ZECURION

ZECURION DLP

DATASHEET

www.zecurion.com

PROPOSITO DEL DLP

Los datos son el verdadero valor de los negocios. La propiedad intelectual, los datos financieros, la información estratégica, y la información sensible personal de los clientes y empleados son los más valiosos activos que tiene su compañía - y esos datos están en riesgo. Las compañías de todos los tamaños y de todas las industrias pierden datos todos los días. Esto podría resultar de un robo no intencional o una exposición accidental, y el perpetrador podrían podría ser un atacante externo o un empleado en quien se confía. El propósito del DLP (Data Loss Prevention) es proveer una solución para proteger su propiedad intelectual, secretos comerciales y otros datos sensibles. Esto ayuda a ejecutar y mantener cumplimiento con las regulaciones como HIPAA, PCI DSS, y GDPR, y le da la herramienta que usted necesita para prevenir fraude interno y conducir auditorías internas e investigaciones forenses.

LA VENTAJA DE ZECURION DLP

Sus datos son cruciales, y requieren la mejor protección. Es por esto por lo que usted debe escoger Zecurion DLP. Zecurion ha estado ranqueado en el cuadrante mágico de Gartner de DLP empresarial desde 2014. Zecurion fue también listado como uno de los 7 top vendors por IDC en el 2018 y fue incluido por Forrester en el reporte de 2019 DLP Now Tech.

Zecurion DLP es una solución costo-efectiva, simple y completa. Zecurion DLP ofrece una integración rápida con la infraestructura empresarial – hasta 4 veces más rápida que una implementación de DLP empresarial. Una vez implementado, almacena todos los eventos, archivos, y documentos y provee UBA (user behavior analytics) para detectar en forma proactiva amenazas. Zecurion DLP además reduce la carga de trabajo para los equipos de seguridad y simplifica la gestión diaria con reportes interactivos, graficas, y tablas que proveen una valoración a la vista de su postura de protección a sus datos.

Zecurion DLP está en uso actualmente en organizaciones alrededor del mundo con más de 100,000 usuarios. Los clientes de Zecurion han ganado más de 40 demandas con la ayuda de la evidencia recogida para los litigios contra los “enemigos internos”.

Más que creernos, mire lo que dicen los clientes de Zecurion:

”

VP, Servicios Profesionales y Operaciones Globales, Industria de servicios:

«La experiencia general con Zecurion fue excelente, incluyendo el soporte detallado preventa y postventa en el área de New York.»

”

Director del departamento, Industria de Energía y servicios:

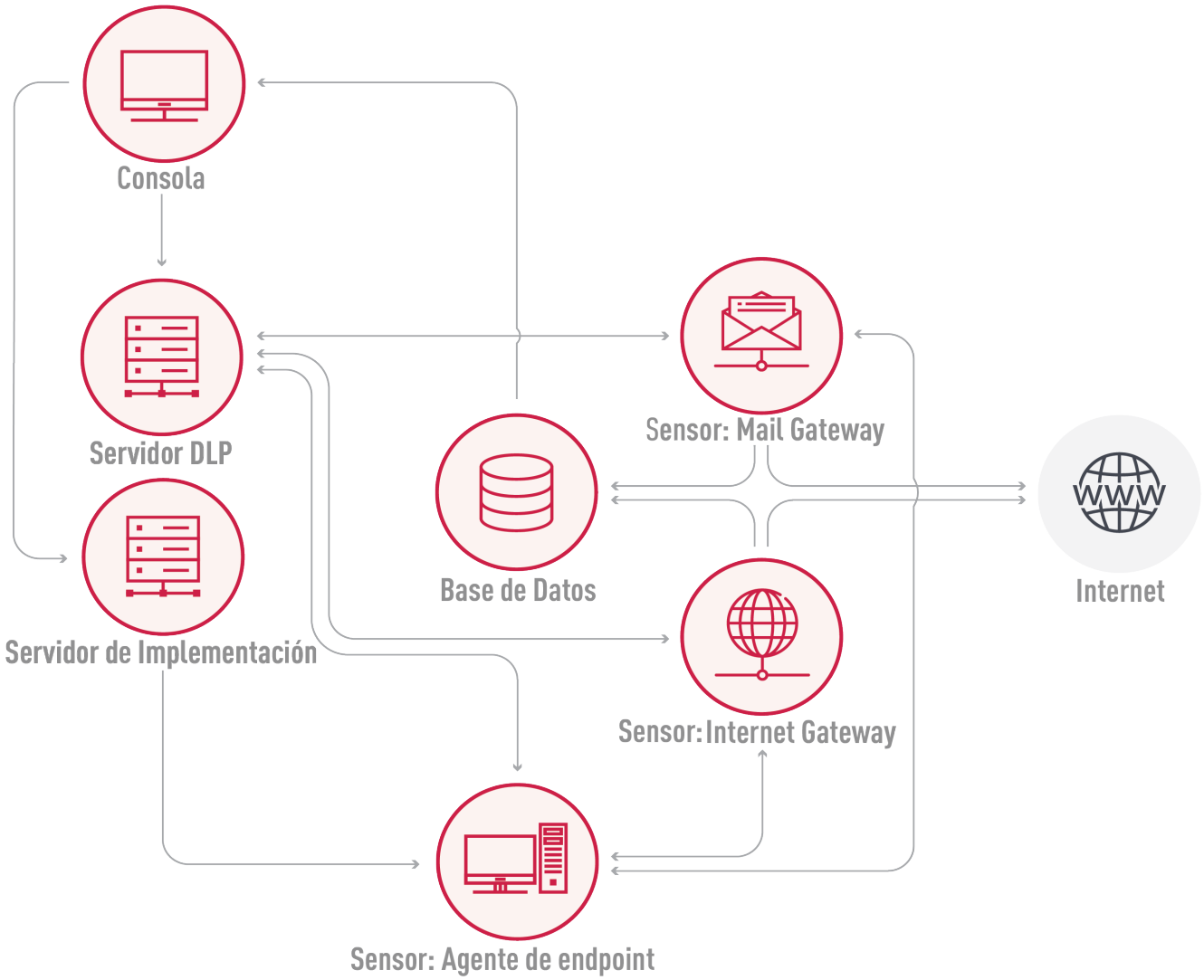
«Podemos asegurar que Zecurion DLP protege la información exitosamente de fugas.»

”

CSO de la industria Financiera

«Usamos productos líderes en sus segmentos. Por lo tanto, escogimos Zecurion.»

ARQUITECTURA DE ZECURION DLP



Sensores: interceptan los canales de transferencia de datos, datos recolectados interceptados, validación de directivas DLP

Archivo: almacena todos los datos interceptados, habilita la respuesta a incidentes y la investigación, el análisis retrospectivo, por ejemplo, aplicar la nueva directiva a los datos históricos (almacenados en MS SQL o Postgree SQL)

Servidor DLP: almacena la configuración y directivas, se las transfiere a los sensores, monitorea sensores

Servidor de Implementación: implementa los sensores y los agentes de endpoint

Consola: gestión flexible basada en web para directivas y reportes

OPCIONES DE IMPLEMENTACIÓN

Cada ambiente de cliente es una mezcla única de segmentos de redes, tipos de endpoint y sistemas operativos, y plataformas diferentes y aplicaciones. Las organizaciones necesitan poder proteger datos a través del ecosistema total con un impacto mínimo de rendimiento y productividad. A la vez, una visibilidad comprensiva y efectiva de la prevención de pérdida de datos confiando en poder monitorear y analizar cada actividad. Zecurion provee un rango diverso de opciones de implementación para asegurar que sus datos son monitoreados y protegidos sin importar como se vea su infraestructura de red.

