معرفی

Zecurion DLP

arka
رایان سامانه آرکا

ZECURION

www.arka.ir

چرا DLP دیگر یک انتخاب نیست؛ یک ضرورت است

در دنیای امروز که ارزشمندترین دارایی سازمان‌ها «داده» است، هر بیت اطلاعات می‌تواند تفاوت بین موفقیت و شکست را رقم بزند. فناوری Data Loss Prevention (DLP) با رویکردی هوشمند، مانع خروج ناخواسته یا غیرمجاز اطلاعات حیاتی شما می‌شود و شکاف‌های امنیتی را پیش از آنکه به فاجعه‌ای جبران‌ناپذیر تبدیل شوند، مسدود می‌کند.

DLP تنها یک ابزار نظارتی نیست؛ بلکه سامانه‌ای جامع برای شناسایی، طبقه‌بندی، نظارت و کنترل جریان داده‌ها است که با استفاده از الگوریتم‌های پیشرفته، هرگونه فعالیت مشکوک را در لحظه تشخیص می‌دهد. این فناوری، چه داده‌ها در حال استفاده باشند، چه در حال انتقال یا در حالت ذخیره، از آن‌ها محافظت می‌کند.

با پیاده‌سازیDLP، سازمان شما:

- ریسک نشت اطلاعات محرمانه را به حداقل می‌رساند.
- با استانداردهای بین‌المللی امنیت اطلاعات (نظیر ISO 27001 و GDPR) همسو می‌شود.
- تصویر برند و اعتماد مشتریان را در برابر تهدیدات سایبری حفظ می‌کند.
- توانایی تحلیل رفتار کاربران داخلی و شناسایی تهدیدات درون‌سازمانی را پیدا می‌کند.

در زمانی که حملات هدفمند و تهدیدات داخلی هر روز پیچیده‌تر می‌شوند، نبود DLP یعنی باز گذاشتن درهای سازمان به روی مهاجمان. آینده امنیت داده‌های شما به تصمیم امروزتان وابسته است.

Zecurion DLP امنیتی فراتر از مرزها

Zecurion DLP یکی از پیشرفته‌ترین راهکارهای پیشگیری از نشت اطلاعات در جهان است که با بیش از 20 سال تجربه و حضور در بیش از 70 کشور، به عنوان انتخاب برتر بسیاری از سازمان‌های بزرگ شناخته می‌شود.

نسخه جدید Zecurion DLP، نسل جدید راهکارهای پیشگیری از نشت اطلاعات است که با معماری بهینه، هوش مصنوعی پیشرفته و سرعت پردازش بالاتر، امنیت داده‌های سازمان را در سه لایه Data in Use, Data in Motion, Data at Rest تضمین می‌کند. این نسخه با امکاناتی مانند تحلیل رفتار کاربر(UBA) ، شناسایی تهدیدات داخلی و کنترل کامل بر تمام کانال‌های ارتباطی، استانداردی جدید در امنیت اطلاعات ایجاد کرده است.

ZECURION

CERTIFICATE

Authorized Exclusive Distributor

We confirm that

Rayan Samaneh Arka

is trusted to fully manage their business channel/market and provide Zecurion sales program to their partners.

in the following territory:
Iran

Alexey Raevsky
CEO & General manager

Valid until January 1st, 2029

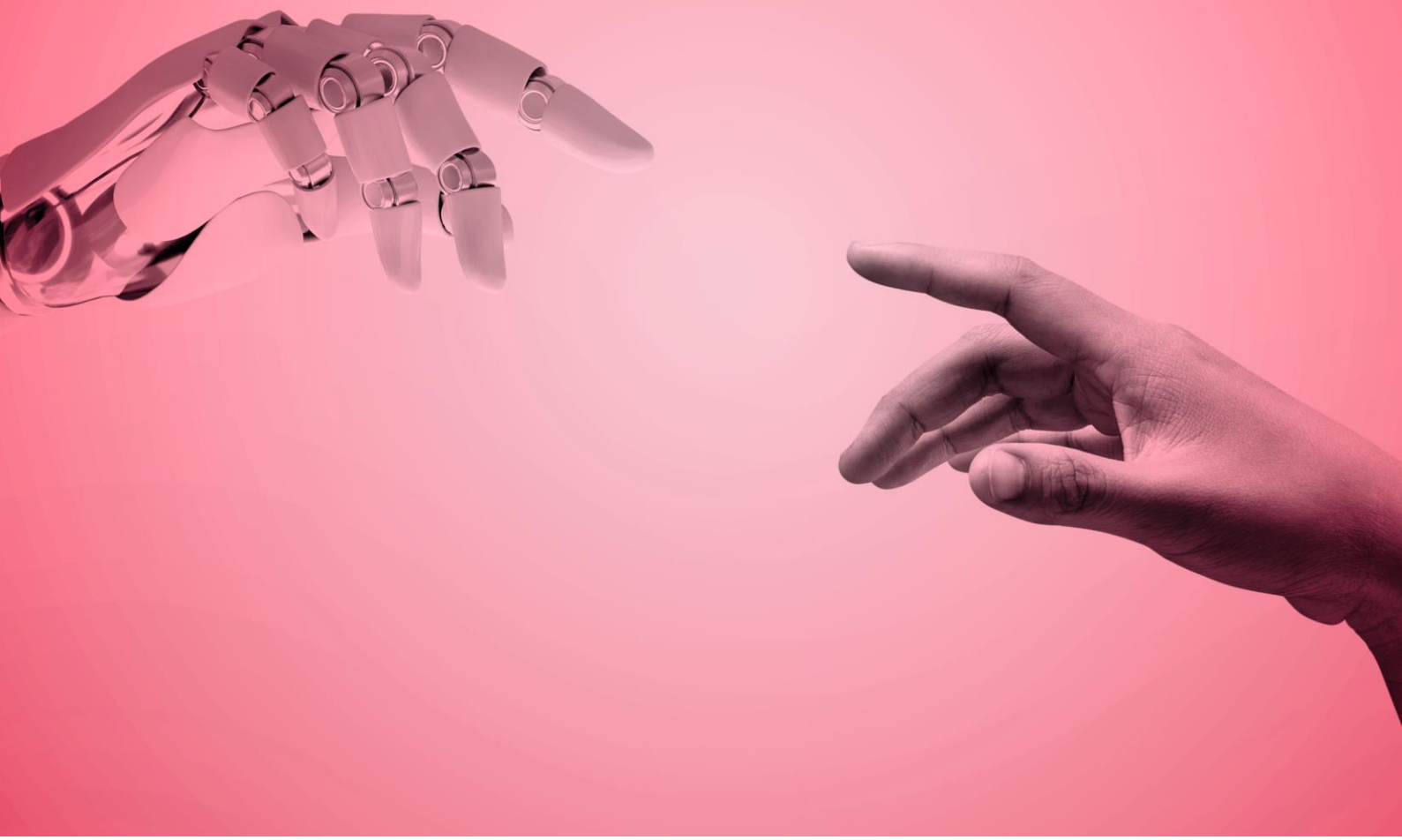
بروشور

Zecurion DLP

arka
رایان سامانه آرکا

ZECURION

www.arka.ir



نسل جدید DLP

ZECURION DLP 13 + AI

آگاهی بیشتر، ریسک کمتر.

Rev 1.6

ZECURION

arka
رایان سامانه آرکا

20 ویژگی کلیدی DLP نسل جدید Zecurion

1
مدیریت کامل کانال‌های نشت داده

مدیریت تمامی کانال‌های بالقوه نشت داده به منظور کاهش ریسک نشت اطلاعات و اطمینان از رعایت مقررات و استانداردها.

2
سیاست‌ها و مقررات تطبیقی

ایجاد یک سیاست واحد برای چندین یا تمامی کانال‌های انتقال داده با بهره‌گیری از روش‌های مختلف شناسایی محتوا.

3
فهرست هوشمند کارکنان

نظارت بر شاخص‌های حیاتی مانند سطح ریسک، بهره‌وری، رویدادها، سیاست‌های فعال‌شده و وضعیت‌های احساسی.

4
کنسول مدیریت یکپارچه

Zecurion DLP رابطی مبتنی بر وب برای تمام ماژول‌ها ارائه می‌دهد که داشبورد قابل تنظیمی دارد و مدیریت متمرکز از راه دور را آسان و کارآمد می‌سازد.

5
ذخیره‌سازی فایل‌ها و پیام‌ها

تمامی داده‌های جمع‌آوری‌شده مانند فایل‌ها، پیام‌ها، رویدادها و رخدادها در یک پایگاه‌داده امن ذخیره می‌شوند. این امکان را فراهم می‌کند تا گزارش‌هایدقیق تهیه کرده، تحقیقات قانونی انجام دهید و مدارک لازم برای فرآیندهای حقوقی را گردآوری کنید.

6
استخراج محتوای فایل

با استفاده از شناسایی خودکار بیش از ۵۰۰ قالب فایل بر اساس ساختار داخلی آن‌ها (و نه فقط پسوند)، این سیستم می‌تواند فایل‌های رمزگذاری‌شده را نیز شناسایی کرده و فایل‌های فشرده (حتی تو در تو) را استخراج کند. بنابراین هیچ داده‌ای بدون تحلیل کامل از شبکه خارج نمی‌شود.

