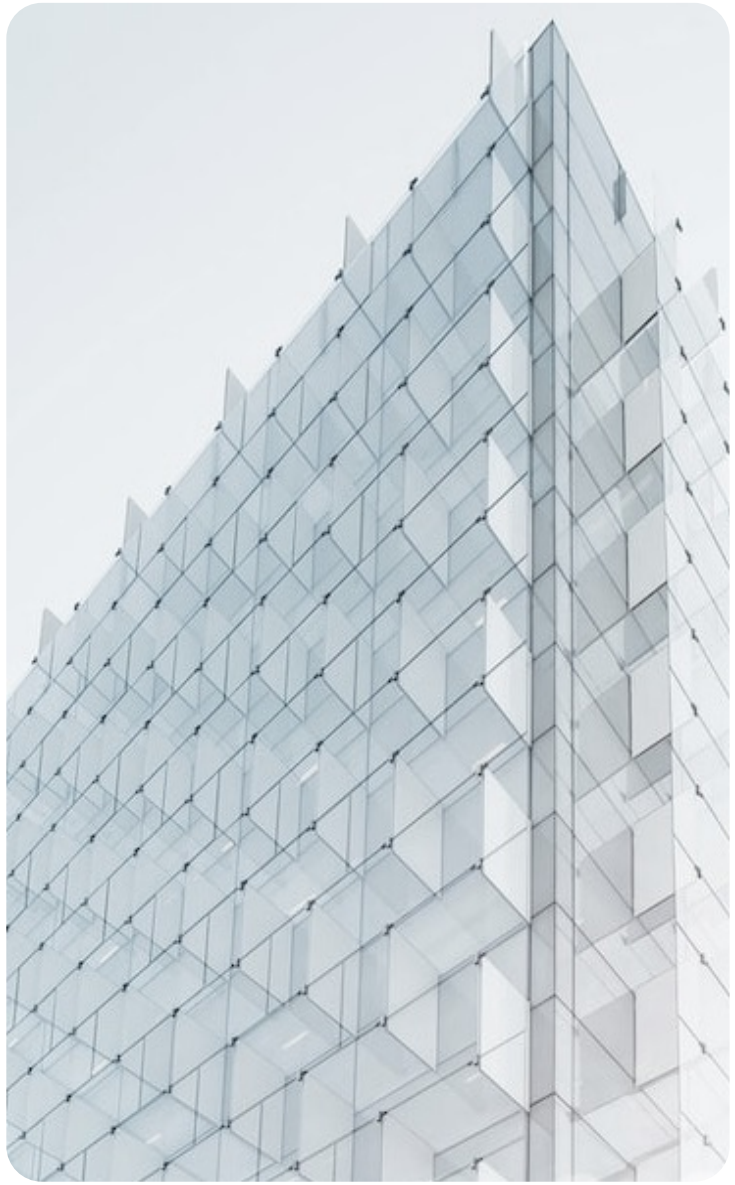
ZECURION

ZECURION
DLP INTRODUCTION
2023



/ Zecurion / Zecurion / Zecurion

INTRODUCING
ZECURION

ZECURION

About Zecurion

- Established in **2001**
- Focused **internal security** vendor
- Offices and **Moscow** and **New York**
- More than **10,000 customers** from SMB to enterprises on all continents

- Featured by **Gartner**, **IDC**, **Forrester**, Radicati, Markets and Markets, etc.
- Products received numerous **international awards**

ZECURION

PRODUCTS

Zecurion DLP – Data Loss Prevention

Network, endpoint, discovery

Zecurion SWG – Secure Web Gateway

Control access to web sites and protect against mixed threats

Zecurion DCAP – Data-Centric Audit and Protection

Data security monitoring, auditing and governance

ZECURION

ZECURION AWARDS

Cybersecurity Excellence Awards (2021)

Gold Winner

Softshell Vendor Award (Germany, 2017)

Bronze

SC Magazine (2020)

5.00/5 score, Recommended

Enterprise Security Magazine (2020)

Top 10 Fraud and Breach Prevention Solutions

ZECURION

ZECURION
CUSTOMERS

DLP MARKET
FACTS AND TRENDS

DLP MARKET

DRIVING FORCES

Gartner

Regulatory compliance

Intellectual property (IP) and trade secrets protection

NEXT GENERATION DLP

Internal security and forensic investigations

DLP Evolution

ZECURION

NEXT GENERATION DLP

Compliance DLP

IP and trade secret protection DLP

Internal security DLP

?

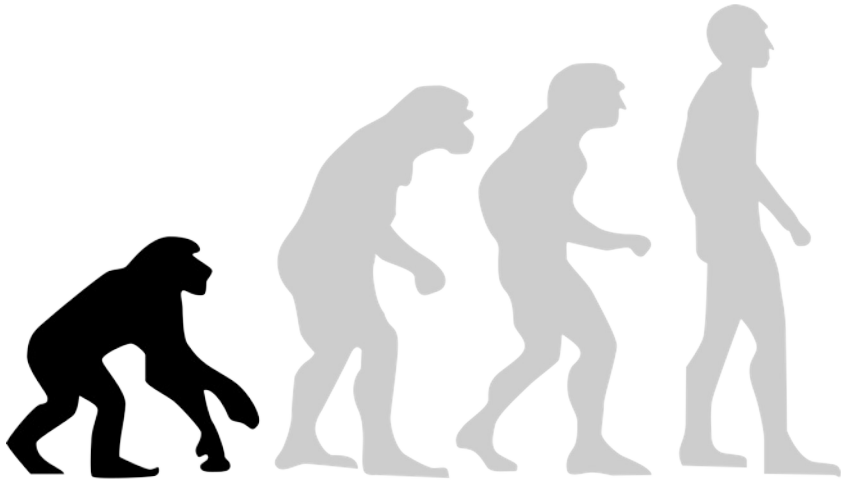
ZECURION

COMPLIANCE
DLP

TREND MICRO

SOPHOS

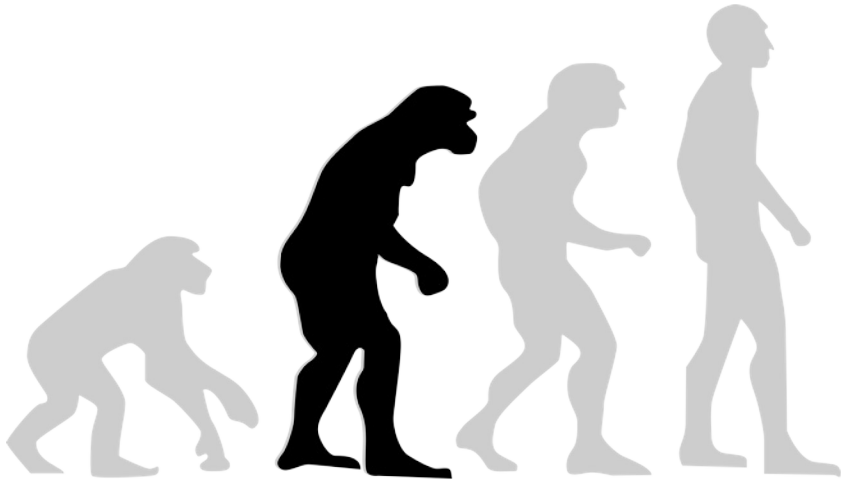
safetica



- **Limited features** and/or channels
- **Embedded feature** in another product (e.g. cloud security gateway)
- **Side product** to extend portfolio (e.g. in AV companies)
- **Relatively easy** implementation and maintenance

