



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

ارائه کننده راهکارهای نوین امنیت فناوری اطلاعات

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.

| پلاتینی | طلایی | نقره ای | سطوح خدمات پشتیبانی محصولات |
|---------|-------|---------|---|
| ✓ | ✓ | ✓ | 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 تهدیدها |
| ✓ | ✓ | ✓ | آگاه سازی و آموزش همگانی • ایمیل و پیامک هشدار امنیتی • عضویت در خبرنامه • 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 |
| ✓ | ✓ | ✓ | عضویت در باشگاه مشتریان و برخورداری از تخفیف ویژه سالانه |

مهمترین هدف ما ارائه فناوریهای نوین حفاظتی و نیز برترین محصولات بین المللی 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



پیشگیری از نشت اطلاعات



مدیریت نصب اصلاحیه



ضد بدافزار یکپارچه



مدیریت دسترسی



مدیریت جامع تهدیدها



مدیریت رخدادهای امنیتی



مدیریت آسیب پذیری



مدیریت پشتیبانی اطلاعات

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.

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 می سازد 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 می سازد.

- 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 گرافیکی کاربردی
- شناسایی انواع Intrusion
- تحلیل لاگها برای یافتن رخدادها
- رصد کلاینتها با File Integrity Monitoring
- کنترل انطباق پیکربندی ها با استانداردها و سیاستهای سازمانی
- شناسایی انواع rootkit و بدافزارهای جدید
- دریافت اطلاعات از Threat Intelligence
- جمع آوری انواع لاگ از تجهیزات
- دید وسیع از وضعیت امنیتی شبکه
- پیش 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 کلاینتها
- قابلیت NetFlow برای رصد ارتباطات
- شناسایی و دسته بندی آسیب پذیرها
- سازگاری با Docker

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 افزارها و سخت افزارها برای اجرای حملات هستند. راهکار اساسی برای پیشگیری و دفع تهدیدهای ناشناخته، شناسایی و رسیدگی بموقع به نشانه های رخدادها می باشد.

AT&T security



ALIEN VULET OSSIM

شرکت AT&T Cybersecurity نرم افزار 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 تهدیدها
- آنالیز ارتباطات و حملات
- شناسایی بیش از ۱۹ میلیون تهدید جدید با Threat Intelligence
- دریافت اطلاعات نقاط ضعف و تهدیدها 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 کلاینتها با Agent و یا Agentless
- قابلیت نصب افزونه Endpoint

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.



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 گartner 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 رخداد های 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 کاربران 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 جزئیات 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، قابلیت های 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

پروتکل های گرافیکی: Remote App، VNC، RDP، X11 و over RDP

پروتکل های وب: HTTP، HTTPS

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.

ابزارهای پیشگیری از نشت اطلاعات (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
- 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
- شناسایی داده های حساس با روش کاوش
- 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 فایل های 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

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 می باشد که در دنیای امروز بعنوان دارایی های اطلاعاتی با ارزش محسوب می گردد. در این میان، دامنه تهدیدهایی 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.



- سامانه پیشگیری از نشت اطلاعات Safetico 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 هشدارها و گزارشات دریافت نمایید.
- شرکت علم و صنعت نماینده رسمی فروش و پشتیبانی محصولات Safetico در ایران با در اختیار داشتن کادر فنی مجرب و مورد تایید، خدمات مشاوره، پیاده سازی و نگهداری محصولات Safetico 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 GDPR، PCI-DSS، HIPAA و IEC / ISO27001

Gartner

FORRESTER



Cyber Security Awards

Finalist 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 آسیب پذیری در حمله به سازمانها و کسب و کارها مورد استفاده قرار گرفته است.

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 می گردد. 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 شبکه های 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

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 می سازد.

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 آسیب پذیری 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، Linux و Windows، macOS
- پویش با استفاده از Agent یا Agentless
- بررسی دوره ای وضعیت آسیب پذیری
- به روز رسانی خودکار و مستقیم
- نصب خودکار اصلاحیه های سیستم های 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

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.