7
پروفایل‌های رفتاری

توسعه پروفایل‌های رفتاری بر اساس الگوهای مشخص (مثلاً کاربران از راه دور، کارکنان بخش‌های خاص و...)، Zecurion DLP نشان می‌دهد که رفتار یک کاربر تا چه حد با الگوهای مشخص‌شده تطابق دارد. همچنین، گردآوری و سازمان‌دهی تمامی آدرس‌های ایمیل، پروفایل‌های شبکه‌های اجتماعی و حساب‌های پیام‌رسانی فوری کارکنان برای اطمینان از قابلیت پیگیری ارتباطات کاربران.

8
تحلیل رفتار کاربر با شناسایی ناهنجاری‌ها

ایجاد پروفایل‌های رفتاری برای تمامی کاربران به‌منظور شناسایی فعالیت‌های غیرعادی مانند: وضعیت کارمند جدید، اولین اتصال از راه دور، افزایش فعالیت، تعامل با افراد ناشناس و... شناسایی تهدیدها به‌صورت پیشگیرانه، تیم امنیتی را هشدار داده و امکان واکنش سریع را فراهم می‌سازد.

9
ثبت وقایع

ثبت خودکار تمامی رویدادهای داخلی و اقدامات مدیر سیستم جهت تسهیل نگهداری و ردیابی سریع مشکلات احتمالی. این کار به ارزیابی ریسک و پیشگیری از رویدادهای امنیتی کمک می‌کند.

10
رابط برنامه‌نویسی REST API

بسیاری از وظایف مدیریتی و نظارتی از طریق درخواست‌های HTTP REST API قابل انجام است که امکان خودکارسازی امنیت و یکپارچه‌سازی با سایر ابزارها و پلتفرم‌های زیرساخت IT شما را فراهم می‌کند.

11
NEW!
حالت تعلیق عامل DLP در نقطه پایانی

امکان توقف فعالیت عامل نقطه پایانی توسط کاربر (با تایید مسئول امنیتی)، که انعطاف‌پذیری بیشتری را فراهم می‌سازد در حالی که پروتکل‌های امنیتی همچنان مؤثر باقی می‌مانند.

12
ارزیابی احساسی

ارزیابی احساسات کارکنان بر اساس هشت واکنش احساسی پایه برای شناسایی گروه‌های پرریسک. سیستم گزارشی از پویایی احساسی هر کارمند ارائه می‌دهد که در قالب نموداری واضح و قابل درک نمایش داده می‌شود. این قابلیت دید عمیق‌تری نسبت به احساسات کارکنان فراهم کرده و در شناسایی اعضای تیم با وفاداری پایین مؤثر است.

ZECURION

13
مقایسه رفتارها

تحلیل رفتار کاربران (UBA) رفتار فعلی کاربران را با میانگین رفتار آن‌ها مقایسه می‌کند. انحرافات قابل توجه ممکن است نشانه‌ای از تهدیدات احتمالی امنیت اطلاعات یا استفاده غیرمجاز از اعتبارنامه‌ها باشد. همچنین می‌توان رفتار دو کاربر یا یک کاربر با یک گروه را مقایسه کرد.

14
نقشه ارتباطات کاربران

Zecurion DLP یک نمودار تعاملی از ارتباطات و کانال‌های ارتباطی کاربران ایجاد می‌کند که امکان شناسایی روابط پنهان را فراهم می‌سازد. این ابزار تحلیل ارتباطات مشکوک که ممکن است نشان‌دهنده کلاهبرداری داخلی یا خطر نشت داده باشند را ممکن می‌کند.

15
گزارش‌گیری جامع

با بیش از ۲۰ گزارش از پیش تنظیم‌شده و گزینه‌های سفارشی‌سازی، این پلتفرم ابزاری قدرتمند برای ممیزی امنیتی و تحقیقات فراهم می‌سازد. می‌توان به‌راحتی گزارش‌ها را تولید و تحلیل کرد و با چند کلیک جزئیات رخدادها را بررسی کرد.

16
یکپارچه‌سازی با Active Directory

کاربران، گروه‌ها و نام میزبان رایانه‌ها با Active Directory هماهنگ می‌شوند تا یکپارچگی با زیرساخت IT شما را بهبود بخشند. این امر امکان شناسایی کاربران با نام در گزارش‌ها و رویدادها را فراهم می‌سازد و روند مدیریت را ساده‌تر می‌کند.

17
ارزیابی مبتنی بر ریسک

Zecurion DLP امتیاز ریسک و روند آن را برای هر کارمند نمایش می‌دهد. هر پروفایل کاربر شامل پنج شاخص ریسک است که اطلاعاتی دقیق برای تحقیقات ارائه می‌دهند: میانگین ریسک شرکت، ریسک روز گذشته، ریسک کنونی، میانگین ریسک روزانه، و میانگین ریسک روزانه در هفت روز گذشته.

18
ماژول تحقیقات

این ماژول روند بررسی رویدادها را ساده کرده و مدت زمان واکنش به حوادث را کاهش می‌دهد. با ارائه نمای ۳۶۰ درجه از وظایف در حال انجام، وضعیت آن‌ها، مراحل تحقیق، افراد مسئول و مهلت‌ها، بار کاری تیم امنیت سایبری را کاهش می‌دهد. اعضای تیم می‌توانند در طول بررسی نظر بدهند، همکاری کنند، مستندات پیوست کنند و رویدادها را به‌عنوان شواهد ضمیمه نمایند.

NEW!

19
شکستن رمز عبور برای فایل‌های آرشیو شده رمزنگاری‌شده

Zecurion DLP امنیت داده را ارتقاء می‌دهد و امکان بررسی فایل‌های حساس را فراهم می‌سازد. با استفاده از واژه‌نامه داخلی قابل تنظیم، مسئول امنیت می‌تواند رشته‌های رمز عبور احتمالی را تعیین کند تا فرآیند رمزگشایی تقویت شود. هنگام شناسایی یک آرشیو رمزنگاری‌شده، سیستم به‌طور خودکار روش‌های رمزگشایی را در درگاه‌ها و نقاط پایانی اعمال می‌کند. پس از رمزگشایی، تحلیل دقیق فایل انجام می‌شود تا از نشت داده جلوگیری و رعایت قوانین حفظ شود.

NEW!

20
سیاست‌های تقویت‌شده آنلاین/آفلاین و واکنش‌های سیستمی

سیاست‌های به‌روزرسانی‌شده به عامل نقطه پایانی اجازه می‌دهد اتصال به شبکه سازمان را تشخیص داده و بر اساس آن، مجموعه‌ای خاص از سیاست‌ها را اجرا کند. واکنش‌های جدید سیستم شامل اجرای اسکریپت پیوست‌شده یا اجرای یک برنامه مشخص، آغاز وظیفه‌ای جدید در ماژول IRP (برنامه واکنش به حادثه) و تنظیم سطوح دسترسی فایل‌ها برای رد دسترسی در ACL فایل می‌باشد.

ADVANCED FEATURES

کشف عکس‌برداری از صفحه‌نمایش

AI

این قابلیت نوآورانه مبتنی بر هوش مصنوعی، نحوه برخورد با امنیت را متحول کرده و کاربرانی را شناسایی می‌کند که پیش‌تر قابل‌ردیابی نبودند. هرگاه فردی تلاش کند از صفحه‌نمایش با گوشی هوشمند عکس بگیرد، Zecurion DLPفوراً این اقدام را از طریق وب‌کم تشخیص داده و بلافاصله رایانه را غیرفعال می‌کند. این فناوری پیشرفته با استفاده از دو شبکه عصبی، شناسایی قابل اطمینانی از گوشی هوشمند ارائه می‌دهد و در مدت زمان بسیار کوتاه (تا ۰٫۰۶ ثانیه) حادثه امنیتی را گزارش می‌کند.

واترمارک صفحه‌نمایش

مسئولین امنیت می‌توانند واترمارک‌هایی شامل نام کاربر، اطلاعات رایانه و تاریخ را روی برنامه‌های خاص) مانندMS Office ، CRMو (...اعمال کنند. این واترمارک‌ها به‌طور واضح برای کاربران قابل مشاهده هستند و ممکن است آن‌ها را از گرفتن اسکرین‌شات یا عکس از فایل‌های حساس منصرف کند.

گزارش شبیه به چت

این گزارش یکپارچه تحلیل ارتباطات بین دو کاربر را با گردآوری تمامی پیام‌ها از پلتفرم‌های مختلف پیام‌رسانی (مانند واتساپ، تلگرام و...) در یک رابط شبیه به برنامه‌های پیام‌رسان محبوب، ساده می‌سازد. این رابط امکان مشاهده تمام پیام‌های ثبت‌شده، دسترسی به فایل‌ها، و گوش دادن به پیام‌های صوتی و تماس‌ها را از یک مکان مرکزی فراهم می‌کند.

ضبط میکروفون و وب‌کم

NEW!

با فعال‌سازی قابلیت ضبط از میکروفون یا وب‌کم هر رایانه در هر زمان، می‌توان هر رایانه‌ای را به یک سیستم نظارتی تبدیل کرد. هنگامی‌که کاربر بین برنامه‌های فعال دسکتاپ جابه‌جا می‌شود، می‌توان اسکرین‌شات یا تصویر وب‌کم تولید کرد.

اتصال زنده به دسکتاپ و وب‌کم

اتصال بلادرنگ به رایانه کارمند جهت ارزیابی فوری فعالیت‌های او. امکان مشاهده هم‌زمان تصویر زنده از طریق وب‌کم برای درک بهتر شرایط فراهم است.

جلوگیری از اسکرین‌شات

در صورت نیاز، مسئول امنیت می‌تواند قابلیت گرفتن اسکرین‌شات را برای کاربر غیرفعال کند.

