ZECURION
NEXT GENERATION DLP

Know more. Risk less.

Version 11

ZECURION

THE NEXT GENERATION DLP

Reality is changing, so do technologies. Still, every change is driven by people. People create, provide, exchange, purchase and sell, keep and transmit data. There is no unified formula on how they use it and no certainty in whom you can trust.

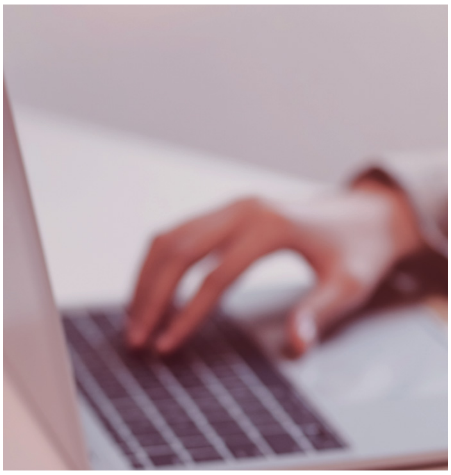
Legacy solutions, covering compliance issues or detecting your data losses, won't help. As well as rigid software, prohibiting almost everything to everyone. The key to peace of mind is in understanding the processes behind employee fraud and abuse, insider threats, and human mistakes.

Focus on a User Behavior

According to ACFE 2020 Global Study on Occupational Fraud and Abuse, organizations lose 5% of revenue to fraud each year. Typical fraud case lasts 14 months before detection and leads to a $1,509,000 average loss per case. During this time, the perpetrator will often display certain behavioral traits that tend to be associated with fraudulent conduct. At least one behavioral red flag was present in 85% of the cases, and multiple red flags were present in 49% of cases.[1]

Assess risks and individualize data protection

Employees can choose to work from their preferred location or use their own devices. Whatever boosts their productivity, works for business. But the way an employee interacts with data may differ on various devices, accounts, cloud services, etc. Organizations need to dynamically assess risks and identify anomalies to minimize false positives. This will allow low-risk users to proceed as usual, while high-risk employees will be under closer supervision.



Trust, but verify

With data being everywhere it is easy to lose context. Without it, the details, needed for forensic investigations, will be incomplete and might lead to inaccurate conclusions.

The Next Generation DLP has to maintain a comprehensive archive of files and events to provide the big picture of the organization's security state. Relying only on policies and classification is erroneous as it will provide a vision of a picture at-a-time, not a proper historical overview.

Know more, risk less

Zecurion Next Generation DLP provides a 360° view of all processes, associated with your employees. Facilitated by modular architecture, the solution allows you to create your perfect cybersecurity blend for ultimate control.

[1] ACFE 2020 Global Study on Occupational Fraud and Abuse, www.acfe.com/report-to-the-nations/2020/

THE ARCHITECTURE

Zecurion Next Generation DLP provides a mixed architecture that combines data control modules at the level of email, network gateways, and workstations, archiving solution, and Discovery module to inspect repositories of sensitive information.

Endpoint Agent is able to control external devices, printers, network traffic and employees' activity. The client agents reside on the end-user workstations and also have discovery capabilities.

Gateway Module may be used for controlling internet traffic and email messages.

Archive stores all intercepted data, enables incident response and investigation, retrospective analysis i.e. apply the new policy to the historical data.

Policy Server provides centralized management of settings, policies, content libraries, dictionaries and other necessary information for the DLP system.

Installation server is necessary for centralized deployment of endpoint agents.

Discovery Server is used for scanning server locations of confidential information.

Scalable architecture. Zecurion DLP is perfectly scalable from as least as 10 nodes up to tens of thousands. For minimal deployment, just one virtual or physical server is required. Any server component could be placed in public or private cloud.

HARDWARE AND SOFTWARE REQUIREMENTS

Minimal requirements for endpoint agent deployment:

- Intel P4;
- 1GB RAM.

OS:

- Microsoft Windows XP SP3;
- Vista SP1;
- Microsoft Windows 7/8/10;
- Microsoft Windows Server 2003 SP2, 2008 R2, 2012, 2012 R2, 2016, Linux.

Network:

- Active Directory or domainless.

Database:

