

ZECURION DLP

جامع‌ترین راهکار جلوگیری از نشت داده





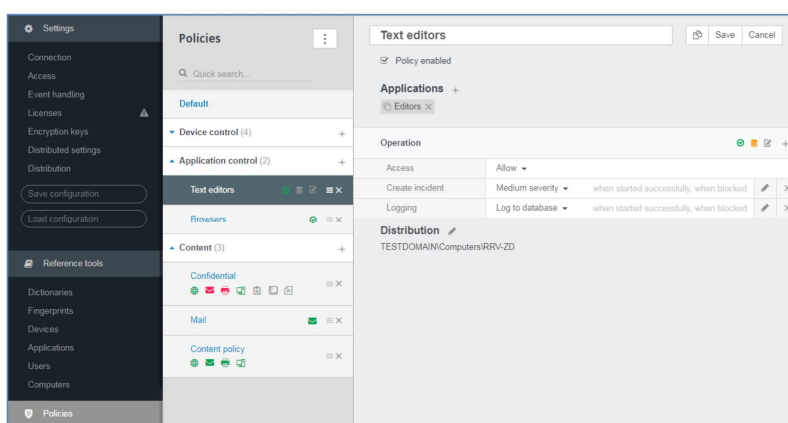
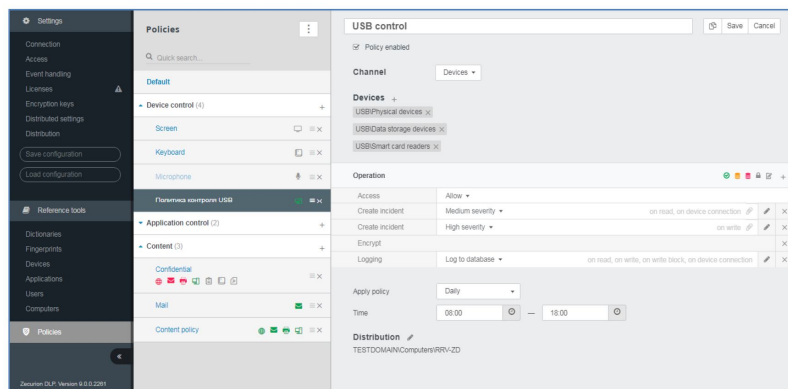
- شناسایی و جلوگیری از نشت اطلاعات حساس سازمان
- پشتیبانی از کانالهای نشت اطلاعات شامل ایمیل، اینترنت، فایل و چاپگر
- کنترل دسترسی انعطاف پذیر و دانه ای برای دستگاه های جانبی
- تجزیه و تحلیل رفتار کارکنان و مطابقت آن با رفتار سازمانی
- ضبط و ذخیره تمامی فعالیتهای کاربران
- گزارش گیری و لاگ تمامی اتفاقات جهت پیگیری قانونی
- بایگانی کپی های سایه
- رمزگذاری فایل های حساس
- یکپارچگی با اکتیو دایرکتوری

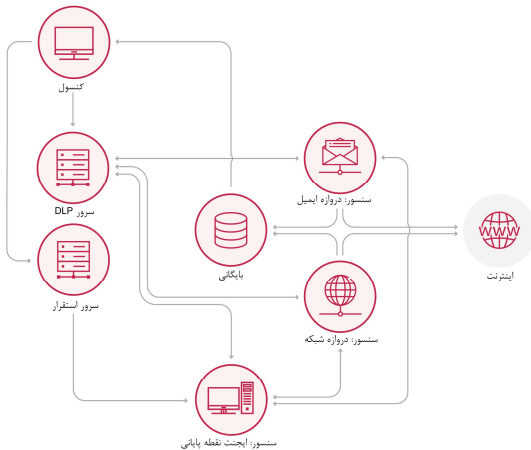
معرفی:

داده ها، شریان اصلی یک کسب و کار است. مالکیت معنوی، داده های مالی، اطلاعات استراتژیک و اطلاعات شخصی حساس در مورد مشتریان و کارمندان، با ارزش ترین دارایی شرکت محسوب می شود. باید توجه داشت که این داده ها همواره در معرض خطر هستند. صرف نظر از اندازه و نوع فعالیت، این شرکت ها روزانه داده های خود را از دست می دهند. این امر ممکن است ناشی از سرقت عمدی یا غیر عمدی توسط کارمندان و یا حمله خارجی صورت گیرد. هدف از پیشگیری از نشت داده ها - یا DLP - ارائه یک راه حل برای محافظت از مالکیت معنوی، اسرار تجاری و سایر داده های حساس است. این امر به شما کمک می کند مقرراتی نظیر HIPAA، PCI DSS و GDPR را کسب کرده و همچنین ابزار لازم را برای جلوگیری از کلاهبرداری داخلی و انجام ممیزی های داخلی و تحقیقات پزشکی قانونی به شما ارائه می دهد.