ZECURION

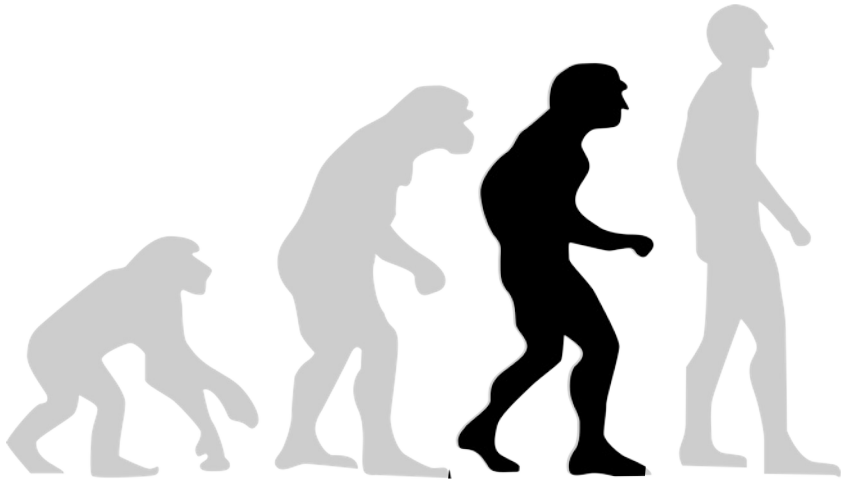
IP PROTECTION
DLP



- **Full coverage** of channels
- **Standalone** product
- **Advanced content detection** (fingerprints, machine learning)
- **Requires more attention** during deployment and maintenance
- **Transitionary class** to the next level

Internal security
DLP

ZECURION



- **All features** of IP Protection DLP
- Advanced features for **forensic investigations and internal control**
- **Powerful tool** for security officers
- “Money Loss Prevention”

ZECURION

COMPLIANCE & INTERNAL SECURITY

Protection from leaks of **regulated data** (PII/PHI/…)

Users are **honest** (“good guys”), but make mistakes

Ask **user’s confirmation** of suspicious operation

“**Fire & forget**” usage scenario

“**Checkmark**” solution for Cloud Cuckoo Land

Internal control, security and forensic investigation

Users are **malicious**

Hide endpoint agent from the user

Security officers **permanently** work with the system

Organization-level **Big Brother**

ACFE REPORT 2020

ZECURION

Global study on occupational fraud and abuse

2,504 cases, 125 countries

Total loss more than $3.6 billion

Average loss is $1.5 million

Organizations lose 5% of revenue to fraud each year => $4.5 trillion globally

CONCEPT

ZECURION DLP

ZECURION

Classic DLP: protection from data leaks

Zecurion DLP: protection from insider threats

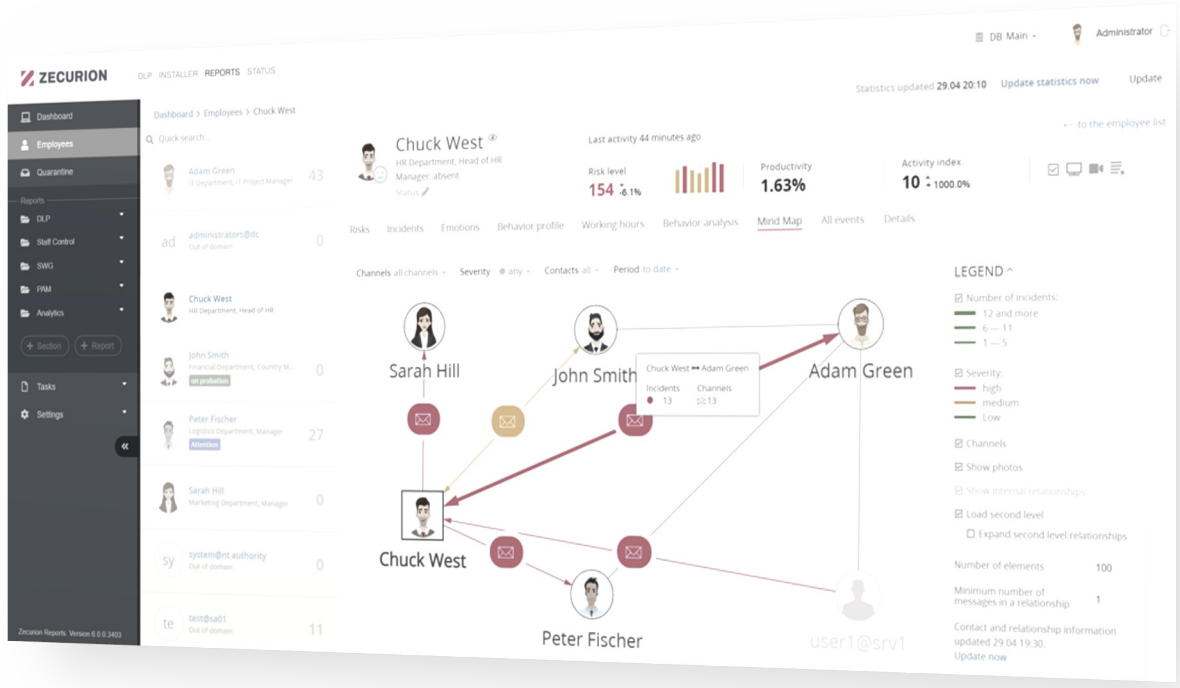
- Data leaks prevention
- Detection of internal fraud
- Reveal employee's misbehavior
- Conduct forensic investigations
- Improve internal security