OPCION DE IMPLEMENTACION	CANALES CONTROLADOS	ACCION
SPAN port mirroring	SMTP, IMAP, POP3, HTTP, FTP	Detectar
IServidor ICAP Servidor TMG	HTTP/HTTPS	Detectar y bloquear
Agente de control de tráfico (endpoint)	HTTP/HTTPS	Detectar y bloquear
	Correo (SMTP, IMAP, POP3), FTP, mensajerías	Detectar
Zecurion SWG	HTTP/HTTPS	Detectar y bloquear
	FTP	Detectar
MS Exchange plugin	Correo (incluyendo interno)	Detectar y bloquear
SMTP proxy	Correo (SMTP)	Detectar y bloquear
SMTP journal Casillas de correo (POP3, IMAP, Exchange HTTPS)	Correo	Detectar
Agente de control de dispositivos (endpoint)	USB Impresoras Dispositivos removibles	Detectar y bloquear
	CD/DVD RDP disks, clipboard	Detectar
	Pantalla Clipboard Teclado Micrófono	Detectar / Grabar
Agente de descubrimiento (endpoint)	Escaneo de drives locales Drive local en tiempo real	Detectar
Servidor de descubrimiento	Folder compartido de red MS SharePoint MS Exchange Cualquier DB	Detectar

PRINCIPALES CARACTERISTICAS DE ZECURION DLP

Zecurion DLP entrega lo que usted necesita para controlar canales de fuga, monitorear la manipulación de datos de los empleados y prevenir fuga de datos.

Control sencillo de canales de fuga de datos. Controle todos los posibles canales de fuga de datos para minimizar el riesgo de una fuga de datos y asegurar el cumplimiento de los requerimientos regulatorios.

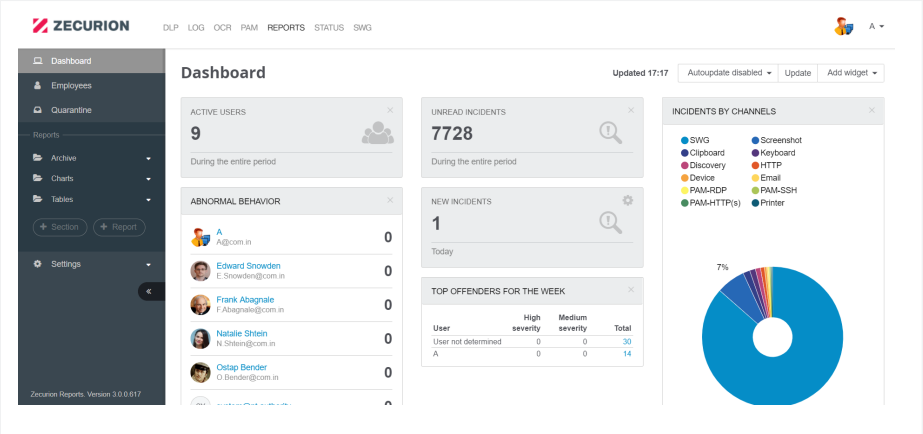
Reglas y directivas flexibles. Configure una directiva para algunos o todos los canales de transferencia y use una variedad de técnicas de detección de contenido y condiciones de datos para predecir y prevenir cualquier escenario de fuga datos.

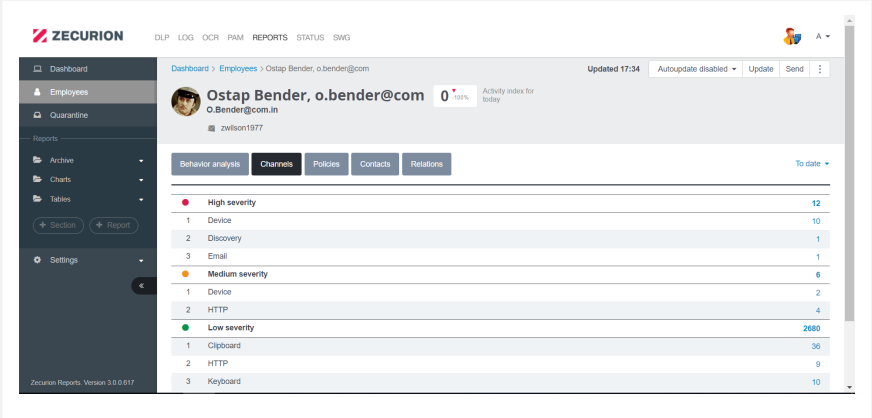
Extracción de contenido de archivo. Con la detección automática de archivos para más de 500 formatos de archivos basados en su estructura interna y no por su extensión, así como la posibilidad de reconocer archivos cifrados y desempaquetarlos, incluyendo archivos anidados; no hay datos que se escapen de la red sin análisis.