ویژگیها و مزایا

- ضبط میکروفون
- ضبط تصویر و صفحه کلید
- کنترل برنامه
- کنترل جامع کانال های نشت داده ها
- گزارش های قدرتمند
- تجزیه و تحلیل رفتار کاربر
- کنترل دسترسی انعطاف پذیر و دانه ای برای دستگاه های جانبی
- تلفیق با اکتیو دایرکتوری
- گزارش جامع از تهدیدات و عملکرد کاربران
- تکنیک های پیشرفته تشخیص محتوا
- کنترل ترافیک به صورت فعال یا آینه ای
- اسکن کلیه مکانهای ممکن برای ذخیره داده
- اسکن ایمیل ها و حذف اطلاعات محرمانه از داخل آن





مزایای Zecurion DLP

داده های شما بسیار مهم است و لذا بهترین محافظت را می طلبد. به همین دلیل است که باید Zecurion DLP را انتخاب کنید. Zecurion از سال 2014 در Gartner Enterprise DLP Magic Quadrant رتبه بندی شده است. Zecurion همچنین به عنوان 7 فروشنده برتر در IDC توسط سال 2018 معرفی شد و توسط Forrester در گزارش 2019 DLP Now Tech معرفی شد. Zecurion DLP یک راه حل مقرون به صرفه، کارآمد و جامع است. این محصول، به سرعت با زیرساخت های سازمانی یکپارچه می شود. و استقرار آن به طور متوسط چهار برابر سریعتر از سایر محصولات DLP انجام می پذیرد.

پس از استقرار، زکوریون همه وقایع، پرونده ها و اسناد را بایگانی کرده و رفتار کاربران را به منظور شناسایی فعال تهدیدها تجزیه و تحلیل می کند. Zecurion DLP همچنین باعث کاهش حجم کار تیم امنیتی شده و مدیریت روزانه را با گزارش های تعاملی، نمودارها و گرافهایی که ارزیابی لحظه ای از وضعیت محافظت از داده های شما ارائه می دهند، ساده می کند.

Zecurion DLP در حال حاضر در سراسر جهان در سازمان هایی با بیش از 100000 کاربر در حال استفاده است. از میان مشتریان Zecurion، به کمک شواهد جمع آوری شده برای دادخواست علیه خودی های مخرب، تاکنون بیش از 40 دادخواست برنده شده است.

گزینه های استقرار

هر محیط سازمانی ترکیبی منحصر به فرد از بخش های شبکه، انواع نقاط پایانی، سیستم عامل ها، پلتفرم ها و برنامه های مختلف است. سازمانها باید با حداقل تأثیر بر عملکرد و بهره وری بتوانند از داده ها در کل اکوسیستم محافظت کنند. در عین حال، دید جامع و جلوگیری از نشت داده ها، به توانایی نظارت و تحلیل هر فعالیتی متکی است. Zecurion طیف متنوعی از گزینه های استقرار را برای اطمینان از نظارت و محافظت از اطلاعات شما بدون توجه به آنچه در زیرساخت شبکه شما وجود دارد فراهم می کند.

ساختار Zecurion DLP

سنسورها: رهگیری کانال های انتقال داده، جمع آوری داده های رهگیری شده، اجرای سیاست های DLP بایگانی: کلیه داده های رهگیری شده را ذخیره می کند، پاسخ و تحقیقات در مورد حادثه را امکان پذیر می کند، تجزیه و تحلیل گذشته نگر یعنی سیاست جدید را برای داده های گذشته اعمال می کند (MS SQL یا PostgreSQL)

سرور DLP: تنظیمات و خط مشی را ذخیره می کند، آنها را به حسگرها سوق می دهد، حسگرها را مانیتور می کند
استقرار سرور: سنسورها و عوامل انتهایی (Endpoint Agent) را مستقر می کند
کنسول: مدیریت انعطاف پذیر مبتنی بر وب سیاست ها و گزارش ها

