falcongaze™
Going Global with Security

کنترل کامل روی نشت داده‌ها

آیا شرکت شما از کانال‌های انتقال داده‌ی زیادی استفاده می‌کند؟

آیا کارمندان شما به اسناد حساس و محرمانه دسترسی دارند؟

آیا فکر می‌کنید که همه‌ی کارمندان شما وفادار هستند؟

SecureTower

با سیستم حفاظت در مقابل نشت داده‌ی SecureTower،
کسب و کار خود را از تهدیدات خارجی مصون نگه دارید.

از هسته‌ی کسب و کار خود حفاظت کنید

SecureTower یک راهکار پیچیده و سطح بالا است که برای حفاظت در مقابل نشت داده‌ها و نظارت بر فعالیت‌های کارمندان در شبکه طراحی شده است.

SecureTower یک سیستم ترکیبی است که به راحتی با شبکه‌ی شرکت یکپارچه شده و موارد زیر را برای کسب و کار به ارمغان می‌آورد:

- کنترل کامل روی نشت احتمالی داده‌ها از طریق کانال‌های مختلف
- ردگیری فعالیت‌های کارمندان در شبکه
- ارزیابی کارآمدی استفاده از منابع سازمان توسط کارمندان
- ایجاد بایگانی یکپارچه از ارتباطات سازمانی

SecureTower یک راهکار نرم‌افزاری است که کنترل روی نشت داده‌ها را در کانال‌های زیر فراهم می‌آورد:

- ایمیل‌هایی که در پروتکل‌های POP۳، SMTP و IMAP ساخته می‌شوند (مانند MS Outlook، Thunderbird، The Bat)، ایمیل‌های MS Exchange Server
- تمام ترافیک وب، شامل ایمیل‌های خارجی (مانند جی‌میل)، پیام‌ها در فروم‌ها و پست‌های ارسالی، شبکه‌های دیده شده در شبکه‌های اجتماعی و دیگر سرویس‌های وب که از پروتکل HTTP استفاده می‌کنند.
- چت‌ها و مکالمه‌هایی که در نرم افزارهای پیام‌دهی رد و بدل شده و از OSCAR (ICQ/AIM)، MSN: Windows Live Messenger، XMPP/Jabber، Miranda، Google Talk، PSI و دیگر پروتوکل‌های پیام‌دهی آنی مانند Skype استفاده می‌کنند.
- انتقال فایل از طریق پروتکل‌های HTTP، FTP و HTTPS، تبادل فایل‌ها از طریق پیام‌رسان‌های آنی مانند Windows Live، ICQ، Skype Messenger و غیره، و همچنین فایل‌های پیوست ایمیل‌ها.
- ترافیک SSL که از طریق پروتکل‌های رمزنگاری شده (HTTPS، ایمیل و ICQ رمز نگاری شده و غیره) صورت می‌پذیرد.
- داده‌هایی که به دستگاه‌های ذخیره‌ساز خارجی منتقل می‌شوند (ذخیره‌سازهای USB،هاردهای خارجی، کارت حافظه، سی‌دی/دی‌وی‌دی و دیسک‌های فلاپی)
- پرینت داده‌ها روی پرینترهای داخلی و پرینترهای متصل به شبکه

از تمام ارتباطات در شبکه مطلع باشید

فعالیت‌های شبکه را نظارت کنید

SecureTower گزارش‌های آماری جامعی را در مورد فعالیت‌های کارمندان در شبکه تهیه کرده و شما با کمک چارت‌ها و دیاگرام‌های ارائه شده می‌توانید مشاهده کنید که منابع سازمانی شما چگونه مورد استفاده قرار گرفته و از این رو کارآمدی کارمندان خود را ارزیابی کنید. SecureTower گزارش‌هایی تفصیلی از رویدادهای نشت داده برایتان مهیا می‌کند که در آن مشخص شده است که رویداد مورد نظر چه وقت، توسط چه کسی، در کدام شبکه، و در کدام کامپیوتر صورت پذیرفته است.