Una sola consola. Zecurion DLP provee una consola web para todos los módulos y un tablero personalizable de reportes para administración centralizada remota que es simple y sencilla.

Archivado de mensajes y documentos. Todos los datos interceptados— archivos, mensajes, incidentes, eventos y más— se almacenan en una DB así que se tiene todo los necesario para generar reportes detallados, ejecutar investigaciones forenses comprensivas, y recolectar la evidencia para las acciones legales.

Catalogo inteligente de empleados. Recolecte e indexe todos los datos de los empleados: dirección de correo, redes sociales y cuentas de mensajerías instantáneas para asegurar toda la comunicación es atribuida a un usuario específico.





User behavior analysis. Calcula perfiles de comportamiento para todos los usuarios y habilita la detección de actividad anómala. En forma proactiva alerta la detección de amenazas al equipo de seguridad y provee prevención temprana de fugas de datos.

Mapa de conexiones de usuario. Zecurion DLP desarrolla diagramas navegables de conexiones de usuarios y canales de comunicación para detectar conexiones ocultas y le permite analizar comunicaciones sospechosas que podrían sugerir fraude interno o una fuga de datos.

Poderosos reportes. Más de 20 reportes preconfigurados y opciones de personalización proveen una herramienta poderosa para la auditoría de seguridad e investigación. Se puede generar y analizar fácilmente reportes, y rápidamente expandir detalles de un incidente específico en unos cuantos clics.

Registro de eventos. Automáticamente registre todos los eventos internos y acciones del administrador para un fácil mantenimiento y trazabilidad rápida de cualquier asunto que se presente.

Integración con Directorio Activo. Usuarios, Grupos y nombres de computadores se sincronizan del directorio activo para dar una mejor integración con su infraestructura IT y permitir que Zecurion DLP identifique usuarios por nombre en los incidentes y reportes para simplificar la administración.

REST API. La mayoría de las tareas de administración y monitoreo están disponibles a través de solicitudes REST API HTTP para permitir la automatización de la seguridad y la automatización con otras herramientas y plataformas en su infraestructura IT.

Características Avanzadas

Grabación de micrófono

Convierta cualquier PC o laptop en un sistema de vigilancia de audio al grabar del micrófono de cualquier computador en cualquier momento.

Grabación de pantallazos y teclado

Se pueden grabar todas las digitaciones de usuarios designados o grupos y guardar pantallazos de cualquier computador a intervalos definidos, usted siempre sabrá los que hacen sus empleados y podrá reforzar la seguridad interna y la manipulación de directivas para detectar y prevenir fugas potenciales de datos.

Control de aplicaciones

Elimine el riesgo de que los empleados usen aplicaciones peligrosas (clientes TOR y Torrent, anonimizadores, juegos). Se puede restringir que aplicaciones se permite usar creando una lista blanca (o negra) de aplicaciones para un grupo específico de usuarios o grupos.

TECNICAS DE DETECCION DE CONTENIDO

Zecurion DLP usa una variedad de técnicas de detección para dar una prevención comprensiva de pérdida de datos. Sin importar si los datos están siendo robados o comprometidos intencionalmente o expuestos sin intención, una de estas técnicas de detección de contenido lo encontrará:

Palabras claves y diccionarios

Esta técnica busca las concordancias exactas para palabras designadas. Un administrador de IT o un oficial de seguridad puede crear un diccionario para cualquier asunto o categoría, tal como documentos de salud, documentos financieros, búsquedas de trabajo, etc., e incluir las palabras que serán señaladas. Hay más de 30 diccionarios predefinidos incluidos en el Sistema por defecto.