DEPLOYMENT OPTION	CONTROLLED CHANNELS	ACTION
SPAN port mirroring	SMTP, IMAP, POP3, HTTP, FTP	Detect
ICAP server	HTTP/HTTPS	Detect and block
TMG server	HTTP/HTTPS	Detect and block
Traffic Control Agent (endpoint)	SMTP, IMAP, POP3, FTP, messengers	Detect
Zecurion SWG	HTTP/HTTPS	Detect and block
	FTP	Detect
MS Exchange plugin	email (including internal)	Detect and block
SMTP proxy	Email (SMTP)	Detect and block
SMTP journal	email	Detect
Technical mailbox (POP3, IMAP, Exchange HTTPS)		
Device Control Agent (endpoint)	USB	Detect and block
	Printing	Detect and block
	Removable drives	Detect and block
	CD/DVD	Detect
	RDP disks, clipboard	Detect / Record
	Screen	Detect / Record
	Clipboard	Detect / Record
	Keyboard	Detect / Record
	Microphone	Detect / Record
Discovery Agent (endpoint)	Local drive scan	Detect
	Local drive real-time	Detect
Discovery Server	Network Shared folder	Detect
	MS SharePoint	Detect
	MS Exchange	Detect
	Any Database	Detect

جمع آوری و فهرست بندی می شود تا اطمینان حاصل شود که تمام مکاتبات متعلق به یک کاربر خاص است.

ویژگیهای ممتاز

Zecurion DLP همه قابلیت های مورد نیاز برای کنترل کانال های نشت داده، نظارت بر پردازش داده توسط کارمندان و همچنین جلوگیری از نقض داده، ارائه می دهد.

کنترل جامع کانال های نشت داده ها

کلیه کانالهای احتمالی نشت داده ممکن را کنترل می کند تا خطر نقض داده ها به حداقل رسیده و از مطابقت با الزامات نظارتی اطمینان حاصل شود.

سیاست ها و قوانین انعطاف پذیر

پیگر بندی خط مشی را برای چندین یا همه کانال های انتقال داده تنظیم می کند و با استفاده از انواع تکنیک های تشخیص محتوا و شرایط داده، تا امکان هرگونه سناریوی نقض پیش بینی و جلوگیری شود.

استخراج محتوای فایل

با تشخیص خودکار فایل برای بیش از 500 قالب فایل بر اساس ساختار داخلی (و نه پسوند پرونده) و همچنین امکان تشخیص پرونده های رمزگذاری شده و باز کردن پرونده های بایگانی شده (از جمله بایگانی های تو در تو) هیچ داده ای بدون تجزیه و تحلیل از شبکه خارج نمی شود.

مدیریت متمرکز

Zecurion DLP از یک کنسول تحت وب برای مدیریت همه مازول ها بهره می برد. همچنین یک داشبورد قابل سفارشی سازی برای مدیریت از راه دور متمرکز فراهم می کند که بسیار کاربر پسند است.

بایگانی پرونده ها و پیام ها

تمام داده های رهگیری شده (پرونده ها، پیام ها، حوادث، رویدادها و موارد دیگر) در یک پایگاه داده ذخیره می شوند، بنابراین شما تمام امکانات لازم برای تهیه گزارش های دقیق، انجام تحقیقات پزشکی قانونی جامع و جمع آوری مدارک برای اقدامات قانونی را در اختیار خواهید داشت.

کاتالوگ هوشمند کارمندان

اطلاعات مربوط به تمامی آدرس های ایمیل، شبکه های اجتماعی و حساب های پیام رسان فوری مربوط به کارمندان،

تجزیه و تحلیل رفتار کاربر

پروفایل های رفتاری برای همه کاربران محاسبه می شود تا بتوان فعالیت غیر عادی را تشخیص داد. با تشخیص تهدید فعال، به تیم امنیتی هشدار داده می شود تا از نقض اولیه داده ها جلوگیری شود.

نقشه اتصال کاربر

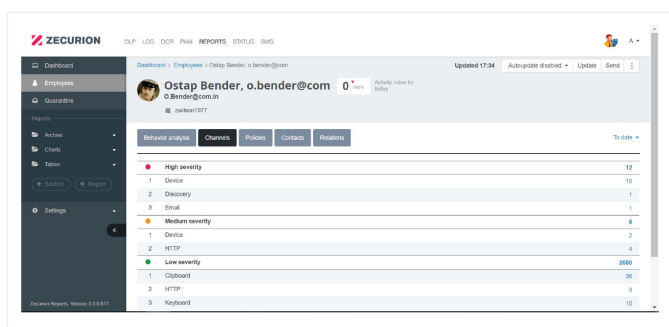
Zecurion DLP برای شناسایی اتصالات پنهان، نمودار قابل کلیک از اتصالات کاربر و کانالهای ارتباطی ایجاد می کند و به شما امکان می دهد ارتباطات مشکوکی را که ممکن است تقلب داخلی یا نقض اطلاعات را نشان دهد، تجزیه و تحلیل کنید.

