ZECURION

ZECURION DLP

DATASHEET

www.zecurion.com

PURPOSE OF DLP

Data is the currency of business. The intellectual property, financial data, strategic information, and sensitive personal information on customers and employees are the most valuable assets your company has — and that data is at risk. Companies of all sizes and across all industries lose data every day. It may result from intentional theft or accidental exposure, and the perpetrator could be an external attacker or a trusted employee. The purpose of data loss prevention — or DLP — is to provide a solution to protect your intellectual property, trade secrets, and other sensitive data. It helps you achieve and maintain compliance with regulations like HIPAA, PCI DSS, and GDPR, and gives you the tools you need to prevent internal fraud and conduct internal audits and forensic investigations.

THE ADVANTAGE OF ZECURION DLP

Your data is crucial, and it demands the very best protection. That's why you should choose Zecurion DLP. Zecurion has been ranked on the Gartner Enterprise DLP Magic Quadrant since 2014. Zecurion was also listed as a top 7 DLP vendor by IDC in 2018 and was featured by Forrester in the 2019 DLP Now Tech Report.

Zecurion DLP is a cost-effective solution, streamlined and comprehensive. Zecurion DLP provides fast integration with enterprise infrastructure — 4 times faster than the average enterprise DLP deployment. Once deployed, it archives all events, files and documents and provides user behavior analytics to proactively detect threats. Zecurion DLP also reduces the workload for the security team and simplifies day-to-day management with interactive reports, graphs, and charts that provide an at-a-glance assessment of your data protection posture.

Zecurion DLP is a currently in use around the world across organizations with more than 100,000 users. Zecurion customers have won more than 40 lawsuits with the help of evidence gathered for litigation against malicious insiders.

Don't just take our word for it, though. Listen to what Zecurion customers have to say:

VP, Global Operations & Professional Service, Services Industry:

«Overall experience with Zecurion was excellent including attentive pre-sales and post-sales support in greater New York area.»

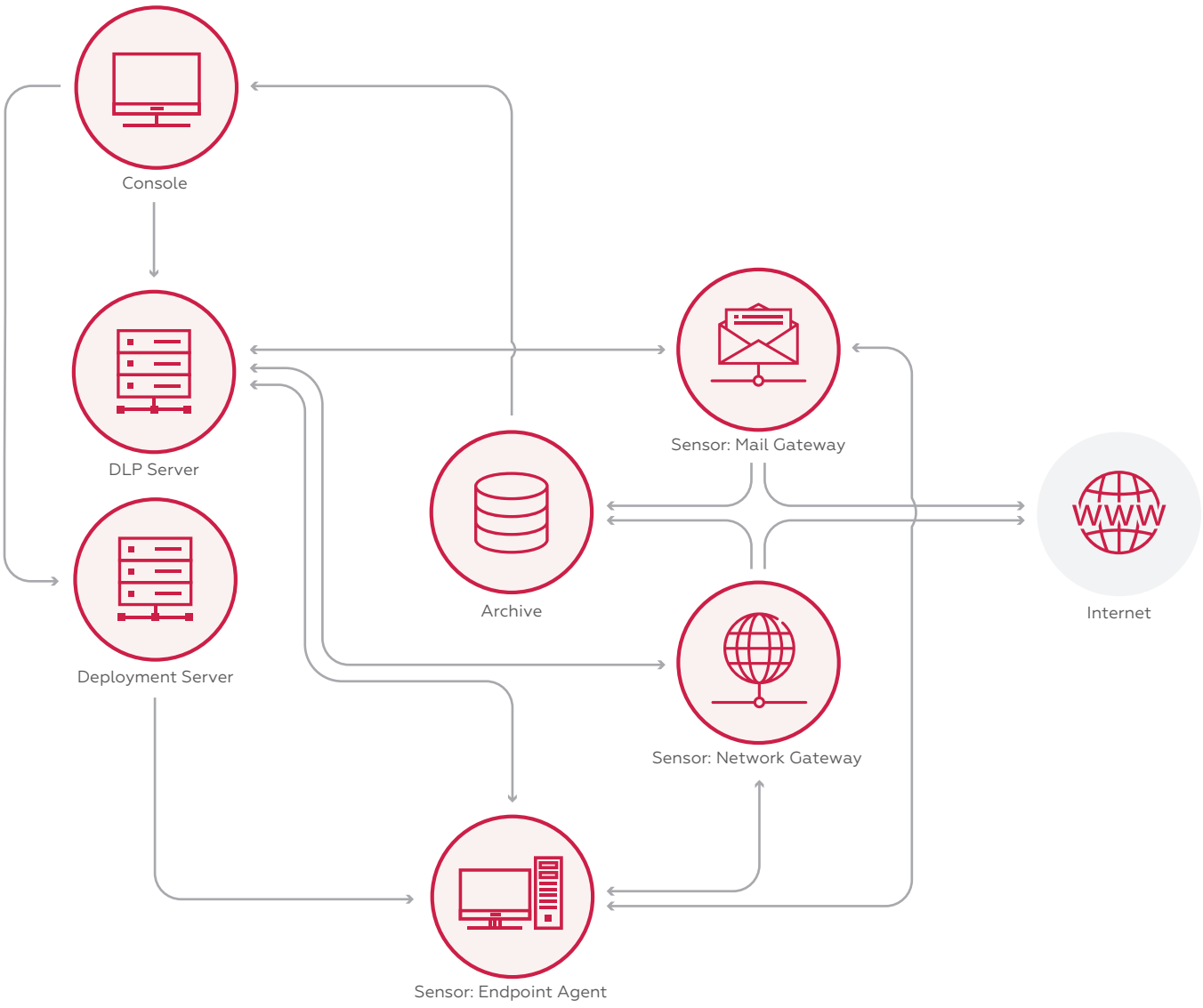
Head of Department, Energy and Utilities Industry:

«We can be sure that Zecurion DLP successfully protects the information from leaks.»

CSO,
Finance Industry:

«We use products that are leaders in their segments. Therefore, we chose Zecurion.»

ZECURION DLP ARCHITECTURE



Sensors: intercept data transfer channels, collect intercepted data, enforce DLP policies

Archive: stores all intercepted data, enables incident response and investigation, retrospective analysis i.e. apply the new policy to the historical data (MS SQL or PostgreSQL)

DLP server: stores settings and policies, pushes them to sensors, monitors sensors

Deployment server: deploys sensors and endpoint agents

Console: flexible web-based management of policies and reports

ZECURION DLP DEPLOYMENT OPTIONS

Every customer environment is a unique mix of network segments, endpoint types and operating systems, and different platforms and applications. Organizations need to be able to protect data across the entire ecosystem with minimal impact to performance and productivity. At the same time, comprehensive visibility and effective data loss prevention rely on being able to monitor and analyze every activity. Zecurion provides a diverse range of deployment options to ensure your data is monitored and protected no matter what your network infrastructure looks like.

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

KEY FEATURES OF ZECURION DLP

Zecurion DLP delivers everything you need to control data leak channels, monitor employee handling of data, and prevent data breaches.

Comprehensive control of data leak channels. Control all possible data leak channels to minimize the risk of a data breach and ensure compliance with regulatory requirements.

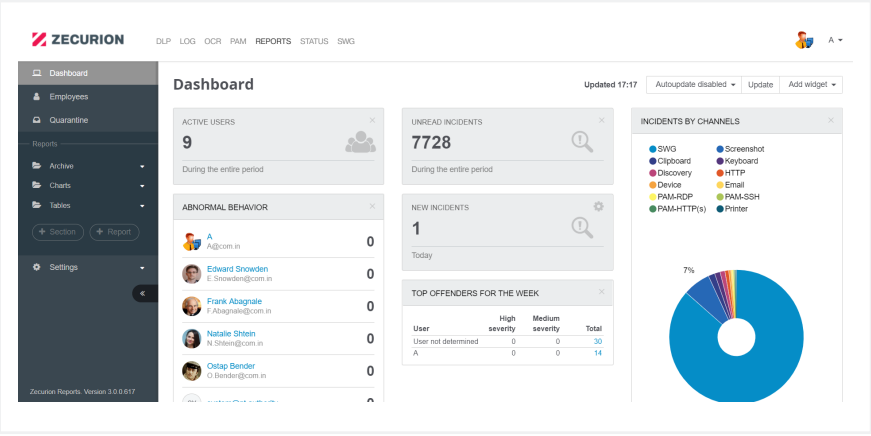
Flexible policies and rules. Configure on policy for several — or all — data transfer channels and use a variety of content detection techniques and data conditions to foresee and prevent any possible data breach scenario.

