت و استاندارد می باشد. برای تحقق این هدف، محصولات دفاعی برتر توسط تیم تحقیق و توسعه ما مورد بررسی قرار گرفته و بهترین محصولات بر اساس پارامترهایی مانند سازگاری، یکپارچگی و نیز توانایی، برای ارائه به مشتریان در سبد محصولات قرار گرفته اند.

دسته بندی محصولات

استراتژی ما در جلب رضایت مشتریان، ارائه خدمات پشتیبانی منعطف و منطبق با نیازها و درخواستها و با در نظر گرفتن بالاترین سطح کیفیت می باشد. بر این اساس، خدمات پشتیبانی محصولات امنیت فناوری اطلاعات علم و صنعت در سه سطح نقره ای، طلایی و پلاتینی ارائه می گردد.

سطوح خدمات پشتیبانی محصولات	نقره ای	طلایی	پلاتینی
بازدید حضوری بمنظور نصب و راه اندازی اولیه محصولات	✓	✓	✓
نصب و راه اندازی اولیه یا مجدد محصولات از راه دور (Remote)	✓	✓	✓
بازدید حضوری بمنظور نصب مجدد محصولات	✓	✓	✓
پشتیبانی از راه دور • پاسخگویی تلفنی • پاسخگویی در پورتال پشتیبانی • پاسخگویی به ایمیل • رفع اشکال از راه دور (Remote)	✓	✓	✓
بررسی و رفع اشکال بصورت حضوری		✓	✓
رسیدگی ۲۴ ساعته در ۷ روز هفته به رخدادهای امنیتی			✓
کنترل دوره ای عملکرد محصولات از راه دور(Remote)		✓	✓
بازدید دوره ای حضوری از عملکرد محصولات در مقابله با تهدید ها			✓
آگاه سازی و آموزش همگانی • ایمیل و پیامک هشدار امنیتی • عضویت در خبرنامه • دسترسی به پایگاه دانش • دوره های آموزشی (Remote) • منابع فارسی آموزش راهبری محصولات • برگزاری وبینارهای های آگاه سازی	✓	✓	✓
برگزاری دوره های حضوری آموزش محصولات و مباحث امنیت			✓
اختصاص کارشناس فنی مقیم به پروژه نگهداری سامانه های امنیتی			طبق توافقات
عضویت در باشگاه مشتریان و برخورداری از تخفیف ویژه سالانه	✓	✓	✓

متخصصان فنی ما با برگزاری جلسات و ارائه اسناد و اطلاعات فنی و نیز انجام نصب آزمایشی جهت اطمینان از سازگاری، شما را در انتخاب محصولات مناسب همراهی می کنند.

مدیریت رخدادهای امنیتی (Security Information and Event Management)

حمله های سایبری بطور روز افزون در سراسر جهان در حال انجام بوده و نفوذگران بی وقفه به دنبال سوء استفاده از ضعفهای امنیتی در سیستم ها، نرم افزار ها و سخت افزارها برای اجرای حملات هستند. راهکار اساسی برای پیشگیری و دفع تهدید های ناشناخته، شناسایی و رسیدگی بموقع به نشانه های رخدادها می باشد.

AT&T security

ALIEN VULET OSSIM

شرکت AT&T Cybersecurity نرم‌افزار مدیریت رخدادهای امنیتی خود را در دو قالب متن باز با عنوان OSSIM و محصول تجاری با عنوان USM برای پشتیبانی از شبکه های محلی و ابری ارائه می نماید. این محصول با شناخت کامل از نیازهای امنیت سازمان، امکانات جامعی را برای یکپارچه سازی شناسایی تهدیدها، پیش از وقوع حملات برای شما فراهم می کند.

- تایید شده توسط موسسه Gartner
- پیاده سازی و راه اندازی آسان
- بهره گیری از آزمایشگاه AT&T Alien برای شناسایی تهدید ها
- آنالیز ارتباطات و حملات
- شناسایی بیش از ۱۹ میلیون تهدید جدید با Threat Intelligence
- دریافت اطلاعات نقاط ضعف و تهدید ها از OpenIOC، CSV و STIX
- شناسایی هویت ارتباطات با Netflow
- اعلام هشدار در زمان شناسایی رخداد
- مورد تایید بیش از ۷۰۰۰ سازمان بین المللی
- تایید شده توسط موسسه SANS
- شناسایی و اولویت بندی نقاط ضعف
- کاوش و دسته بندی دارایی های IT
- مجهز به Intrusion Detection System
- قابلیت Host Intrusion Detection
- امکان شناسایی و تحلیل رفتار
- دسترسی کاربران به منابع و اطلاعات تهدیدها
- ارتباط با کلایتها با Agent و یا Agentless
- قابلیت نصب افزونه Endpoint