ثبت اسکرین‌شات و کلیدهای فشرده‌شده

امکان پایش تمام کلیدهای فشرده‌شده توسط کاربران یا گروه‌های مشخص و گرفتن اسکرین‌شات در بازه‌های زمانی تعیین‌شده از هر رایانه. این ویژگی به اجرای سیاست‌های امنیت داخلی و مدیریت داده‌ها کمک کرده و از نشت احتمالی اطلاعات جلوگیری می‌کند.

کنترل برنامه‌ها، نرم‌افزار و سخت‌افزار

NEW!

برای کاهش ریسک استفاده کاربران از برنامه‌های مضر) مانندTOR ، کلاینت‌های تورنت، ابزارهای ناشناس‌ساز و بازی‌ها(، می‌توان دسترسی به برنامه‌ها را مدیریت کرد. می‌توان فهرست سفید یا سیاه از برنامه‌ها برای کاربران یا گروه‌های خاص ایجاد کرد. همچنین قابلیت عامل DLP ارتقاء یافته و می‌تواند تغییرات در فهرست نرم‌افزارهای نصب‌شده و پیکربندی سخت‌افزار را شناسایی و پایش کند.

مخفی‌سازی عامل نقطه پایانی از کاربران

این راهکار می‌تواند عامل DLP را از دید کاربران درTask Manager ، برنامه‌ها و ویژگی‌ها، کنسول‌های خدمات سیستم و File Explorer مخفی نگه دارد تا هیچ اثری از آن برای کاربر قابل مشاهده نباشد.

COMPONENT OVERVIEW

Traffic Control	پایش ترافیک شبکه و مدیریت جریان داده‌ها در بیش از ۱۰۰ سرویس مختلف به منظور کاهش خطر نشت اطلاعات، چه به‌صورت عمدی و چه ناخواسته.
Device Control	رویکردی دقیق و سطح‌بندی‌شده برای محدودسازی دسترسی و حفاظت از داده‌ها فراهم می‌کند، در حالی‌که استفاده قانونی و مجاز از اطلاعات را تسهیل می‌نماید.
Discovery	اطلاعات حساس ذخیره‌شده به‌صورت نامناسب را در دیسک‌های محلی، پوشه‌های اشتراکی، Microsoft SharePoint، Microsoft Exchangeو هر پایگاه داده‌ای که از ODBCاستفاده می‌کند، شناسایی کرده و امکان اتخاذ اقدامات پیشگیرانه برای جلوگیری از نشت یا سرقت داده‌ها را فراهم می‌سازد.
Staff Control NEW!	راهکار مدیریت پیشرفته برای دورکاری، Staff Control، ساعات کاری را پایش می‌کند، فعالیت‌های کارکنان در محیط کار را ثبت می‌نماید و سطح بهره‌وری را ارزیابی می‌کند. گزارش فعالیت کاربران با جزئیات پیشرفته، در نسخه جدید در دسترس است.
User Behavior Analytics	این ماژول از ۱۵ شاخص استفاده می‌کند و از پروفایل‌سازی احساسی بهره می‌برد. تحلیل رفتار کاربران پارامترهای فعلی کارمندان را با مقادیر آماری میانگین آن‌ها مقایسه می‌کند، و انحراف‌های قابل‌توجه به‌عنوان شاخص‌های احتمالی تهدید در نظر گرفته می‌شوند.
Screen Photo Detector AI	این قابلیت نوآورانه مبتنی بر هوش مصنوعی، تحول بزرگی در حوزه امنیت ایجاد کرده است، چراکه فعالیت‌های پنهان پیشین کاربران داخلی را شناسایی و متوقف می‌کند. هنگامی‌که فردی تلاش می‌کند با استفاده از گوشی هوشمند از صفحه‌نمایش عکس بگیرد، Zecurion DLPبلافاصله از طریق وب‌کم این اقدام را تشخیص داده و سیستم را قفل می‌کند. این فناوری انقلابی با بهره‌گیری از دو شبکه عصبی، شناسایی دقیق گوشی‌های هوشمند را تضمین کرده و در کمتر از ۰.۰۶ ثانیه وقوع حادثه امنیتی را علامت‌گذاری می‌نماید.
Investigation Workflow Automation	این ماژول فرآیند تحقیقات را ساده کرده و چرخه واکنش به حوادث را کاهش می‌دهد. با ارائه یک نمای ۳۶۰ درجه جامع از وظایف در حال اجرا — شامل وضعیت‌ها، میزان پیشرفت تحقیقات، افراد مسئول و مهلت‌ها — حجم کاری تیم امنیت سایبری را به‌طور قابل‌توجهی کاهش می‌دهد. در جریان تحقیقات، اعضای تیم می‌توانند روی وظایف نظر ثبت کنند، پیشرفت‌ها را با همکاران در تمامی سطوح(از CISO تا تحلیل‌گران) به اشتراک بگذارند و اسناد و شواهد مربوط به حادثه را ضمیمه کنند.
Risk-based Assessment	دیدی جامع از فعالیت‌های کارکنان ارائه می‌دهد و آن‌ها را بر اساس پارامترهای کلیدی از جمله ریسک، بهره‌وری، تطابق با سیاست‌ها و وضعیت احساسی ارزیابی می‌کند. هر پروفایل کارمند، تمام رویدادهای مرتبط را در یک صفحه واحد و به‌صورت ترتیب زمانی نمایش می‌دهد؛ هر رویداد نیز قابل کلیک بوده و اطلاعات جزئی را در اختیار قرار می‌دهد. افسر امنیتی کارکنانی با ریسک بالا را با دقت بیشتری زیر نظر خواهد داشت، در حالی‌که افراد کم‌ریسک با محدودیت‌های کمتری مواجه خواهند بود.
Data Classification AI	Zecurion از تکنیک‌های پیشرفته‌ای مانند اثر انگشت دیجیتال، تحلیل مبتنی بر واژه‌نامه، یادگیری ماشین و تطبیق الگوها برای شناسایی و مدیریت دقیق داده‌ها در سراسر چرخه عمر آن‌ها استفاده می‌کند. این فناوری‌ها، حفاظتی قدرتمند برای اطلاعات حساس فراهم می‌سازند؛ صرف‌نظر از قالب یا محل ذخیره‌سازی آن‌ها. علاوه بر این، فناوری تشخیص نوری نویسه (OCR) با استخراج جزئیات حساس از اسناد اسکن‌شده یا عکس‌برداری‌شده، دقت طبقه‌بندی داده‌ها را به‌طور چشمگیری افزایش می‌دهد.

طبقه‌بندی داده‌ها با هوش مصنوعی

راهکار Zecurion DLP از تکنیک‌های متنوعی برای شناسایی داده‌ها بهره می‌برد تا حفاظت کامل در برابر نشت اطلاعات فراهم شود. فرقی نمی‌کند که داده‌ها به‌صورت عمدی به سرقت رفته باشند، به خطر افتاده باشند یا ناخواسته به اشتراک گذاشته شده باشند؛ یکی از این روش‌های شناسایی می‌تواند موضوع را کشف کرده و هشدار دهد.

کلیدواژه‌ها و واژه‌نامه‌ها

این روش از مجموعه‌ای از رشته‌های متنی همراه باwildcard ها برای شناسایی موضوعات خاص استفاده می‌کند. این تکنیک امکان تطبیق دقیق کلمات را فراهم کرده و در عین حال، با استفاده از صرف(morphology) ، ریشه‌یابی و ترکیب کلمات، خطاهای مثبت کاذب را کاهش می‌دهد. همچنین کاربران می‌توانند علاوه بر ۳۰+ واژه‌نامه از پیش‌تعریف‌شده، واژه‌نامه‌های سفارشی خود را نیز ایجاد کنند.

الگوها و عبارات منظم

ابزاری قدرتمند برای جستجوی داده‌های ساختاریافته هستند که می‌توانند الگوهایی مانند شماره کارت اعتباری، شماره تأمین اجتماعی، شماره حساب IBAN، آدرس‌های URL و ایمیل را شناسایی کنند.

اثر انگشت دیجیتال

از طریق جمع‌آوری انواع خاصی از اسناد، امکان شناسایی نسخه‌های واقعی اسناد یا بخش‌هایی از آن‌ها را فراهم می‌کند. این اثرانگشت‌ها به‌صورت خودکار هنگام افزودن اسناد جدید به‌روزرسانی می‌شوند. الگوریتم‌های Shingles و روش بیزی برای ردیابی توالی واژگان و وزن‌دهی دسته‌بندی‌ها استفاده می‌شوند تا دقت شناسایی اسناد افزایش یافته و سرعت پردازش بهبود یابد.

اثر انگشت فرم‌های خالی

NEW!

این ویژگی به سیستم اجازه می‌دهد تا فرم‌های متنی پرشده را شناسایی کند. این قابلیت به سازمان‌ها کمک می‌کند تا اسناد حاوی اطلاعات حساس را حتی در صورتی که فرم اولیه خالی بوده باشد، بهتر شناسایی و مدیریت کنند.

اثر انگشت فایل‌های باینری با استفاده از الگوریتم SHA-256

NEW!

SHA-256 یک تابع هش رمزنگاری است که مقدار هش ۲۵۶ بیتی (۳۲ بایتی) تولید می‌کند و معمولاً به‌صورت عدد هگزادسیمال نمایش داده می‌شود. این الگوریتم به‌طور گسترده برای تأیید صحت و یکپارچگی داده‌ها استفاده می‌شود، چرا که برای هر ورودی منحصربه‌فرد، یک هش منحصربه‌فرد تولید می‌کند. حتی تغییر کوچکی در ورودی باعث تغییر کامل هش خواهد شد، که برگشت‌ناپذیر بودن و احتمال بسیار پایین تلاقی را تضمین می‌کند. این به‌روزرسانی، روشی قدرتمندتر برای شناسایی و طبقه‌بندی فایل‌های باینری فراهم می‌سازد و دقت محافظت از داده‌ها را افزایش می‌دهد.

