ZECURION DLP INTRODUCTION

19 Feb 2019

Dr. Alexey Raevsky, MBA
CEO @ Zecurion

ZECURION

Agenda

- Data Leak Prevention market overview and driving forces
- DLP evolution
- DLP architecture and features

INTRODUCING ZECURION

About Zecurion

- Established in 2001
- Focused internal security vendor
- Offices in 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 PAM — Privileged Access Management

Control and record sessions of privileged users

Zecurion SWG — Secure Web Gateway

Control access to web sites and protect against mixed threats

Zecurion Awards

- Bronze, Softshell Vendor Award (Germany, 2017)
- Gold Winner, Golden Bridge Awards (USA, 2014)
- Gold in Hot Companies & Organizations, Bronze in Security Software, Network Products Guide (USA, 2014)
- Best Products and Services, Network Products Guide (USA, 2009)
- Tomorrow’s Technology Today and Global Product Excellence, Info Security Products Guide (USA, 2009)
- Product of the Year (Russia, 2007 and 2008)

Zecurion Customers

CRÉDIT AGRICOLE

SOCIETE GENERALE

СВЯЗНОЙ

СБЕРБАНК

ГАЗПРОМ

РОСНЕФТЬ

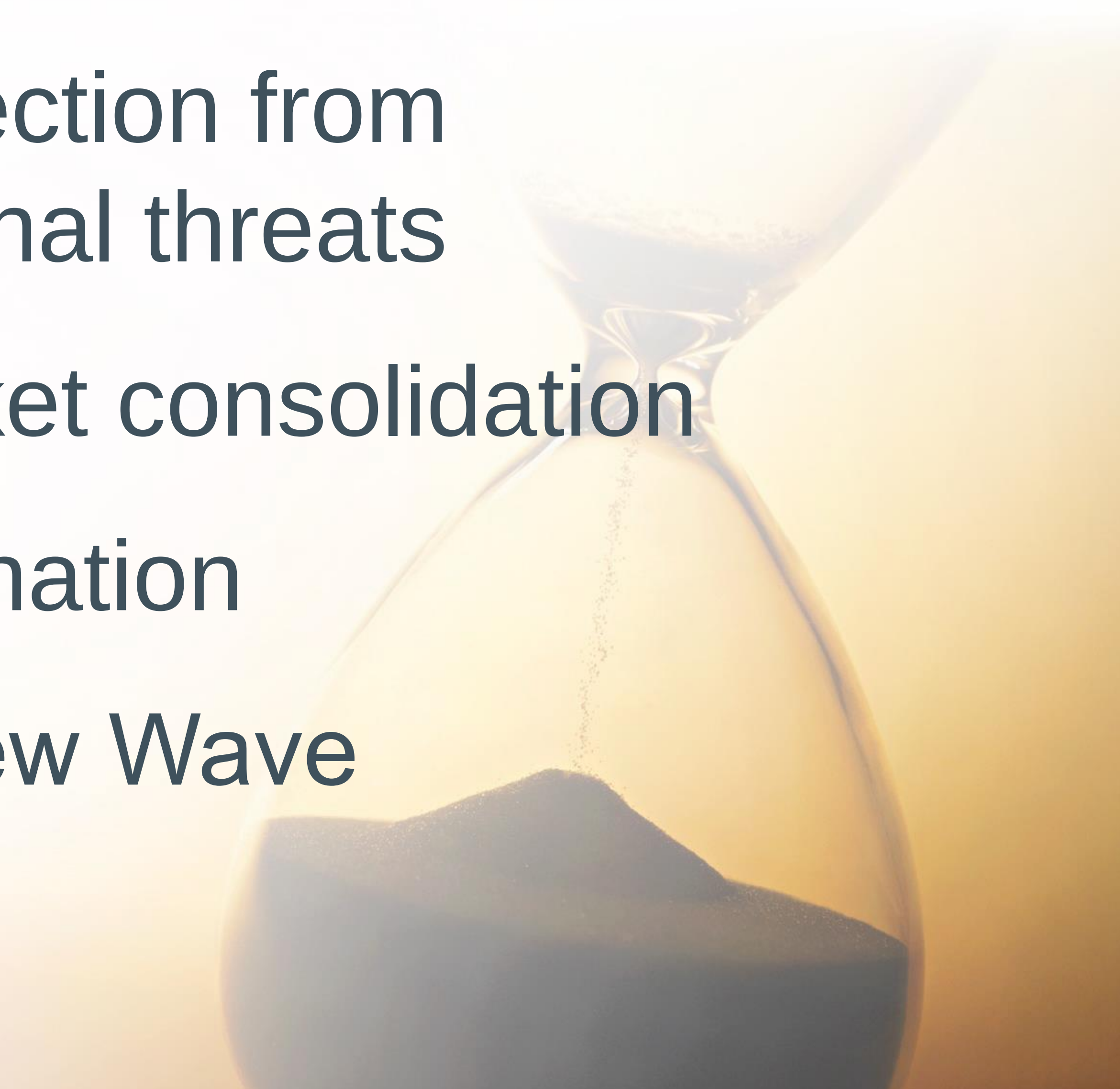
ВТБ ПЕНСИОННЫЙ ФОНД

Allianz

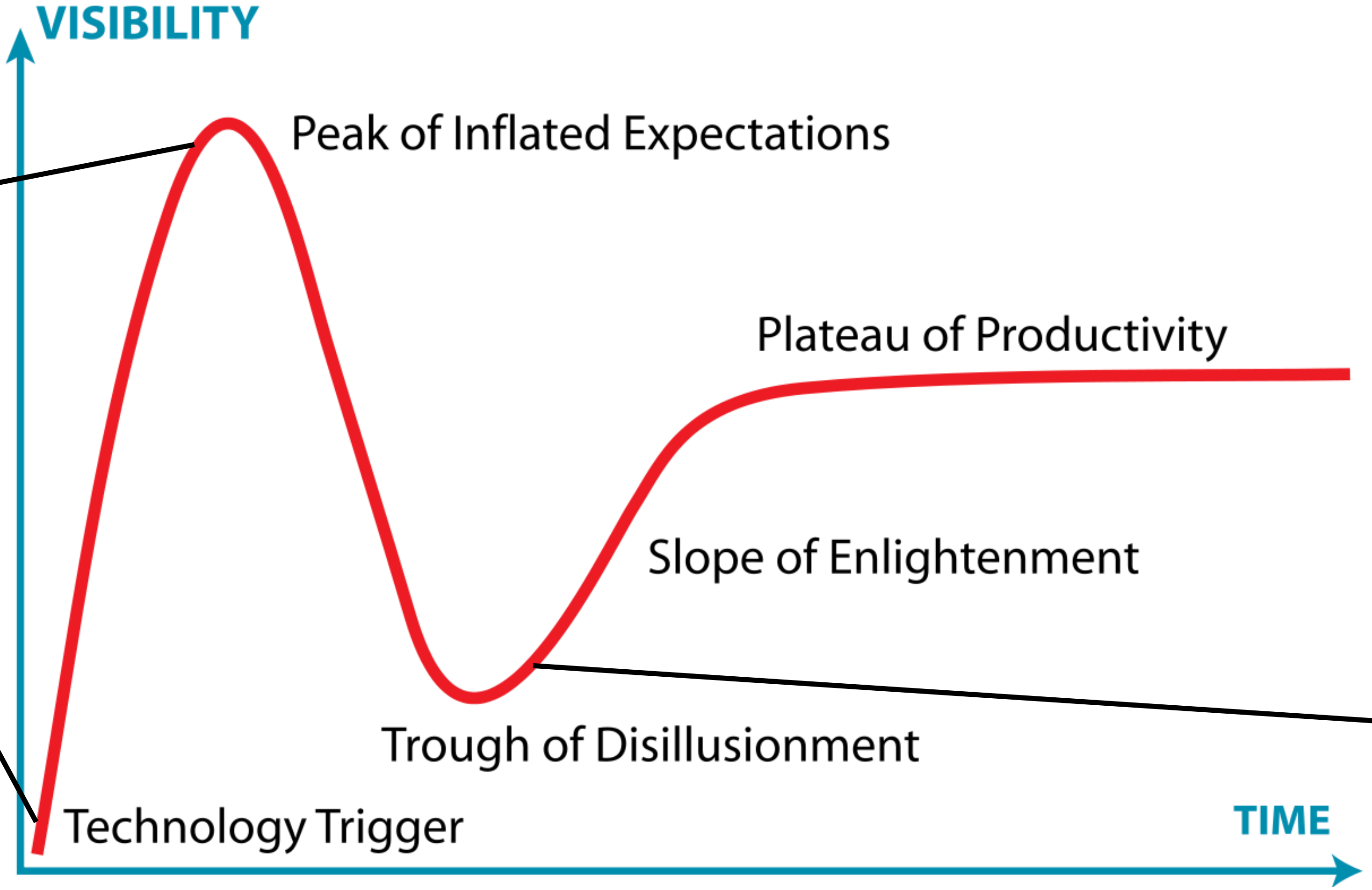
DLP MARKET FACTS AND TRENDS

DLP Historical Overview

- 2000-2001: protection from internal vs. external threats
- 2007-2008: market consolidation
- 2008-2016: stagnation
- 2017-…: DLP New Wave



