Next Generation Data Loss Prevention
الجيل الجديد من أدوات منع تهريب الوثائق

Table of Contents جدول المحتويات

What is new in Next Gen DLP? ما هو المميز في الجيل الجديد من أدوات منع تهريب الوثائق؟

Zecurion is a next generation DLP which differs from Legacy DLP systems (such as Forcepoint, WatchGuard, Microsoft, Symantec) by:

تعتبر زكوريون من منتجات الجيل الجديد لأدوات منع فقدان البيانات والتي تختلف عن الأنظمة التقليدية القديمة مثل فورس بوينت وسيمانتك وواتش جارد ومايكروسوفت وغيرها كما يلي:

* Zecurion covers more channels of leakage. Traditional channels of leaking include USB, Dropbox, email attachment, Whatsapp web, etc.

* تغطي زكوريون المزيد من قنوات التسرب. تشمل قنوات التسريب التقليدية USB، وDropbox، ومرفقات البريد الإلكتروني، وWhatsApp web، وما إلى ذلك.

* Zecurion covers when someone tries to take a photo of the screen to capture the document using his cell or read it to someone else. Zecurion uses AI for that.

* كما تمنع تقنيات زكوريون عندما يحاول شخص ما تصوير الشاشة لالتقاط صورة للمستند الرقمي باستخدام هاتفه الخلوي أو قراءتها لشخص آخر. تستخدم شركة زكوريون الذكاء الاصطناعي لذلك.

* Zecurion has its own data Classification tool, while legacy ones use 3rd party tools such Boldon James, Get Visibility, Titus, etc.

* تمتلك زكوريون أدوات تصنيف البيانات الخاصة بها، بينما تستخدم اللأنظمة القديمة أدوات تابعة لجهات خارجية مثل بولدن جيمس و جيت فيسيبيليتي وتايتاس وما إلى ذلك.

* Zecurion has its own digital watermark technology. It does not require 3rd party tools such as Data Patrol or Seclore. While older systems need these 3rd party tools.

* تمتلك زكوريون تقنية العلامة المائية الرقمية الخاصة بها. لا يتطلب ذلك أدوات خارجية مثل داتا باترول أو سيكلور. بينما تحتاج الأنظمة القديمة إلى أدوات الطرف الثالث هذه.

* Zecurion has DLP, Staff Control, and Behavioral Analysis together in one platform. Zecurion monitors behavior to detect potential cyber threats, such as document leakage.

* توفر شركة زكوريون أدوات منع فقدان البيانات ومراقبة الموظفين والتحليل السلوكي معًا في منصة واحدة. تقوم تقنيات زكوريون بمراقبة السلوك للكشف عن التهديدات السيبرانية المحتملة، مثل تسرب المستندات.

* It gives you control of what employees are doing. It monitors behavior, and it alerts administrators when something suspicious happens before documents leaking starts.

* بما يمنح العميل السيطرة على ما يفعله الموظفون. فهو يراقب السلوك، وينبه المسؤولين عند حدوث شيء مريب قبل أن يبدأ تسرب المستندات.

* Zecurion provides DCAP (Document Centric Audit and Protection) capabilities to track documents and monitor their lifecycle.

* توفر زكوريون إمكانات DCAP (التدقيق والحماية المرتكزة على المستندات) لتتبع المستندات ومراقبة دورة حياتها في كل البيئة الرقمية الخاصة بالعميل.

* All of these modules are managed through one interface - single pane of glass.

* تتم إدارة كل هذه الوحدات من خلال واجهة واحدة - لوح زجاجي واحد.

Zecurion Next Generation DLP Features مكونات الجيل الجديد من أدوات
منع تهريب الوثائق من زكوريون

Screen Photo Detection (AI Based) الحماية من تصوير الشاشة / الوثيقة الإلكترونية عبر الهاتف الجوال - بالذكاء الاصطناعي

This unique AI-based feature changes the game, stopping the insiders (Employees or others) that Zecurion stops from taking photos of the electronic documents with their phones. These were not previously being stopped by other tools.

تعمل هذه الميزة الفريدة المستندة إلى الذكاء الاصطناعي على تغيير قواعد اللعبة، حيث توقف الموظفين أو أي أحد من الدخلاء الذين يحاولون تصوير الوثائق الإلكترونية عبر هواتفهم.
هؤلاء الذين لم يتمكن أي نظام آخر في السابق من الإمساك بهم.

Whenever someone tries to photograph a screen by the smartphone, Zecurion DLP immediately detects it via webcam and blocks the computer (on-the-fly logout).