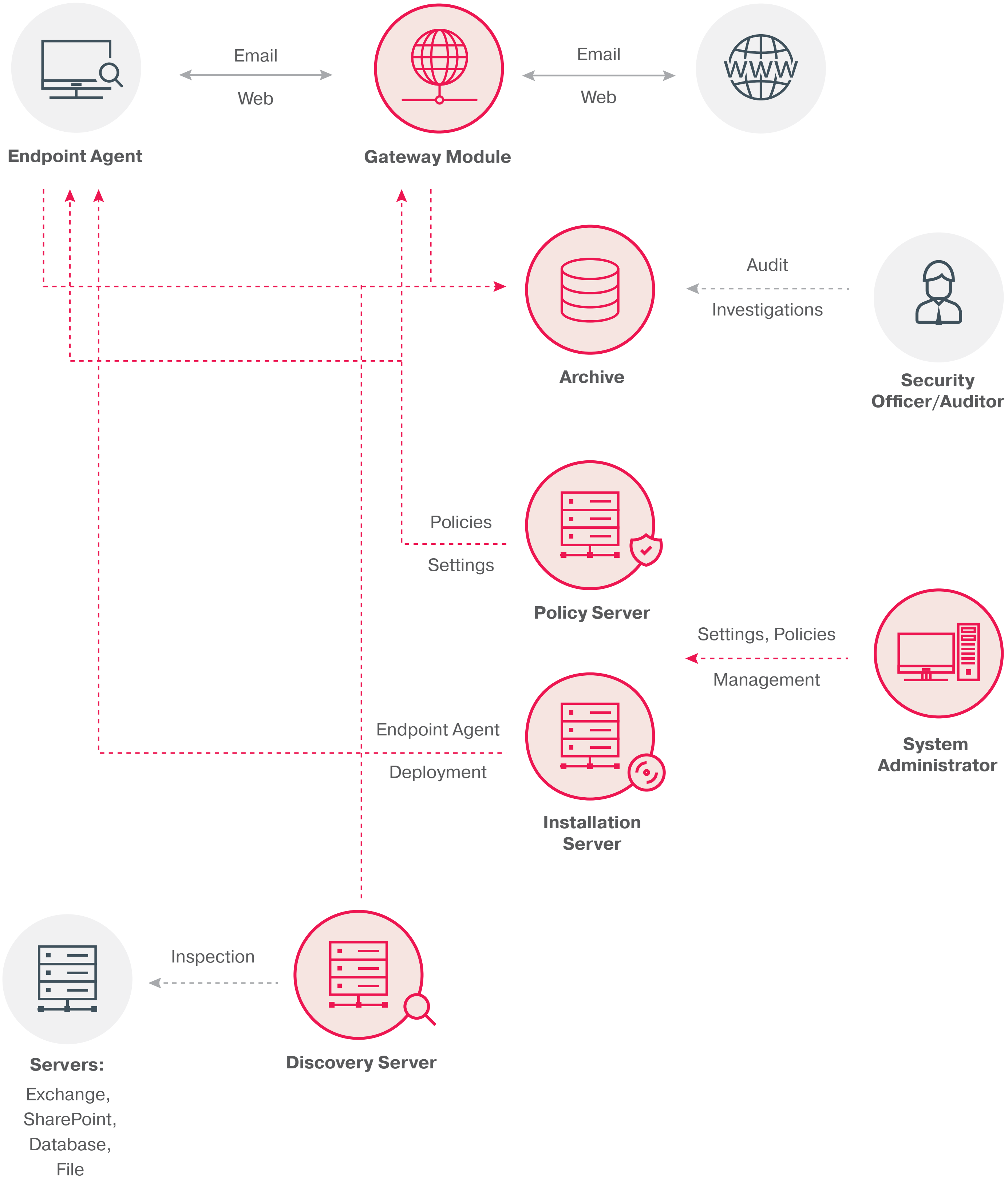
- Microsoft SQL or PostgreSQL.

Server:

- Dual-core CPU;
- 2GB RAM, at least 5 GB of free space on the system volume;
- Microsoft Windows 7/8/10 64-bit;
- Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019.

Zecurion is deployed 4 times faster compared to other enterprise DLP (installation in 1-2 days regardless of network architecture).

DLP ARCHITECTURE



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 on 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	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 and record
Discovery Agent (endpoint)	Local drive scan Local drive real-time	Detect and delete
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.

Ultimate channel control

- Comprehensive control of data leak channels;
- File content extraction and analysis.

Deep context

- Archive files and messages;
- Powerful reports;
- Events logging;
- Investigation module.

Risk-based supervision

- Smart catalogue of employees;
- User connection map;
- Risk-based assessment.

Easy management

- Flexible policies and rules;
- Single console;
- Active Directory integration;
- Rest API.

UBA

- User Behavior Analysis with detection of anomalies;
- Emotional evaluation;
- Behavioral profiles;
- Behavior comparison.

Unique features

- Screen Photo Protection;
- Screen Watermarks;
- Blocking of screenshots;
- Chat-like report;
- Microphone and Webcam recording;
- Live connection to desktop and webcam;
- Screenshot and keyboard recording;
- Application control;
- Hiding of endpoint agent from the user.

FEATURES

KEY FEATURES OF ZECURION DLP

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.

Smart catalog of employees

Identify dynamics of all key indicators including risk level, productivity, incidents, policies triggered, and emotional state. Collect and index all employees' email addresses, social networks, and instant messenger accounts to ensure all communication is attributed to a specific user. The security officer can set data display in a few clicks with filters and quick search.

Single console

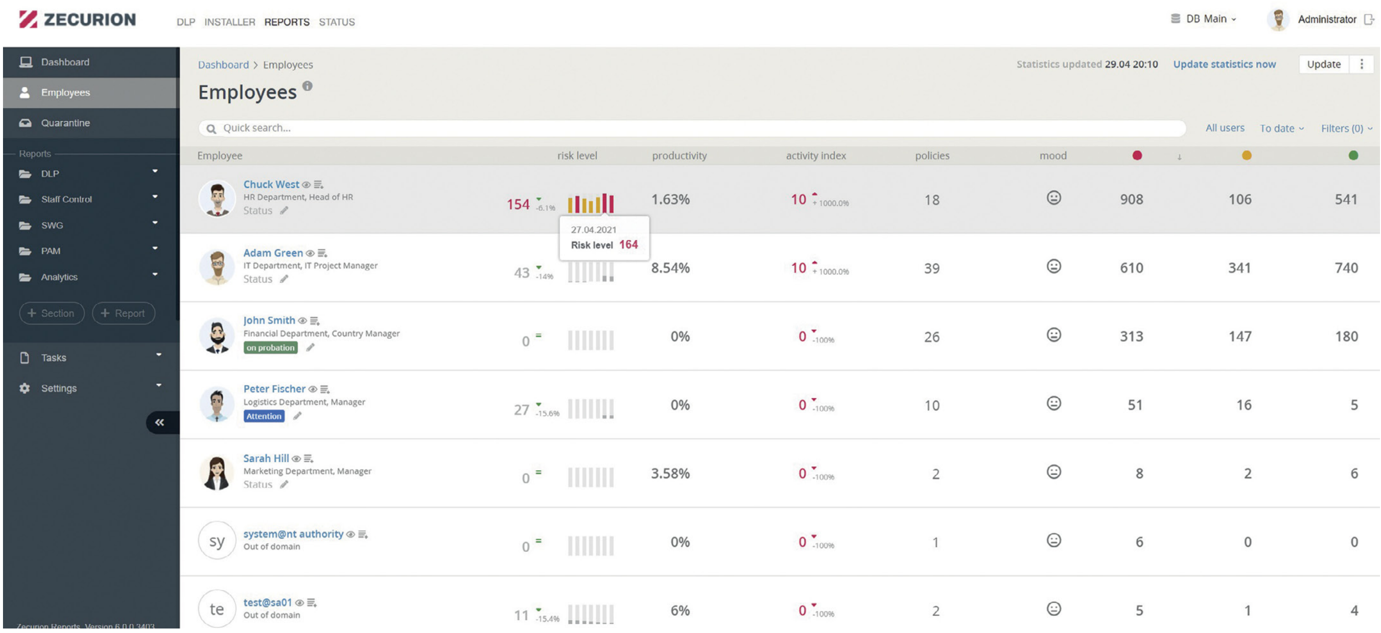
Zecurion DLP provides a web-based console for all modules and a customizable dashboard for centralized remote administration that is simple and streamlined.