گزارش های قدرتمند

بیش از 20 گزارش از پیش تعیین شده و گزینه های سفارشی سازی، ابزاری قدرتمند برای ممیزی امنیتی و تحقیقات فراهم می کند. شما می توانید گزارش ها را به راحتی تولید و تجزیه و تحلیل کنید و به سرعت در چند کلیک به یک حادثه خاص بپردازید.

لاگ رویدادها

به طور خودکار تمام رویدادهای داخلی و اقدامات مدیر شبکه برای نگهداری آسان و ردیابی سریع هر مسئله ای که پیش می آید، لاگ می شود.



یکپارچگی با اکتیو دایرکتوری

کاربران، گروه ها و نام کامپیوترها از Active Directory همگام سازی می شود تا یکپارچه سازی بهتر با زیرساخت های IT شما فراهم شود و Zecurion DLP را قادر سازد تا کاربران را با نام کاربر در حوادث و گزارش ها شناسایی کند.

API REST

اکثر وظایف مدیریت و نظارت از طریق درخواست های REST API HTTP برای فعال کردن اتوماسیون امنیتی و ادغام با سایر ابزارها و سیستم عامل ها در زیرساخت IT شما در دسترس هستند.

ویژگیهای پیشرفته**ضبط میکروفون**

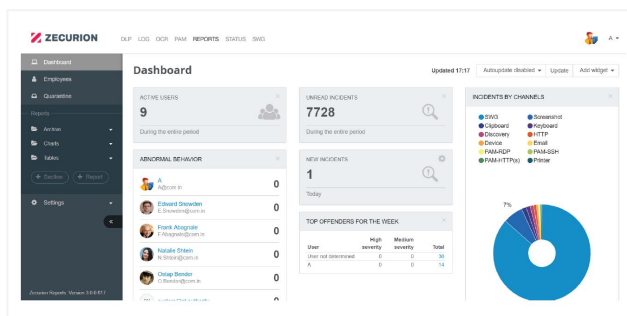
با ضبط از میکروفون هر رایانه در هر زمان ، هر رایانه یا لپ تاپ را به یک سیستم نظارت صوتی تبدیل کنید.

ضبط تصویر و صفحه کلید

شما می توانید کلیه کلیدهای مربوط به کاربران یا گروههای تعیین شده را ضبط کرده و تصاویر را از هر رایانه ای در فواصل زمانی مشخص ذخیره کنید ، بنابراین همیشه می دانید کارمندانان چه کاری انجام می دهند و می توانید سیاست های امنیتی داخلی و دستیابی به داده ها را برای شناسایی و جلوگیری از نقض احتمالی داده ها به کار گیرید.

کنترل برنامه

خطر استفاده کارمندان با استفاده از برنامه های بالقوه خطرناک (TOR و تورنت ، ناشناس کننده ها ، بازی ها) را از بین ببرید. همچنین می توانید با ایجاد لیست سفید یا لیست سیاه برنامه های کاربردی ، برای کاربران یا گروه های تعیین شده ، برنامه های مجاز برای استفاده را مشخص کنید.

**تکنیک های تشخیص محتوا**

Zecurion DLP از انواع تکنیک های تشخیص محتوا برای پیشگیری جامع از نشت دست داده استفاده می کند. صرف نظر از اینکه داده ها به عمد دزدیده شده یا به خطر افتاده ، یا سهواً به اشتراک گذاشته شده یا در معرض دید عموم قرار گرفته ، یکی از این تکنیک های تشخیص محتوای زیر آن را نشانه گذاری می کند:

کلمات کلیدی و فرهنگ لغت

این تکنیک به دنبال تطابق دقیق کلمات تعیین شده است. یک مدیر IT یا مأمور امنیت می تواند یک فرهنگ لغت برای هر موضوع یا دسته ای مانند اسناد مراقبت های بهداشتی ، اسناد مالی ، جستجوی شغل و غیره ایجاد کند و آن را با کلماتی که باید پرچم گذاری شود ، جمع کند. بیش از 30 فرهنگ لغت از پیش تعریف شده به طور پیش فرض در سیستم وجود دارد.

قالب ها و عبارات منظم

برخی از داده های حساس از یک ساختار یا قالب از پیش تعریف شده پیروی می کنند که می تواند برای شناسایی و کشف آن استفاده شود. شماره کارت های اعتباری ، شماره های تأمین اجتماعی ، حساب های IBAN ، آدرس های اینترنتی ، آدرس ایمیل و سایر داده های مشابه را می توان با استفاده از قالب ها و عبارات منظم شناسایی کرد.