Microsoft* System Center Configuration Manager

راهکار System Center Configuration Manager (SCCM) یکی از فراگیرترین 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

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 می دهند. 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.

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 می گردد.

- 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

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 شبکه های 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
- گروه بندی و مدیریت آسان رایانه ها بصورت متمرکز
- پوشش مستمر شبکه برای تشخیص اصلاحیه های مورد نیاز
- سازگار با سیستم های عامل Linux، Microsoft و MacOS
- مدیریت شبکه با استفاده از Agent و یا بصورت Agentless

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

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



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 می سازد.

- 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

kaspersky

شرکت Kaspersky با بکارگیری امکانات و فناوری های نوین و قدرتمند از جمله شبکه سراسری اطلاعات تهدیدها 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 ۷۲۰۰۰۰۰ شبکه بزرگ، ۴۰۰ میلیون کاربر از ۱۹۹۷
- موفقیت 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

محصولات مدیریت پشتیبانی اطلاعات شما را قادر می سازند تا با بازگرداندن داده ها در شرایط بحرانی، خسارتهای ناشی از رخدادهای امنیتی را کاهش داده و سرویسهای حساس را به چرخه کاری بازگردانید.

ویژگیهای کلیدی

- فناوری Veeam DataLabs برای کنترل وقفه در سرویس
- پشتیبانی از زیرساختهای فیزیکی و نیز مجازی مانند VMware، Microsoft Hyper-V، vSphere 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 سازی اطلاع از صحت بازگردانی نسخه های پشتیبان
- دریافت عنوان پیشتاز در سال ۲۰۱۹ از موسسه Gartner
- ابزار مدیریتی متمرکز و یکپارچه
- فناوری پیشرفته برای حفاظت از داده های بدون ساختار 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
- سازگاری با فناوریهای حفاظتی سیستمهای عامل نظیر Microsoft Volume Shadow Copy و Oracle Recovery Manager

بازگشت از بحران، مفهومی حیاتی در فناوری اطلاعات می باشد که دامنه آن به کاهش زمان توقف سرویس پس از وقوع رخدادهای ناشی از انواع تهدیدها و نیز کاهش خسارتهای ختم می گردد و مدیریت پشتیبانی اطلاعات از زیر شاخه های مهم در طراحی مدل بازگشت از بحران می باشد. پیروی از استانداردهای تهیه نسخه های پشتیبان اطلاعات بر اساس عمر مفید داده های قابل بازیابی و مقدار حساسیت سازمان در خصوص توقف سرویس، 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 می باشند.

VEEAM

Veeam Backup Essentials محصولی با قابلیت های منحصر بفرد در پیاده سازی مدل های مختلف مدیریت پشتیبانی اطلاعات و بازگشت از بحران می باشد. این محصول با بهره مندی از فناوریهای پیشرفته شما را قادر می سازد تا از صحت نسخه های پشتیبانی اطمینان حاصل کرده و در صورت وقوع بحران، در کوتاهترین 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
- فناوری منحصر بفرد برای بازگردانی در لایه برنامه های کاربردی

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.

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.



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



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



ویژگی ها

مطالعه و بکارگیری استانداردهای جهانی

بازنگری مداوم سطح کیفیت خدمات

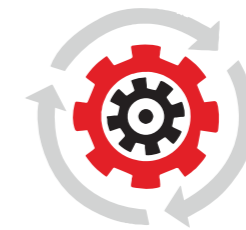
تشخیص صحیح نیازمندیهای مشتریان

تحقیق و توسعه راهکارهای نوین

ارائه راهکارهای سازگار با کسب و کار

تیم فنی متخصص

برنامه ریزی و مدیریت پروژه



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

بین المللی

شرکت کامپیوتری
علم و صنعت



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.