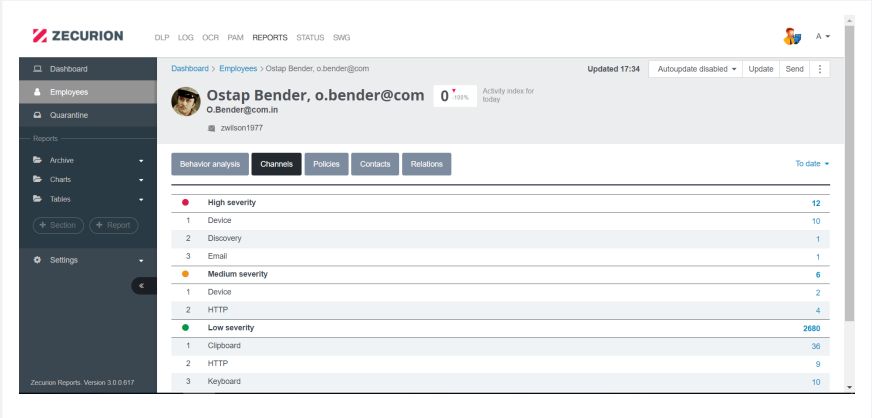
File content extraction. With automatic file detection for over 500 file formats based on internal structure rather than the file extension, and an ability to recognize encrypted files and unpack archived files — including nested archives — no data will escape the network without analysis.

Single console. Zecurion DLP provides web-based console for all modules and a customizable dashboard for centralized remote administration that is simple and streamlined.

Archive files and messages. All intercepted data — files, messages, incidents, events, and more — are stored in a database so you have everything you need to generate detailed reports, conduct comprehensive forensic investigation, and gather evidence for legal actions.

Smart catalog of employees. Collect and index all employee email addresses, social network and instant messenger accounts to ensure all communication is attributed to a specific user.





User behavior analysis. Calculate behavior profiles for all users to enable detection of anomalous activity. Proactive threat detection alerts the security team and provides early data breach prevention.

Emotional profiling. Evaluate employees' emotions using eight basic behavioral reactions and bring out high-risk groups. The system creates the emotional dynamics report for each user with an easy-to-understand diagram. This feature provides more information about employees and helps to reveal disloyal team members.

User connection map. Zecurion DLP develops clickable diagram of user connections and communication channels to detect hidden connections and allow you to analyze suspicious communications that might suggest internal fraud or a data breach.

Powerful reports. More than 20 preset reports and options to customize provide a powerful tool for security auditing and investigation. You can easily generate and analyze reports, and quickly drill down to a specific incident in a few clicks.

Events logging. Automatically log all internal events and administrator actions for easy maintenance and quick traceability of any issues that arise.

Active Directory integration. Users, Groups, and computer host names are synced from Active Directory to provide better integration with your IT infrastructure and enable Zecurion DLP to identify users by name in incidents and reports to simplify administration.

REST API. Most administration and monitoring tasks are available through REST API HTTP requests to enable security automation and integration with other tools and platforms in your IT infrastructure.

Advanced Features

Microphone and Webcam Recording

Turn any PC or laptop into a surveillance system by recording from either the microphone or the web camera of any computer at any time.

Screenshot and Keyboard Recording

You can record all keystrokes of designated users or groups and save screenshots from any computer at defined intervals so you always know what your employees are doing and you can enforce internal security and data handling policies to detect and prevent potential data breaches.

Application Control

Eliminate the risk of employees using potentially dangerous applications (TOR and torrent clients, anonymizers, games). You can restrict what applications are allowed to be used by creating a whitelist or blacklist of applications for designated users or groups.

CONTENT DETECTION TECHNIQUES

Zecurion DLP utilizes a variety of content detection techniques to provide comprehensive data loss prevention. Regardless of whether data is intentionally stolen or compromised, or inadvertently shared or exposed, one of these content detection techniques will flag it:

Keywords and dictionaries

This technique looks for exact matches of designated words. An IT administrator or security officer can create a dictionary for any subject or category, such as healthcare documents, financial documents, job searches, etc. and populate it with words that should be flagged. There are 30+ predefined dictionaries included in the system by default.