سامانه مدیریت رخدادهای امنیتی **Security Information and Event Management** ضمن جمع آوری حجم عظیم رخدادها از انواع تجهیزات شبکه، سامانه های امنیتی و سیستم های عامل، پس از غنی سازی و ایجاد همبستگی بین رخدادهای مرتبط، شما را قادر می‌سازد تا با شناسایی حملات در حال وقوع، بر وضعیت امنیت سازمان مسلط شده و با اعمال تدابیر امنیتی، از وقوع رخدادها پیشگیری نمایید.

elastic stack

محصول Elastic Stack تولید شده بر مبنای نرم افزار متن باز بوده و با بکارگیری دانش نوین داده، امکان پالایش و تحلیل داده های عظیم را فراهم آورده است.این محصول با قابلیت تحلیل رفتار تهدیدها، ارتباطات و بدافزارها، رفتارها و ارتباطات مشکوک را از بین انبوه اطلاعات جمع آوری شده از تجهیزات شبکه شناسایی کرده و شما را از احتمال وقوع حملات سایبری آگاه می‌سازد.

- جمع آوری انواع لاگ از تجهیزات
- دید وسیع از وضعیت امنیتی شبکه
- پایش مقدار استفاده پردازشها از منابع
- رصد وضعیت کارایی برنامه ها
- پشتیبانی از شبکه محلی و ابری
- مجهز به فناوری یادگیری ماشین
- قابلیت نصب Agent بر روی کلایتها
- قابلیت NetFlow برای رصد ارتباطات
- شناسایی و دسته بندی آسیب پذیریها
- سازگاری با Docker
- شناسایی ناهنجاری ها با قواعد خودکار ATT&CK-aligned
- موتور جستجوی قدرتمند در انبوه رخدادها
- کنترل وضعیت احراز هویت در شبکه
- ابزار مدیریتی با امکانات گرافیگی کاربردی
- شناسایی انواع Intrusion
- تحلیل لاگها برای یافتن رخدادها
- رصد کلایتها با File Integrity Monitoring
- کنترل انطباق پیکربندی ها با استانداردها و سیاستهای سازمانی
- شناسایی انواع rootkit و بدافزارهای جدید
- دریافت اطلاعات از Threat Intelligence

در طراحی ساختار امنیت فناوری اطلاعات، سرور ها و سرویسها مهمترین منابع و دارایی محسوب می شوند و از این رو دسترسی به آنها صرفاً برای کاربران ممتاز با سطح دسترسی مدیر سیستم و سرویس محدود می گردد. با گسترش انواع حملات سایبری، حفاظت از دسترسیهای اعطا شده به این دسته از کاربران و نیز نظارت بر عملکرد آنها به چالشی بزرگ مبدل شده است.

FUDO SECURITY

شرکت Fudo Security از پیشگامان توسعه دهنده فناوری های امنیتی بوده و فناوری نوین PAM را مبتنی بر هوش مصنوعی ارائه نموده است.

نام این فناوری منحصر بفرد، بعنوان یکی از برترین محصولات حوزه PAM در جدول برترینهای موسسه گارتنر درج شده و نیز با توجه به نیاز حفاظت از دسترسی کاربران، مورد استقبال سازمانها و شرکتهای مختلف قرار گرفته است.

• تحلیل هوشمند با روشهای زیست سنجشی (Biometrics)

با استفاده از راهکار پیشرفته ردیابی مبتنی بر فناوری های زیست سنجشی بکار رفته در سامانه مدیریت دسترسی کاربران ممتاز Fudo، قادر به تشخیص کمترین مقدار تغییر در رفتار کاربران در زمان استفاده از پودمانهای SSH و RDP خواهید بود. در این روش، تمام ارتباطات برقرار شده بطور لحظه ای مورد پایش قرار گرفته و امتیازدهی می شوند تا امکان تشخیص سوء استفاده از دسترسی ها و نیز بررسی اقدامات انجام شده توسط کاربر فراهم گردد.

همچنین این سامانه با اعلام هشدار شما را از وقوع رخدادهای مشکوک مانند تعداد ارتباطات برقرار شده توسط کاربر بیش از اندازه تعیین شده و یا دسترسی های طولانی مدت و نامتعارف، آگاه می سازد.

• مدیریت دسترسی ها بر پایه پودمانهای گوناگون

در سامانه Fudo PAM، کاملترین امکانات پایش کابران ممتاز نظیر امکان نظارت لحظه ای و تصویربرداری از ارتباطات برقرار شده، اتصال همزمان چند کاربر به منابع و همچنین امکان ارائه دسترسی های محافظت شده به اشخاص ثالث، گردآوری شده است.