DLP Market Now



2007-2008

2000-2001

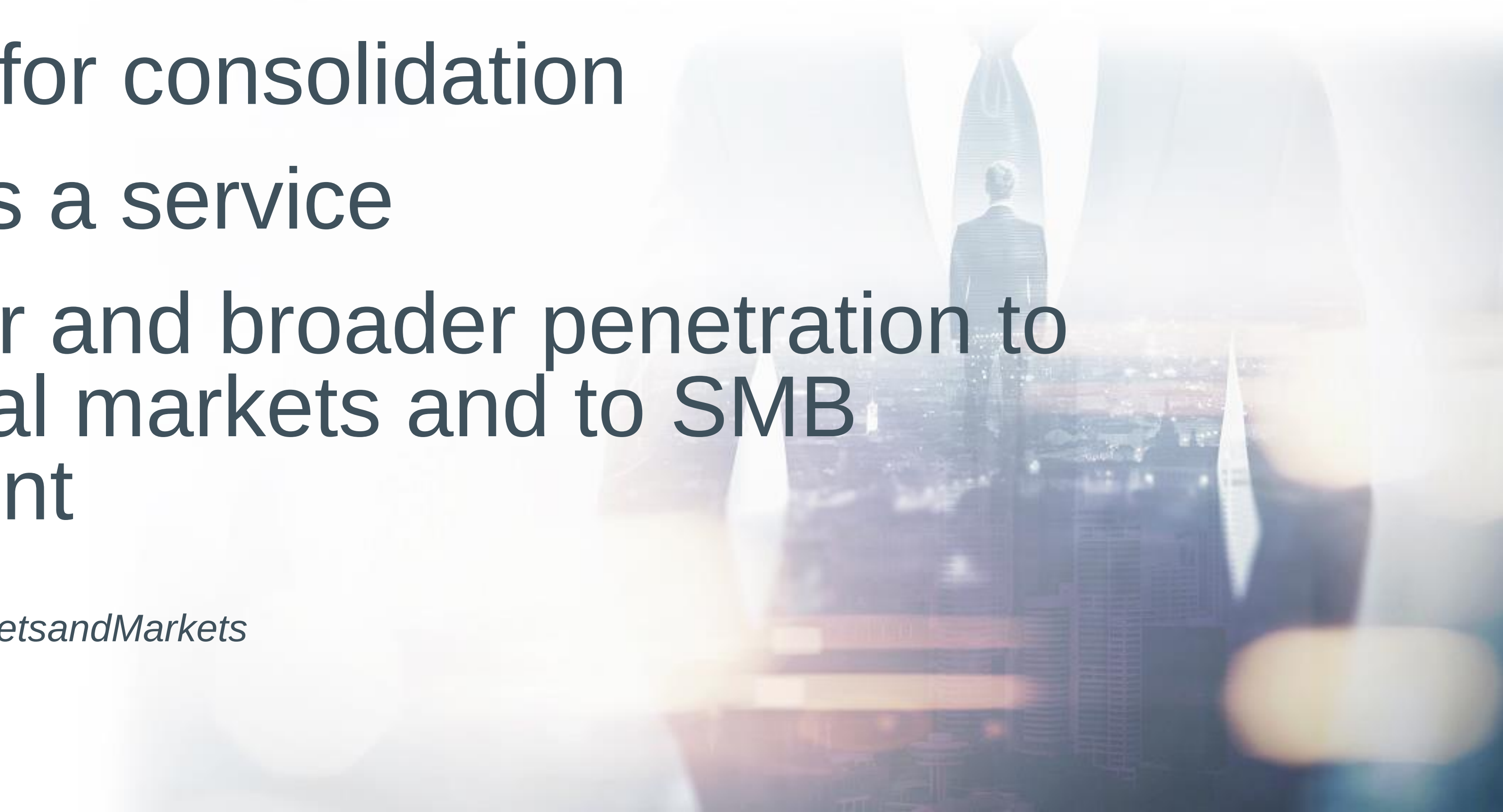
NOW

ZECURION

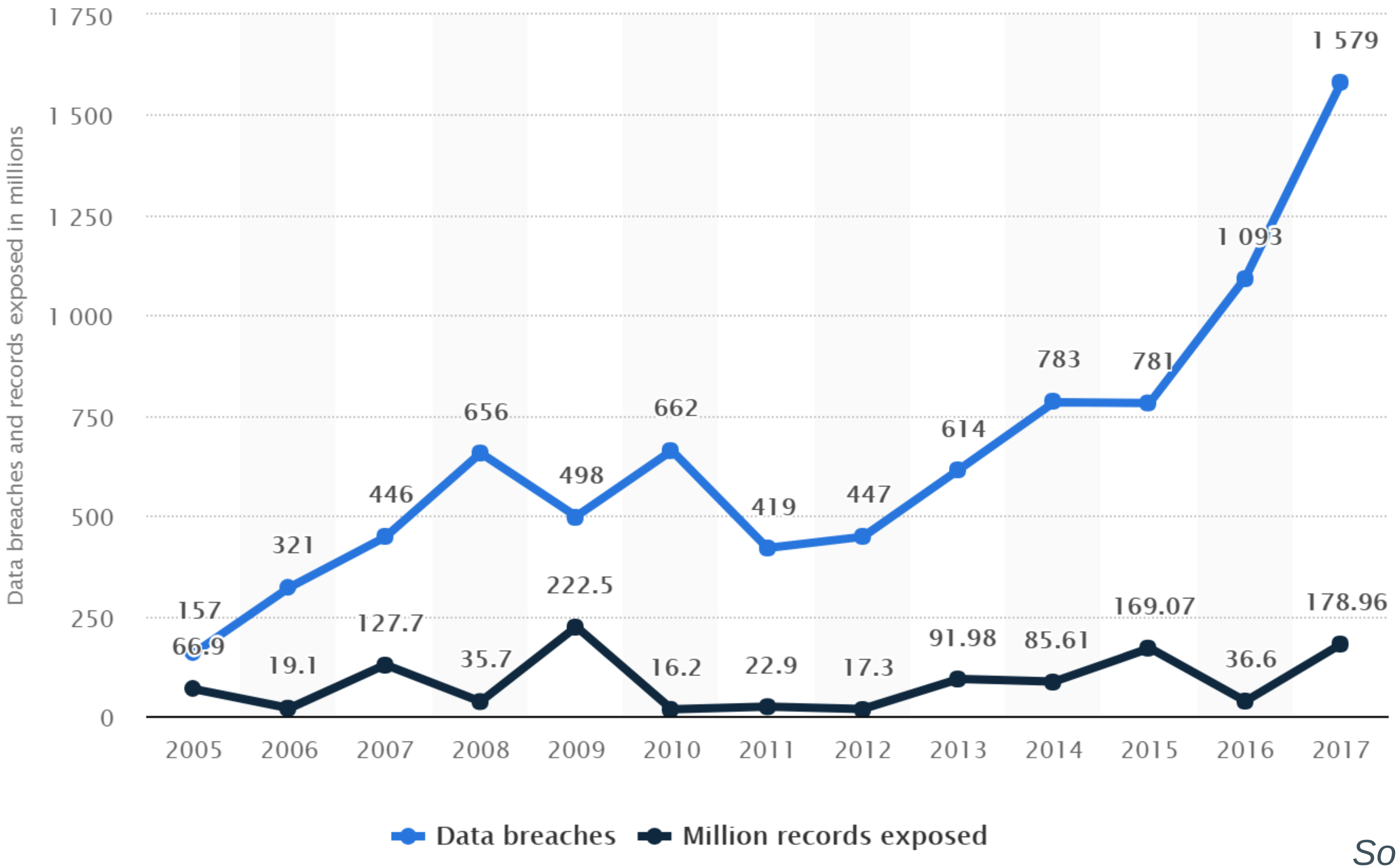
DLP Market Overview

- Will grow from $0.96bn in 2015 to $2.64 by 2020 (CAGR 22.3%)*
- Room for consolidation
- DLP as a service
- Deeper and broader penetration to regional markets and to SMB segment