بصری سازی فعالیت کارمندان، امکان مقایسه‌ی نظیر به نظیر آن‌ها و شاخص‌های فعالیت آن‌ها را فراهم آورده که برای بازه‌ی زمانی خاصی تعیین شده باشد. با استفاده از این محصول، مدیریت سازمان و تیم امنیتی که می‌خواهند بدانند کارمندان سازمان چگونه از منابع شرکت استفاده می‌کنند، می‌توانند فعالیت‌های کارمندان را ردگیری و نظارت کنند. نتایج بدست آمده کمک می‌کند تا حجم کاری کارمندان را در طول روز، و همچنین کارآمدی استفاده از منابع سازمان را ارزیابی کرد. برای مثال می‌توانید مدت زمانی را که کارمندان صرف فعالیت غیر مرتبط با کار می‌کنند تخمین بزنید (مانند مکالمه‌های خصوصی و چت توسط برنامه‌های پیام‌رسان، یا بازدید از وب سایت‌های غیر مرتبط با کار، و غیره).

SecureTower به عنوان یک ابزار منابع انسانی

SecureTower نه تنها می‌تواند مورد استفاده‌ی دپارتمان امنیت قرار گیرد، بلکه می‌تواند یکی از ابزارهای متخصصان منابع انسانی باشد.

تحلیلگر گرافیکی ارتباطات کارمندان کمک می‌کند تا فعال ترین کارمندان شناسایی شده و نحوه‌ی تعاملات ایشان با رقبا نظارت شده و کارمندان به صورت خودکار غربال شوند.

از این رو **SecureTower** می‌تواند ابزار بسیار خوبی برای دپارتمان منابع انسانی باشد، زیرا به آن‌ها کمک می‌کند تا استراتژی‌های مربوط به کارمندان را به نحو موثرتری تدوین کرده و سیستم مدیریت کارمندان بهتری داشته باشند.

بایگانی یکپارچه‌ی ارتباطات

شرکت‌های بزرگ تمایل دارند که تمامی ارتباطات نوشتاری را، چه داخلی و چه خارجی، نگهداری کنند. در صورتی که اطلاعات مورد بحث توسط کارمندان و مدیران و یا مشتریان گم شوند یا در مورد آن‌ها سوء تفاهم پیش بیاید و یا فراموش شود، ارتباطات نوشتاری می‌توانند کمک خوبی باشند تا به سرعت اطلاعات لازم پیدا شده و رویدادهای گذشته بازیابی شوند.

تمام اطلاعات پایش شده تحلیل شده و در یک پایگاه داده ذخیره می‌شوند، از این رو سازمان‌ها قادر خواهند شد تا رویدادهای نشت داده را از جنبه‌ی زمان گذشته بررسی کنند. بعد از انتخاب یک پیام مشخص، تاریخچه‌ی کامل پیام فراهم خواهد شد.

دستیابی به بالاترین سطح امنیت

عملکرد بالا برای کنترل داده‌ها

SecureTower با تحلیل تمام ترافیک بر مبنای زمینه‌ها، مولفه‌ها و قوانین آماری که از پیش تعریف شده اند نشت داده‌ها را نظارت کرده و در این فرآیند مورفولوژی را هم در نظر می‌گیرد. این سیستم اطلاعات تفصیلی را در مورد ارسال کننده‌ی داده و گیرنده‌ی آن و همچنین متن کامل پیام مهیا می‌کند. با استفاده از کنترل داده‌ها بر اساس اصطلاحات و عبارات عادی و اثرانگشت‌های دیجیتال اسناد و پایگاه داده‌ها، حفاظت کامل امری تضمین شده است.

خط مشی‌های امنیتی انعطاف پذیر

SecureTower نشت داده‌ها را با تحلیل ترافیک بر مبنای قوانین امنیتی از پیش تعیین شده کنترل می‌کند. در صورتی که یک نشت امنیتی اتفاق بیفتد، SecureTower به صورت خودکار یک ایمیل هشدار را به مدیر امنیت اطلاعات ارسال می‌کند.