بکارگیری امکاناتی نظیر تحلیل پروتکل HTTPS در این سامانه، حداکثر ضریب اطمینان از روش نظارت بر دسترسی ها را فراهم ساخته و همچنین، امکانات پایشی کنشگرا، ضمن اعلام انواع هشدار، هر نوع ارتباط و دسترسی مشکوک را تعلیق یا لغو می نماید.

• نظارت بر بازدهی کاربران

سامانه Fudo PAM عملکرد کاربران را بر اساس رفتار آنها تشخیص داده و شما را قادر می سازد تا بر اساس ارزیابی عملکرد کاربران، زمان و هزینه نگهداری سرویسهای فناوری اطلاعات را به مقدار مورد نیاز کاهش دهید.

راهکار مدیریت دسترسی کاربران ممتاز **Privileged Access Management** یا به اختصار **PAM**، بعنوان یک راهکار حفاظتی حیاتی با جدا نمودن کامل ارتباط مستقیم بین کاربران ممتاز و منابع مهم فناوری اطلاعات و نیز پایش و ثبت جزییات دسترسی ها و اقدامات صورت گرفته توسط کاربران، امکان نظارت بر عملکرد کاربران را فراهم کرده و همچنین با بکارگیری فناوریهای هوش مصنوعی و یادگیری ماشین، قادر به تشخیص رفتارهای مشکوک کاربران جهت پیشگیری از سوء استفاده از دسترسی های اعطا شده می باشد.

• برقراری ارتباط امن با منابع

پورتال کاربران سامانه Fudo PAM، امکان دسترسی سریع، آسان و در عین حال امن کاربران به منابع را با لحاظ کردن روشهای احراز هویت یکپارچه SSO، فراهم می آورد.

• پشتیبانی از سامانه مدیریت کاربران

قابلیت پشتیبانی از سامانه های Active Directory و LDAP بمنظور وارد کردن خودکار کاربران و کلمه های عبور آنها در سامانه Fudo PAM فراهم می باشد.

• اعمال قواعد حفاظتی

سامانه Fudo PAM قابلیت شناسایی متن از تصویر (OCR) را داشته و شما را قادر می سازد تا با تعریف قواعد حفاظتی، در صورت اجرای فرمانهای غیر مجاز و مشکوک توسط کاربر، ضمن اعلام هشدار، ارتباطات برقرار شده را قطع و دسترسی کاربر را به منابع حذف نماید.

• تصویر برداری از ارتباطات و گزارش های کاربردی

سامانه Fudo PAM مجهز به امکان ثبت و نگهداری از تصاویر ارتباطات و اقدامات انجام شده توسط کاربران می باشد. همچنین در این سامانه، امکان تولید گزارش های گوناگون بمنظور نظارت بر عملکرد کاربران فراهم می باشد.

• تایید هویت چند لایه بر روی تلفن همراه

تایید هویت چند لایه در سامانه Fudo PAM که از آن با نام 4-Eyes نام برده می شود، قابلیت دریافت تایید از مدیر سیستم را پیش از ورود فراهم می نماید.

• انطباق با توپولوژی های شبکه

امکان پیاده سازی این سامانه در انواع توپولوژی های شبکه با روشهای Transparent Gateway، و Proxy فراهم می باشد.

همچنین بمنظور افزایش توان عملیاتی و تقسیم بار کاری، قابلیتهای پیشرفته Clustering سامانه Fudo PAM مانند Load Balancing و High availability، امکان نصب آن را در شبکه های وسیع و بزرگ فراهم می سازد.

• پودمانها و استانداردهای قابل پشتیبانی

پشتیبانی از خط فرمان: SSH، Telnet 3270، Telnet 5250

پروتکلهای گرافیکی: Remote App، VNC، RDP over RDP و X11

پروتکلهای وب: HTTPS، HTTP

شبکه های صنعتی: Modbus

پشتیبانی از IPV6

• برچسب زنی بر روی ارتباطات و تحلیل در عمق

تمام ارتباطات تحت نظارت سامانه Fudo PAM قابلیت درج برچسب و توضیحات را دارد.