عندما يحاول شخص ما تصوير شاشة باستخدام الهاتف الذكي، تكتشف تقنية زكوريون ذلك على الفور عبر كاميرا الويب ويتم حظر الكمبيوتر (تسجيل الخروج مباشرة).

The revolutionary technology uses 2 neural networks to ensure reliable smartphone detection and flags cybersecurity incidents in a blink of an eye (from 0.06 seconds).

تستخدم هذه التقنية الثورية شبكتين عصبيتين من الذكاء الاصطناعي لضمان اكتشاف موثوق للهواتف الذكية والإبلاغ عن حوادث الأمن السيبراني وعن محاولات تصوير الوثائق في غمضة عين (من 0.06 ثانية).

It uses the PC/Laptop web camera to detect attempts to take photos of the screen through a smartphone.

ويستخدم كاميرا الويب للكمبيوتر الشخصي/الكمبيوتر المحمول لاكتشاف محاولات التقاط صور للشاشة من خلال الهاتف الذكي.

It provides multiple options to react to such attempts (alerting the cyber security officer, saving webcam image, blocking user account in Active Directory).

ويوفر خيارات متعددة للرد على مثل هذه المحاولات (تنبيه مسؤول الأمن السيبراني، وحفظ صورة كاميرا الويب، وحظر حساب المستخدم في Active Directory).

In case the web camera is not working, then the system will have a “camera is not working” alarm without blocking the computer.

في حالة عدم عمل كاميرا الويب، سيصدر النظام إنذار "الكاميرا لا تعمل" دون حجب جهاز الكمبيوتر.

The system supports recording the user’s voice as evidence of leakage through a call.

يدعم النظام تسجيل صوت المستخدم كدليل على التسرب من خلال المكالمة.

Built-in Staff Control Module نظام مراقبة الموظفين المدمج

Documents do not leak by themselves. They leak because a staff member (insider) decided to leak them intentionally or by mistake.

الوثائق لا تتسرب من تلقاء نفسها. إنها تتسرب لأن أحد الموظفين (من الداخل) قرر تسريبها عن قصد أو عن طريق الخطأ.

This is why we need a risk score for each staff member through behavioral analysis to anticipate such risks.

ولهذا السبب نحتاج إلى درجة المخاطر لكل موظف من خلال التحليل السلوكي لتوقع مثل هذه المخاطر.

Staff Control provides User Behavioral Analysis (UBA). It provides UBA Index for each user.

يوفر التحكم في الموظفين تحليل سلوك المستخدم (UBA). ويوفر مؤشر UBA لكل مستخدم.

It provides fast risk-based assessment, user connection diagrams, and detection of anomalies (such as activities during holidays, first remote connection, first use of a new device, etc.).

وهو يوفر تقييمًا سريعًا قائمًا على المخاطر، ومخططات اتصال المستخدم، واكتشاف الحالات الشاذة (مثل الأنشطة أثناء العطلات، وأول اتصال عن بعد، والاستخدام الأول لجهاز جديد، وما إلى ذلك).

It has monitoring and control capabilities that include keyboard recording tools, workspace screenshots, microphone recording, webcam recording, application control, and passwords/accounts capturing.

يتمتع بإمكانيات المراقبة والتحكم التي تشمل أدوات تسجيل لوحة المفاتيح ولقطات شاشة مساحة العمل وتسجيل الميكروفون وتسجيل كاميرا الويب والتحكم في التطبيقات والتقاط كلمات المرور/الحسابات.

Staff Control keeps track of working hours, logs employees' actions at workplaces, and evaluates

يقوم نظام مراقبة الموظفين بتتبع ساعات العمل، ويسجل تصرفات الموظفين في أماكن العمل، ويقيم الكفاءة.

the efficiency. The module checks the activities of personnel for compliance with corporate standards and safety policies.

تتحقق الوحدة من أنشطة الموظفين للتأكد من امتثالها لمعايير الشركة وسياسات السلامة.

* Employee card. Each dossier contains detailed information on efficiency and activity at the workplace in dynamics. The Administrator can also review staff incidents in a convenient format.

* بطاقة الموظف. يحتوي كل ملف على معلومات مفصلة عن الكفاءة والنشاط في مكان العمل في الديناميكيات. يمكن للمسؤول أيضًا مراجعة حوادث الموظفين بتنسيق مناسب.

* Report designer with 15 indicators. Now reports include a table with fast filters, groups, and data from up to tens of thousands of PCs.

* مصمم التقارير مع 15 مؤشرا. تتضمن التقارير الآن جدولاً يحتوي على عوامل تصفية سريعة ومجموعات وبيانات من ما يصل إلى عشرات الآلاف من أجهزة الكمبيوتر الشخصية.