** Source: MarketsandMarkets*



Data Breach Statistics



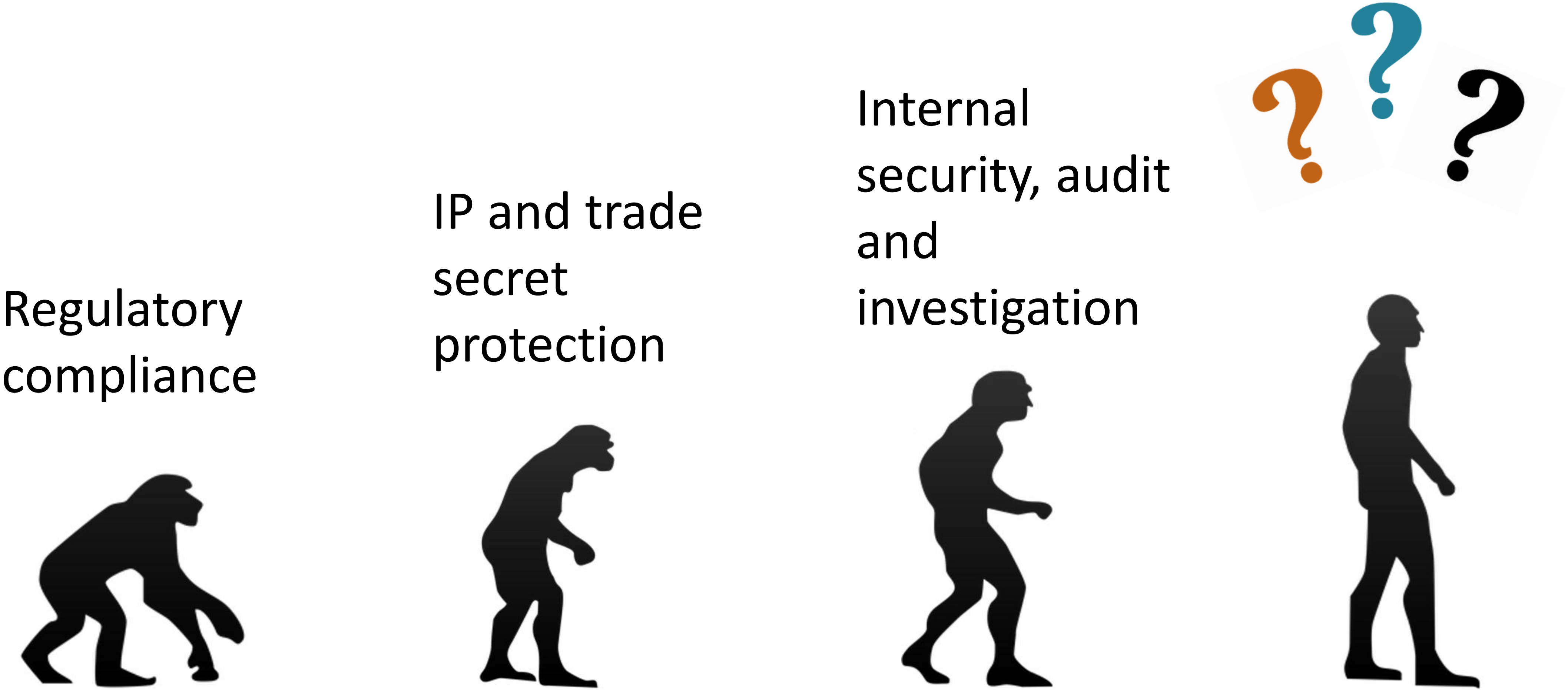
ZECURION

Source: Statista

DLP Market Driving Forces

- Regulatory compliance
- Intellectual property (IP) and trade secrets protection
- Internal control & security, audit & investigations