Templates and regular expressions

Some sensitive data follows a predefined structure or format that can be used to identify and detect it. Credit card numbers, Social Security numbers, IBAN accounts, URLs, email addresses and other similar data can be detected using templates and regular expressions.

Digital fingerprints

By collecting a number of documents of a specific type or category and providing them as input, Zecurion DLP creates a digital fingerprint that can detect exact documents or their parts. Once the digital fingerprint is created, Zecurion DLP can identify any document from the collection, or any part, or combination of parts from the document collection. New documents can be added to the collection and Zecurion DLP will automatically update the digital fingerprints.

Machine learning

Another technique similar to digital fingerprints is the use of machine learning. The initial setup is similar — providing a collection of files for Zecurion DLP to analyze. Where digital fingerprints detect exact matches of content, though, machine learning can be used to detect documents that are similar to the submitted collection based on keywords and/or semantic indicators.

Image templates

Image templates are effective for detecting things like signatures, stamps, letterhead, or documents with a defined structure like passports or driver's licenses. This method is also similar to digital fingerprints, but rather than detecting specific text, it detects image patterns. Like digital fingerprints and machine learning, the initial setup requires providing a collection of files that Zecurion DLP can analyze to develop the recognition necessary to detect it later.

OCR (Optical Character Recognition)

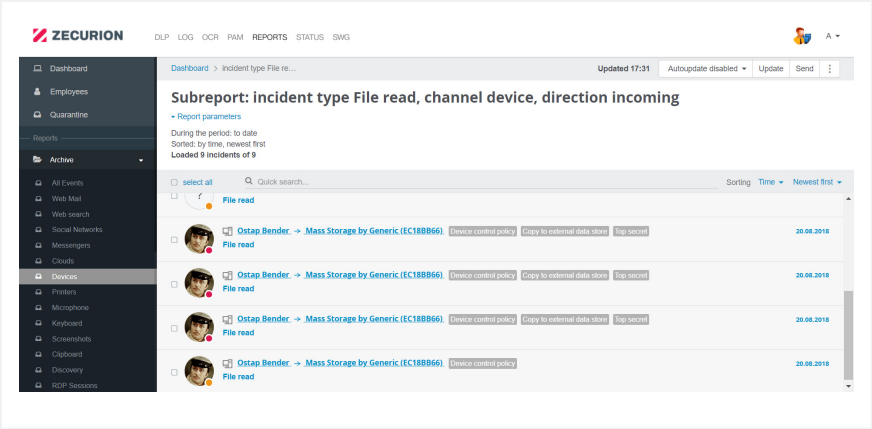
This technique is valuable for identifying sensitive or confidential data that has been somehow scanned or photographed in an attempt to bypass other detection methods. Zecurion DLP leverages third-party optical character recognition engines to extract text from scanned documents. Zecurion DLP integrates with the ABBYY FineReader and Google Tesseract to be able to extract and identify text from an image.

DEVICE CONTROL

Devices like external hard drives or USB thumb drives can pose a significant risk when it comes to data loss. Technology has evolved to the point where even microSD cards can store 1TB of data. A disgruntled employee could steal gigabytes or terabytes of data in their pocket. Data on portable devices poses a risk even with loyal employees, because the devices are easily lost or stolen.

In many cases, though, portable storage and other devices can be a crucial part of working effectively and efficiently. Simply blocking all USB thumb drives or access to USB ports is too strict or draconian and can negatively impact productivity.

Zecurion DLP gives you the following very granular device control so you can limit access and protect your data without hindering legitimate use of devices:



Flexible and granular access controls for peripheral devices

You can enable only company issued or approved devices or enable only the devices that are deemed necessary for business with policy controls that can grant or deny access based on the type, class, vendor, model, or serial number of the device. Policies can be applied to groups or individuals, and separate policies can be applied depending on whether the endpoint is connected to the network, connected remotely over VPN, or disconnected.

Company-wide device catalog

Device descriptions are stored in a company-wide catalog, and policy can be created based off of the descriptions in the catalog, enabling policy creation even when a device itself is not accessible.