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 a comprehensive forensic investigation, and gather evidence for legal actions.

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.



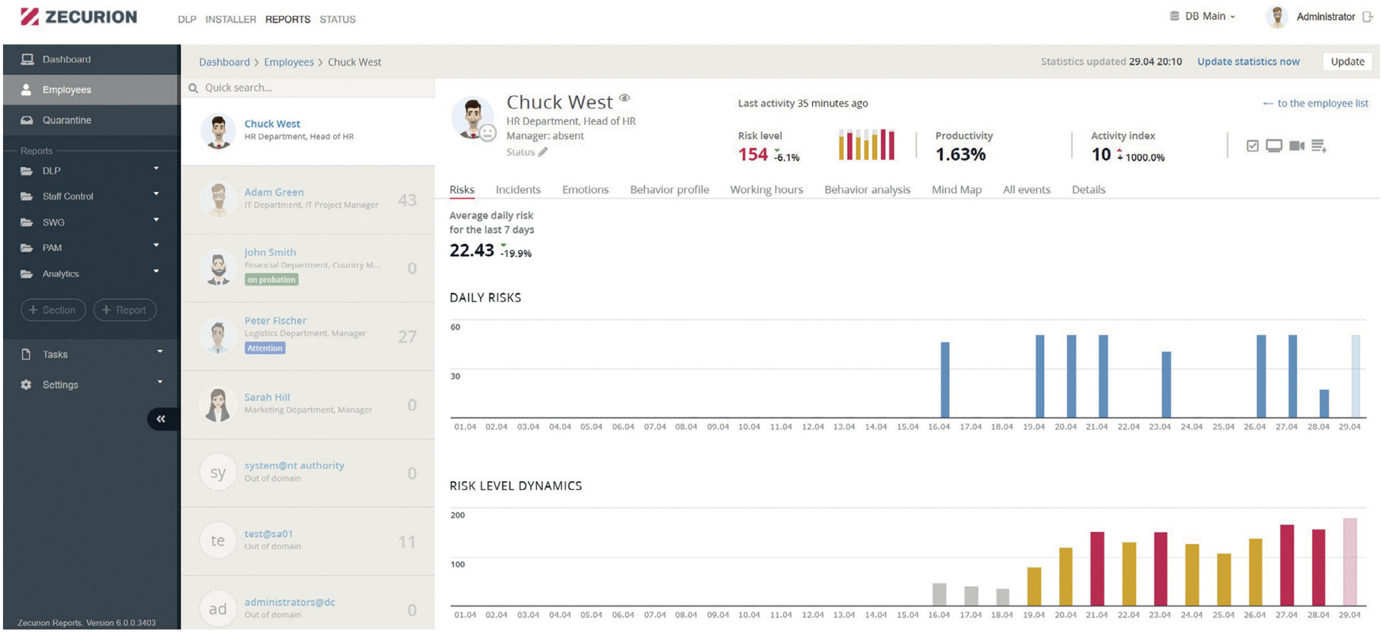
Employees

Statistics updated 29.04 20:10

Employee	risk level	productivity	activity index	policies	mood	●	●	●
Chuck West HR Department, Head of HR Status	154 -6.1%	1.63%	10 + 1000.0%	18	☺	908	106	541
Adam Green IT Department, IT Project Manager Status	43 -14%	8.54%	10 + 1000.0%	39	☺	610	341	740
John Smith Financial Department, Country Manager on probation	0 =	0%	0 -100%	26	☺	313	147	180
Peter Fischer Logistics Department, Manager Attention	27 -15.6%	0%	0 -100%	10	☺	51	16	5
Sarah Hill Marketing Department, Manager Status	0 =	3.58%	0 -100%	2	☺	8	2	6
system@nt authority Out of domain	0 =	0%	0 -100%	1	☺	6	0	0
test@sa01 Out of domain	11 -15.4%	6%	0 -100%	2	☺	5	1	4

User behavior analysis with detection of anomalies

Calculate behavior profiles for all users to enable detection of anomalous activity. Anomalies include: new employee, activity at holidays, first remote connection, the first use of the new device, using more than one account in social networks/messengers, higher activity comparing to company/group, number of contacted people is higher than average across the company, contacts with unknown people, absence for more than 40 days. Proactive threat detection alerts the security team and provides early data breach prevention.