ZECURION

یادگیری ماشین (Machine Learning)

یادگیری ماشین اسنادی را شناسایی می‌کند که از نظر کلیدواژه‌ها و شاخص‌های معنایی، شباهت زیادی به گروه اسناد ارسالی دارند.

الگوهای تصویری مبتنی بر هوش مصنوعی (AI-Based Image Templates)

این ویژگی قادر است امضاها، مهرها و اسناد ساختاریافته مانند گذرنامه یا گواهی‌نامه رانندگی را از طریق شناسایی الگوهای تصویری – نه فقط متن – تشخیص دهد. این قابلیت نیازمند تنظیم اولیه فایل‌های تحلیلی است تا سیستم بتواند در آینده، موارد مشابه مانند تصویر مهر شرکت (با هر رنگ یا زاویه‌ای) را به‌عنوان اطلاعات محرمانه شناسایی کند.

تشخیص نوری نویسه (OCR)

یک تکنیک ارزشمند برای شناسایی اطلاعات حساس یا محرمانه‌ای است که از طریق اسکن یا عکس‌برداری ذخیره شده‌اند تا از روش‌های دیگر شناسایی در امان بمانند Zecurion DLP. این قابلیت را با ادغام موتورهای قدرتمند شخص ثالث مانند ABBYY FineReader و Google Tesseract توسعه داده تا بتواند متن را از تصاویر استخراج و شناسایی کند.

ماشین بردار پشتیبان (SVM - Support Vector Machine)

این روش امکان ایجاد یک طبقه‌بند را فراهم می‌سازد که متون مرتبط با یک موضوع خاص را بر اساس تحلیل دو مجموعه سند شناسایی می‌کند: اسناد مرتبط با موضوع و اسنادی با زبان مشابه که مرتبط نیستند. هرچه تعداد اسناد در هر مجموعه بیشتر باشد، دقت طبقه‌بندی بالاتر خواهد رفت. در آزمایش‌های بعدی، زمانی که احتمال تطبیق برای اسناد مرتبط بیش از ۹۰٪ باشد، عملکرد سیستم قابل قبول تلقی می‌شود.

NEW!

شناسایی الحاق فایل‌های باینری (Binary File Concatenation Detection)

این قابلیت به شناسایی زمانی کمک می‌کند که چند فایل باینری در یک فایل بزرگ‌تر ادغام شده‌اند. این امر امکان ردیابی بهتر اطلاعات حساس پنهان‌شده یا ترکیب‌شده در فایل‌های دیگر را فراهم می‌سازد.

NEW!

شناسایی اتصالات پروتکل ریموت دسکتاپ (RDP Detection)

سیستم قادر است اتصال‌های RDP را شناسایی کند تا دسترسی‌ها بهتر مدیریت شده و جلسات ریموتی که ممکن است اطلاعات حساس را در معرض خطر قرار دهند، به‌طور کامل نظارت شوند. این موضوع امنیت کلی را ارتقاء می‌دهد.

NEW!

تحلیل محتوای کدهای QR (QR Content Analysis)

این ویژگی کدهای QR موجود در اسناد یا تصاویر را تحلیل می‌کند تا محتوای درون آن‌ها بررسی شود. از این طریق، سازمان‌ها می‌توانند خطرات احتمالی ناشی از کدهای QR را شناسایی کرده و از دسترسی غیرمجاز به داده‌ها جلوگیری کنند و در عین حال، با سیاست‌های امنیتی مطابقت داشته باشند.

ZECURION

شرکت رایان سامانه آرکا، توزیع کننده انحصاری Zecurion در ایران

درباره Zecurion

شرکت Zecurion در سال ۲۰۰۱ در مسکو تأسیس شد و از آن زمان تاکنون به یکی از مراجع جهانی در حوزه راهکارهای امنیت فناوری اطلاعات تبدیل شده است. این شرکت از منافع بیش از ۱۰۰۰۰ مشتری سازمانی در بیش از ۷۰ کشور در سراسر جهان محافظت می‌کند.

Zecurion به دلیل نوآوری‌های برجسته خود، از جمله فناوری‌های ثبت اختراع‌شده، شناخته‌شده است و محصولاتی پیشرفته ارائه می‌دهد؛ از جمله:

- سیستم پیشگیری از نشت داده نسل جدید
- نظارت و محافظت متمرکز بر داده‌ها
- درگاه امن وب

با دریافت تقدیر و جوایز از مراجع معتبر بین‌المللی مانند Gartner و IDC، Zecurion همواره در خط مقدم صنعت امنیت اطلاعات قرار داشته و راهکارهایی پیشرفته، با قابلیت استقرار سریع و تمرکز بر کاهش تهدیدات درون‌سازمانی ارائه می‌دهد .

شرکت رایان سامانه آرکا، بیش از 15 سال سابقه در ارائه، نصب، راه‌اندازی، استقرار و پشتیبانی محصولات DLP، یکی از شرکت‌های پیشرو در امر راهکارهای جلوگیری از نشت داده است.

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۰۲۱-۹۱۳۰۰۴۷۶ | دورنگار: ۰۲۱-۸۸۸۰۴۹۶۱ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
www.arka.ir info@arka.ir
رایان سامانه آرکا

شرکت رایان سامانه آرکا، توزیع کننده انحصاری Zecurion در ایران

مقایسه

Zecurion DLP

با سایر DLPها

arka
رایان سامانه آرکا

ZECURION

www.arka.ir

Zecurion DLP 12.0

comparison with Symantec DLP

DLP architecture. DLP deployment modes and implementation options

	ZECURION	Symantec
Gateway-based deployment implementation mode	✓	✓
Fully agent-based interception deployment mode	✓	✓
Web traffic interception on corp gateway using integration with a SWG proxy server with ICAP protocol	✓	✓
Integration using plugin for on-prem MS Exchange instance	✓	✗
Implementation in “Mixed mode” (gateway and agent)	✓	✓
Integration with the mail server through the service mailbox using POP3 protocol	✓	✗
Own operational SWG web proxy server to block web users on corp gateway	✓	✓
Blockage with operational corp gateway SWG server over ICAP	✓	✓
Integration with corp SIEM instance	✓	✓
Domain-less standalone PCs support and monitor	✓	✓
Zecurion Installation server for endpoints with web console	✓	✓

Leakage vectors detection methods and onboard data classification tools

	ZECURION	BROADCOM Symantec
Detection content of the document	✓	✓
Verification with the customizable dictionaries	✓	✓
Regular expressions	✓	✓
Digital fingerprints	✓	✓
Support Vector Machine method	✓	✓
Bayes data classification method	✓	✗
Control of documents containing seals or signatures	✓	✗
Integration with text recognition (OCR) engines (Abbyy and Tesseract)	✓	✓
Screen Photo Detector endpoint AI module to capture the attempts of making photo of the screen with smartphones	✓	✗
Speech-to-text feature for captured audio files	✓	✗

Traffic control module. Email control features

	ZECURION	Broadcom Symantec
Inbound\Outbound SMTP mail capturing	✓	Outgoing mails only
Microsoft Exchange internal mail capturing	✓	Outgoing mails only
POP3 mail protocol support	✓	✗
IMAP mail protocol support	✓	✗
Mail Quarantine Zone	✓	Symantec Messaging Gateway module is required
Message modification	✓	✓
Office 365 and Exchange Online support	✓	✓
Ability to capture mail traffic at endpoint using deep API integration with the mail clients: Outlook, Thunderbird and Lotus Notes	✓	✗
Mail relay MTA module in-between for mail blockage	✓	✓

Traffic control module. Internet web control and monitoring features

	ZECURION	Symantec
HTTPS traffic capturing with MITM algorithm	✓	✓
Ability to capture https traffic at endpoint using deep API integration with the browsers: Chrome, IE 8+, Firefox etc.	✓	✓
Ability to block https traffic at endpoint using deep API integration with the browsers	✓	✗
HTTP inbound traffic capturing	✓	✓
Outgoing HTTP traffic capturing	✓	✓
Public Webmail services (Gmail, Yahoo Mail etc) capturing	✓	✓
Social networks	✓	✓
FTP	✓	✓
Office 365	✓	✓
Web Clouds (OneDrive, Dropbox etc)	✓	✓

Traffic control module. Instant Messaging monitoring and blockage

	ZECURION	BROADCOM Symantec
Yahoo! Messenger	✓	✓
Skype for business (MS Lync)	✓	✓
ICQ	✓	✗
Viber	✓	✗
Skype	✓	✓
Jabber	✓	✓
Microsoft Teams	✓	✓
Telegram desktop application protocol (with blockage option)	✓	✗
Telegram web application protocol (with blockage option)	✓	✗
WhatsApp desktop application protocol (with blockage option)	✓	✗
WhatsApp web protocol interception (with blockage option)	✓	✗

Device Control. Endpoint control features

	ZECURION	BROADCOM Symantec
Agent stand-alone mode without access to the server	✓	✓
Blocking leakage via USB and other devices	✓	✓
Block leakage through printing using content analysis rule	✓	✓
USB read only mode	✓	✓
USB shadow copying	✓	✓
Customizable file size limit for shadow copies	✓	✗
Manage settings and volume of the local storage of logs and shadow copies on Endpoints	✓	✓
Application startup control and blockage	✓	✓
Encrypting files when writing to USB	✓	✗
Content analysis based encryption	✓	✗
Access control for encryption keys by user / group of users	✓	✓