Plantillas y expresiones regulares

Algunos datos sensibles siguen una estructura predefinida o un formato que puede ser usado para identificarlos y detectarlo números de tarjetas de crédito, números de documentos de identidad, cuentas IBAN, URLS, direcciones de correo y otros datos similares que pueden ser detectados usando plantillas y expresiones regulares

Huellas Digitales

Al recolectar una cantidad de documentos de una categoría o tipo específico e incluirlos en Zecurion DLP, se crea una huella digital que puede detectar documentos exactos o sus partes. Una vez que la huella digital se crea, Zecurion DLP puede identificar cualquier documento de un conjunto o alguna parte, o combinación de partes del conjunto de documentos. Nuevos documentos pueden agregarse a la colección y Zecurion DLP actualizará automáticamente las huellas digitales.

Machine learning

Otra técnica similar a las huellas digitales es el uso de machine learning. La configuración inicial es similar – incluir un conjunto de archivos a Zecurion DLP para ser analizados. Donde las huellas digitales detectan una concordancia exacta de contenido, machine learning se puede usar para detectar documentos que son similares a los del conjunto suministrado basado en palabras claves y/o indicadores de semántica.

Plantilla de imágenes

Las plantillas de imágenes son efectivas para detectar elementos como firmas, estampillas, encabezados de cartas o documentos con una estructura definida como pasaportes o documentos de identidad. Este método es además similar a las huellas digitales, pero en vez de detectar un texto específico, se detecta patrones de imagen. Similar a las huellas digitales y al machine learning, la configuración inicial requiere un conjunto de archivos que Zecurion DLP pueda analizar y desarrollar el reconocimiento necesario para detectarlos luego.

OCR (Optical Character Recognition)

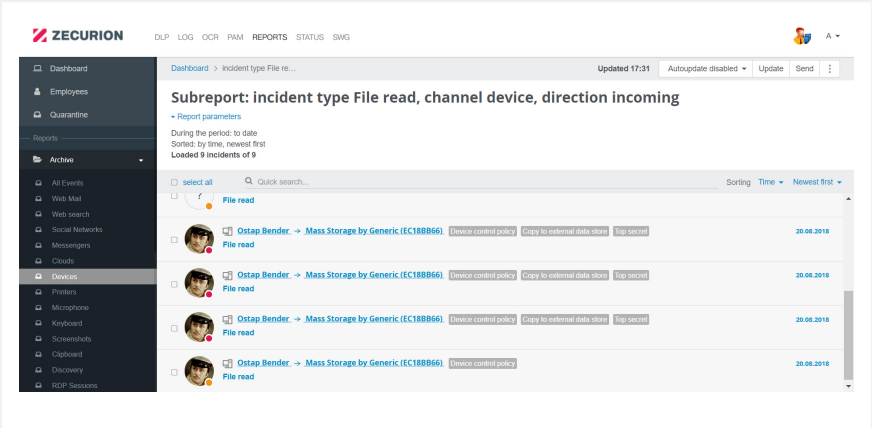
Esta técnica es valiosa para identificar datos sensibles o confidenciales que han sido de alguna forma escaneados o fotografiados intentado evitar otros métodos de detección. Zecurion DLP usa motores de reconocimiento de terceros para extraer texto de los documentos escaneados. Zecurion DLP se integra con ABBYY FineReader y con Google Tesseract para extraer e identificar texto de cualquier imagen.

CONTROL DE DISPOSITIVOS

Dispositivos tales como discos duros externos o USBs pueden volverse un riesgo significativo cuando se habla de pérdida de datos. La tecnología ha evolucionado al punto donde aún las pequeñas tarjetas microSD puede almacenar 1TB de datos. Un empleado inconforme pudiese fácilmente robar gigabytes o terabytes de datos y llevarlos en su bolsillo. Los datos en los dispositivos portátiles ponen en riesgo aún a los empleados leales, ya que sus dispositivos pudiesen ser robados o perdidos.

En muchos casos los dispositivos portátiles de almacenamiento y otros dispositivos pueden ser parte crucial de trabajar efectiva y eficientemente, y bloquear todos los accesos a puertos USBs puede ser muy restrictivo e impactar negativamente la producción.