Dashboard > Employees > Chuck West

Statistics updated 29.04 20:10 Update statistics now

Chuck West
HR Department, Head of HR
Manager: absent
Status

Last activity 35 minutes ago

Risk level 154 -6.1%

Productivity 1.63%

Activity index 10 1000.0%

Average daily risk for the last 7 days 22.43 -19.9%

Chuck West — HR Department, Head of HR

Adam Green — IT Department, IT Project Manager — 43

John Smith — Financial Department, Country M... — on probation — 0

Peter Fischer — Logistics Department, Manager — Attention — 27

Sarah Hill — Marketing Department, Manager — 0

system@nt authority — Out of domain — 0

test@sa01 — Out of domain — 11

administrators@dc — Out of domain — 0

Zecurion Reports. Version 6.0.0.3403

Behavioral profiles

Create behavioral profiles based on certain patterns (e.g. remote user, a user from specific department, etc.). Zecurion DLP displays the degree to which user behavior is similar to an existing profile. This simplifies risk assessment and prevents potential security incidents.

Emotional evaluation

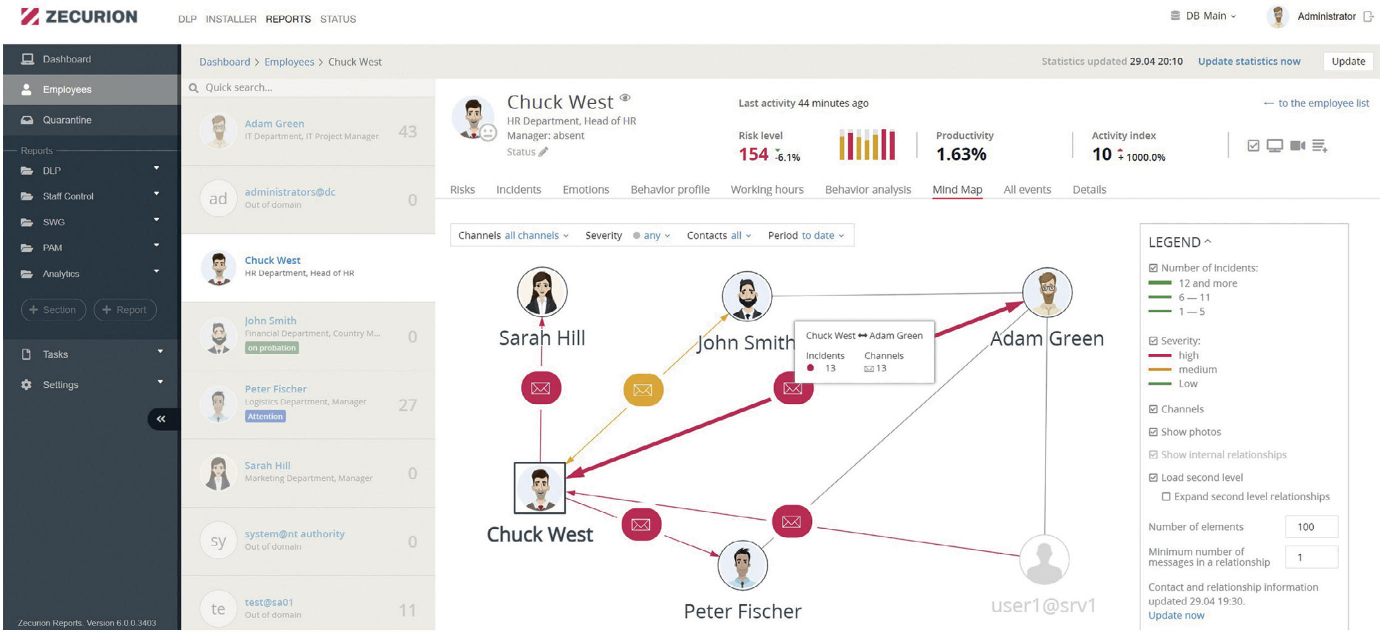
Evaluate employees' emotions using eight basic behavioral reactions and bring out high-risk groups. The system creates the emotional dynamics report for each user with an easy-to-understand diagram. This feature provides more information about employees and helps to reveal disloyal team members.

Behavior comparison

UBA compares current employees' parameters with their average values. A sharp deviation may signal a potential threat to information security or indicate a compromise of user credentials. You can also compare behavioral parameters of two users or user and a group.

User connection map

Zecurion DLP develops a 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.



Zecurion Reports. Version 6.0.0.3403

Adam Green	IT Department, IT Project Manager	43
administrators@dc	Out of domain	0
Chuck West	HR Department, Head of HR	
John Smith	Financial Department, Country M... on probation	0
Peter Fischer	Logistics Department, Manager Attention	27
Sarah Hill	Marketing Department, Manager	0
system@nt authority	Out of domain	0
test@sa01	Out of domain	11

Statistics updated 29.04 20:10

Chuck West
HR Department, Head of HR
Manager: absent
Status

Last activity 44 minutes ago

Risk level 154 -6.1%

Productivity 1.63%

Activity index 10 + 1000.0%

Channels all channels · Severity ● any · Contacts all · Period to date

Chuck West ⟷ Adam Green
Incidents ● 13
Channels ✉ 13

☑ Number of incidents:
- 🟩 12 and more
- 🟩 6 — 11
- 🟩 1 — 5

☑ Severity:
- 🟥 high
- 🟧 medium
- 🟩 Low

☑ Channels

☑ Show photos

☑ Show internal relationships

☑ Load second level

☐ Expand second level relationships

Number of elements: 100

Minimum number of messages in a relationship: 1

Contact and relationship information updated 29.04 19:30.