از این رو دپارتمان امنیت هر بار به صورت خودکار هشدارهایی را درباره‌ی انتقال غیر مجاز داده ها و اطلاعات حساس دریافت می‌کند، **حتی اگر این اطلاعات از طریق کانال‌های رمزنگاری شده یا پروتکل‌های SSL ارسال شده باشند.**

شناسایی کاربران به صورت آنی

آیا کارمندان شما از ترمینال سرور برای ارتباط به شبکه استفاده می‌کنند؟ ما یک راهکار عالی برای شما در نظر داریم! SecureTower می‌تواند با ایستگاه‌های نقطه انتهایی که به ترمینال سرور متصل شده اند کار کند. می‌توانید این کاربران را شناسایی کرده، و به صورت خودکار تمام ترافیک آن‌ها را آنالیز کنید. در حقیقت برای SecureTower فرقی نمی‌کند که ارتباط از نوع عادی می‌باشد یا سرور ترمینال، تمام کاربران به یک صورت کنترل می‌شوند.

SecureTower با شناسایی دقیق کاربر ارسال کننده‌ی داده‌ها ساعت‌های کاری که صرف بازرسی‌ها و تحقیقات مربوط به نشت داده‌ها می‌شوند را به حداقل می‌رساند.

یکپارچه شدن با اکتیو دایرکتوری

زمانی که یک محصول DLP را نصب می‌کنید، باید به آن آموزش دهید تا تمام کاربران شبکه ی شما را شناسایی کند. با SecureTower، این کار به سادگی تمام انجام می‌شود. زیرا تمام کاربران اکتیو دایرکتوری شما می‌توانند به آسانی با این محصول یکپارچه شوند. تنها با یک کلیک، تمام کاربرانی که در اکتیو دایرکتوری شما ثبت شده اند در رابط کاربری SecureTower وارد می‌شوند. این قابلیت مخصوصاً برای شرکت‌های بزرگ با تعداد کارمندان بالا بسیار اهمیت دارد زیرا کار دفتر امنیت را بسیار کاهش می‌دهد.

نیازمندی‌های فنی و سخت افزاری:

CPU: پنتیوم 2 گیگاهرتز به بالا

آداپتور شبکه: 100 Mbit/1 Gbit

RAM: حداقل 2 گیگابایت (به علاوه‌ی 0.5 گیگابایت به ازای هر 100 کلاینت تحت کنترل)

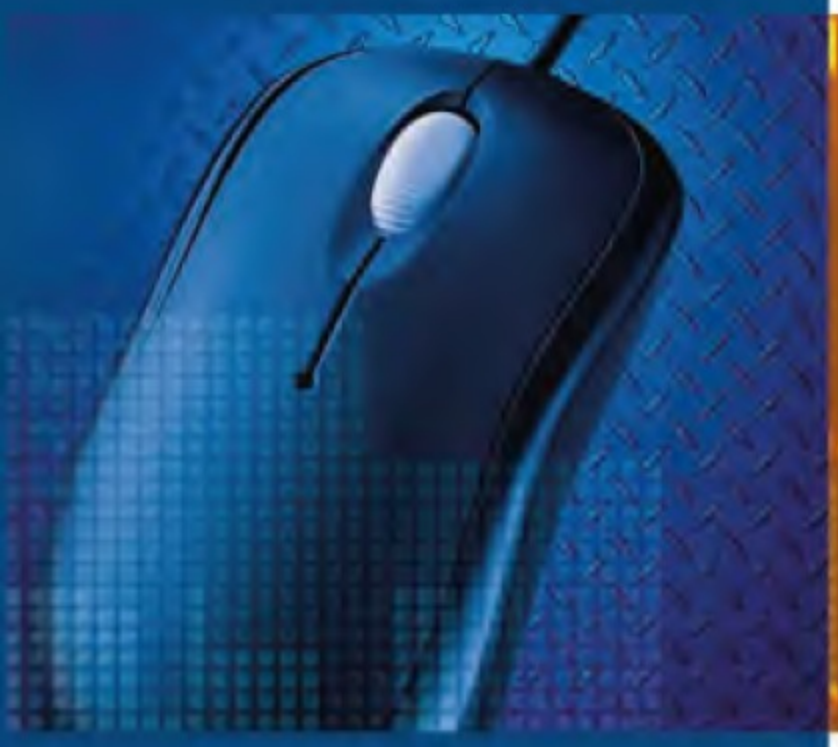
HDD: تا 110 مگابایت فضای آزاد برای فایل‌های برنامه ای و حداقل 30 فضای ترافیک کنترل شده برای فایل‌های اندیس جست و جو، 300 مگابایت برای برنامه‌های کلاینت