پیشگیری از نشت اطلاعات (Data Loss Prevention)

با فراگیر شدن فناوری اطلاعات در چرخش کار، انبوهی از داده ها با درجه اهمیت متفاوت مانند اطلاعات مشترکین و مشتریان، تامین کنندگان، اسرار فنی پروژه ها و محصولات و اطلاعات تعاملات داخلی، توسط سازمانها در حال جمع آوری، پالایش و تبادل می‌باشد که در دنیای امروز بعنوان دارایی های اطلاعاتی با ارزش محسوب می گردد. در این میان، دامنه تهدید هایی مانند سرقت، تغییرات غیر مجاز عمدی یا سهوی، انتشار ناخواسته و نیز حملات سایبری، به از دست رفتن دارایی های اطلاعاتی حساس ختم شده و موجب خسارتهای جبران ناپذیر می گردد.

safetica®

سامانه پیشگیری از نشت اطلاعات Safetica امکان رصد تبادل داده از کانالهای مختلف از جمله ایمیل، وب و وسایل ذخیره سازی را فراهم نموده و شما را قادر می سازد تا با پایش دسترسی کاربران، سیاستهای امنیت اطلاعات را در لحظه اعمال نموده و تاثیر سیاستهای اعمال شده را از طریق هشدار ها و گزارشات دریافت نمایید.

شرکت علم و صنعت نماینده رسمی فروش و پشتیبانی محصولات Safetica در ایران با در اختیار داشتن کادر فنی مجرب و مورد تایید، خدمات مشاوره، پیاده سازی و نگهداری محصولات Safetica را در ایران عرضه می نماید.

- پیشگام در اتحاد فناوری با شرکتهای Microsoft Fortinet و ESET بعنوان Gold Partner
- رتبه بندی شده توسط موسسات Gartner و Forrester
- پشتیبانی و سازگاری با سیستم های عامل Microsoft Windows و macOS و نیز انواع نرم افزارهای کاربردی
- پیشگیری از نشت اطلاعات، تحلیل رفتار سازمانی کاربران و کنترل اپلیکیشن ها بطور یکپارچه
- منطبق بر استانداردهای HIPAA، PCI-DSS، GDPR و ISO27001 / IEC

ابزارهای پیشگیری از نشت اطلاعات Data Loss Prevention (DLP) با رویکرد های حفاظتی مختلف شما را قادر می سازند تا با پایش روشهای تبادل داده ها و نیز کنترل رفتار سازمانی، سیاستهای امنیتی را بمنظور تامین امنیت دارایی های اطلاعاتی ارزشمند اعمال نمایید.

• ویژگیهای کلیدی

- تعریف چرخش کار و زمانبندی برای تبادل داده ها
- شناسایی داده های حساس با روش کاوش Discovery
- سرعت عملکرد بی نظیر در اعمال قواعد به سیستمها و دریافت بازخوردها در شبکه های بزرگ
- مدیریت استفاده از سخت افزارهای مجاز
- پایش و آنالیز رفتار کاربران و تولید گزارش از بازدهی کاربران
- کنترل و اعمال محدودیت در تصویر برداری
- نظارت و اعمال محدودیت چاپ اطلاعات
- رمزنگاری تجهیزات ذخیره سازی
- کنترل دسترسی به شاخه های اشتراکی محلی و ابری
- تولید گزارش و ارسال هشدار برای آگاهی از رخدادها امنیتی
- سازگاری با سامانه های Active Directory
- حفاظت خودکار از سامانه DLP و Agent در برابر دسترسی های غیر مجاز
- سازگاری با انواع SIEM بمنظور یکپارچگی گزارشات
- محیط کاربری مبتنی بر وب با کاربری آسان
- حفاظت از فایلهای در حال تبادل از طریق RDP
- مدیریت تکثیر اطلاعات از طریق CD/DVD و USB Flash
- حفاظت از ایمیل های حساس بدون وابستگی به نرم افزارهای تبادل ایمیل
- گزارش اختصاصی از عملکرد کاربران راه دور
- دسته بندی اطلاعات توسط کاربران ممتاز
- پایداری در شناسایی فایلهای برچسب دار قبل یا بعد از اعمال تغییرات نرم افزاری
- حفاظت از اطلاعات در حال تبادل در بستر وب بدون وابستگی به نرم افزارهای مرورگر و پشتیبانی از End-to-end Encryption
- شناسایی مستندات حساس با زبان فارسی
- کنترل انواع نرم افزارهای کاربردی بدون محدودیت در نوع و یا نسخه نرم افزار

Gartner

FORRESTER®

RED HERRING EUROPE WINNER 100

Cyber Security Awards Finalist 2019

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

حمله های سایبری بی وقفه در حال انجام بوده و نفوذگران هیچ فرصتی را برای هدف قرار دادن سرویسها و زیرساختها از دست نمی دهند. بر اساس آمار بین المللی تنها در سال ۲۰۱۹ از بیش از ۱۷۰۰۰ آسیبب پذیری در حمله به سازمانها و کسب و کارها مورد استفاده قرار گرفته است.