اثر انگشت دیجیتال

Zecurion DLP با جمع آوری تعدادی از اسناد از یک نوع یا دسته خاص و ارائه آنها به عنوان ورودی ، اثر انگشت دیجیتالی ایجاد می کند که می تواند اسناد دقیق یا قسمت هایی از آنها را تشخیص دهد. پس از ایجاد اثر انگشت دیجیتال ، Zecurion DLP می تواند هر مدرکی را از مجموعه یا هر قسمت یا ترکیبی از قسمتهای مجموعه اسناد مشخص کند. اسناد جدید را می توان به مجموعه اضافه کرد و Zecurion DLP به طور خودکار اثر انگشت های دیجیتال را به روز می کند.

یادگیری ماشین

روش دیگر شبیه به اثر انگشت دیجیتال استفاده از یادگیری ماشین است. راه اندازی اولیه مشابه است: تهیه مجموعه ای از پرونده ها برای تجزیه و تحلیل Zecurion DLP. هر چند که در اثر انگشت های دیجیتالی ، تطابق دقیق محتوا را تشخیص دهند ، می توان از یادگیری ماشین برای تشخیص اسنادی که مشابه

جلوگیری از استفاده مشروع از دستگاه ها ، دسترسی و محافظت از داده های خود را محدود کنید:

کنترل دسترسی انعطاف پذیر و دانه ای برای دستگاه های

جانبی

شما می توانید فقط دستگاه های صادر شده یا تأیید شده شرکت را فعال کنید یا فقط دستگاه هایی را که برای تجارت ضروری به نظر می رسند با کنترل خط مشی فعال کنید. می توان دسترسی را براساس نوع ، کلاس ، فروشنده ، مدل یا شماره سریال دستگاه مجاز یا غیرمجاز کرد. خط مشی ها را می توان برای گروه ها یا افراد اعمال کرد و بسته به اینکه آیا نقطه انتهایی به شبکه وصل شده باشد ، از راه دور از طریق VPN متصل شده یا قطع شده است ، می توان خط مشی جداگانه ای اعمال کرد.

کاتالوگ دستگاه های شرکت

توضیحات دستگاه در یک کاتالوگ در سطح شرکت ذخیره می شود ، و می توانید خط مشی ها را بر اساس توضیحات موجود ایجاد کنید.

کپی سایه

کنترل دستگاه زکوریون می تواند یک نسخه از هر پرونده ای را که برای یک دستگاه خارجی نوشته شده یا چاپ شده ذخیره کند و این امکان را برای شما فراهم می کند تا فعالیت ها را حتی در صورت عدم نقض خط مشی امنیتی نظارت کنید و ابزاری برای انجام تحلیل های گذشته نگر ، حسابرسی ها ، و تحقیقات پزشکی قانونی در اخطار شما قرار می دهد.

خط مشی های مبتنی بر محتوا با استفاده از الگوریتم های

تحلیل محتوا

شما می توانید ضمن اینکه امکان استفاده عمومی از چاپگرها و دستگاههای ذخیره سازی قابل حمل را فراهم می کنید امکان ذخیره یا چاپ فایل هایی که حاوی داده های حساس یا محرمانه هستند را محدود کنید. خط مشی مبتنی بر الگوریتم های تحلیل محتوا می تواند به صورت فعالانه داده های حساس را شناسایی و محافظت کند.

تجزیه و تحلیل محتوای پیشگیرانه

تجزیه و تحلیل محتوای پیشگیرانه زکوریون که ثبت اختراع هم شده است ، تضمین می کند که داده های محرمانه و حساس هرگز در وهله اول به دستگاه های خارجی ارسال نمی شوند.

مجموعه ارائه شده است بر اساس کلمات کلیدی و یا شاخص های معنایی استفاده کرد.

الگوهای تصویر

الگوهای تصویر برای تشخیص مواردی مانند امضا ، تمبر ، نامه یا اسناد با ساختار مشخص مانند گذرنامه یا گواهینامه رانندگی مؤثر است. این روش همچنین شبیه به اثر انگشت های دیجیتال است ، اما به جای شناسایی متن خاص ، الگوهای تصویر را تشخیص می دهد. مانند اثر انگشت های دیجیتال و یادگیری ماشین ، راه اندازی اولیه نیاز به تهیه مجموعه ای از پرونده هایی دارد که Zecurion DLP می تواند آنالیز کند تا تشخیص لازم را برای شناسایی بعدی آن فراهم کند.