Microsoft .Net Framework: 4.0

سیستم عامل برای عناصر سرور: Microsoft Windows Server2003 / Server2008 x86 x64

سیستم عامل برای عناصر کلاینت: Microsoft Windows XP / Vista/ 7 / Server2003 Server2008 / x86 x64

پایگاه داده پشتیبانی شده: اوراکل، Microsoft SQL Server, SQLite و Postgre SQL



چرا SecureTower؟

کنترل جامع و کامل روی نشت داده‌های شخصی و محرمانه

تمام مکالمات کنترل می‌شوند، برنامه‌های پیام رسان مانند اسکایپ، ایمیل‌های برونسو و درونسو و فایل‌های پیوست مربوط به آن‌ها، سرور ایمیل MS Exchange، و داده‌های منتقل شده به درایورهای جداشدنی، سی‌دی/ دی‌وی‌دی و پرینترها. همچنین محتوای اسناد و پایگاه داده‌های حساس که حاوی اطلاعات شخصی حساسی می‌باشند نیز تحت کنترل قرار خواهند گرفت.

SecureTower یک سیستم چندین جزئی است و به راحتی مقیاس پذیر است

این سیستم حاوی عامل‌های سرور متعددی است که هرکدام وظایف گوناگونی را انجام می‌دهند و شامل یک ابزار منحصر به فرد برای ردگیری تمام داده‌های منتقل شده، صرف نظر از سایز و توپولوژی شبکه می‌باشد. این محصول هم در شبکه‌های کوچک و هم در شبکه‌های بزرگ به یک اندازه موثر عمل می‌کند. حتی اگر شبکه‌ی شما دارای یک ساختار چند سطحی با کلاینت‌های بسیار زیادی باشد، SecureTower شما را قادر می‌سازد تا همه چیز را تحت کنترل کامل خود داشته باشید. این سیستم برای برطرف کردن هر گونه نیازی در هر شبکه ای، بسیار مقیاس پذیر می‌باشد.

نصب متمرکز تمام عوامل سیستم و کار در یک کنسول کاربری واحد

با در نظر داشتن ماموریت یک سیستم DLP و پیچیدگی‌های خاص آن، یک محصول مناسب باید گزینه‌های نصب انعطاف پذیری داشته و بتواند سیستم را برای نیازهای خاص یک سازمان شخصی سازی کند. در دیگر موارد این امر به استفاده از ابزارهای پیچیده‌ی متعددی منجر می‌شود که کار با محصول را به یک چالش تبدیل می‌کند. بعد از نصب SecureTower، شما کارآیی آن را حس خواهید کرد. تمام عوامل در یک کنسول واحد جای گرفته اند و همیشه به تمام چیزهایی که نیاز دارید دسترسی دارید.

قابلیت نصب آسان و یکپارچه شدن با شبکه‌ی موجود

برای نصب این محصول هیچ تجربه‌ی خاصی مورد نیاز نیست. اگر توانسته باشید هر نرم افزار دیگری را در محیط ویندوز نصب کرده باشید، پس این محصول را هم به راحتی می‌توانید نصب کنید. بسته به ویژگی‌های شبکه‌ی شما، می‌توانید تمام عوامل این محصول را در یک کامپیوتر نصب کرده یا آن را میان سیستم‌های مختلفی تقسیم کنید. لازم نیست هیچ تغییری در شبکه‌ی خود اعمال کنید. SecureTower می‌تواند با هر چیزی که می‌بیند به خوبی کار کند.