DLP Evolution

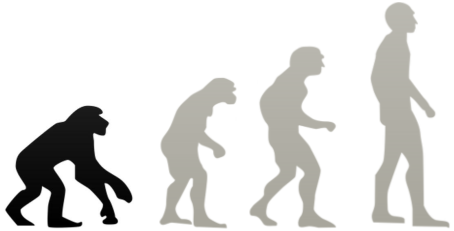


Regulatory compliance

IP and trade secret protection

Internal security, audit and investigation

DLP FOR COMPLIANCE



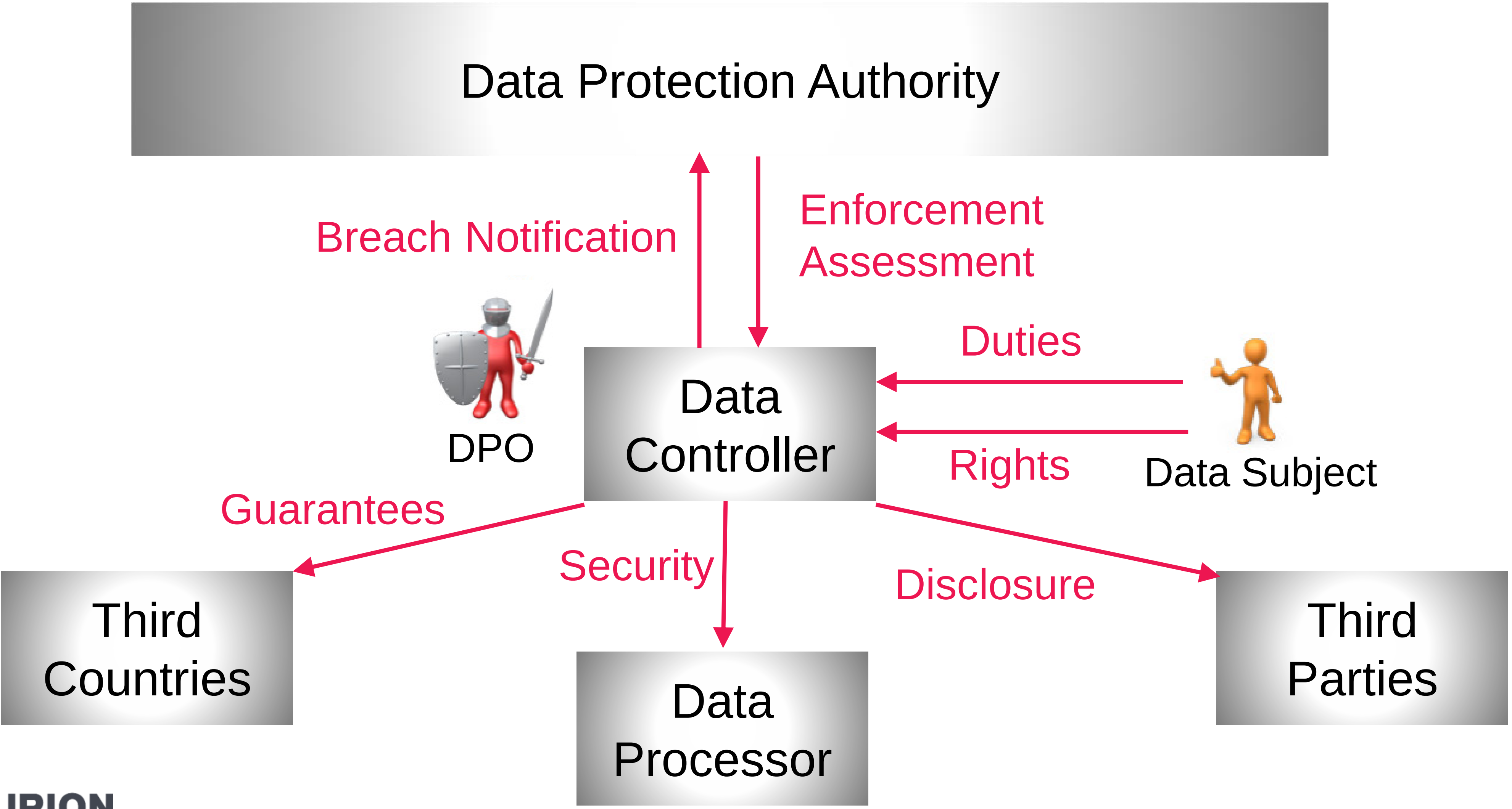
Regulations: National & Industry

- US regulations
  - Fragmented legislations for certain sectors and states (HIPAA, GLBA, CA SB 1386)
- Industry standards (PCI DSS)

Regulations: GDPR

- Most important change in data privacy regulation in the past 20 years
- Intended to strengthen and unify data protection for individuals
- Came into force 25 May 2018
- Extends the scope of EU privacy law to all entities processing data of EU residents