OCR (تشخیص نوری کاراکتر)

این تکنیک برای شناسایی داده های حساس یا محرمانه که به نوعی در تلاش برای دور زدن سایر روش های تشخیص اسکن شده یا از آن عکس گرفته شده ، بسیار ارزشمند است. Zecurion DLP از موتورهای تشخیص نوری کاراکتر برای استخراج متن از اسناد اسکن شده استفاده می کند. Zecurion DLP از محصولات Google Tesseract و ABBYY FineReader می کند. بهره می گیرد تا بتواند متن را از یک تصویر استخراج و شناسایی کند.

کنترل دستگاه

دستگاه هایی مانند هارد دیسک های خارجی یا درایوهای انگشت شست USB می توانند خطرات قابل توجهی را در هنگام از بین رفتن اطلاعات ایجاد کنند. این فناوری تا حدی تکامل یافته است که حتی کارتهای microSD نیز می توانند 1 ترابایت داده را ذخیره کنند. یک کارمند ناراضی می تواند گیبابایت یا ترابایت داده را در جیب خود دزدی کند. اطلاعات مربوط به دستگاه های قابل حمل حتی برای کارمندان وفادار نیز خطری ایجاد می کند ، زیرا دستگاه ها به راحتی از بین می روند یا سرقت می شوند.

در بسیاری موارد ، ذخیره سازی قابل حمل و سایر دستگاه ها امری ضروری است و لذا مسدود کردن تمام درایوهای USB یا دسترسی به پورت های USB بسیار سخت است و می تواند بر بهره وری تأثیر منفی بگذارد. Zecurion DLP کنترل دستگاه گرانولار زیر را در اختیاران می گذارد ، بنابراین می توانید بدون

کنترل ترافیک

اینترنت ستون فقرات تجارت امروز است - اما همچنین داده ها را در معرض خطر قابل توجهی قرار می دهد. اگر کارمندان یا مشتریان بتوانند به منابع شرکت متصل شده و به داده های حساس یا محرمانه دسترسی پیدا کنند ، ممکن است مهاجمان نیز بتوانند آن داده ها را به خطر بیندازند ، افشا کنند یا سرقت کنند. از آنجا که کاربران از طریق ایمیل یا سیستم های پیام رسانی با یکدیگر ارتباط برقرار می کنند ، ممکن است سهواً داده های حساس را فاش کنند. برخی از کاربران ممکن است برای ذخیره سازی و انتقال داده ها از سیستم های ذخیره سازی غیر مجاز ابری استفاده کنند و داده ها را در معرض خطر قرار دهند. برای سازمانها نظارت بر ترافیک و کنترل جریان داده ها از طریق کانالهای اینترنتی بسیار مهم است تا خطر از دست رفتن داده ها چه به صورت عمدی و چه غیر عمدی را به حداقل برساند. کنترل ترافیک زکوریون، طیف وسیعی از ویژگی ها و قابلیت ها را برای کنترل و دید لازم به شما ارائه می دهد:

کنترل کامل کانالهای اینترنتی

Zecurion DLP به شما امکان کنترل کامل داده های خروجی از طریق کانال های متصل به اینترنت ، از جمله ایمیل ، ایمیل مبتنی بر وب ، شبکه های اجتماعی ، سیستم های پیام رسانی و موارد دیگر را می دهد. می توانید ارتباطات شبکه را در اکثر پروتکل ها رهگیری و تجزیه و تحلیل کنید.

تحلیل ترافیک رمزگذاری شده

ترافیک رمزگذاری شده ممکن است باعث شود داده های حساس شناسایی نشده و از شبکه خارج شود. کنترل ترافیک Zecurion اتصالات SSL را با استفاده از یک روش man-in-the-middle (MitM) رمزگشایی می کند و کنترل کامل داده های خروجی حتی هنگام استفاده از HTTPS را کنترل می کند.

قرنطینه ایمیل

Zecurion Traffic Control را می توان طوری پیکربندی کرد که ایمیل های مشکوک را برای بازرسی دستی جدا سازی کند. فعال کردن بازرسی دستی پیامها باعث کاهش خطا شده و با شناسایی پیامهایی که نیاز به اقدام بیشتر دارند ، می توانید دقت بهتری داشته باشید.

پرونده ها تجزیه و تحلیل می شوند و کپی پرونده های حساس مسدود می شود. محصولات رقیب ابتدا فایل را می نویسند (کپی) سپس تجزیه و تحلیل را انجام می دهند و در صورت نقض خط مشی ، محتوا را حذف می کنند.

رمزگذاری

قابلیت رمزگذاری کنترل دستگاه زکوریون انعطاف پذیری و محافظت را فراهم می کند. شما می توانید براساس محتوا و خط مشی های امنیتی ، پرونده هایی که برای دستگاه های خارجی (هارد اکسترنال، USB و ...) نوشته شده است را رمزگذاری کنید. شما می توانید رمزگذاری را پیکربندی کنید تا محتویات رمزگذاری شده فقط از نقاط انتهایی متصل به شبکه شرکتی توسط کاربران مجاز قابل دسترسی باشند.