Zecurion DLP le da la siguiente forma de control de dispositivos granular para que pueda limitar el acceso y proteger sus datos sin impedir le uso legítimo de los dispositivos:



Control de acceso flexible y granular para dispositivos periféricos

Se puede habilitar sólo dispositivos aprobados o entregados por la compañía o habilitar sólo los dispositivos que son considerados necesarios para el negocio con las directivas de control que puede garantizar o negar el acceso basados en tipo, clase, fabricante, modelo o número serial del dispositivo. Las directivas pueden aplicarse a grupos o individuos y directivas separadas se pueden aplicar dependiendo de si el endpoint está conectado a la red, conectado remotamente por VPN o desconectado.

Catálogo de dispositivos para toda la compañía

La descripción de dispositivos está almacenada en un catálogo para toda la compañía y la directiva puede ser creada basada en las descripciones del catálogo, posibilitando la creación de directivas aún y cuando el dispositivo no esté accesible.

Copias en la sombra

El control de dispositivos de Zecurion puede guardar una copia de cada archivo que se escribe a un dispositivo externo o a una impresora – permitiéndole monitorear actividad aún cuando no hay violación de la directiva de seguridad, y dándole todas las herramientas necesarias para conducir un análisis retrospectivo sencillo, auditoría, e investigaciones forenses.

Directivas basadas en contenido que usan algoritmos de análisis de contenido

Se puede permitir el uso de impresoras y dispositivos portátiles, a la vez que se bloquea la posibilidad de guardar o imprimir archivos que tengan datos sensibles o confidenciales. La directiva basada en algoritmos de análisis de contenido puede identificar proactivamente y proteger datos sensibles.

Análisis preventivo de contenido

El análisis preventivo de contenido patentado por Zecurion asegura que los datos confidenciales y sensible no es nunca escrito a un medio externo en primer lugar. Los archivos son analizados y la copia de archivos sensibles se bloquea. Competidores de Zecurion escriben el archivo, luego lo analizan y borran el contenido si viola una directiva.

Cifrado

Las posibilidades de cifrado del control de dispositivos de Zecurion dan flexibilidad y protección. Se puede cifrar archivos automáticamente escritos a un medio externo basados en el contenido y las directivas de seguridad. Se puede configurar el cifrado para que los contenidos cifrados puedan ser sólo accedidos por los usuarios autorizados desde los endpoints conectados a la red corporativa.

Gestión e implementación centralizada

El Control de dispositivos de Zecurion le ofrece una infraestructura para gestión e implementación centralizada de su protección DLP. Los agentes de DLP en el endpoint pueden ser implementados a través de un servidor de implementación o a través de las directivas de grupo del directorio activo (ADGP). Una consola web permite a un administrador conectarse a cualquier endpoint para diagnosticar y le suministra la posibilidad de manejar cientos de miles de endpoints remotamente a través de un tablero sencillo.

Solicitud de acceso a dispositivos

Para minimizar el impacto potencial a la productividad, un empleado remoto puede solicitar acceso para usar un dispositivo específico. Un administrador puede autorizar la solicitud, para una sola vez o crear una directiva que permita el uso del dispositivo sin restricción.

Protección de escucha con el agente de endpoint

Para asegurar la integridad de su protección de datos, Zecurion Device Control alertará al administrador en caso de cualquier intento de espiar o remover o cambiar la configuración del endpoint.

Dispositivos controlados

- Dispositivos
  - USB
  - Red (WiFi, Bluetooth)
  - Puerto LPT/COM
  - FDD
  - DVD/CD
  - PCMCIA
  - IrDA
  - Módem
  - Impresora
  - HDD
  - Otros dispositivos removibles
  - Unidades de Cinta
  - FireWire
- Pantalla
- Clipboard
- Teclado
- Micrófono
- RDP
- Disk
- Smart card
- Puertos

CONTROL DE TRAFICO

Los negocios requieren internet para operar y ser productivos—esto también expone los datos a un riesgo significativos. Si los empleados o clientes pueden conectarse a los recursos de la compañía y acceder datos sensibles o confidenciales, así mismo un atacante pudiese comprometer, exponer o robar estos datos.

Un ataque malicioso es solo una posible amenaza. Los usuarios se comunican por correo o plataformas de mensajería, y pudiesen inadvertidamente revelar datos sensibles. Algunos usuarios podrían permitir que en almacenamientos en la nube no autorizados se guarden o transfieran datos confidenciales – poniéndolos en grave riesgo y comprometerlos.