* Resource usage and timesheets. Suggests detailed information on websites, applications running, and activity period.

* استخدام الموارد والجداول الزمنية. يقترح معلومات مفصلة عن مواقع الويب والتطبيقات قيد التشغيل وفترة النشاط.

Built-in Data Classification Engine محرك تصنيف البيانات المدمج

The Zecurion Data Classification Engine uses keywords and dictionaries, templates, regular expressions, and digital footprints to simplify the classification work.

يستخدم محرك تصنيف البيانات لدى شركة زكوريون الكلمات الرئيسية والقواميس والقوالب والتعبيرات العادية والبصمات الرقمية لتبسيط أعمال التصنيف.

It deploys different machine learning and artificial intelligence algorithms such as:

يستخدم النظام خوارزميات مختلفة للتعلم الآلي والذكاء الاصطناعي مثل:

* Bayes (a set of procedures to “directly” obtain the posterior predictive distribution of the outcomes in the (testing) data without first obtaining the posterior distribution of the parameters given the (training) data).

* بايز (مجموعة من الإجراءات للحصول "مباشرة" على التوزيع التنبؤي الخلفي للنتائج في بيانات (الاختبار) دون الحصول أولاً على التوزيع الخلفي للمعلمات في ضوء بيانات (التدريب)).

* Support Vector Machines (SVM: a supervised machine learning algorithm that classifies data by

* دعم آلات المتجهات (SVM: خوارزمية تعلم آلي خاضعة للإشراف تقوم بتصنيف البيانات من خلال العثور على خط مثالي

finding an optimal line or hyperplane that maximizes the distance between each class in an N-dimensional space).

أو سطح فائق يزيد المسافة بين كل فئة في مساحة ذات أبعاد N).

* AI-Based Image Templates.

* قوالب الصور المبنية على الذكاء الاصطناعي.

The data classification engine has its OCR (Optical Character Recognition).

يحتوي محرك تصنيف البيانات على OCR (التعرف البصري على الأحرف).

Built-in Digital Watermark العلامة المائية الرقمية المدمجة

The Device Control also provides Digital Watermark capabilities.

يوفر التحكم في الجهاز أيضًا إمكانات العلامة المائية الرقمية.

Digital watermarking is a potent tool for protecting intellectual property and copyrighted material. It is a marker embedded in digital content material, typically used to identify the source and ownership of copyrighted material.

تعد العلامة المائية الرقمية أداة فعالة لحماية الملكية الفكرية والمواد المحمية بحقوق الطبع والنشر.
وهي عبارة عن علامة مضمنة في مادة المحتوى الرقمي، تُستخدم عادةً لتحديد مصدر وملكية المواد المحمية بحقوق الطبع والنشر.

Built-in Investigation Workflow Automation أتمتة سير عمل التحقيق المدمج

This module is part of the device control module.

هذه الوحدة هي جزء من وحدة التحكم في الجهاز.

This module simplifies investigations and shortens the incident response cycle. It minimizes the cybersecurity team workload by providing a 360°

تعمل هذه الوحدة على تبسيط التحقيقات وتقصير دورة الاستجابة للحوادث. فهو يقلل من عبء عمل فريق الأمن السيبراني من خلال توفير عرض 360 درجة للمهام الفعلية مع جميع الحالات

والبيانات في مرحلة التحقيق والمنفذين والمواعيد النهائية.

view of actual tasks with all the statuses, data on the investigation stage, executants, and deadlines.

أثناء التحقيق، يمكن لأعضاء فريق الأمن السيبراني ترك تعليقات على المهمة ومناقشة التقدم مع المشاركين الآخرين (من CISO إلى المحلل)، وإرفاق المستندات والحوادث كدليل.

During the investigation, cybersecurity team members can leave comments on the task and discuss progress with other participants (from CISO to analyst), attach documents and incidents as proof.

Built-in DCAP (Document Centric Audit and Protection) Module التدقيق والحماية المرتكزة على المستندات المدمج

يراقب تغييرات الملفات وتصنيفها ووصول المستخدم ويوفر تسجيل تغييرات ACL (قوائم التحكم في الوصول).

Monitors files changes, classification, user access, & provides ACL (Access Controls Lists) changes logging.

وهو يوفر مراقبة سريعة للملفات والمجلدات وتسجيل الأنشطة.

It provides on-the-fly files and folders monitoring and activities logging.