Device Control. Endpoint control features

	ZECURION	BROADCOM Symantec
Re-generation of encryption keys	✓	✓
Save encryption key history	✓	✗
Making workspace screenshots	✓	✗
OCR recognition for screenshots	✓	✗
Set screenshots for list of users	✓	✗
Set screenshots with periodicity	✓	✗
Saving screenshots in different file formats	✓	✗
Saving grayscale screenshots	✓	✗
Hiding agent presence at PC	✓	Partially
Protection against agent disable	✓	✓
Record sound flow through the built-in microphone	✓	✗

Device Control. Endpoint control features

	ZECURION	Symantec
Keyboard typed text capturing tool	✓	✗
Clipboard control	✓	✓
Customizable uninstall password for endpoint agent	✓	✓
Files Removal action in Discovery module	✓	✓
MS Office documents properties attributes verification	✓	✓
TITUS tags verification in MS Office documents properties attributes	✓	✓
Capturing the number of printed pages	✓	✗
Block screenshots taking (Print Screen) in policies	✓	✗
Customizable watermarks on top of specific application launched	✓	✗
Active windows session logout and user blocking in live-mode on target PC for the triggered policy violation	✓	✗

Device Control. Supported device types in endpoint policies

	ZECURION	Broadcom Symantec
Pre-configured lists of typical classes and types of connected devices (Storages, Portable, Media, Security, Tapes etc.)	✓	Partially
USB connected devices class	✓	✓
LPT / COM / irDA ports	✓	✗
FireWire IEEE 1394	✓	✗
CD / DVD drives	✓	✓
External and internal HDDs	✓	✓
Ethernet adapters	✓	✗
Bluetooth / Wi-Fi / Modems	✓	✗
RDP forwarded devices	✓	✓
PCMCIA adapters	✓	✗

Discovery Crawler capabilities

	ZECURION	BROADCOM Symantec
Network storage scanning	✓	✓
Scan local storage	✓	✓
Scan databases	✓	✓
Scan MS SharePoint	✓	✓
Scan MS Exchange	✓	✓
Real-time storage scanning	✓	✓
Scheduled Scan	✓	✓
Security administrator notification of storage policy violations	✓	✓
Alert users about violation of information security policies	✓	✓
Moving / deleting files	✓	✓

Staff control module. Employees productivity analysis

	ZECURION	Broadcom Symantec
User's working time analysis engine	✓	✗
Pre-installed calculated ratings of user's productivity	✓	✗
Inactivity time calculation (absence of user activity while the PC is switched on and locked)	✓	✗
Working days calendar, holidays and working hours customization for the employees	✓	✗
Calculation of users activity in certain websites and applications that are related to the employee's activities	✓	✗
Customization of group of productive and unproductive application and website categories for the employees	✓	✗
Pre-installed list of default categories containing the most popular websites and applications	✓	✗
Employee's timesheets for the dates when the employee was present at work (discipline analysis)	✓	✗
Remote work detection	✓	✗
Advanced reports with activity classification and user's structured timesheets	✓	✗

DLP extensions. File monitoring and analysis using DCAP modules

	ZECURION	Symantec
Endpoint-based file monitoring module in workstation	✓	✓
Ability to install file monitoring module on corp File Server	✓	✗
On-the-fly monitoring for the selected target files or folders in PC, shared folders on File Server	✓	✗
On-the-fly monitoring of changes made by system admins in MS Active Directory	✓	✗
Data classification capabilities using active DLP policies	✓	✓
Access rights summary for inspected files and folders	✓	✗
Ability to integrate DCAP dashboard of monitored user in his system profile in DLP management web console	✓	✗
Quick summary events log section for selected files and folders in web management console	✓	✗
User's cumulative file\folders access summary report	✓	✗
File duplicates identification summary report	✓	✗

Management tools and capabilities for officers and operators

	ZECURION	Broadcom Symantec
Single management console for Operators and Sys Admins	✓	✓
Single unified console for the system Repository	✓	✓
“Dark Style” mode for operator’s eye saving	✓	✗
Setting alerts and notifications using private Telegram bot	✓	✗
Web console management	✓	✓
SWG/NGFW-like policy creation interface and implementation	✓	✗
Deploy and upgrade through own Installation server / console	✓	✓
Deep separation of administrator roles and ACLs	✓	✓
Incident response platform (IRP) task tracker for teams	✓	✗
Incident response platform (IRP) customizable workflow templates	✓	✗
Ability to unload and backup all settings to a structured XML file	✓	✗

User-centric data organization. Reporting tools for security officers

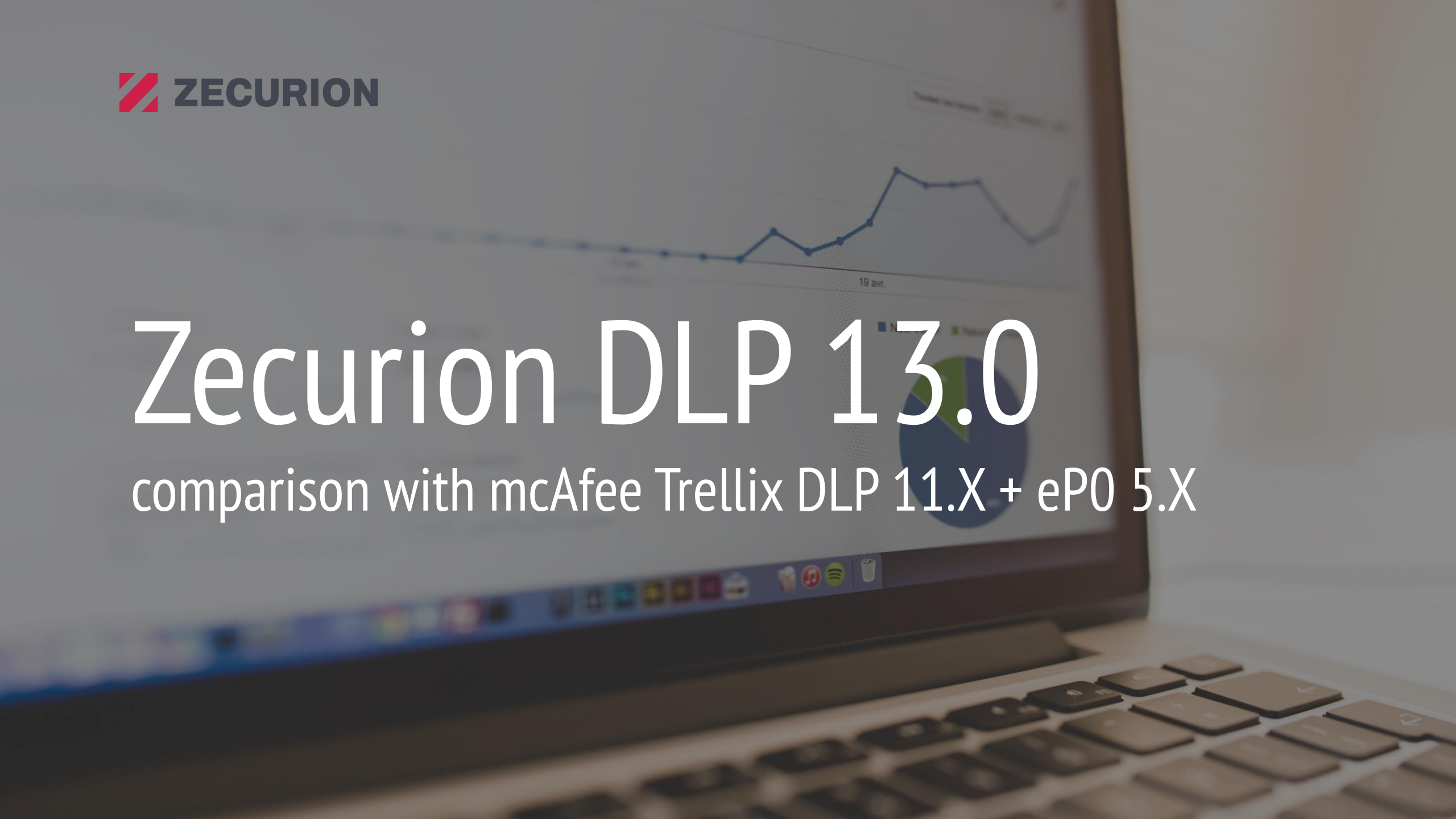
	ZECURION	Symantec
Unified UI user's profile with tabs and data mining capabilities	✓	✗
Tabular reports in console	✓	✓
List of messages in a table with the ability to view their contents	✓	✓
Unified graphic reports and dashboards in console	✓	✓
User connections diagram in user profile	✓	✗
User emotional status diagrams in user profile	✓	✗
User Behavior Analytics based on composite everyday indicator (incidents, files, traffic volume etc.)	✓	Additional module is required
Ability to compare current UBA rates with historical data for previous period	✓	Additional module is required
Risk-based assessment engine for the monitored staff	✓	Additional module is required
Ability to calculate daily risk score dynamic for the last month	✓	Additional module is required