Powerful reports

More than 20 preset reports and options 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 hostnames 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.

Investigation Module

This module simplifies investigations and shortens the incident response cycle. It minimizes the cybersecurity team workload by providing a 360° view of actual tasks with all the statuses, data on the investigation stage, executants, and deadlines. 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.

Risk-based assessment

Zecurion DLP displays the risk score and its dynamics for an employee. Each employee profile contains 5 risk indexes to provide comprehensive details for forensic investigation: company average risk level, risk yesterday, risk today, average daily risk, average daily risk during the last 7 days.

Zecurion UBA

Among all information security threats, it is insiders, that are the most dangerous. No wonder, as they already have keys to the front door of your organization. Acting from the inside, they can steal or misuse sensitive data. Traditional DLP systems will not spot it.
Zecurion Next Generation DLP is a complete solution with the UBA module aiming to gain understanding of the context of user action and their intent. The solution ensures a comprehensive view of risks with 5 additional parameters, emotions, behavior profile and analysis, working hours, connection map and many more.

Anomalies detection

To be able to analyze user behavior, the system must know, what it's like to be that particular user. After in-depth research of not less than one week, Zecurion UBA displays anomalies in employee's behavior and suggests similar behavior patterns.

Context in details

Each employee profile contains all events associated with the user on a single page. The Security Officer can choose period and learn detailed information on various incidents (marked upon the severity), user connections, utilized channels, applied policies and more. All events are shown in chronological order and are clickable for more information.

Individual approach

Zecurion Next Generation DLP provides a risk score and change dynamics to assess employees. The Security Officer will put more supervision to high risk employees, while low-risk ones will be able to operate with less limitations.

Higher productivity

The module ensures automation of UBA and makes supervision easy with visually descriptive reports.

Absolute visibility

Zecurion UBA analyzes all employee activity and evaluates it on main parameters: risk, productivity, policies, and emotional state. The Security Officer reviews employee's Connection Map to see all user connections within and outside of the corporate network.

Proactive monitoring

Zecurion DLP calculates an employee's emotional state by analysis of his/her outgoing messages. Each can receive up to 3 emotional attributes of the following: joy, trust, surprise, anticipation, sadness, disgust, fear, and anger. The module calculates dynamics on each emotion, highlighted by according color.

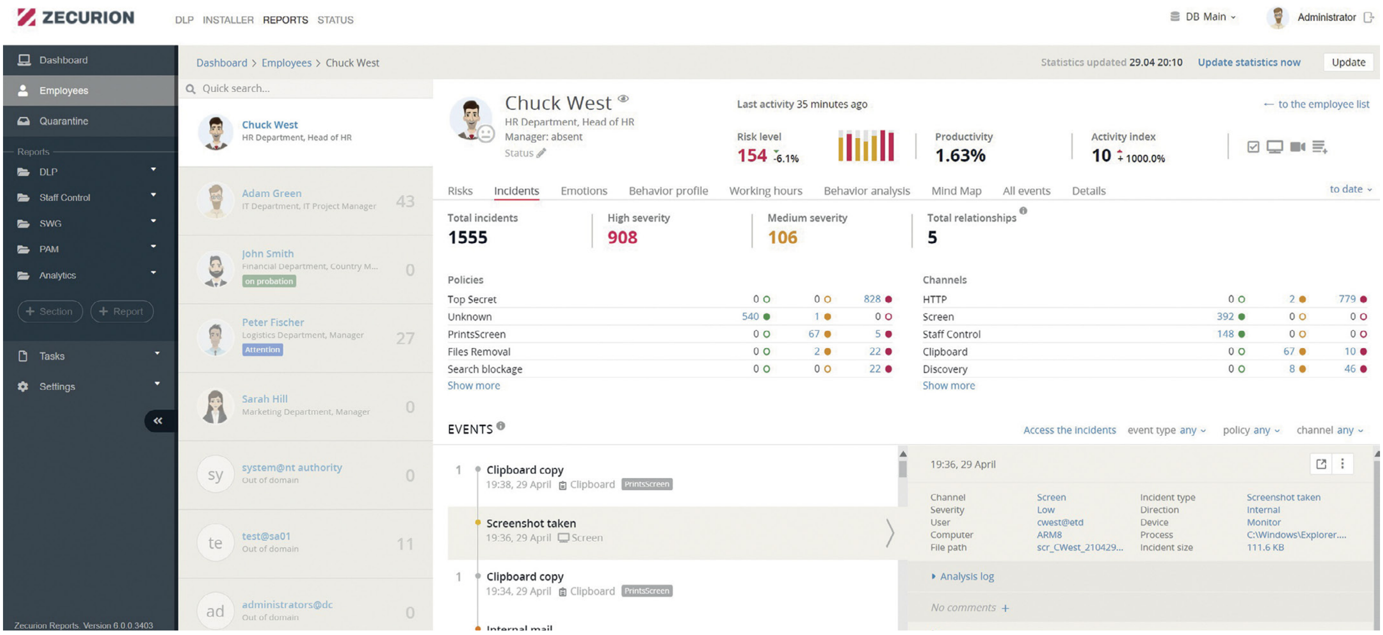
Real-time alerts

Zecurion UBA provides accurate analysis of hundreds user activities and interactions. In case of sudden anomaly of user behavior, the Security Officer can connect via an employees' webcam or review his/her desktop in real-time at any moment. UBA has to be ready to react quickly.