Zecurion Traditional DLP Features المكونات التقليدية في أدوات منع فقدان البيانات من زكوريون

Traffic Control Web / Mail (Data in Motion) - التحكم في حركة مرور البيانات عبر الويب/البريد البيانات المتحركة

Monitors traffic and controls flow of data across more than a 100 devices to minimize the intentional or inadvertent data loss.

يراقب حركة مرور البيانات ويتحكم في تدفق البيانات عبر أكثر من 100 جهاز لتقليل فقدان البيانات المتعمد أو غير المقصود.

It provides traffic control of internet channels such as SMTP email, webmail, social networks, messengers, cloud, etc.

يوفر التحكم في حركة المرور لقنوات الإنترنت مثل البريد الإلكتروني SMTP وبريد الويب والشبكات الاجتماعية والمراسلين والسحابة وما إلى ذلك.

This covers SSL web and Instant Messaging traffic monitoring and blockage - both on endpoint and gateway levels (MITM and browser API Level).

يغطي هذا مراقبة حركة مرور ويب SSL والمراسلة الفورية وحظرها - سواء على مستوى الأجهزة الطرفية أو البوابة (MITM ومستوى واجهة برمجة التطبيقات للمتصفح).

Instant messaging tools captured include: Skype, Teams, Viber, Lync, WhatsApp, Telegram, Discord, and Zoom.

تتضمن أدوات المراسلة الفورية التي تم التقاطها: Skype وTeams وViber وLync وWhatsApp وTelegram وDiscord وZoom.

It also supports modern cloud services such as Office 365 and Google Docs.

كما أنه يدعم الخدمات السحابية الحديثة مثل Office 365 وGoogle Docs.

It can integrate with Secure Web Gateways over ICAP Protocol. It has options for endpoint and gateway-based deployments.

يمكن أن يتكامل مع بوابات الويب الآمنة عبر بروتوكول ICAP. لديها خيارات لعمليات التركيب المستندة إلى الأجهزة الطرفية والبوابة.

Device Control for Endpoints (Data in Use) التحكم بالاجهزة - البيانات قيد الاستخدام

Guarantees granular approach to limit access and protect data without hindering legitimate use.

يضمن اتباع نهج دقيق للحد من الوصول إلى البيانات وحمايتها دون إعاقة الاستخدام المشروع.

It provides content-based policies and data classification with granular access control lists (ACL) for used peripheral devices connections.

فهو يوفر سياسات قائمة على المحتوى وتصنيفًا للبيانات مع قوائم التحكم في الوصول الدقيقة (ACL) لاتصالات الأجهزة الطرفية المستخدمة.

It provides the ability to encrypt copied files on removable drives on-the-fly to prevent using the files.

فهو يوفر القدرة على تشفير الملفات المنسوخة على محركات الأقراص القابلة للإزالة أثناء التنقل لمنع استخدام الملفات.

The policies set will be synchronized with local stand alone endpoints with advanced capturing options such as keyboard text, web camera, screenshots, etc.

ستتم مزامنة مجموعة السياسات مع نقاط النهاية المحلية المستقلة مع خيارات الالتقاط المتقدمة مثل نص لوحة المفاتيح وكاميرا الويب ولقطات الشاشة وما إلى ذلك.

The deployment and management can be centralized.

يمكن أن يكون التركيب والإدارة مركزيين.

Discovery Crawler (Data in Rest) مكتشف البيانات الزاحف - البيانات في التخزين

Finds improperly stored sensitive data at local drives, shared folders, MS SharePoint, MS Exchange, and any database using ODBC, to take action before it’s lost or stolen.

يبحث عن البيانات الحساسة المخزنة بشكل غير صحيح على محركات الأقراص المحلية والمجلدات المشتركة وMS SharePoint وMS Exchange وأي قاعدة بيانات تستخدم ODBC، لاتخاذ الإجراء المناسب قبل فقدانها أو سرقتها.

It provides the ability to scan all possible storage locations with flexible scan parameters for selected computers or organizational units.

فهو يوفر القدرة على فحص جميع مواقع التخزين الممكنة باستخدام معلمات فحص مرنة لأجهزة الكمبيوتر أو الوحدات التنظيمية المحددة.

It also provides real-time discovery, scanning file on close, file flow tracking inside the local area network (LAN).

كما أنه يوفر اكتشافًا فوريًا ومسحًا ضوئيًا للملفات القريبة وتتبع تدفق الملفات داخل الشبكة المحلية (LAN).

It has the ability to remove files violating the organization’s policy to be removed from local hard drives.

لديه القدرة على إزالة الملفات المخالفة لسياسة المؤسسة لإزالتها من محركات الأقراص الثابتة المحلية.