GDPR Model



Data Protection Authority

Breach Notification

Enforcement
Assessment

DPO

Data Controller

Duties

Rights

Data Subject

Guarantees

Security

Disclosure

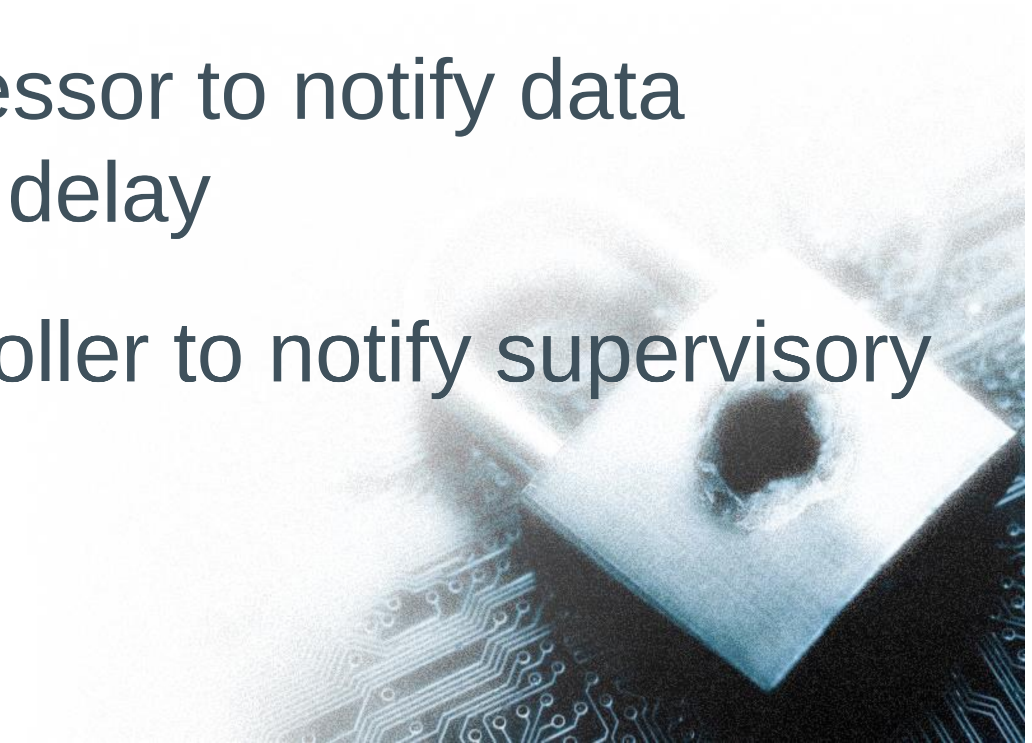
Third Countries

Data Processor

Third Parties

GDPR: Data Breaches

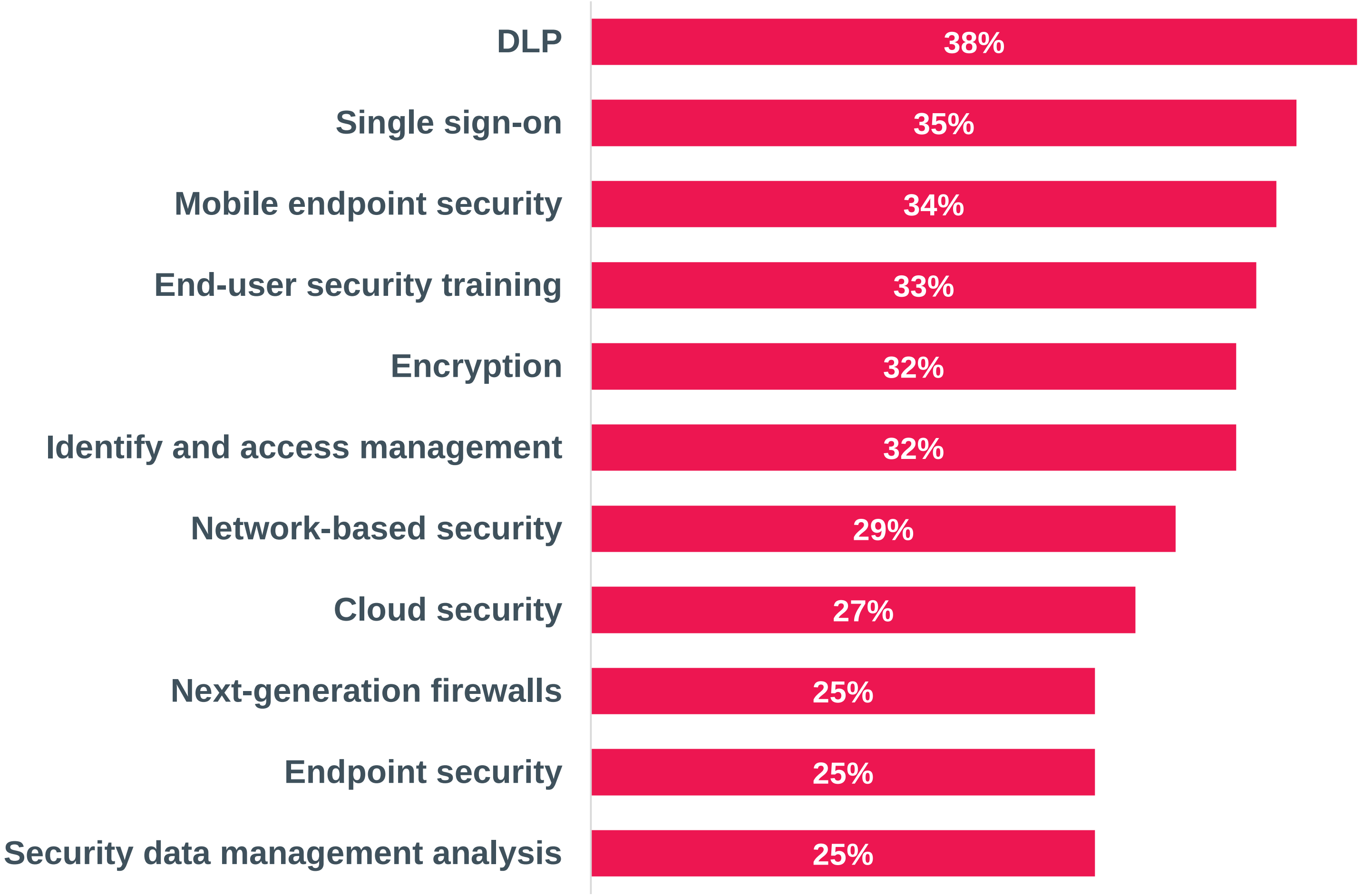
- Personal data breach: destruction, loss, alteration, unauthorized disclosure of or access to personal data
- Obligation for data processor to notify data controller without undue delay
- Obligation for data controller to notify supervisory authority within 72 hours