Shadow copies
Zecurion Device Control can save a copy of every file that is written to an external device or printed — enabling you to monitor activity even when there is no violation of security policy, and giving you the tools you need to conduct comprehensive retrospective analyses, audits, and forensic investigations.

Content-based policies with the use of content analysis algorithms
You can allow the general use of printers and portable storage devices, while blocking the ability to save or print files that contain sensitive or confidential data. Policy based on content analysis algorithms can proactively identify and protect sensitive data.

Preventive content analysis
Zecurion's patented preventive content analysis ensures that confidential and sensitive data is never written to external media in the first place. Files are analyzed and sensitive files are blocked from being written. Competing products write the file first, then perform an analysis and delete the content if it violates policy.

Encryption
The encryption capabilities of Zecurion Device Control provide flexibility and protection. You can automatically encrypt files written to external media based on the content and security policies. You can configure encryption so that encrypted content can only be accessed by authorized users from endpoints connected to the corporate network.

Centralized deployment and management
Zecurion Device Control gives you the framework for centralized deployment and management of your DLP protection. Endpoint agents can be deployed through a dedicated deployment server or using Active Directory Group Policy. A web console enables an Admin to connect to any endpoint for diagnostics, and provide the ability to manage hundreds of thousands of endpoints remotely through a single pane of glass.

Device access request
To minimize the potential impact to productivity, a remote employee can request access to use a specific device. An Admin can grant the request on a one-time basis, or create a policy that permanently allows the use of the device.

Protection from tampering with endpoint agent
To ensure the integrity of your data protection, Zecurion Device Control will alert the Admin in the event of any sort of tampering or attempts to remove or change settings on the endpoint.

Controlled devices:

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

TRAFFIC CONTROL

The internet is the backbone of business today — but it also exposes data to significant risk. If employees or customers can connect to company resources and access sensitive or confidential data, then attackers may also be able to compromise, expose, or steal that data.

A malicious attack is only possible threat, though. As users communicate with one another via email or messaging platforms they may inadvertently reveal sensitive data. Some users may leverage unauthorized cloud storage platforms to store or transfer data — putting it at greater risk of compromise.

It's crucial for organizations to monitor traffic and control the flow of data across internet channels to minimize the risk of intentional or inadvertent data loss. Zecurion Traffic Control provides a range of features and capabilities designed to give you the control and visibility you need:

Total control off internet channels

Zecurion DLP gives you full control of outgoing data over internet-connected channels, including email, web-based email, social networks, messaging platforms, and more. You can intercept and analyze network communications across most protocols.

Analysis of encrypted traffic

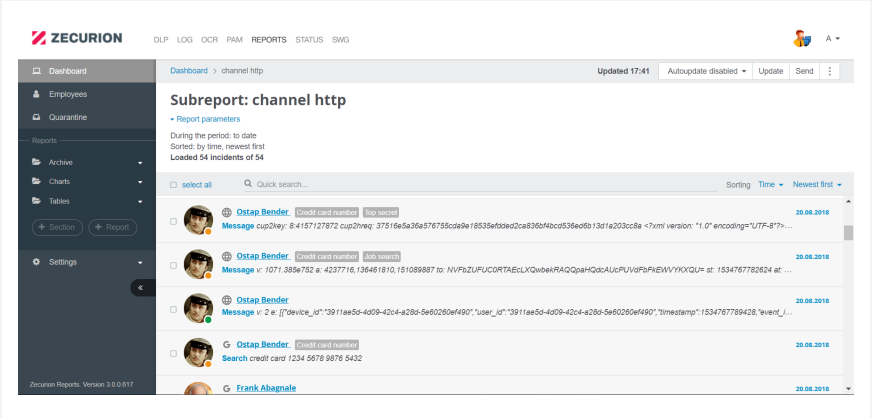
Encrypted traffic may allow sensitive data to escape the network undetected. Zecurion Traffic Control decrypts SSL connections using a man-in-the-middle (MitM) approach, providing full control of outgoing data even when using HTTPS.

Email quarantine

Zecurion Traffic Control can be configured to isolate suspicious emails for manual inspection. Enabling manual inspection of the messages reduces false positives and negatives and allows for better accuracy with identifying messages that require further action.