مدیریت آسیب پذیری بعنوان راهکاری کلیدی، با شناسایی مستمر نقاط ضعف موجود در سطح شبکه، امکان اخذ تصمیمات فنی و تعیین سیاستهای امنیتی بمنظور پیشگیری از سوء استفاده از نقاط ضعف و آسیب پذیر را فراهم می‌سازد.

OpenVAS

Open Vulnerability Assessment Scanner

OpenVAS محصولی متشکل از امکانات شناسایی و مدیریت آسیب پذیری در سطح انواع شبکه ها بوده و در دو قالب نرم افزار متن باز و نیز تجهیزات Greenbone Security Manager ارائه می‌گردد. این محصول با بهره گیری از فناوریهای مختلف شناسایی نقاط ضعف و نیز مقایسه سوابق وضعیت امنیت شبکه شما را قادر می سازد تا تهدید های جدید در سطح شبکه را شناسایی نمایید.

- شناسایی بیش از ۸۹۰۰۰ آسیب پذیری
- به روز رسانی از منابع رسمی بین المللی و اطلاعات اختصاصی
- ارائه شده در قالب ماشین مجازی
- ساختار توزیع یافته مناسب برای شبکه‌های دارای شعب
- نرم افزار متن باز با قدمت فعالیت از ۲۰۰۷
- تولید گزارشات متنوع و ساخت داشبورد
- آگاه سازی روزانه از کشف آسیب پذیری‌ها
- پویش زمانبندی شده و اعلام هشدار
- شناسایی و تحلیل ارتباطات شبکه ای
- پویش آسیب پذیری سرویسهای وب
- به روز رسانی بر خط و برون خط "مناسب برای شبکه های جدا از اینترنت"
- پشتیبانی از شبکه های صنعتی SCADA
- ثبت و مقایسه سوابق پویش
- شناسایی و دسته بندی تجهیزات IT
- شناسایی و درجه بندی ریسک تهدیدها
- پشتیبانی از انواع سیستم های عامل و تجهیزات شبکه
- ارائه API جهت همگام سازی با سایر ابزارهای مدیریت امنیت شبکه

GFI LanGuard™

Network security scanner and patch management

محصول **GFI LanGuard** با رویکرد کاهش بار کاری مدیران شبکه، دارای امکاناتی نظیر شناسایی نقاط ضعف و نصب خودکار اصلاحیه می باشد. طراحی مبتنی بر Agent این محصول شما را قادر می سازد تا علاوه بر شناسایی آسیب‌پذیری و نیز نصب اصلاحیه ها، از اجرای دستورات لازم بمنظور مدیریت امنیت نقاط پایانی اطمینان حاصل نمایید.

- منطبق بر استانداردهای SANS،BugTraq SOX، HIPAA، PCI DSS، CVE، OVAL
- شناسایی بیش از ۶۰۰۰۰ آسیب پذیری
- شناسایی نقاط ضعف سخت افزارهای ارتباطی
- سازگاری با پلتفرم های مجازی سازی
- همگام سازی با سایر نرم افزارهای امنیتی
- پویش و تحلیل ارتباطات شبکه
- دسته بندی و تفکیک تجهیزات IT
- پشتیبانی از انواع سیستم های عامل Microsoft Windows ،macOS و Linux
- پویش با استفاده از Agent یا Agentless
- بررسی دوره ای وضعیت آسیب پذیری
- به روز رسانی خودکار و مستقیم
- نصب خودکار اصلاحیه های سیستم‌های عامل و انواع نرم افزارهای کاربردی
- همگام سازی با سیستم های مدیریت اصلاحیه مانند WSUS
- تولید گزارشهای متنوع
- ابزارش پایش و گزارشگیری مبتنی بر وب
- پیاده سازی بصورت توزیع یافته در شعب

امروزه زنجیره حملات وسیع سایبری با سوء استفاده از نقاط آسیب پذیر در سیستمهای عامل، نرم افزارهای کاربردی و دستگاه‌های ارتباطی آغاز می شود و نفوذگران بمحض انتشار نسخه های جدید محصولات، بررسی های گسترده ای را برای یافتن ضعف های امنیتی و شروع حملات خود انجام می‌دهند. در تقابل با نفوذگران، شرکتهای تولید کننده محصولات نیز بطور مستمر، اصلاحیه های خود را بمنظور رفع آسیب پذیریهای امنیتی، افزایش عملکرد و سازگاری با سایر محصولات نرم افزاری و نیز حفاظت در برابر دسترسی های راه دور، تولید و عرضه می نمایند.

در این میان نقش حیاتی مدیریت نصب و گسترش اصلاحیه ها برای پیشگیری از سوء استفاده نفوذگران و کنترل حملات گسترده، غیر قابل انکار بوده و استفاده از سامانه مدیریت نصب اصلاحیه در هر نوع شبکه با هر مقدار وسعت و بستر ارتباطی الزامی می باشد.