ZECURION DLP
UNIQUE FEATURES

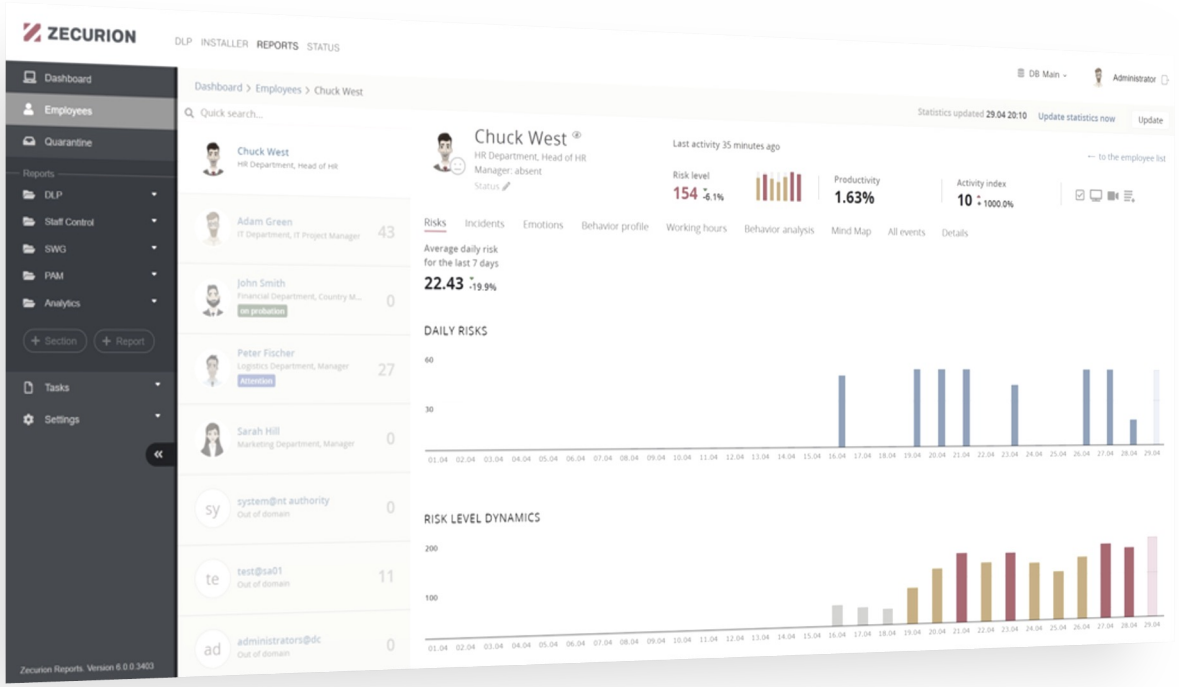
INTELLIGENCE CAPABILITIES

ZECURION

- **Full archive** of files and events
- User behavior analytics (**UBA**)
- Emotional **profiling**
- **Connection diagram** displaying internal users and external contacts



ADVANCED UBA

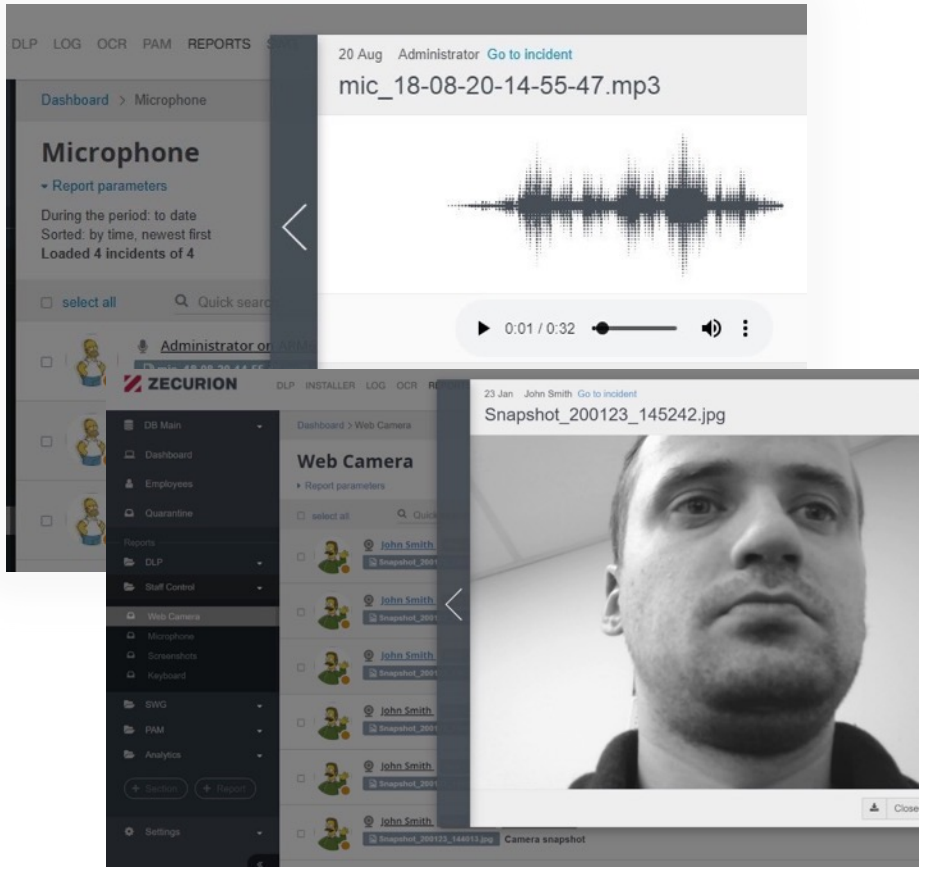


- **UBA** index for each user
- Fast **risk-based assessment**
- **Behavioral profiles** of users and groups, comparison and concordance
- **Detection of anomalies**: activity at holidays, first remote connection, first use of the new device, etc.

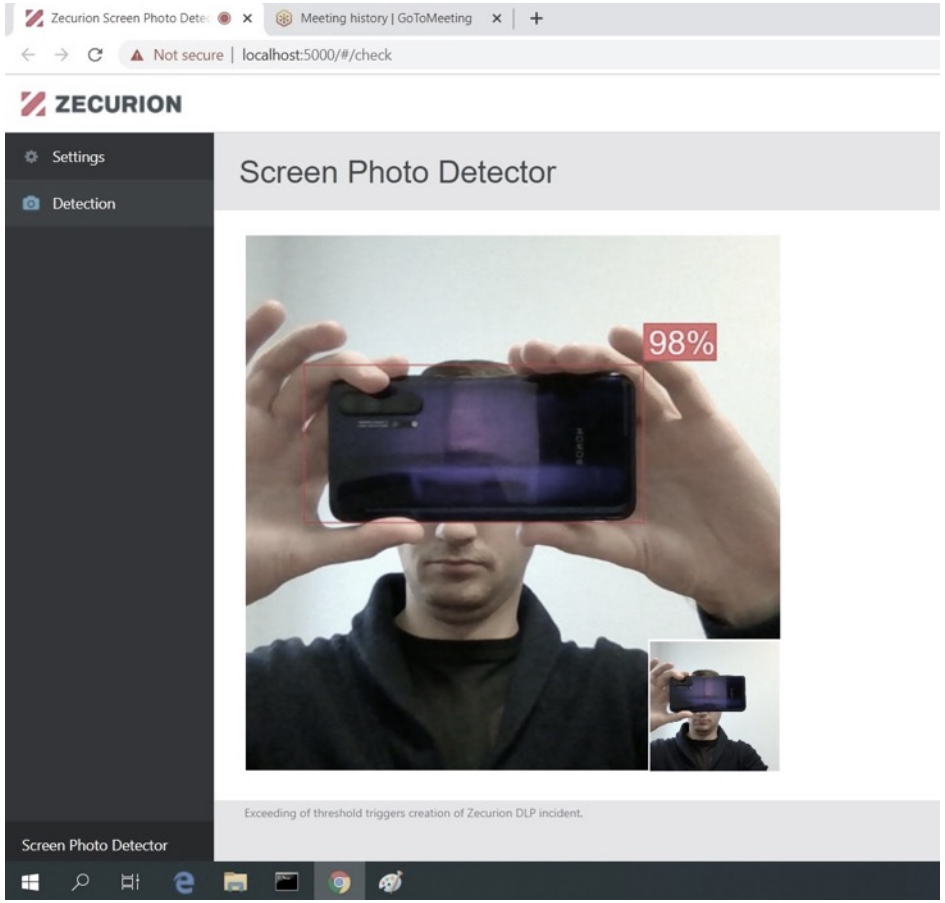
CONTROL CAPABILITIES

ZECURION

- **Keyboard** recording
- User sessions (**screens**) recording
- **Application** control
- **Microphone** recording
- **Webcam** recording