Reporting tools for security officers and operators

	ZECURION	Symantec
Anomalies detection tool (with preinstalled library of cases)	✓	✗
User's anomalies notification	✓	✗
Comparison dashboard for selected employees and departments	✓	✗
Live monitoring of user session with web camera snapshots	✓	✗
Live monitoring of user session with desktop online access on endpoints	✓	✗
Chat-like report to display captured dialogues between persons in different instant messengers	✓	✗
Administrators logging tool	✓	✓
Capabilities to add new users linked account or aliases in user profile	✓	✗
Export reports and rows to expropriated HTML file	✓	✗
Report export tool to PDF, XLSX, CSV, PST file formats	✓	Partially

System requirements and platforms

	ZECURION	BROADCOM Symantec
Server modules and components OS requirements	Windows Server 2008 R2 and later, Ubuntu Linux 22.04	Windows Server 2008 R2 and later. RedHat Linux
OS support by DLP endpoint agents	Windows XPSP3 and later, Windows Server 2008 R2 and later; Linux Ubuntu 16\18\20, Linux Debian;	Windows 7 or later + macOS
Supported SQL Repositories	Microsoft SQL, PostgreSQL	Oracle DB



ZECURION

Zecurion DLP 13.0

comparison with mcAfee Trellix DLP 11.X + ePO 5.X

DLP architecture. DLP deployment modes and implementation options

	ZECURION	McAfee
Gateway-based server deployment mode and traffic interception in-between of operational channel	✓	✓
Fully agent-based interception deployment mode	✓	✓
Web traffic interception on corp gateway using integration with a SWG proxy server with ICAP protocol	✓	✓
Integration using plugin for on-prem MS Exchange instance	✓	✗
Implementation in “Mixed mode” (gateway and agent)	✓	✓
Integration with the mail server through the separating specialized service mailbox	✓	✗
Own operational SWG web proxy server to block web users on corp gateway	Zecurion SWG or Zecurion NGFW	mcAfee Web Gateway is required
Blockage with operational corp gateway SWG server over ICAP	✓	✓
Integration with corp SIEM instance	✓	✓
On-prem DLP installation server for endpoint (Win and Linux)	✓	Linux is not supported

Leakage vectors detection methods onboard and data classification tools

	ZECURION	McAfee
Customizable dictionaries containing keywords with the wildcards option	✓	✓
Detection with regular expressions method	✓	✓
Digital fingerprints for text files	✓	Only in Windows endpoints
Digital fingerprints for images and pictures	✓	✗
Digital fingerprints to detect filled text forms	✓	✗
Digital fingerprints for files using SHA256 hash algorithm	✓	✗
Digital fingerprints to detect scope of rows from DB	✓	✗
Support Vector Machine SVM machine learning method	✓	✗
Bayesian data classification probabilistic method	✓	✗
Labels and tags analysis in file's metadata	✓	✓

Leakage vectors detection methods onboard and data classification tools

	ZECURION	McAfee
QR-code presence identification in attached document and pictures. QR content text analysis	✓	✗
Binary files concatenation presence identification	✓	✓
Password cracking for encrypted archives. Internal dictionary with the scope of text strings of possible passwords.	✓	✗
Encrypted files detection and identification	✓	✓
Nested archive files detection and identification	✓	✓
MS Office documents file properties attributes and third party tagging identification	✓	✓
Integration with text recognition (OCR) engines (Abbyy and Tesseract) both for endpoint PC and server modules	✓	✓
Screen Photo Detector endpoint AI module to capture the attempts of making photo of the screen with smartphones	✓	✗
Speech-to-text feature for captured audio files	✓	✗

Traffic control module. Email control features

	ZECURION	McAfee
Inbound\Outbound SMTP mail capturing	✓	✓
Microsoft Exchange internal mail capturing	✓	✓
POP3 mail protocol support	✓	✓
IMAP mail protocol support	✓	✓
Mail relay MTA server module in-between for mail blockage	✓	✗
SMTP mail quarantine zone in-between operational channel	✓	Only using third-party standalone on-prem MTA
Exchange Online gateway based capturing MTA mode	✓	McAfee MVISION Cloud CASB is required
Ability to capture mail traffic at endpoint using deep API integration with the mail clients: Outlook, Thunderbird and Lotus Notes	✓	✗
Message modification	✓	✓

Traffic control module. Internet web control and monitoring features

	ZECURION	McAfee
HTTPS traffic capturing with MITM algorithm	✓	✓
Ability to capture https traffic at endpoint using deep API integration with the browsers: Chrome, IE 8+, Firefox etc.	✓	✓
Ability to block https traffic at endpoint using deep API integration with the browsers	✓	✗
HTTP inbound traffic capturing	✓	✗
Outgoing HTTP traffic capturing	✓	✓
Public Webmail services (Gmail, Yahoo Mail etc) capturing	✓	✓
Social networks	✓	✓
FTP	✓	✓
Office 365	✓	✓
Web Clouds (OneDrive, Dropbox etc)	✓	✓

Traffic control module. Instant Messaging monitoring and blockage

	ZECURION	McAfee
Yahoo! Messenger	✓	Only File Access blockage for IM desktop app
Skype for business (MS Lync)	✓	Only File Access blockage for IM desktop app
Viber	✓	Only File Access blockage for IM desktop app
Skype	✓	Only File Access blockage for IM desktop app
Jabber	✓	Only File Access blockage for IM desktop app
Microsoft Teams	✓	✓
Telegram desktop application protocol (with blockage option)	✓	✗
Telegram web application protocol (with blockage option)	✓	✗
WhatsApp desktop application protocol (with blockage option)	✓	✗
WhatsApp web protocol interception (with blockage option)	✓	✗

Device Control. Endpoint control features

	ZECURION	McAfee
Agent stand-alone mode without access to the server	✓	✓
Blocking leakage via USB and other devices	✓	✓
Block leakage through printing using content analysis rule	✓	Only in for Windows clients
Shadow copying for file and documents being transferred to USB device	✓	✓
Customizable file size limit for shadow copies	✓	✗
Manage settings and volume of the local storage of logs and shadow copies on Endpoints	✓	✓
Encrypting files when writing to USB	✓	McAfee Endpoint Protection module is required
Content analysis based encryption for copied outside file	✓	✗
Re-generation of encryption keys	✓	✗
Save encryption key history	✓	✗

Device Control. Endpoint control features

	ZECURION	McAfee
Application startup control and blockage	✓	McAfee Endpoint Protection module is required
USB memory device read only mode	✓	✓
Making workspace screenshots	✓	✗
OCR recognition for screenshots	✓	✗
Set making screenshots with certain periodicity (in secs)	✓	✗
Saving screenshots in different file formats	✓	✗
Set the limit of data transfer to DB server	✓	✗
Total hiding of DLP agent presence at PC (Task Manager, Win Services console, dlp app program folders)	✓	✗
Protection against agent disable	✓	✓
Customizable uninstall password for endpoint agent	✓	Using admin confirmed one time code

Device Control. Endpoint control features

	ZECURION	McAfee
Keyboard typed text capturing tool	✓	✗
Clipboard control	✓	Only in Windows clients
Record sound flow through the built-in microphone	✓	✗
Corp domain availability monitor (offline/online policies)	✓	✓
MS Office documents properties attributes verification	✓	✓
TITUS tags verification in MS Office documents properties attributes	✓	✓
Capturing the number of printed pages	✓	✗
Block screenshots taking (Print Screen) in policies	✓	Only in Windows clients
Customizable watermarks for documents on top of specific application launched	✓	✗
Active windows session logout and user blocking in live-mode on target PC for the triggered policy violation	✓	✗

Device Control. Supported device types in endpoint policies

	ZECURION	McAfee
Pre-configured lists of typical classes and types of connected devices (Storages, Portable, Media, Security, Tapes etc.)	✓	✓
USB connected devices class	✓	✓
LPT / COM / irDA ports	✓	✗
FireWire IEEE 1394	✓	✓
CD / DVD drives	✓	✓
External and internal HDDs	✓	✓
Ethernet adapters	✓	✗
Bluetooth / Wi-Fi / Modems	✓	Only Bluetooth
RDP forwarded devices	✓	✓
PCMCIA adapters	✓	✓

Discovery Crawler capabilities

	ZECURION	McAfee
Network storage scanning	✓	✓
Scan local storage	✓	✓
Scan local on-prem databases	✓	✓
Scan local on-prem MS SharePoint	✓	✓
Scan local on-prem MS Exchange	✓	✗
Real-time storage scanning	✓	✓
Set file deny access right in file ACL	✓	✗
Security administrator notification of storage policy violations	✓	✓
Alert users about violation of information security policies	✓	✓
Moving / deleting files	✓	✓

DLP extensions. Staff control module. Employees productivity analysis

	ZECURION	McAfee
User's working time analysis engine	✓	✗
Pre-installed calculated ratings of user's productivity	✓	✗
Inactivity time calculation (absence of user activity while the PC is switched on and locked)	✓	✗
Working days calendar, holidays and working hours customization for the employees	✓	✗
Calculation of users activity in certain websites and applications that are related to the employee's activities	✓	✗
Customization of group of productive and unproductive application and website categories for the employees	✓	✗
Pre-installed list of default categories containing the most popular websites and applications	✓	✗
Employee's timesheets for the dates when the employee was present at work (discipline analysis)	✓	✗
User remote work connections detection	✓	✗
Advanced reports with user's activity classification (+timesheets)	✓	✗

DLP extensions. Screen Photo Detection endpoint module.