Es vital para una organización monitorear el tráfico y controlar el flujo de datos por los canales de internet para minimizar el riesgo de pérdida de datos intencional o inadvertida. El módulo de Zecurion Traffic Control da un rango de características y posibilidades diseñadas para darle el control y la visibilidad que usted necesita:

Control total de los canales de internet

Zecurion Traffic Control le da control total de los datos que salen por los canales conectados a internet, incluyendo correo, correo basado en web, redes sociales, plataformas de mensajería y más. Se puede interceptar y analizar las Comunicaciones de la red a través de la mayoría de los protocolos.

Análisis de tráfico cifrado

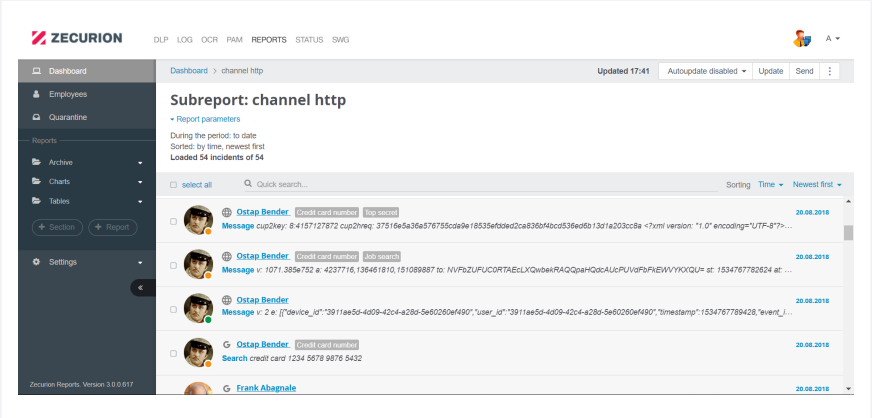
El tráfico cifrado podría permitir que los datos sensibles fluyan en la red sin ser detectados. El módulo de Zecurion Traffic Control descifra las conexiones SSL usando una aproximación de hombre en el medio (MitM), dando un control total de los datos que salen de su empresa, aunque se use HTTPS.

Cuarentena de correo

Zecurion Traffic Control se puede configurar para aislar correos sospechosos para inspección manual. El permitir la inspección manual de los mensajes reduce los falsos positivos y negativos y ofrece más precisión al identificar los mensajes que requieren acciones posteriores.

Dos formas de implementación

Zecurion Traffic Control puede operar como un filtro activo o puede solo analizar el tráfico espejo. El filtro activo monitorea el tráfico y bloquea transacciones peligrosas en tiempo real. Las organizaciones pueden también implementar por fases, comenzando con una configuración de espejo que permite verificar las directivas y ajustarlas para una máxima efectividad y eficiencia y luego cambiar a un filtro activo.



Análisis del tráfico de correo interno

Zecurion Traffic Control le permite monitorear y rastrear datos confidenciales dentro de su red. Un conector con Microsoft Exchange le da control avanzado y le permite analizar el tráfico de correo interno.

Modificación de mensaje

Se puede proteger sus datos sin obstaculizar la productividad al seleccionar la remoción de información sensible o confidencial. Zecurion Traffic Control da un método flexible y poco intrusivo de prevención de fugas, permitiendo modificar los mensajes al remover los archivos confidenciales mientras que deja otros archivos intactos y así permitiendo que los mensajes sean entregados.

Notificación de incidentes

Cuando ocurre un evento o incidente de seguridad, Zecurion Traffic Control puede notificar al usuario final y al encargado de seguridad para una rápida reacción y una respuesta ágil al incidente.

Diferentes opciones de implementación

Una de las principales fortalezas de Zecurion Traffic Control es la diversidad de formas de implementación. Hay opciones de operación pasiva como Puerto SPAN en espejo, y modos de operación activa como el agente de endpoint el SMTP relay, el conector de Microsoft Exhange y otras. Sin importar el tamaño de su organización o de como se vea su infraestructura IT, Zecurion Traffic Control le ofrece una forma rápida y simple de implementación.