GFI LanGuard

Network security scanner and patch management

راهکار GFI LanGuard از جمله محصولات تکامل یافته بمنظور شناسایی و رفع نقاط ضعف سیستم های عامل و نرم افزارهای کاربردی می باشد. این محصول با استفاده از Agent و یا بصورت Agentless در انواع شبکه از جمله شبکه‌های جدا از اینترنت (Air Gap Network) قابل پیاده سازی بوده و برای پشتیبانی و مدیریت شعب شبکه های گسترده، امکاناتی از قبیل Relay را فراهم نموده است.

از جمله امکانات این محصول امکان یکپارچگی آن با سرویس WSUS بمنظور تمرکز سرویس دهی در شبکه های مبتنی بر محصولات Microsoft بوده و نیز ویژگی هایی مانند تعریف و اعمال قواعد متنوع و منعطف، استفاده از این محصول را برای راهبران آسان نموده است.

- شناسایی خودکار ایستگاه های کاری، سرور، دستگاه های ارتباطی
- گروهبندی و مدیریت آسان رایانه ها بصورت متمرکز
- پویش مستمر شبکه برای تشخیص اصلاحیه های مورد نیاز
- سازگار با سیتم های عامل Linux، Microsoft و MacOS
- مدیریت شبکه با استفاده از Agent و یا بصورت Agentless

ManageEngine Patch Manager Plus

نرم افزار Patch Manager Plus ارائه شده توسط شرکت ManageEngine از جمله محصولات کارآمد در زمینه مدیریت اصلاحیه در سطح شبکه بوده و دارای قابلیت های منحصر بفرد مانند تست اصلاحیه ها قبل از نصب، شناسایی اصلاحیه های مورد نیاز انواع برنامه های کاربردی و یکپارچگی با زیرساخت شبکه های مبتنی بر محصولات Microsoft می باشد.

این محصول با در نظر گرفتن انواع شرایط شبکه های بزرگ و متوسط، امکان پیاده سازی در شبکه محلی و با شبکه ابری (Cloud) را داشته و در قالب دو بسته Professional برای شبکه های محلی و Enterprise برای شبکه های گسترده ارائه می‌گردد.

- بیش از ۶۰۰۰ مشتری بزرگ و ۳۰۰۰۰۰۰ رایانه تحت پوشش
- پشتیبانی از بیش از ۳۰۰ نرم افزار کاربردی مختلف و نیز انواع سیستم های عامل
- امکان تست سازگاری اصلاحیه ها قبل از نصب و گسترش در شبکه
- قابل پیاده سازی در شبکه محلی و نیز شبکه ابری
- گزارشات جامع و کاربردی جهت ممیزی و صحت عملکرد رایانه ها

Microsoft System Center Configuration Manager

راهکار System Center Configuration Manager (SCCM) یکی از فراگیر ترین راهکارهای شرکت Microsoft برای مدیریت رایانه های تحت شبکه می باشد.

این راهکار علاوه بر بهره گیری از سرویس نام آشنای Windows Server Update Service (WSUS) بمنظور نصب و گسترش اصلاحیه های سیستم های عامل و نرم افزارهای کاربردی، دارای امکاناتی برای شناسایی دارایی های IT سازمان، کنترل صحت عملکرد سیستمها، اطمینان از اعمال قواعد و سیاستهای سازمانی در سطح شبکه، نصب برنامه از راه دور، و نیز مدیریت سیستمهای عامل و محصولات شرکت Microsoft می باشد.

- سازگاری کامل با محصولات شرکت Microsoft
- یکپارچگی با راهکارهای مدیریت شبکه های مبتنی بر سرویسهای Microsoft
- قابل پیاده سازی در شبکه های متوسط و بزرگ
- بکارگیری پایگاه داده Microsoft SQL Server
- پشتیبانی از بسترهای مجازی Hyper-V و VMware

ضدبد افزار یکپارچه (Endpoint Security)

افزایش چشمگیر حملات بدافزار ها به چالشی بی پایان برای مدیران و راهبران فناوری اطلاعات مبدل شده و آمارهای بین المللی نشان دهنده افزایش پیچیدگی و سرعت انتشار انواع تهدید ها با اهداف گوناگون می باشد. شرکتهای برتر تولید کننده محصولات ضدبدافزار بر اساس مفاهیم امنیت، امکانات مختلفی را در محصولات خود بکار گرفته اند.

kaspersky

شرکت Kaspersky با بکارگیری امکانات و فناوری های نوین و قدرتمند از جمله شبکه سراسری اطلاعات تهدید ها با عنوان Kaspersky Security Network، رفتار شناسی، هوش مصنوعی و یادگیری ماشین، Application Control رمزنگاری، SandBox، مدیریت آسیب پذیری و نصب اصلاحیه، کنترل سخت افزار و دیگر امکانات برتر، راهکارهای جامع خود را در دسته بندی های مختلف، بمنظور پوشش دهی نیازهای کاربران عرضه می نماید.