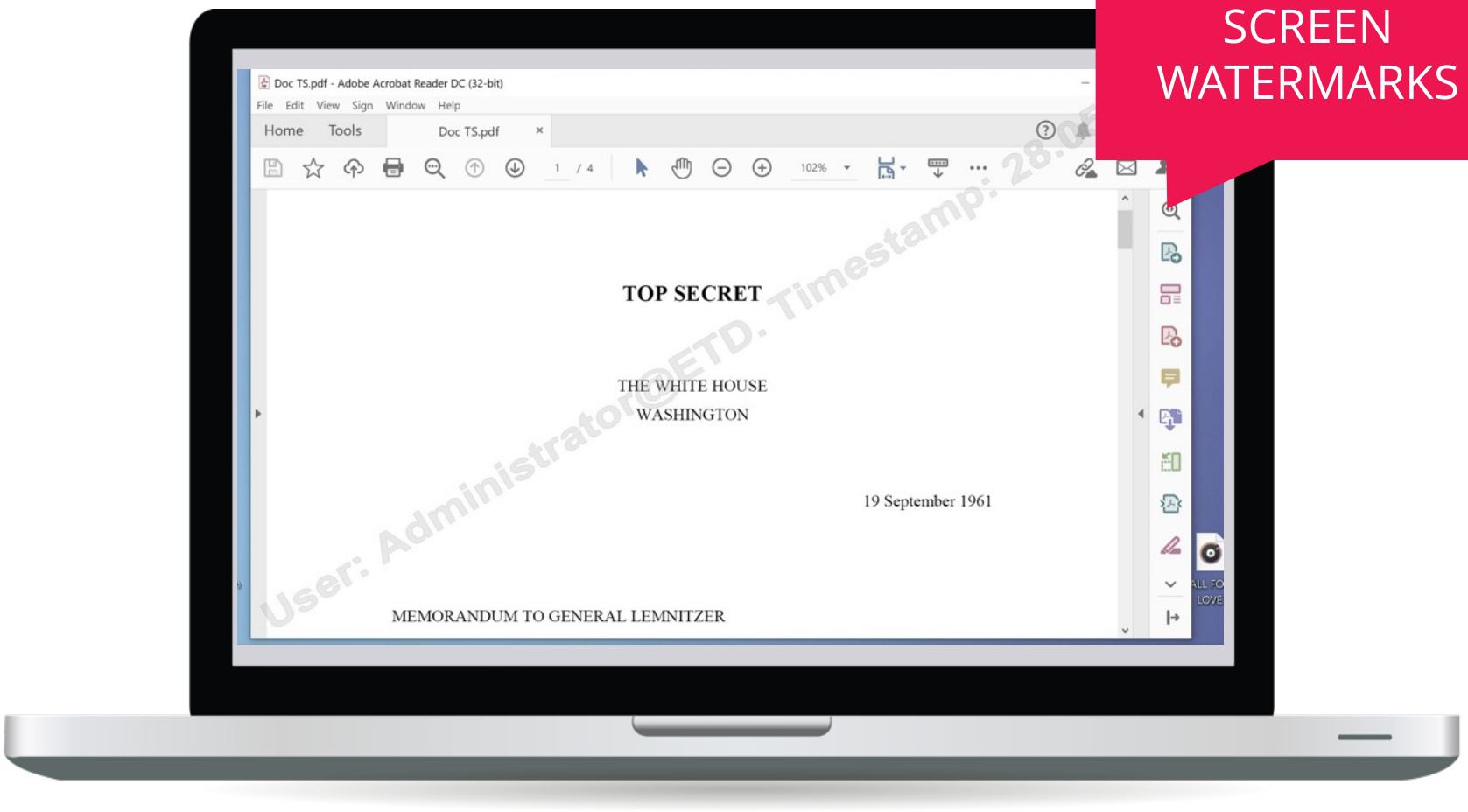
SCREEN PHOTO DETETCTION



- **Detection of attempts** to make a photo of the screen
- Using PC or laptop **web camera**
- **AI-based algorithm** (2 neural networks)
- **Wide choice of reactions**: alerting security officer, saving webcam image and screenshot, blocking user account
- Detection of **all smartphones**