استقرار و مدیریت متمرکز

کنترل دستگاه زکوریون، چارچوبی را برای استقرار و مدیریت متمرکز DLP شما فراهم می کند. ایجنت (Agent) دستگاههای انتهایی می توانند از طریق سرور مستقر یا با استفاده از Active Directory Group Policy مستقر شوند. مدیر شبکه به کمک یک کنسول وب می تواند برای تشخیص به هر نقطه پایانی متصل شود و توانایی مدیریت صدها هزار نقطه انتهایی را از راه دور دارد.

درخواست دسترسی به دستگاه

برای به حداقل رساندن تأثیر احتمالی بر بهره وری ، یک کارمند از راه دور می تواند دسترسی به استفاده از یک دستگاه خاص را درخواست کند. یک سرپرست می تواند درخواست را بصورت یک بار اعطا کند ، یا سیاستی را ایجاد کند که به طور دائم امکان استفاده از دستگاه را فراهم کند.

محافظت در برابر دستکاری با عامل انتهایی

برای اطمینان از صحت محافظت از داده های خود ، زکوریون در صورت بروز هرگونه دستکاری و یا تلاش برای حذف یا تغییر تنظیمات در نقطه انتهایی ، به مدیر هشدار می دهد.

دستگاه های مورد پشتیبانی

•Devices: -USB -Network (WiFi, Bluetooth) LPT/COM Port -FDD -DVD/CD -PCMCIA -IrDA -Modem -Printer -HDD -Other removable drives -Tape drives -FireWire
•Screen • Clipboard • Keyboard • Microphone • RDP • Disk • Smart card • Port

پروتکلها و کانالهای کنترل شده



Email

SMTP
IMAP
POP3
MAPI



Web

HTTP(S)
FTP



Messengers

ICQ
MSN
Mail.ru Agent
MS Lync
Skype
Viber
XMPP (Jabber)



Cloud

OneDrive
DropBox
Google Drive
Yandex disk
Mail.ru Files



Social networks

Facebook
VKontakte
Odnoklassniki
LinkedIn
MySpace
Twitter

دو گزینه برای حالت استقرار

کنترل ترافیک Zecurion می تواند به عنوان یک فیلتر فعال عمل کند و یا اینکه فقط می تواند ترافیک آینه را تحلیل کند. فیلتر فعال بر ترافیک نظارت می کند و تبادلات خطرناک را در زمان واقعی مسدود می کند. سازمانها همچنین می توانند از یک رویکرد مرحله ای استفاده کنند بدین صورت که ابتدا از طریق تنظیمات آینه ای شروع می کنند تا امکان کنترل و تنظیم سیاست ها برای حداکثر کارایی را فراهم کنند و سپس به سمت فیلتر فعال سوق داده شوند.

تحلیل ترافیک ایمیل داخلی

کنترل ترافیک به شما امکان می دهد تا داده های محرمانه را درون شبکه خود نظارت و ردیابی کنید. افزونه Microsoft Exchange کنترل پیشرفته ای به شما می دهد و به شما امکان می دهد ترافیک ایمیل داخلی را تجزیه و تحلیل کنید.

دستکاری پیام

شما می توانید با حذف انتخابی اطلاعات حساس یا محرمانه و بدون افت کارایی ، از داده های خود محافظت کنید. به این صورت که صرفا اطلاعات محرمانه از پیام حذف می شود در حالیکه سایر قسمتهای پیام ارسال می شود.

گزینه های متنوع استقرار

یکی از نقاط قوت اصلی کنترل ترافیک زکوریون، تنوع گزینه های استقرار است. گزینه های حالت منفعل مانند آینه سازی پورت SPAN و گزینه های حالت فعال مانند Endpoint Agent ، رله SMTP ، افزونه Microsoft Exchange و موارد دیگر وجود دارد. مهم نیست سازمان شما چه اندازه باشد یا زیرساخت فناوری اطلاعات شما چطور باشد ، کنترل ترافیک Zecurion قابلیت استقرار سریع و ساده را دارد.