- حفاظت از ۷۲۰۰۰۰ شبکه بزرگ، ۴۰۰ میلیون کاربر از ۱۹۹۷
- موفَقیت در تمام آزمونهای ارزیابی عملکرد محصولات امنیتی
- یکپارچگی امکانات و پوشش تمام نیازها در یک راهکار جامع
- شناسایی نسل جدید حملات هدفمند و پیشرفته
- پیاده سازی و راهبری آسان در انواع بسترهای شبکه

ESET

شرکت ESET با دسته بندی محصولات ضدبدافزار خود بر اساس نیازهای شبکه های کوچک، متوسط و بزرگ و بکارگیری ابزارمدیریتی پیشرفته، امکان مدیریت امنیت در لایه های مختلف را در شبکه محلی و یا سرویس مبتنی بر رایانش ابری فراهم نموده است.

فناوری های منحصر بفرد بکار رفته در این ضدبدافزار شامل ESET Augur، ESET DNA، ESET LiveGrid،، شناسایی رفتار Botnet، Protection و Ransomware Shield بوده که پیشگیری از فعالیت نسل جدید بدافزار مانند Fileless Malware و Advanced Persistent Threats را میسر می‌سازد.

- پیاده سازی شده در ۴۰۰۰۰۰ شبکه سازمانی از ۱۹۹۲
- دارای ۱۳ مرکز بین المللی تحقیق و توسعه امنیت
- کمترین مقدار مصرف منابع سخت افزار
- کمترین مقدار خطا در شناسایی بدافزار
- خصوصیات متنوع برای پوشش نیازهای امنیتی کاربران

Bitdefender

شرکت Bitdefender با بهره گیری از ابزارمدیریتی کارآمد با نام GravityZone، راهکار ضدبدافزار خود را مبتنی بر رایانش ابری و نیز در شبکه محلی، در قالب بسته های مختلف بر اساس سطوح گوناگون امنیت ارائه نموده است. این محصول از امکانات پیشرفته ای مانند Endpoint Risk Analytics، هوش مصنوعی، مدیریت اصلاحیه، فناوری یادگیری ماشین، کنترل سخت افزار و برنامه ها و نیز Sandbox Analyzer، برای حفاظت و دفع حملات بهره می برد.

- حفاظت از بیش از ۵۰۰ میلیون رایانه از سال ۲۰۰۱
- معماری امنیتی چند لایه در بستری یکپارچه
- بیش از ۳۰ امکان حفاظتی برتر به همراه افزونه های جانبی
- نصب و راه اندازی آسان در بستر مجازی
- پیاده سازی در پروژه های بزرگ و کسب و کارهای متوسط

مدیریت پشتیبانی اطلاعات (Backup Management)

بازگشت از بحران، مفهومی حیاتی در فناوری اطلاعات می باشد که دامنه آن به کاهش زمان توقف سـرویس پس از وقوع رخدادهای ناشـی از انـواع تهدید ها و نیز کاهش خسارتها ختم می گردد و مدیریت پشتیبانی اطلاعات از زیر شاخه های مهم در طراحی مدل بازگشـت از بحران می باشـد. پیروی از استانداردهای تهیه نسخه های پشتیبان اطلاعات بر اسـاس عمر مفید داده های قابل بازیابی و مقدار حساسـیت سـازمان در خصوص توقف سـرویس، انتخاب روش و محل مناسب نگهداری اطلاعات حساس و نیز اطمینان از بازگشت پذیری نسخه های پشتیبان در زمان وقوع بحران، عواملی موثر در طراحی فرایند حفظ و بازگرداندن اطلاعات حیاتی می‌باشند.

محصولات مدیریت پشـتیبانی اطلاعات شـما را قادر می سازند تا با بازگرداندن داده ها در شـرایط بحرانی، خسـارتهای ناشـی از رخدادهـای امنیتی را کاهش داده و سرویسـهای حساس را به چرخه کاری بازگردانید.