Two deployment mode options

Zecurion Traffic Control can function as either an active filter or it can just analyze mirrored traffic. The active filter monitors traffic and blocks dangerous transactions in real time. Organizations can also take a phased approach — starting out with a mirrored setup to allow for policies to be tested and tuned for maximum effectiveness and efficiency, and then transitioning over to active filtering.



Analysis of internal email traffic

Traffic Control lets you monitor and track confidential data inside your network. A Microsoft Exchange plugin gives you advanced control and allows you to analyze internal email traffic.

Message modification

You can protect your data without impeding productivity by selectively removing sensitive or confidential information. Traffic Control provides a more flexible and less intrusive method of leak prevention by enabling you to modify messages to remove confidential files while leaving other files intact and still allowing the message to be delivered.

Notification about incident

When a security event or incident occurs, Traffic Control can notify the end user and IT security for a quicker reaction and faster incident response.

Diverse deployment options

One of the primary strengths of Zecurion Traffic Control is the diversity of deployment options. There are passive mode options like SPAN port mirroring, and active mode options such as endpoint agents, SMTP relay, Microsoft Exchange plugin, and more. No matter what size your organization is or what your IT infrastructure looks like, Zecurion Traffic Control offers a fast and simple deployment capability.

Controlled channels and protocols:

Email

SMTP
IMAP
POP3
MAPI

Web

HTTP(S)
FTP

Messengers

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

Cloud

OneDrive
Office 365
DropBox
WeTransfer
Box.com
Google Drive
Google Docs
Yandex Disk
Mail.ru Files

Social networks

Facebook
VKontakte
Odnoklassniki
LinkedIn
MySpace
Twitter

DISCOVERY

One of the biggest challenges facing companies when it comes to data security and data loss prevention is knowing where sensitive data is stored in the first place and enforcing policies to ensure sensitive and confidential data is properly labeled and stored.

As companies move to the cloud and embrace hybrid or multi-cloud environments that span local data centers plus one or more private or public cloud platforms, the opportunity for data sprawl increases exponentially. The more data is spread to the dark reaches of your network and stored in places it should not be, the more inevitable a data breach becomes.

Zecurion DLP Discovery gives you the tools you need to find improperly stored sensitive files proactively to take action before your data is lost or stolen.

Scan of all possible data storage locations

Zecurion Discovery offers complete coverage off all possible file storage locations throughout your organization, including an endpoint agent to ensure that all data stored on endpoints is identified.

Flexible scan parameters

Configure Discovery scans as often or infrequent as you like and customize a schedule that is convenient for your organization. You can configure scans daily, weekly, or monthly and designate specific organizational units or endpoints to be scanned.

Real-time discovery

In addition to scheduled scans, Zecurion Discovery can also analyze files immediately as they are copied or saved to provide immediate, real-time detection of policy violations.

Create detection rules as DLP policies

Using all available content detection techniques and context rules, you can create universal DLP policies to make administration simple and straightforward.

Microsoft Exchange scan can detect sophisticated threats

Zecurion DLP Discovery can help detect scenarios that may circumvent Traffic Control detection. If a malicious user creates an email with confidential information and saves it to the Drafts folder, then downloads the message from the Outlook web client and deletes it, it is never actually “sent”. Discovery can ensure you still identify this activity.

Alert users and security administrators

Zecurion Discovery can send alerts directly to users and IT administrators when policy violations occur to ensure a fast reaction and quick incident response.

Supported storage:

- Local drives
- Shared folders
- MS SharePoint
- MS Exchange
- Any database using ODBC

CONFIDENCE AND PEACE OF MIND

Zecurion DLP provides everything you need from a data loss prevention solution: an affordable platform that delivers streamlined deployment, comprehensive breach prevention and compliance, and detailed archiving and reporting. Zecurion DLP is the most technologically advanced DLP system available, and it has everything you need to prevent, detect, and investigate data breaches.

ABOUT ZECURION

- Zecurion is a world-class vendor of IT security solutions helping companies to protect against insider threats
- Founded in 2001
- Headquartered in New York and Moscow
- Recognized by “Big 3”: Gartner, Forrester, IDC
- SC Labs Recommended: 5.00/5 score
- More than 150 partners and over 10,000 customers worldwide

www.zecurion.com

sales@zecuiron.com

+1 866 581 09 99


ZECURION