اکتشاف

یکی از بزرگترین چالش های پیش روی شرکت ها هنگام امنیت داده و جلوگیری از از بین رفتن داده ها ، دانستن مکان ذخیره داده های حساس در درجه اول و اجرای سیاست هایی برای اطمینان از داده های حساس و محرمانه است که به درستی برچسب خورده و ذخیره می شوند. با حرکت شرکتها به ابر و پذیرای محیط های ترکیبی یا چند صدایی که مراکز داده محلی را به علاوه یک یا چند سیستم عامل ابری خصوصی یا عمومی در بر می گیرد ، فرصت پراکندگی داده ها بصورت نمایی افزایش می یابد. هرچه داده ها بیشتر در قسمت تاریک شبکه شما پخش شود و در مکان هایی ذخیره نشود که نباید باشد ، نقض اطلاعات اجتناب ناپذیرتر می شود. Zecurion DLP Discovery ابزارهایی را که می خواهید برای پیدا کردن پرونده های حساس ذخیره شده به صورت غیرفعالانه فعال کنید به شما می دهد تا قبل از گم شدن یا سرقت داده های خود دست به اقدام بزنید

قوانین تشخیص را به عنوان خط مشی DLP ایجاد کنید

با استفاده از تمام تکنیک های موجود در زمینه کشف محتوا و قوانین زمینه ، می توانید سیاست های کلی DLP ایجاد کنید تا مدیریت را ساده و سراسر کنید.

اسکن مایکروسافت Exchange جهت تشخیص تهدیدهای پیچیده

Zecurion DLP Discovery می تواند به تشخیص سناریوهای که ممکن است کنترل ترافیک را دور بزنند ، کمک کند. اگر کاربر مخرب ایمیلی را با اطلاعات محرمانه ایجاد کرده و آن را در پوشه Drafts ذخیره کند ، آنگاه پیام را از سرویس گیرنده وب آوتلوک بارگیری کرده و آن را حذف می کند ، در واقع پیام "ارسال" نمی شود. اکتشاف اطمینان می دهد که هنوز هم می توانید این فعالیت را شناسایی کنید.

هشدار به کاربران و مدیران امنیتی

Zecurion Discovery هنگام بروز نقض خط مشی می تواند به طور مستقیم هشدارهایی را برای کاربران و سرپرستهای فناوری اطلاعات ارسال کند تا از واکنش سریع نسبت به حادثه اطمینان حاصل شود.

آرامش خاطر با زکوریون

Zecurion DLP همه آنچه را که شما نیاز دارید از یک راه حل پیشگیری از نشت داده انتظار دارید، ارائه می دهد: یک بستر مقرون به صرفه با استقرار کارآمد ، جلوگیری از نقض خط مشی به صورت جامع و انعطاف پذیر، و بایگانی و گزارش دقیق. Zecurion DLP پیشرفته ترین سیستم DLP موجود در جهان است و همه آنچه را که شما برای برای پیشگیری ، کشف و بررسی نقض داده ها نیاز دارید را پوشش می دهد.

درباره:

Zecurion یک شرکت تولید کننده محصولات امنیتی از کشور روسیه است. زکوریون از سال 2014 در Gartner Enterprise DLP Magic Quadrant رتبه بندی شده است. زکوریون همچنین به عنوان 7 فروشنده برتر DLC توسط IDC در سال 2018 معرفی شد و توسط Forrester در گزارش DLP Now 2019 Tech معرفی شد. Zecurion DLP یک راه حل مقرون به صرفه، کارآمد و جامع است.

اسکن کلیه مکانهای ممکن برای ذخیره داده

Zecurion Discovery پوشش کاملی را در کلیه مکانهای ذخیره سازی احتمالی پرونده در سراسر سازمان شما ، از جمله نقاط انتهایی برای ارائه اطمینان از شناسایی تمام داده های ذخیره شده در نقاط انتهایی ارائه می دهد.

پارامترهای اسکن انعطاف پذیر

پیکربندی Discovery را هر طور که دوست دارید انجام دهید و برنامه ای مناسب برای سازمان خود تنظیم کنید. می توانید اسکن های روزانه ، هفتگی یا ماهانه را پیکربندی کنید و واحدهای خاص سازمانی یا نقاط پایانی را برای اسکن تعیین کنید.

کشف زمان واقعی

علاوه بر اسکنهای برنامه ریزی شده ، Zecurion Discovery همچنین می تواند پرونده ها را فوراً تجزیه و تحلیل کند. به هنگام کپی شده یا ذخیره شدن فایلها، زکوریون می تواند فوراً و در زمان واقعی نقض خط مشی را کشف کند.

رایان سامانه آرکا - نماینده انحصاری زکوریون در ایران

تهران، خیابان شهید بهشتی، خیابان پاکستان، کوچه چهارم، پلاک 11، طبقه چهارم، واحد 7
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی: ۱۵۳۱۶۴۵۹۱۸
www.arka.ir | info@arka.ir