• ویژگیهای کلیدی

- فناوری Veeam DataLabs برای کنترل وقفه در سرویس
- پشـتیبانی از زیرسـاختهای فیزیکـی و نیز مجـازی مانند VMware vSphere ،Microsoft Hyper-V و Nutanix AHV
- پایش و اعلام هشدار برای پیشگیری از خرابی اطلاعات
- کاهش ۲۰% از مصرف پهنای باند و افزایش ۵۰% در سرعت تبادل داده با فناوری Built-in WAN Acceleration
- قابلیت Deduplication و Compression در تهیه پشتیبان
- فناوری SureReplica برای خودکار سـازی اطلاع از صحت بازگردانی نسخه های پشتیبان
- دریافت عنوان پیشتاز در سال ۲۰۱۹ از موسسه Gartner
- ابزار مدیریتی متمرکز و یکپارچه
- فناوری پیشـرفته برای حفاظت از داده های بدون سـاختار و ذخیره سازی بر روی NAS و یا سایر تجهیزات ذخیره سازی
- سازگاری با انواع سیستم های عامل Windows و Linux
- پشتیبانی از مدل Image-based backup
- ۵ برابر افزایش سرعت در پشتیبان گیری و بازگردانی VMs
- سـازگاری با فناوریهای حفاظتی سیسـتمهای عامل نظیر Microsoft Volume Shadow Copy و Oracle Recovery Manager

Veeam Backup Essentials محصولـی بـا قابلیت هـای منحصر بفـرد در پیاده سـازی مـدل هـای مختلـف مدیریت پشـتیبانی اطلاعات و بازگشت از بحران می باشد. این محصول با بهره مندی از فناوریهای پیشـرفته شـما را قادر می سازد تا از صحت نسخه های پشتیبانی اطمینان حاصل کرده و در صورت وقوع بحران، در کوتاهتریـن زمان، گردش کار را به حالت عادی بازگردانید.

- مورد تایید بیش از ۳۷۵۰۰۰ مشتری سازمانی
- سازگاری با انواع سیستم های ذخیره سازی اطلاعات
- افزایش لحظه ای فضای ذخیره سازی بر اساس SOBR
- حفاظت از فایلها و رفع بحرانهای ناشی از فعالیت باج افزارها
- فنـاوری منحصـر بفرد بـرای بازگردانی در لایـه برنامه های کاربردی

چرا علم و صنعت

گروه امنیت فناوری اطلاعات علم و صنعت با توان و ظرفیتهای ۳۰ ساله این شرکت و به پشتوانه تجربه متخصصان حوزه امنیت فناوری اطلاعات، با هدف ایجاد تحول در روند ارائه راهکارهای نوین حوزه امنیت فناوری اطلاعات، در سال ۱۳۹۸ شروع به فعالیت نمود.

شناسایی نیازمندیهای مشتریان ایرانی و نیز مطالعه و بکارگیری استانداردهای جهانی در ارائه محصولات برتر و خدمات با کیفیت، سرلوحه فعالیت های علم و صنعت می باشد. این شرکت با بهره مندی از گسترده ترین شبکه نمایندگی در سراسر کشور، تجربه استفاده از نسل جدید خدمات و محصولات امنیت فناوری اطلاعات را به مشتریان محترم تقدیم می نماید.

توانمندی ها

وسیع ترین شبکه نمایندگی فروش محصولات و خدمات پس از فروش در کشور

تیم تخصصی طراحی و استقرار راهکارها

بزرگترین گروه پشتیبانی محصولات و خدمات پس از فروش در کشور

ارایه محصولات و راهکارهای نوین شرکتهای برتر بین‌المللی

ویژگی ها

مطالعه و بکارگیری استانداردهای جهانی

بازنگری مداوم سطح کیفیت خدمات

تشخیص صحیح نیازمندیهای مشتریان

تحقیق و توسعه راهکارهای نوین

ارائه راهکارهای سازگار با کسب و کار

تیم فنی متخصص

برنامه ریزی و مدیریت پروژه

خط مشی

افزایش سطح امنیت کسب و کار

ارتقاء سطح آگاهی و دانش مشتریان

پوشش دهی درخواستهای مشتریان ایرانی

جلب اعتماد و حفظ رضایت مشتریان

کسب دانش و شناسایی راهکارهای نوین

افزایش سطح کیفیت خدمات

گسترش خدمات و راهکارها

ارزش سازمانی

حقوق بشر و ارزشهای انسانی

وظیفه شناسی و مسئولیت پذیری

گسترش نیروی انسانی و افزایش انگیزه کاری

مشتری مداری و تامین خواسته های مشتریان

استمرار و پایداری در تداوم کسب و کار

اخلاق و رقابت حرفه ای

خلاقیت و نوآوری

ما در مسیر ارائه بالاترین سطح کیفیت خدمات امنیت فناوری اطلاعات، از توانمندی مجرب ترین نیرو های متخصص بهره گرفته ایم تا با ایجاد تحول، تجربه ای منحصر بفرد از خدمات ویژه را به شما تقدیم کنیم.

شرکت کامپیوتری
علم و صنعت