Protocolos y canales controlados:

Correo

SMTP
IMAP
POP3
MAPI

Web

HTTP(S)
FTP

Mensajeria instantanea

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

Nube

OneDrive
DropBox
Google Drive
Yandex disk
Mail.ru Files

Redes sociales

Facebook
VKontakte
Odnoklassniki
LinkedIn
MySpace
Twitter

DESCUBRIMIENTO

Uno de los retos más importantes para una compañía, cuando se habla de seguridad de datos y prevención de pérdida de datos, es primero saber dónde se almacenan los datos sensibles y luego asegurar que los datos confidenciales están almacenados y marcados apropiadamente.

A medida que las compañías migran a la nube e instalan ambientes híbridos o multi nube que dispersan los datos en varios datacenter además de una o más plataformas de nube publica y privada, la posibilidad de una pérdida de datos se disparará exponencialmente. Mientras más disperso estén los datos más posibilidades hay que estén almacenados en los lugares menos apropiados y ahí es donde viene una fuga de datos.

Zecurion DLP Discovery le ofrece las herramientas para encontrar datos almacenados donde no deben estar y proactivamente tomar acciones antes de alguna pérdida o robo de información.

Escanee todos los sitios posibles de almacenamiento de datos

Zecurion DLP Discovery le ofrece un cubrimiento competo de todos los sitios posibles de almacenamiento en su organización, incluyendo un agente de endpoint para asegurar que todos los datos almacenados en los endpoint se identifiquen.

Parámetros flexibles de escaneo

Configure el escaneo de Zecurion DLP Discovery tan seguido como quiera y personalice la programación que es más conveniente para su organización. Puede configurarse escaneos diarios, semanales, o mensuales para unidades organizacionales o endpoints que se van a escanear.

Descubrimiento en tiempo real

Además de programar escaneos, Zecurion DLP Discovery puede también analizar archivos inmediatamente a medida que son copiados o guardados para dar informe en tiempo real de detección de violación de directivas.

Cree reglas de detección como directivas de DLP

Usando las técnicas disponibles de detección de contenido y reglas de contexto, se puede crear directivas universales de DLP para simplificar la administración y ser más eficiente.

El escaneo de Microsoft Exchange puede detectar amenazas sofisticadas

Zecurion DLP Discovery puede ayudar a detectar escenarios que se le pudiesen pasar a la detección de control de tráfico. Si un usuario malicioso crea un correo con información confidencial y lo guarda en el fólder de borradores, y luego lo descarga desde el cliente Outlook en la web y lo borra, realmente la información nunca fue enviada pero la fuga se dio. Discovery asegura que este tipo de actividad se identifique.

Alerte usuarios y administradores de seguridad

Zecurion DLP Discovery puede enviar alertas directamente a los usuarios y a los administradores IT cuando una violación a la directiva ocurra, asegurando una respuesta rápida a cualquier incidente.

Almacenamiento soportado:

- Unidades locales
- Fólderes compartidos
- MS SharePoint
- MS Exchange
- Cualquier DB que use ODBC

TRANQUILIDAD Y PAZ

Zecurion DLP le da lo que usted necesite de una solución de prevención de pérdida de datos: una plataforma razonable que le ofrece una implementación eficiente, prevención de fugas sencilla y cumplimiento, y reportes detallados de eventos y archivos. Zecurion DLP es el Sistema de tecnología DLP más avanzado y tiene todo lo que usted necesita para prevenir, detectar, investigar y predecir fugas de datos.

ACERCA DE ZECURION

- Zecurion es un fabricante de soluciones de seguridad IT de clase mundial que ayuda a compañías en el mundo a protegerse de amenazas internas.
- Fundada en 2001
- Oficinas en New York y Moscú
- Reconocido por los “Big 3”: Gartner, Forrester, IDC
- Más de 150 asociados y más de 10,000 clientes en el mundo

www.zecurion.com

sales@zecuiron.com
callejm@cadsecurity.org

+1 866 581 09 99
+57 300 6885204


ZECURION