ADVANCED FEATURES

Screen Photo Protection

This unique AI-based feature changes the game, stopping the insiders that were previously not being able to catch. Whenever someone tries to photograph a screen by the smartphone, Zecurion DLP immediately detects it via webcam and blocks the computer. 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).



Chuck West
HR Department, Head of HR

Adam Green
IT Department, IT Project Manager
43

John Smith
Financial Department, Country M...
on probation
0

Peter Fischer
Logistics Department, Manager
Attention
27

Sarah Hill
Marketing Department, Manager
0

sy system@nt authority
Out of domain
0

te test@sa01
Out of domain
11

ad administrators@dc
Out of domain
0

Chuck West
HR Department, Head of HR
Manager: absent
Status

Last activity 35 minutes ago

Risk level 154 -6.1%
Productivity 1.63%
Activity index 10 + 1000.0%

Total incidents 1555
High severity 908
Medium severity 106
Total relationships 5

Policies			
Top Secret	0 ○	0 ○	828 ●
Unknown	540 ●	1 ●	0 ○
PrintsScreen	0 ○	67 ●	5 ●
Files Removal	0 ○	2 ●	22 ●
Search blockage	0 ○	0 ○	22 ●

Channels			
HTTP	0 ○	2 ●	779 ●
Screen	392 ●	0 ○	0 ○
Staff Control	148 ●	0 ○	0 ○
Clipboard	0 ○	67 ●	10 ●
Discovery	0 ○	8 ●	46 ●

EVENTS

1 Clipboard copy
19:38, 29 April Clipboard PrintsScreen

Screenshot taken
19:36, 29 April Screen

1 Clipboard copy
19:34, 29 April Clipboard PrintsScreen

Internal mail

19:36, 29 April

Channel	Screen	Incident type	Screenshot taken
Severity	Low	Direction	Internal
User	cwest@etd	Device	Monitor
Computer	ARM8	Process	C:\Windows\Explorer....
File path	scr_CWest_210429...	Incident size	111.6 KB

Screen Watermarks

The security officer can set watermarks with the name of a user, PC, and date over certain windows (e.g. MS Office, CRM, and others). Users initially see the watermarks and will reconsider taking screenshots or photos of sensitive files.

Chat-like Report

This integrative report simplifies the analysis of communications between two users by displaying all messages from different messengers (Skype, WhatsApp, Telegram, etc.) in one chat-like window. This window looks like your favorite messenger, allowing you to read all captured messages, files, listen to audio messages and calls from a single point.

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.

Live Connection to Desktop and Webcam

Connect to any employee computer in real-time for an immediate evaluation of their activity. Receive more context details by reviewing live footage from the webcam.

Blocking of screenshots

If circumstances require more rigid measures, the Security Officer can block the option of screenshots on the user’s PC.

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.

Hiding of Endpoint Agent from the User

The solution can make endpoint agent invisible in Task Manager, Programs and Features, System Services consoles, and in File Explorer.

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.

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.

Keywords and dictionaries

This technique looks for exact matches of designated words. The 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.

AI-based 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.

DLP POLICIES

Zecurion Next Generation DLP policies consist of 3 easy setting blocks.

01

Define rules and conditions

- Detect content using 10+ technologies;
- Scan the data inside files and archives;
- Check 500+ file types (text, graphic, audio, video, archive, executable, etc.) including encrypted and camouflaged by internal structure rather than by extension;
- Consider context attributes (user, host IP, sender, recipient, etc,);
- Document labels of third-party data classification software;
- Create composite rules with logical operators (AND, OR, NOT).

02

Select data leakage channel

- Network channels and internet services (applications, browsers, email, messengers, etc.);
- Local devices and ports (USB devices, printers, screen, clipboard, keyboard, microphone, web camera, DVD/CD drives, removable media, modems, IEEE 1394 (FireWire), WiFi, etc.).

03

Set an action

- Create incident in system repository / Event log / Syslog / third-party SIEM instance;
- Notify user and/or a Security Officer: send customizable notification by email, display notification alert in Windows Notification Area on endpoint;
- Save to the archive;
- Cancel action, remove attachments or place in quarantine: block file or message, place email in quarantine for manual inspection, block screenshots on workstation while specific application is running, remove file from email body or user workstation;
- Control a user and terminate activity: screenshot of the user’s workspace, web camera snapshot on endpoint, specific status label to the user, customizable watermark on top of the specific application, forced logout on target PC;
- Encrypt file or document being copied to external drive.

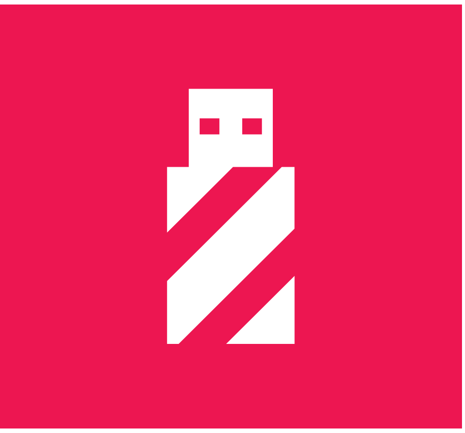
Omnichannel policies

The Security Officer can create a policy once and apply it to any (or all) target channels: Mail, Web, Messengers, Devices, Printers, Discovery crawler, etc. Policies will work on gateways and endpoints autonomously, not requiring permanent connection to the DLP Server.

Cascading policy support

The Security Officer can configure cascading policies when one policy is triggering after another.