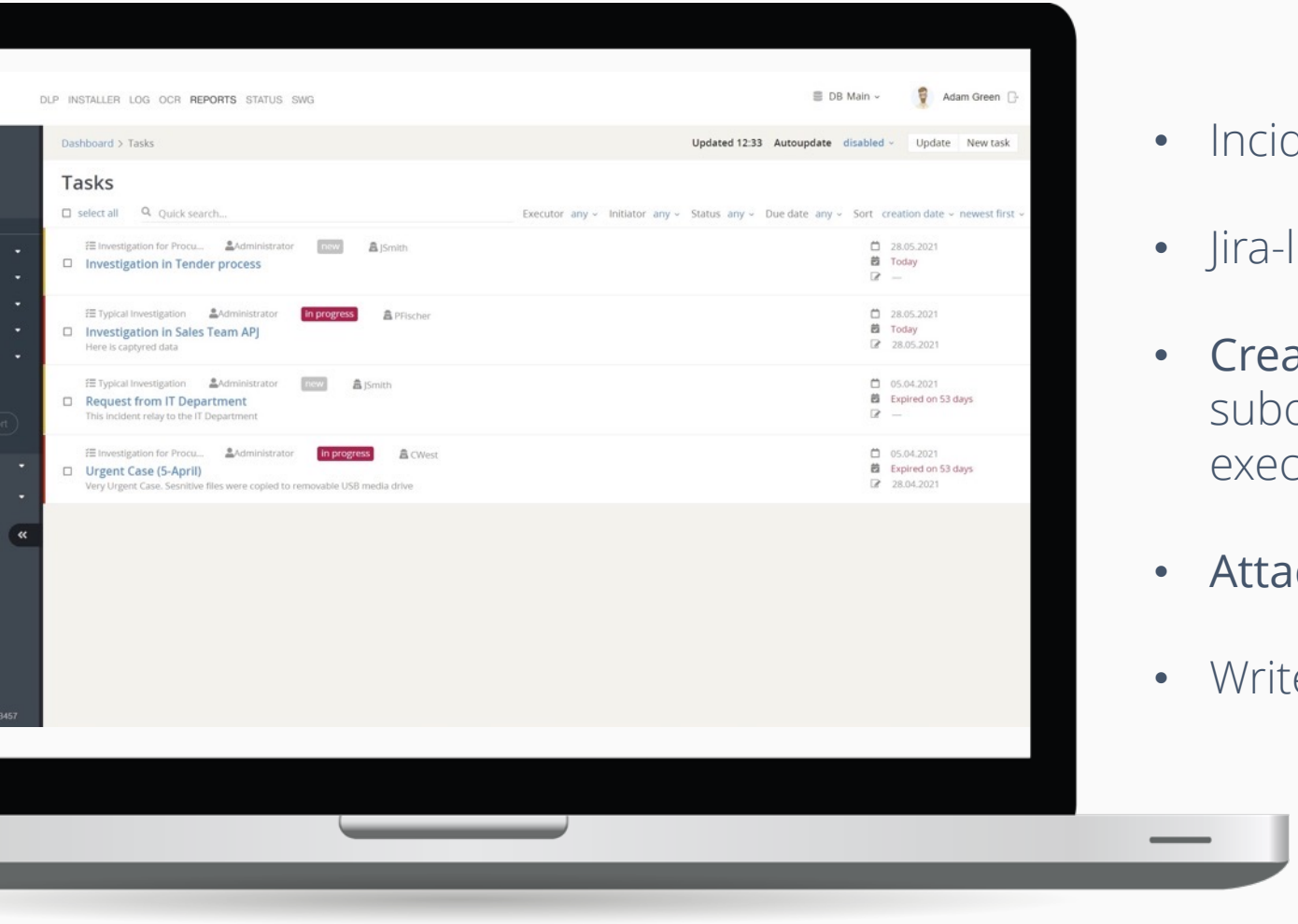
ZECURION

SCREEN WATERMARKS



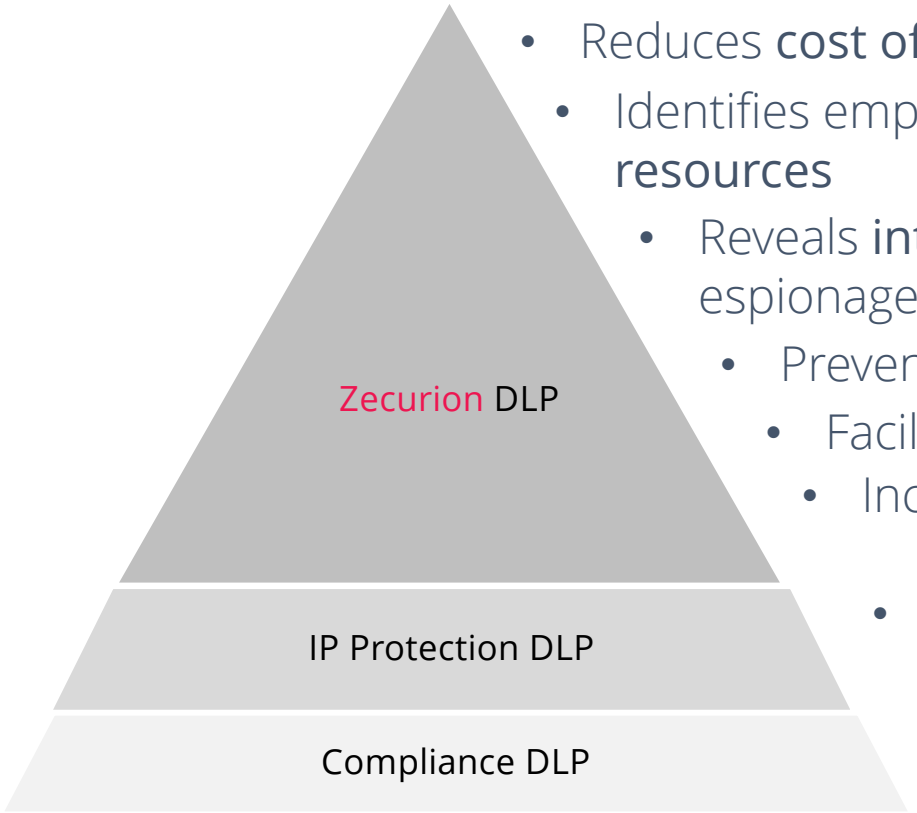
INCIDENT RESPONSE WORKFLOW

ZECURION



- Incident investigation **workflow automation**
- Jira-like **task tracker**
- **Create** new investigation, **assign** tasks to subordinate security officers, **control** execution
- **Attach** incidents and files from DLP archive
- Write **comments**

ZECURION DLP BENEFITS



- Reduces **cost of investigation**
- Identifies employees misbehavior, **misuse of organization's resources**
- Reveals **internal fraud**, financial manipulations, embezzlement, espionage
- Prevents real **financial losses**
- Facilitates **early risk detection** and mitigation
- Increases **comfort level** of senior management
- Protects **sensitive data** from leaks
- Provides **compliance**

ZECURION DLP
DETAILS

KEY FACTS

ZECURION

- Three components
- Exists since 2005
- Totally rebuilt in 2014
- Modern look
- New technologies
- Unifying architecture concept

Traffic Control

Device Control

Discovery

Staff Control

KEY FEATURES

ZECURION

- **Control** all possible data leak channels
- **Omni-channel** policies
- File content **extraction and analysis**
- **Single web console** with customizable dashboard and iPad application
- **Full archive** for investigation and retrospective analysis
- **Powerful reports** builder
- **Flexible access** control
- **13 deployment options**: fits any IT infrastructure
- **Integration**: TITUS, SIEM, REST API

DLP POLICY

ZECURION

Define rules

- 10+ content-detection technologies
- Scans the data inside of files and archives
- 500+ file types including encrypted and camouflaged files
- Context attributes (user, host IP, ...)
- Composite rules using AND, OR and NOT logical operators

Select data leakage channel

- Network channels and internet services

- Local devices and ports

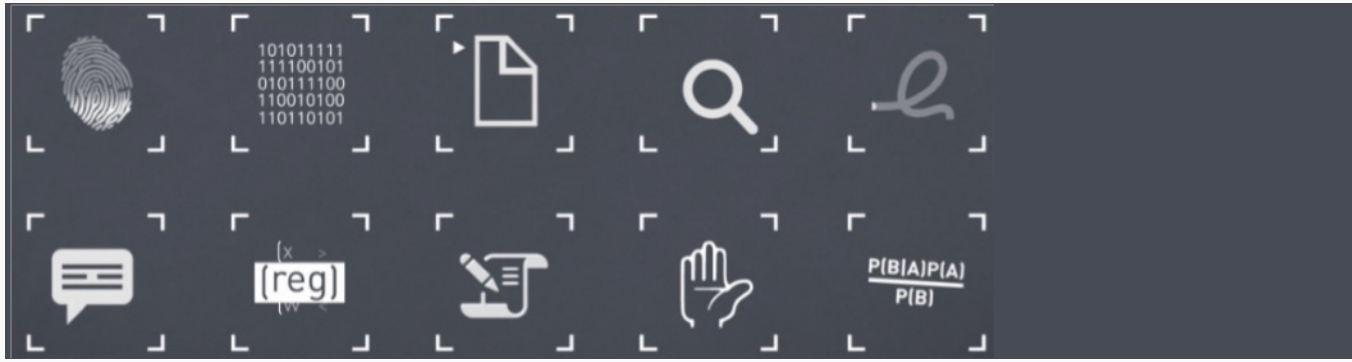
Set an action

- Block
- Save to the archive
- Notify user and/or security officer
- Put to quarantine for manual inspection
- Remove attachment
- ...