	ZECURION	McAfee
AI based tools to detect mobile phone frame in web camera screenshots images on user's PC	✓	✗
Incident creation at the time of user's attempts of making photo	✓	✗
Possibility to detect web-camera sheltering	✓	✗
Possibility to create and save screenshot of user's PC workspace at a time of making photo	✓	✗
Management of PC's web-camera screenshots making frequency (time per 1,2,3 …n seconds)	✓	✗
Ability to block user's AD credentials in corp domain in case of making photo of the computer monitor	✓	✗
Possibility to create pop-up bubble warning message in system tray in user's PC	✓	✗
Possibility to identify full context of the event (user name, computer name etc)	✓	✗
Assign risk scoring and ГИФ changes for this user-offender	✓	✗

DLP extensions. DCAP monitoring and analysis capabilities

	ZECURION	McAfee
Ability to install monitoring module in user's PC	✓	✗
Ability to install monitoring module on corp file server	✓	✗
On-the-fly monitoring for the selected target files or folders in PC, shared folders on file server	✓	✗
Ability to install monitoring module in corp MS AD server	✓	✗
On-the-fly monitoring of changes made by system admins in MS Active Directory	✓	✗
On-premise NextCloud instance support	✓	✗
On-premise NetApp server hardware storage support	✓	✗
On-premise Dell server hardware storage support	✓	✗
Data classification capabilities using active DLP policies	✓	✗
One single endpoint agent with DLP and DCAP component	✓	✗

DLP extensions. DCAP reporting tools and data analysis

	ZECURION	McAfee
Ability to integrate DCAP dashboard of monitored user in his system profile in DLP management web console	✓	✗
Preinstalled library which contains more than 150 prebuild out of the box reports (users, channels, folders/files etc)	✓	✗
Quick summary events log section for selected files and folders in web management console	✓	✗
User's cumulative file/folders access summary report	✓	✗
File duplicates identification summary report	✓	✗
Detection of massive file operations on endpoint PC	✓	✗
Detections of the source of file which is being copied	✓	✗
Access rights summary for inspected files and folders	✓	✗
Reporting tool of changes made by system admins in MS Active Directory	✓	✗

System Management tools and capabilities for security officers and sysadmins

	ZECURION	McAfee
Single management console for Operators and Sys Admins	✓	✓
Multi-factor authentication (MFA) for authorization	✓	✓
“Dark Style” mode for operator’s eye saving	✓	✗
Setting alerts and notifications using private Telegram bot	✓	✗
Web console widget management and customization	✓	✓
Deploy and upgrade endpoint through own Installation server / console in Windows and Linux environment	✓	✓
Deep granular separation of administrator roles and ACLs for certain web-panels and reports	✓	✓
Incident response platform (IRP) task tracker for teams	✓	✓
Incident response platform (IRP) customizable workflow templates	✓	✓
Ability to unload and backup all settings to a structured XML file	✓	✓

Reporting tools for security officers. User-centric data organization model.

	ZECURION	McAfee
User-centric data organization and visualization. Unified user's profile with tabs and data mining capabilities in one place	✓	✗
Tabular customizable reports in web-console	✓	✓
List of incidents (violence) in a table with the ability to view their contents, metadata and context	✓	✓
Unified graphic reports and dashboards in console	✓	✓
User connections\communication graph diagram in user personal profile	✓	✗
User emotional status diagrams in user profile	✓	✗
User Behavior Analytics based on composite everyday indicator (incidents, files, traffic volume etc.)	✓	Additional module is required
Ability to compare current UBA rates with historical data for previous period	✓	✗
Risk-based assessment engine for the monitored staff	✓	Additional third-party Risk engine is required
Ability to calculate daily risk score dynamic for the last month	✓	✗

Reporting tools for security officers. Diagrams and monitoring tools

	ZECURION	McAfee
Anomalies detection tool (with preinstalled library of cases)	✓	✗
User's anomalies notification	✓	✗
Comparison dashboard for selected employees and departments	✓	✗
Live monitoring of user session with web camera snapshots	✓	✗
Live monitoring of user session with desktop online access on endpoints	✓	✗
Chat-like report to display captured dialogues between persons in different instant messengers	✓	✗
Administrators logging tool (logons, sessions)	✓	✓
Detect and trace the changes in the list of installed software on the PC, and its hardware configuration	✓	✗
Export reports and rows to expropriated HTML file	✓	✓
Report export tool to PDF, XLSX, CSV, PST file formats	✓	Partially

Sysadmin management tools. Policy management and tools in the Policy Server

	ZECURION	McAfee
One single unified Policy Server for policy creation and deployment to all modules and endpoint agents	✓	✓
Policy orientated deployment approach: Target Channel -> Filtering Condition -> System full-auto Reaction	✓	✗
Modern SWG/NGFW-like policy creation interface	✓	✗
Omni-policy concept. One single policy can be deployed in all target channels and crawler modules	✓	✗
Multi-level condition section to combine filtering expression with AND, OR, NOT Boolean operators in policies	✓	✓
Possibility to turn on\off physical blockage mode for selected policy in selected channels in “one click”	✓	✓
Online/offline policies (inside/outside corp network)	✓	✓
Endpoint agent by request suspending mode	✓	Policy bypass option only
Manual tracert option to check agent-server connection	✓	✓
Run an attached script or specific application in policy	✓	✗

System requirements and platforms

	ZECURION	McAfee
Server modules and components OS requirements	Windows Server 2008 R2 and later, Ubuntu Linux 22.04 and later	Windows Server 2008 R2 and later.
OS support by DLP endpoint agents	Windows XPSP3 and all later, Windows Server 2008 R2 and later; Linux Ubuntu 18\20\22, Linux Debian;	Windows 7 and all later, macOS
Supported SQL Repositories	Microsoft SQL, PostgreSQL	Microsoft SQL

ZECURION

Zecurion DLP 13.0

comparison with Safetica One DLP 11

FOR INTERNAL USE ONLY

DLP architecture. DLP deployment modes and implementation options

	ZECURION	safetica
Gateway-based server deployment mode and traffic interception in-between of operational channel	✓	✗
Fully agent-based interception deployment mode	✓	✓
Web traffic interception on corp gateway using integration with a SWG proxy server with ICAP protocol	✓	✗
Integration using plugin for on-prem MS Exchange instance	✓	✗
Implementation in “Mixed mode” (gateway and agent)	✓	✗
Integration with the mail server through the service mailbox using POP3 protocol	✓	✗
Own branded operational SWG web proxy server to block web users on corp gateway	Zecurion SWG + Zecurion NGFW	Web filtering policies on DLP endpoint
Blockage with operational corp gateway SWG server over ICAP	✓	✗
Integration with corp SIEM instance	✓	✓
On-prem installation server with for endpoint (Win and Linux)	✓	Only for windows PC

Leakage vectors detection methods onboard and data classification tools

	ZECURION	safetica
Customizable dictionaries containing keywords with the wildcards option	✓	✓
Detection with regular expressions method	✓	✓
Digital fingerprints for text files	✓	✗
Digital fingerprints for images and pictures	✓	✗
Digital fingerprints to detect filled text forms	✓	✗
Digital fingerprints for files using SHA256 hash algorithm	✓	✗
Digital fingerprints to detect scope of rows from DB	✓	✗
Support Vector Machine SVM machine learning method	✓	✗
Bayesian data classification probabilistic method	✓	✗

Leakage vectors detection methods onboard and data classification tools

	ZECURION	safetica
QR-code presence identification in attached document and pictures. QR content text analysis	✓	✓
Binary files concatenation presence identification	✓	✓
Password cracking for encrypted archives. Internal dictionary with the scope of text strings of possible passwords.	✓	✓
Encrypted files detection and identification	✓	✗
Nested archive files detection and identification	✓	✗
MS Office documents file properties attributes and third party tagging identification	✓	✗
Integration with text recognition (OCR) engines (Abbyy and Tesseract) both for endpoint PC and server modules	✓	✗
Screen Photo Detector endpoint AI module to capture the attempts of making photo of the screen with smartphones	✓	✗
Speech-to-text feature for captured audio files	✓	✗

Traffic control module. Email control features

	ZECURION	safetica
Inbound\Outbound SMTP mail capturing	✓	✓
Microsoft Exchange internal mail capturing	✓	✗
POP3 mail protocol support	✓	✓
IMAP mail protocol support	✓	✓
Mail relay MTA server module in-between for mail blockage	✓	✗
SMTP mail quarantine zone in-between operational channel	✓	✓
Office 365 and Exchange Online support	✓	✓
Ability to capture mail traffic at endpoint using deep API integration with the mail clients: Outlook, Thunderbird and Lotus Notes	✓	✓
Message modification	✓	✓

Traffic control module. Internet web control and monitoring features

	ZECURION	safetica
HTTPS traffic capturing with MITM algorithm	✓	✓
Ability to capture https traffic at endpoint using deep API integration with the browsers: Chrome, IE 8+, Firefox etc.	✓	✓
Ability to block https traffic at endpoint using deep API integration with the browsers	✓	✗
HTTP inbound traffic capturing	✓	✓
Outgoing HTTP traffic capturing	✓	✓
Public Webmail services (Gmail, Yahoo Mail etc) capturing	✓	✓
Social networks	✓	✓
FTP	✓	✓
Office 365	✓	✓
Web Clouds (OneDrive, Dropbox etc)	✓	✓

Traffic control module. Instant Messaging monitoring and blockage

	ZECURION	safetica
Yahoo! Messenger	✓	✓
Skype for business (MS Lync)	✓	✓
ICQ	✓	✗
Viber	✓	✓
Skype	✓	✓
Jabber	✓	✓
Microsoft Teams	✓	✓
Telegram desktop application protocol (with blockage option)	✓	✓
Telegram web application protocol (with blockage option)	✓	✓
WhatsApp desktop application protocol (with blockage option)	✓	✓
WhatsApp web protocol interception (with blockage option)	✓	✓