MODULES



DEVICE CONTROL

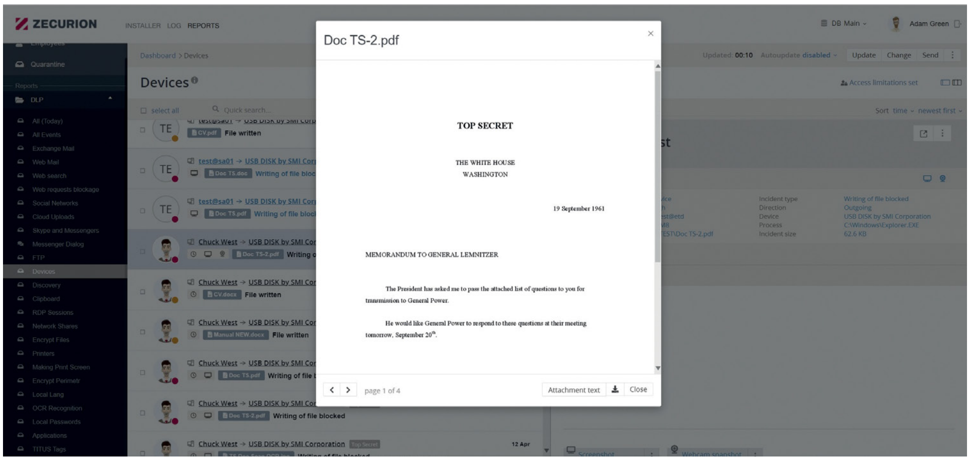
Devices like external hard drives or USB thumb drives can pose a significant risk when it comes to data loss. Technology has evolved to the point where even microSD cards can store 1TB of data. A disgruntled employee could steal gigabytes or terabytes of data in their pocket. Data on portable devices 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 on the descriptions in the catalog, enabling policy creation even when a device itself is not accessible.



Doc TS-2.pdf

TOP SECRET

THE WHITE HOUSE
WASHINGTON

19 September 1961

MEMORANDUM TO GENERAL LEMNITZER

The President has asked me to pass the attached list of questions to you for transmission to General Power.

He would like General Power to respond to these questions at their meeting tomorrow, September 20th.

page 1 of 4 Attachment text Close

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 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

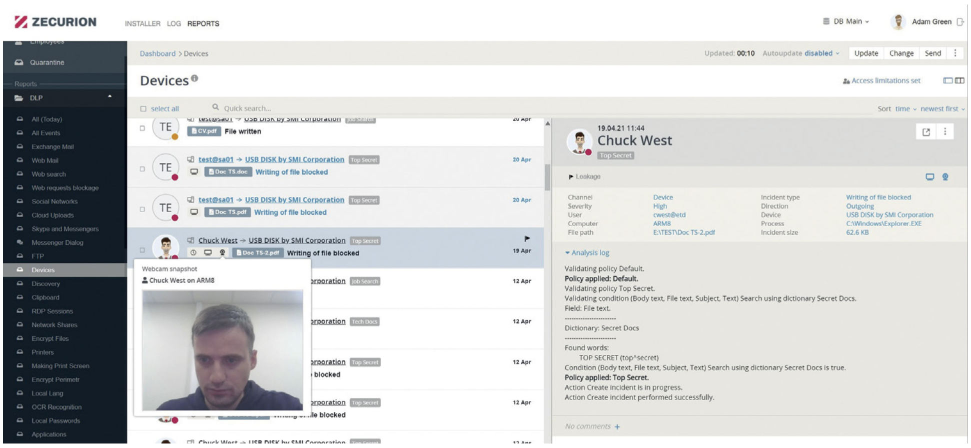
Zecurion Device Control gives you the framework for centralized deployment and management of your DLP protection. Endpoint agents can be deployed through a dedicated deployment server or using Active Directory Group Policy. A web console enables an Admin to connect to any endpoint for diagnostics and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

Device access request by email or phone

To minimize the potential impact on 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 an 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.



Channel Device
Severity High
User cwest@etd
Computer ARM8
File path E:\TEST\Doc TS-2.pdf
Incident type Writing of file blocked
Direction Outgoing
Device USB DISK by SMI Corporation
Process C:\Windows\Explorer.EXE
Incident size 62.6 KB

Analysis log

```
Validating policy Default.
Policy applied: Default.
Validating policy Top Secret.
Validating condition (Body text, File text, Subject, Text) Search using dictionary Secret Docs.
Field: File text.
----------------------
Dictionary: Secret Docs
----------------------
Found words:
    TOP SECRET (top^secret)
Condition (Body text, File text, Subject, Text) Search using dictionary Secret Docs is true.
Policy applied: Top Secret.
Action Create incident is in progress.
Action Create incident performed successfully.
```

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 isn't the 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 of internet channels

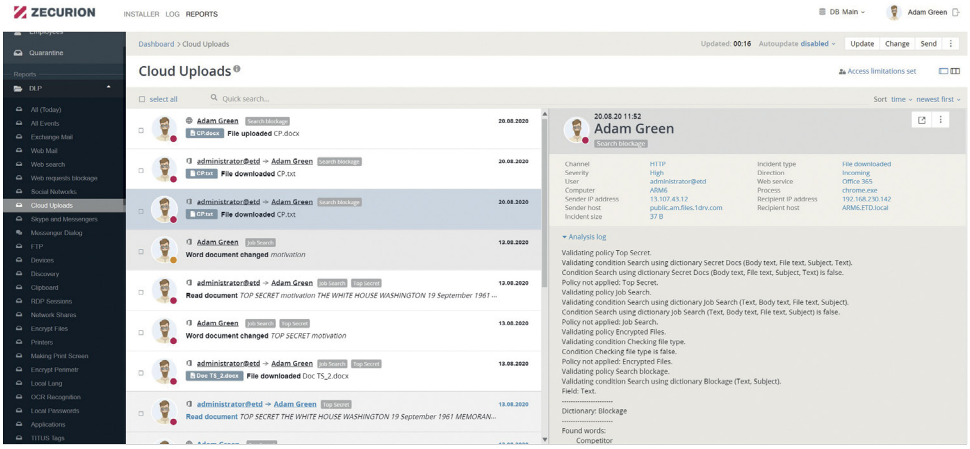
Zecurion DLP gives you full control of outgoing data over internet-connected channels, including email, web-based email, social networks, messaging platforms, and more. You can intercept and analyze network communications across most protocols.