ZECURION

DETECTION

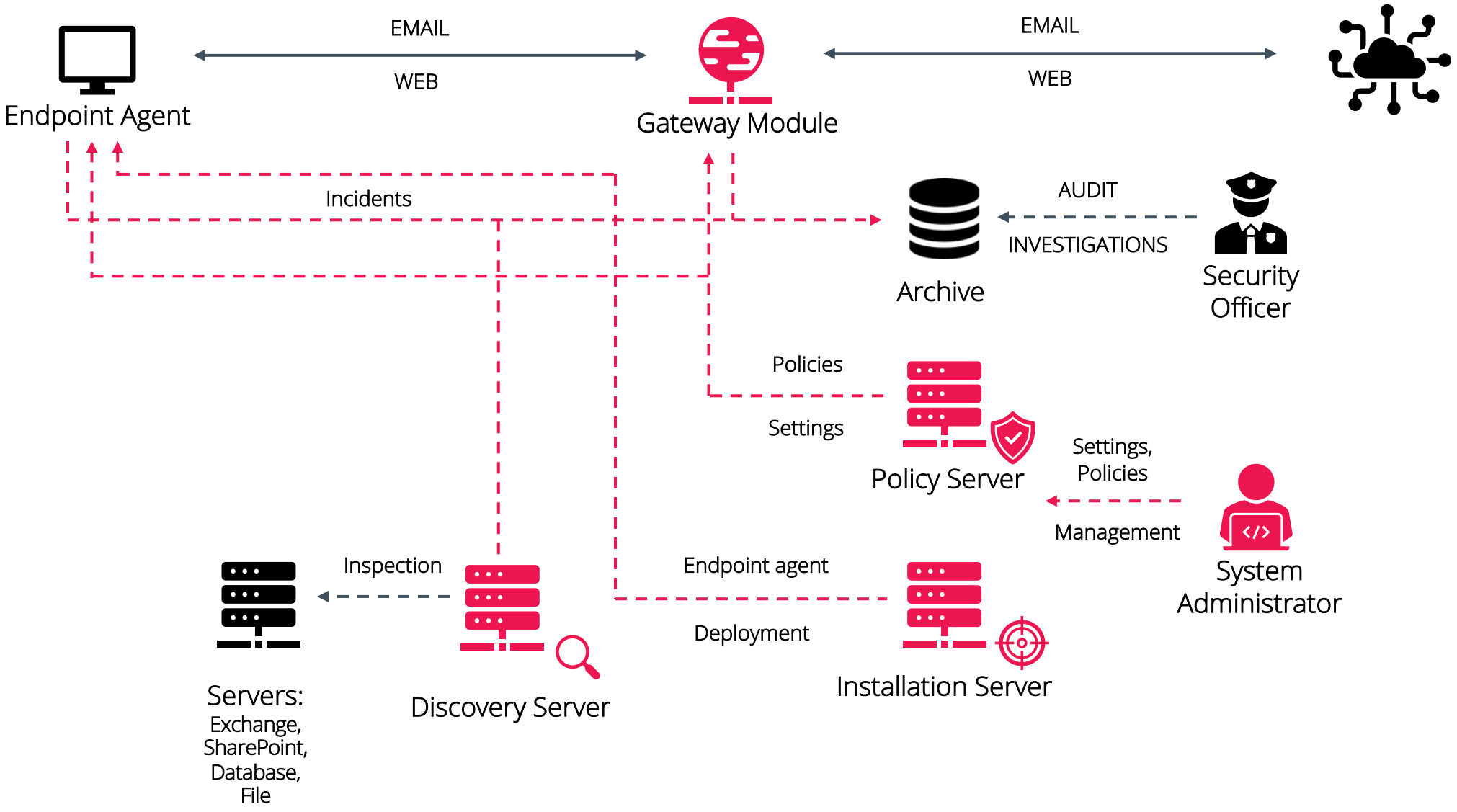
TECHNOLOGIES



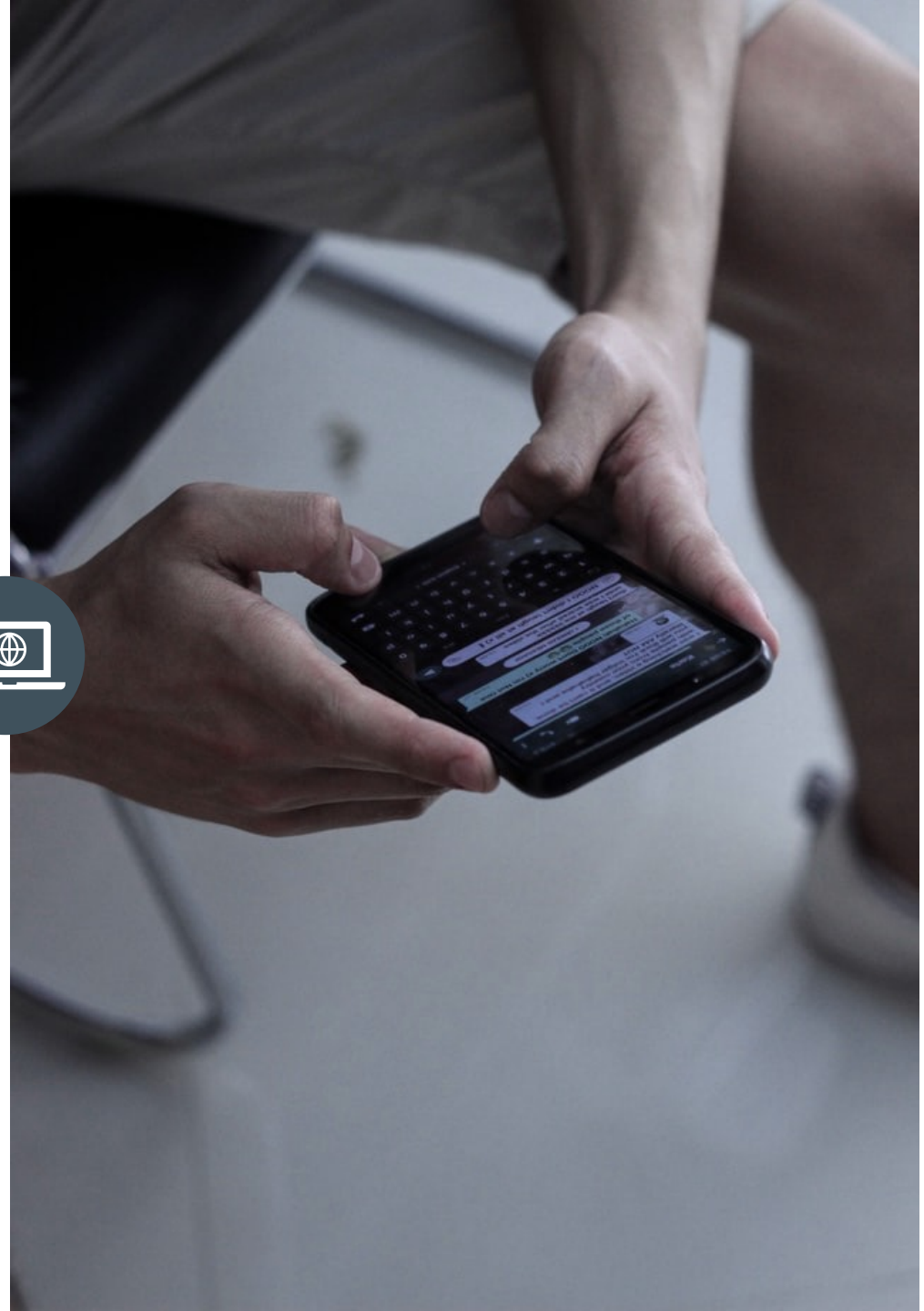
- Keywords and dictionaries
- Morphology
- Regular expressions
- Templates
- Digital fingerprints
- Machine learning: Bayes
- Machine learning: SVM
- AI-based image templates
- OCR
- Manual inspection