رابط کاربرپسند

با توجه به اطلاعاتی که هم اکنون در مورد DLP دارید، ممکن است فکر کنید کار کردن با آن تا حدی مشکل و پیچیده است که سازمان شما نیاز دارد فردی متخصص را استخدام کرده و یا هزینه های زیادی را صرف آموزش کارمندان کنونی خود کند تا کار با این سیستم‌ها را فرا گیرند. ولی لازم است که یک بار دیگر در این مورد فکر کنید. چه می‌شود اگر یک سیستم جلوگیری از نشت داده‌ها مانند یکی نرم افزار عادی ساده باشد؟ SecureTower دقیقا همان محصول است. این نرم افزار بسیار ساده بوده و هرکسی که بتواند با سیستم عامل ویندوز کار کرده و با الزامات امنیتی شرکت آشنا باشد، می‌تواند با SecureTower هم به خوبی کار کند. لازم به ذکر است که سادگی به منزله‌ی ضعف برای ما نیست. این سیستم بسیار قابل شخصی سازی بوده و گزینه‌های کنترلی زیادی را فراهم می‌آورد.

بهبود کارآمدی خدمات امنیتی

SecureTower هزینه و زمان را در بررسی‌ها و تحقیقات مربوط به رویدادهای امنیتی به حداقل می‌رساند زیرا درصد شناسایی‌های اشتباه را کاهش داده و از این رو کارآیی عملکرد دپارتمان امنیتی را بالا می‌برد.

درباره ما

Falcongaze یک شرکت توسعه دهنده‌ی محصولات امنیت داده با عملکرد بالا، پیچیده و در کلاس جهانی می‌باشد. این شرکت راهکارهایی ترکیبی برای کنترل پایستار روی نشت داده‌ها و افشای ناخواسته‌ی اطلاعات سازمانی ارائه می‌دهد که برای نظارت فعالیت کارمندان در شبکه‌ی سازمان طراحی شده است.

محصولاتی که ما تهیه می‌کنیم راهکارهایی معمولی نیستند، بلکه سیستم‌هایی چندعاملی هستند که در شبکه‌های سازمان یکپارچه می‌شوند. تجربه و عملکرد فوق‌العاده‌ی ما در حوزه امنیت اطلاعات در جهت توسعه‌ی تمام محصولات ما پیاده‌سازی شده‌اند.

اصول اساسی ما شامل رویکردی فردی و حداکثر رضایت مشتری است که به محصولاتی شخصی سازی شده برای هر مشتری منجر می‌شود. ما به کاربران نرم افزارهای Falcongaze خدماتی اضافی ارائه می‌دهیم تا تضمین کنیم که عملکرد تمام محصولات ما قابل اطمینان و اعتماد است. مشتریان ما می‌توانند مطمئن باشند که از راهکارهایی استفاده می‌کنند که با تمام نیازهای روز دنیا سازگار بوده و حفاظت حداکثری از داده‌ها را در مقابل تهدیدات داخلی مهیا می‌کند.

ما تمام مشتریان خود را ارج نهاده و آماده ایم تا راهکارهایی ارائه دهیم که به صورت فردی تمام نیازهای مشتریان را از شرکت‌های با سایز کوچک و متوسط گرفته تا سازمان‌های بزرگ را پاسخ دهیم. مشتریان ما طیف وسیعی را شامل می‌شوند، از شرکت‌های کوچکتر با سایز شبکه‌ی متوسط گرفته تا سازمان‌های بزرگ که شبکه‌هایی با توپولوژی بسیار پیچیده دارند.

اولویت کسب و کاری ما در حال حاضر به حداقل رسانی تهدیدات مربوط به نشت داده‌ها در صنایع مختلف و همچنین کنترل استفاده‌ی مناسب از ساعت‌های کاری می‌باشد. از این رو ما همواره در حال گسترش دادن و متنوع ساختن ابزارهای با فناوری بالای خود هستیم تا اطمینان حاصل کنیم که داده‌های مشتریان ما امن خواهند بود.

ارتباط امن
Ertebate Amn

ارتباط امن

تهران – خیابان ولیعصر – نرسیده به سه راه توانیر

برج طلوع – طبقه ۶ – واحد ۶۰۱

تـلفن: ۰۲۱۸۸۷۴۷۳۷۹

فاکس: ۰۲۱۸۸۵۳۲۹۳۲

بخش پشتیبانی فنی:
support@ertebateamn.com

بخش فروش و نمایندگی:
www.ertebateamn.com
sales@ertebateamn.com

سایر بخش ها:
عمومی: info@ertebateamn.com

Going Global with Security
falcongaze™