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 in identifying messages that require further action.



Cloud Uploads

Adam Green Search blockage 20.08.2020
CP.docx File uploaded CP.docx

administrator@etd → Adam Green Search blockage 20.08.2020
CP.txt File downloaded CP.txt

administrator@etd → Adam Green Search blockage 20.08.2020
CP.txt File downloaded CP.txt

Adam Green Job Search 13.08.2020
Word document changed *motivation*

administrator@etd → Adam Green Job Search Top Secret 13.08.2020
Read document *TOP SECRET motivation THE WHITE HOUSE WASHINGTON 19 September 1961 ...*

Adam Green Job Search Top Secret 13.08.2020
Word document changed *TOP SECRET motivation*

administrator@etd → Adam Green Job Search Top Secret 13.08.2020
Doc TS_2.docx File downloaded Doc TS_2.docx

administrator@etd → Adam Green Top Secret 13.08.2020
Read document *TOP SECRET THE WHITE HOUSE WASHINGTON 19 September 1961 MEMORAN...*

20.08.20 11:52
Adam Green
Search blockage

Channel	HTTP	Incident type	File downloaded
Severity	High	Direction	Incoming
User	administrator@etd	Web service	Office 365
Computer	ARM6	Process	chrome.exe
Sender IP address	13.107.43.12	Recipient IP address	192.168.230.142
Sender host	public.am.files.1drv.com	Recipient host	ARM6.ETD.local
Incident size	37 B		

Analysis log

```
Validating policy Top Secret.
Validating condition Search using dictionary Secret Docs (Body text, File text, Subject, Text).
Condition Search using dictionary Secret Docs (Body text, File text, Subject, Text) is false.
Policy not applied: Top Secret.
Validating policy Job Search.
Validating condition Search using dictionary Job Search (Text, Body text, File text, Subject).
Condition Search using dictionary Job Search (Text, Body text, File text, Subject) is false.
Policy not applied: Job Search.
Validating policy Encrypted Files.
Validating condition Checking file type.
Condition Checking file type is false.
Policy not applied: Encrypted Files.
Validating policy Search blockage.
Validating condition Search using dictionary Blockage (Text, Subject).
Field: Text.
----------------------
Dictionary: Blockage
----------------------
Found words:
    Competitor
```

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 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

HTTPS(S)
FTP

Messengers

WhatsApp
Telegram
Skype
MSN
MS Lync
Viber
ICQ
XMPP (Jabber)
Microsoft Teams

Cloud

OneDrive
Office 365
DropBox
WeTransfer
Box.com
Google.Drive
Google Docs

Social Networks

Facebook
LinkedIn
MySpace
Twitter
Google Docs

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 of 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 Officers

Zecurion Discovery can send alerts directly to users and Security Officers 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

STAFF CONTROL

Employee management can make or break the success of the organization. Happy, hardworking employees support their companies on the way to the best results, while lazy, demotivated ones bring them down from the inside.
In an ideal world, employees follow all corporate rules, have great attitudes, and discipline round-the-clock. But this isn't reality.
Zecurion Staff Control keeps track of working hours, logs employees' actions at workplaces, and evaluates the efficiency. The module checks the activities of personnel for compliance with corporate standards and safety policies.
Staff Control will be useful for company executives, security officers, and HR managers.

Employee profile

Each contains detailed information on efficiency and activity at the workplace in dynamics: system login/logout, activity in applications, browsers and on websites, remote desktop connection. Profile visualizes employee activity within a current or previous day, last 14 or 60 days, current or previous month.

Comprehensive user report

Security Officer can review productive time, inappropriate use of PC, utilized applications and websites, and actual working hours. All activity of a user on different devices is accumulated in a single report.

Resource usage and timesheets

Suggests detailed information on what web resources and applications running and their activity period (exact time up to minutes). Timesheets will help managers supervise discipline, including corporate devices management and the working day longevity.

Processes and applications control

Zecurion Staff Control matches the applications in use with an approved list, and if they are not work-related, displays the period as unproductive.

Profile comparison

Zecurion Staff Control compares activity profiles of chosen users. The analysis includes:

1. Activity for the selected period (productive time, inappropriate use of PC, not defined, inactivity, away from the PC);
2. Main indicators (productivity, away from the PC, remote work, productive time, etc.);
3. Applications and categories*;
4. Websites and categories*;
   *Parameters 3 and 4 show categories of applications and websites, which were used by an employee within a chosen period.
5. Discipline (date, arrival to work, departure, time at work, overtime work).

Know more. Risk less.

ZECURION

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.

☎ +1 866 581 09 99

✉ sales@zecurion.com

🌐 www.zecurion.com

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
- Cybersecurity Excellence Awards Winner 2021; “Top Fraud and Breach Solution Providers – 2020” by Enterprise Security Magazine; SC Labs Recommended: 5.00/5 score

150+
partners

10,000
customers worldwide

Recognized by “Big 3”:

Gartner IDC FORRESTER

www.zecurion.com

ZECURION