DLP ARCHITECTURE

ZECURION



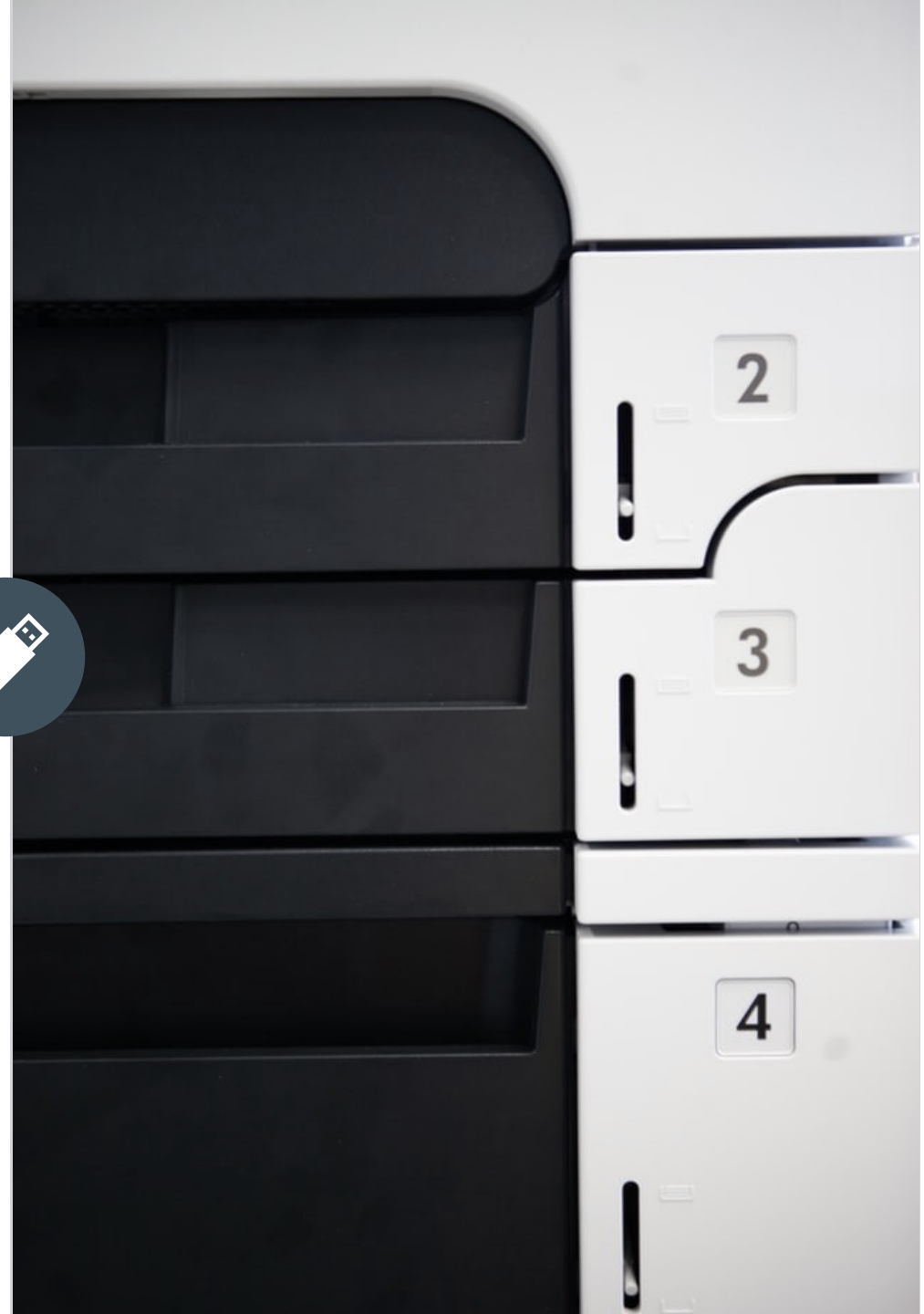
TRAFFIC CONTROL



ZECURION

- Total **control of internet channels**: email, webmail, social networks, messengers, cloud, etc.
- **Support of messengers**: Skype, MS Teams, WhatsApp and Telegram
- **Analysis of SSL-encrypted traffic** both on endpoint and gateway level
- **Support of modern cloud services**, such as Office 365 and Google Docs