Device Control. Endpoint control features

	ZECURION	safetica
Agent stand-alone mode without access to the server	✓	✓
Blocking leakage via USB and other devices	✓	✓
Block leakage through printing using content analysis rule	✓	✓
Shadow copying for file and documents being transferred to USB device	✓	✓
Customizable file size limit for shadow copies	✓	✗
Manage settings and volume of the local storage of logs and shadow copies on Endpoints	✓	✓
Encrypting files when writing to USB	✓	✗
Content analysis based encryption for copied outside file	✓	✗
Re-generation of file encryption keys	✓	✗
Save file encryption key history	✓	✗

Device Control. Endpoint control features

	ZECURION	safetica
Application startup control and blockage	✓	✓
USB memory device read only mode	✓	✓
Making workspace screenshots	✓	✓
OCR recognition for screenshots	✓	✗
Set making screenshots with certain periodicity (in secs)	✓	✓
Saving screenshots in different file formats	✓	✓
Set the limit of data transfer to DB server	✓	✗
Total hiding of DLP agent presence at PC (Task Manager, Win Services console, dlp app program folders)	✓	✓
Protection against agent disable	✓	✓
Customizable uninstall password for endpoint agent	✓	✗

Device Control. Endpoint control features

	ZECURION	safetica
Keyboard typed text capturing tool	✓	✗
Clipboard control	✓	✓
Record sound flow through the built-in microphone	✓	✗
Corp domain availability monitor (offline/online policies)	✓	✗
MS Office documents properties attributes verification	✓	✓
TITUS tags verification in MS Office documents properties attributes	✓	✓
Capturing the number of printed pages	✓	✓
Block screenshots taking (Print Screen) in policies	✓	✗
Customizable watermarks on top of specific application launched	✓	✗
Active windows session logout and user blocking in live-mode on target PC for the triggered policy violation	✓	✗

Device Control. Supported device types in endpoint policies

	ZECURION	safetica
Pre-configured lists of typical classes and types of connected devices (Storages, Portable, Media, Security, Tapes etc.)	✓	✓
USB connected devices class	✓	✓
LPT / COM	✓	✓
FireWire IEEE 1394	✓	✓
CD / DVD drives	✓	✓
External and internal HDDs	✓	✗
Ethernet adapters	✓	✗
Wi-Fi / Modems	✓	✗
Bluetooth	✓	✓
PCMCIA adapters	✓	✗
irDA ports	✓	✗

Discovery Crawler capabilities

	ZECURION	safetica
Network storage scanning	✓	✓
Scan local File Storage	✓	✓
Scan local on-prem databases	✓	✗
Scan local on-prem MS SharePoint	✓	✓
Scan local on-prem MS Exchange	✓	✗
Real-time storage scanning	✓	✓
Set file deny access right in file ACL	✓	✗
Security administrator notification of storage policy violations	✓	✓
Alert users about violation of information security policies	✓	✓
Moving / deleting files	✓	✗

DLP extensions. Staff control module. Employees productivity analysis

	ZECURION	safetica
User's working time analysis engine	✓	✓
Pre-installed calculated ratings of user's productivity	✓	✗
Inactivity time calculation (absence of user activity while the PC is switched on and locked)	✓	✗
Working days calendar, holidays and working hours customization for the employees	✓	✓
Calculation of users activity in certain websites and applications that are related to the employee's activities	✓	✓
Customization of group of productive and unproductive application and website categories for the employees	✓	✓
Pre-installed list of default categories containing the most popular websites and applications	✓	✓
Employee's timesheets for the dates when the employee was present at work (discipline analysis)	✓	Partially
User remote work connections detection	✓	✓
Advanced reports with activity classification and user's structured timesheets	✓	Partially

DLP extensions. Screen Photo Detection endpoint module.

	ZECURION	safetica
AI based tools to detect mobile phone frame in web camera screenshots images on user's PC	✓	✗
Incident creation at the time of user's attempts of making photo	✓	✗
Possibility to detect web-camera sheltering	✓	✗
Possibility to create and save screenshot of user's PC workspace at a time of making photo	✓	✗
Management of PC's web-camera screenshots making frequency (time per 1,2,3 …n seconds)	✓	✗
Ability to block user's AD credentials in corp domain in case of making photo of the computer monitor	✓	✗
Possibility to create pop-up bubble warning message in system tray in user's PC	✓	✗
Possibility to identify full context of the event (user name, computer name etc)	✓	✗
Assign risk scoring and ГИФ changes for this user-offender	✓	✗

DLP extensions. DCAP monitoring and analysis capabilities

	ZECURION	safetica
Ability to install monitoring module in user's PC	✓	✗
Ability to install monitoring module on corp file server	✓	✗
On-the-fly monitoring for the selected target files or folders in PC, shared folders on file server	✓	✗
Ability to install monitoring module in corp MS AD server	✓	✗
On-the-fly monitoring of changes made by system admins in MS Active Directory	✓	✗
On-premise NextCloud instance support	✓	✗
On-premise NetApp server hardware storage support	✓	✗
On-premise Dell server hardware storage support	✓	✗
Data classification capabilities using active DLP policies	✓	✗
One single endpoint agent with DLP and DCAP component	✓	✗

DLP extensions. DCAP reporting tools and data analysis

	ZECURION	safetica
Ability to integrate DCAP dashboard of monitored user in his system profile in DLP management web console	✓	✗
Preinstalled library which contains more than 150 prebuild out of the box reports (users, channels, folders/files etc)	✓	✗
Quick summary events log section for selected files and folders in web management console	✓	✗
User's cumulative file/folders access summary report	✓	✗
File duplicates identification summary report	✓	✗
Detection of massive file operations on endpoint PC	✓	✗
Detections of the source of file which is being copied	✓	✗
Access rights summary for inspected files and folders	✓	✗
Reporting tool of changes made by system admins in MS Active Directory	✓	✗

System Management tools and capabilities for security officers and sysadmins

	ZECURION	safetica
Single unified web-console for Operators and Sys Admins	✓	1 web console for operators and 1 desktop thick console for sys admins
Multi-factor authentication (MFA) for authorization	✓	✓
“Dark Style” mode for operator’s eye saving	✓	✗
Setting alerts and notifications using private Telegram bot	✓	✗
Web console widget management and customization	✓	✓
Deploy and upgrade endpoint through own Installation server / console in Windows and Linux environment	✓	Only for Windows PC
Deep granular separation of administrator roles and ACLs for certain web-panels and reports	✓	Partially
Incident response platform (IRP) task tracker for teams	✓	✗
Incident response platform (IRP) customizable workflow templates	✓	✗
Ability to unload and backup all settings to a structured XML file	✓	✗

Reporting tools for security officers. User-centric data organization model.

	ZECURION	safetica
User-centric data organization and visualization. Unified user's profile with tabs and data mining capabilities in one place	✓	✗
Tabular customizable reports in web-console	✓	✓
List of incidents (violence) in a table with the ability to view their contents, metadata and context	✓	Partially
Unified graphic reports and dashboards in console	✓	✓
User connections\communication graph diagram in user personal profile	✓	✗
User emotional status diagrams timeline in user profile	✓	✗
User Behavior Analytics based on composite everyday indicator (incidents, files, traffic volume etc.)	✓	✗
Ability to compare current UBA rates with historical data for previous period	✓	✗
Risk-based assessment engine for the monitored staff	✓	Partially
Ability to calculate daily risk score dynamic for the last month	✓	✗

Reporting tools for security officers. Diagrams and monitoring tools

	ZECURION	safetica
Anomalies detection tool (with preinstalled library of cases)	✓	✗
User's anomalies notification	✓	✗
Comparison dashboard for selected employees and departments	✓	✗
Live monitoring of user session with web camera snapshots	✓	✗
Live monitoring of user session with desktop online access on endpoints	✓	✗
Chat-like report to display captured dialogues between persons in different instant messengers	✓	✗
Administrators logging tool (logons, sessions)	✓	✓
Detect and trace the changes in the list of installed software on the PC, and its hardware configuration	✓	✗
Export reports and rows to expropriated HTML file	✓	✗
Report export tool to PDF, XLSX, CSV, PST file formats	✓	Partially

Sysadmin management tools. Policy management and tools in the Policy Server

	ZECURION	safetica
One single unified Policy Server for policy creation and deployment to all modules and endpoint agents	✓	✓
Policy orientated deployment approach: Target Channel -> Filtering Condition -> System full-auto Reaction	✓	✓
Modern SWG/NGFW-like policy creation interface	✓	✓
Omni-policy concept. One single policy can be deployed in all target channels and crawler modules	✓	✓
Multi-level condition section to combine filtering expression with AND, OR, NOT Boolean operators in policies	✓	Partially
Possibility to turn on\off physical blockage mode for selected policy in selected channels in “one click”	✓	✓
Online/offline policies (inside/outside corp network)	✓	✗
Endpoint agent by request suspending mode	✓	✓
Manual tracert option to check agent-server connection	✓	✓
Run an attached script or specific application in policy	✓	✗

System requirements and platforms

	ZECURION	safetica
Server modules and components OS requirements	Windows Server 2008 R2 and all later, Ubuntu Linux 22.04	Windows Server 2016 and later.
OS support by DLP endpoint agents	Windows 7 and all later, Windows Server 2008 R2 and all later; Linux Ubuntu 18\20\22\24, Linux Debian;	Windows 10/11 macOS 12
Supported SQL Repositories	Microsoft SQL, PostgreSQL	Microsoft SQL