DEVICE CONTROL



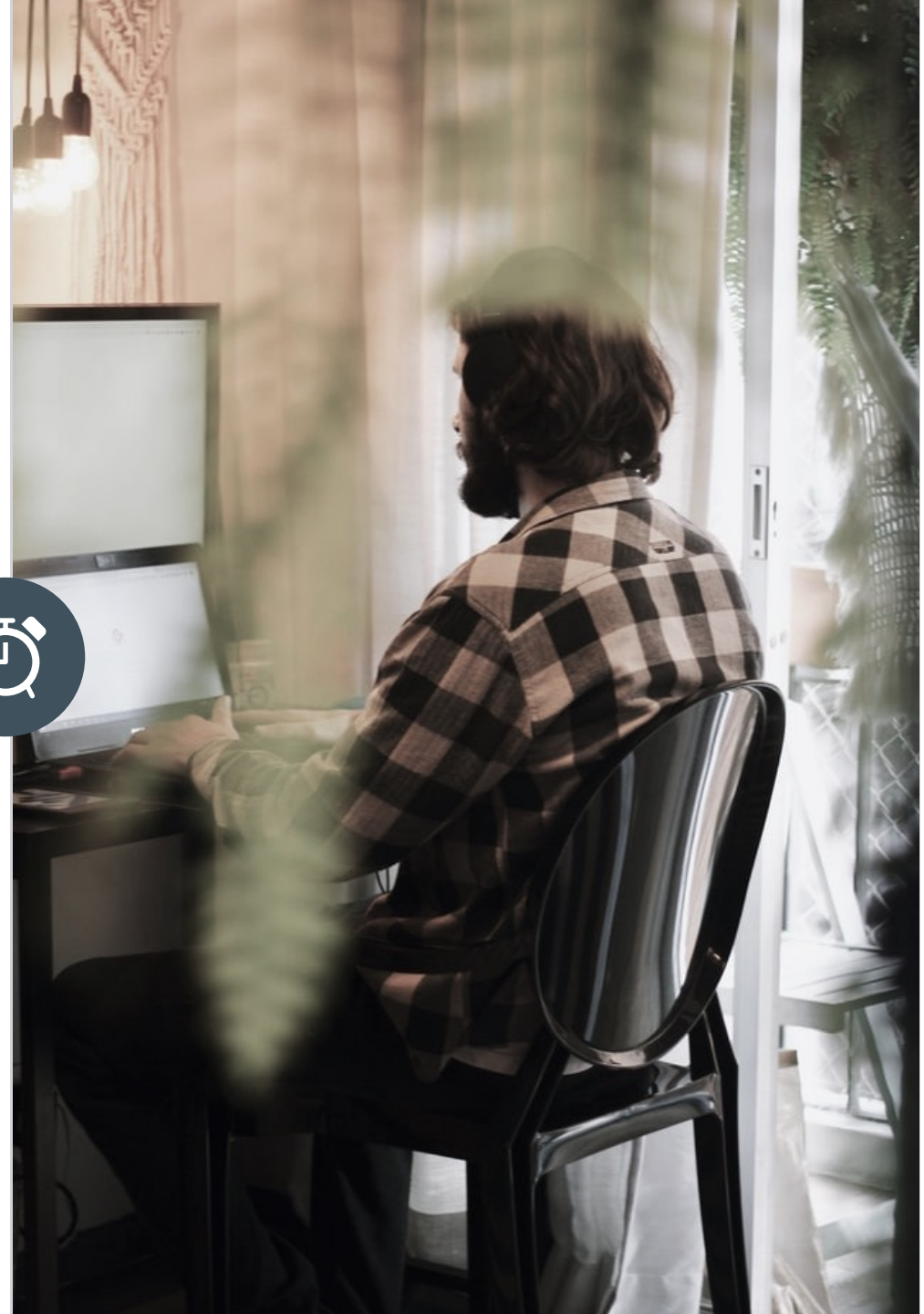
ZECURION

- **Granular access control** for peripheral devices
- **Company-wide device catalog** for easy policy creation
- **Shadow copy** of files being written to external drive or printed
- **Content-based** policies
- **Encryption** of files
- **Centralized deployment** and management
- **Grant device access** by email or phone request
- **Tamper-proof** agent

DISCOVERY

- **Detect** improperly stored sensitive data
- Scan of **all possible data storage locations**: local/network drives, MS Exchange and SharePoint, any database, cloud
- **Flexible scan parameters** – daily/weekly/monthly for selected computers/OUs
- **Real-time discovery** – scan file on close
- **File flow tracking** inside the network

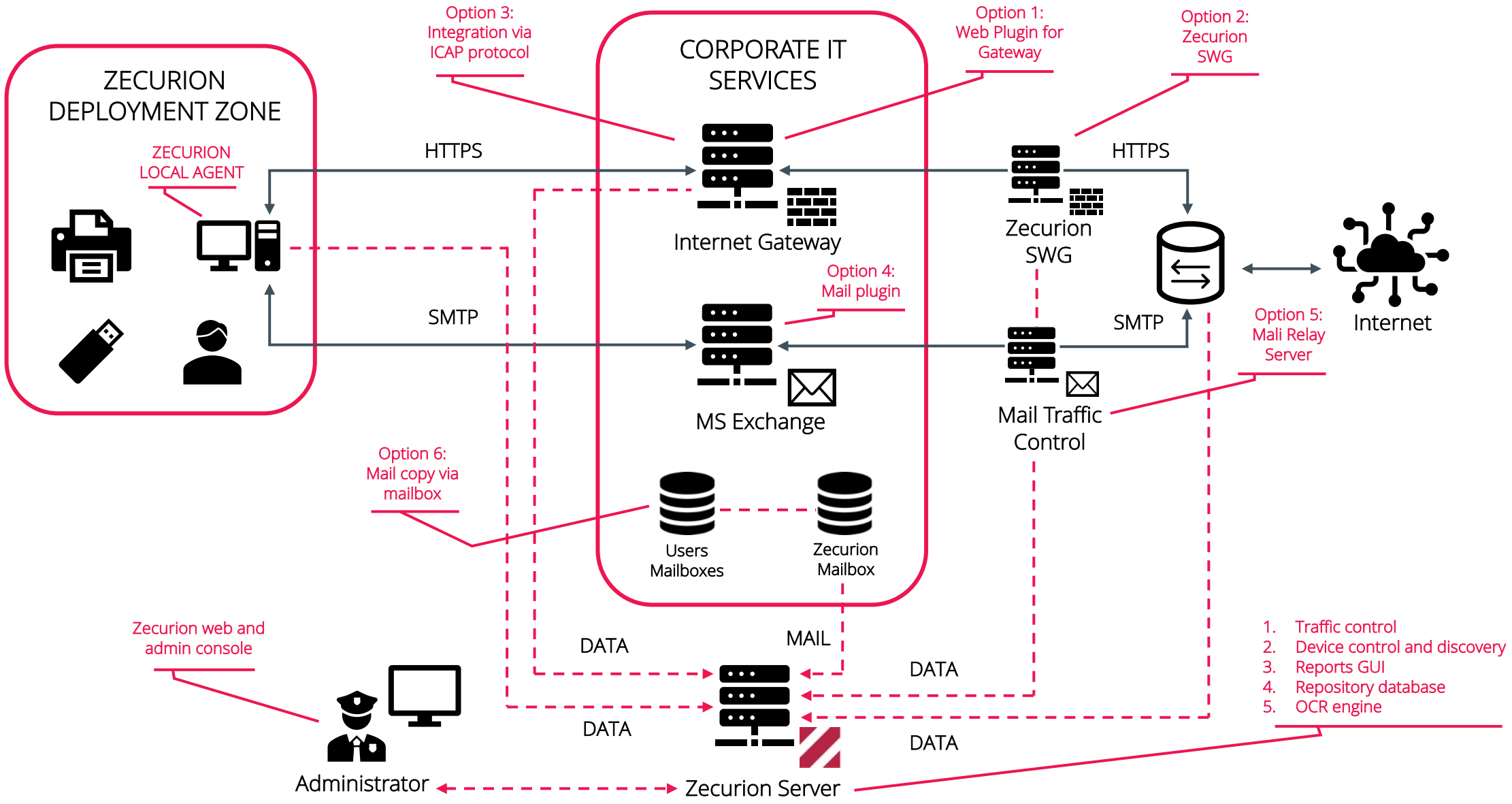
STAFF CONTROL



- **Employees discipline supervision**, both in office and in remote environment
- **Workplace monitoring**: logon/logoff, websites and application usage, activity
- **Websites and application** categories
- **Discipline reports**: late arrivals, early leaving, breaks, time at work, overtime work
- Overall **productivity index**
- **Timesheets**

HOW TO DEPLOY

ZECURION



USE CASES

ZECURION

"Zecurion Device Control not only **met our expectations** in terms of functionality, but also proved to be very **easy to use** and **efficient to manage**»

Allianz

Industry

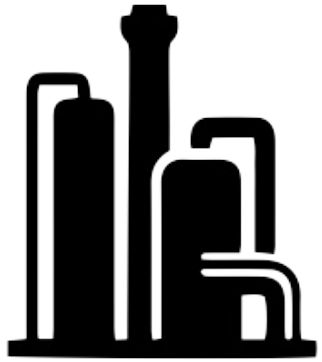
Insurance

Product

Zecurion Device Control

USE CASE

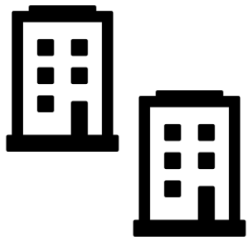
ZECURION



Oil refinery plant

Sells products to fake intermediaries with significant discounts

Set of bogus firms



Resell products to real customers for normal price

Real customers

Difference pocketed by organized insiders group

USE CASE INVESTIGATION

ZECURION

Detection

Managers including C-level engaged in suspicious communications with external contacts, exchanged irrelevant documents

Loss

$25.2M annually

Technologies

Email and instant messengers control, connection diagram, UBA, microphone recording, user session recording

Legal aspect

3 key members of the group were fired, lawsuit for the compensation of damage, criminal case

THANK YOU!

LET'S DISCUSS?