Liabilities and Penalties

- Persons’ rights for judicial remedy in the courts if their rights have been infringed
- Persons’ rights for compensation of damage from the controller or processor
- Controller is liable for damage caused by processor
- Administrative fines are up to €20M or up to 4% of the annual worldwide turnover

Top Security Initiatives

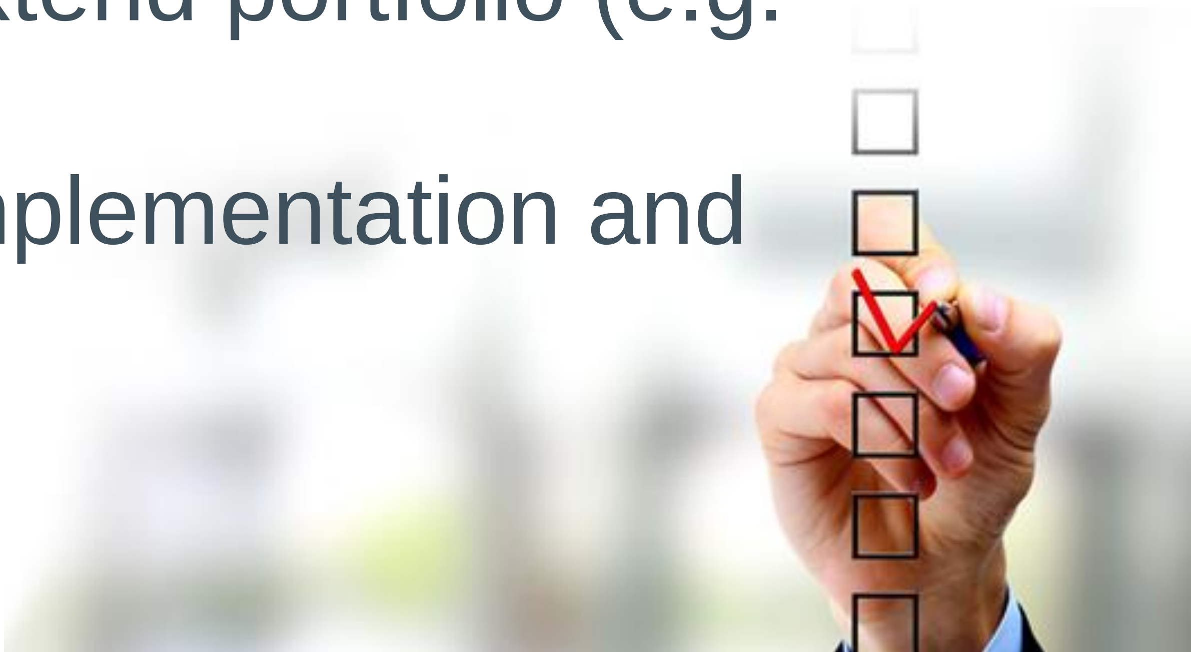


ZECURION

Source: Computer Weekly

Compliance DLP

- 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

Compliance Philosophy

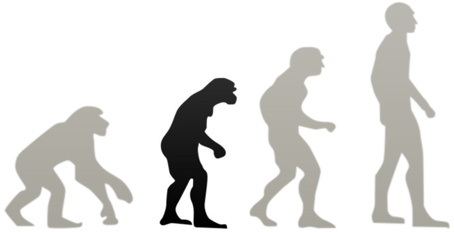
- Main purpose – protection from leaks of regulated data (PII, PHI, etc)
- Main driver – compliance
- Users are honest (“good guys”), but make mistakes
- Signature feature – user’s confirmation of suspicious operation
- Typical scenario – “fire & forget”
- Archive stores only incidents
- “Checkmark” solution

TREND MICRO™

SOPHOS

safetica

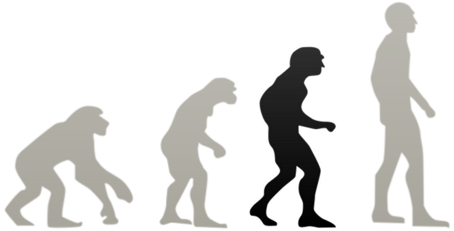
DLP FOR IP PROTECTION



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

DLP FOR INTERNAL SECURITY



Internal Security DLP

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

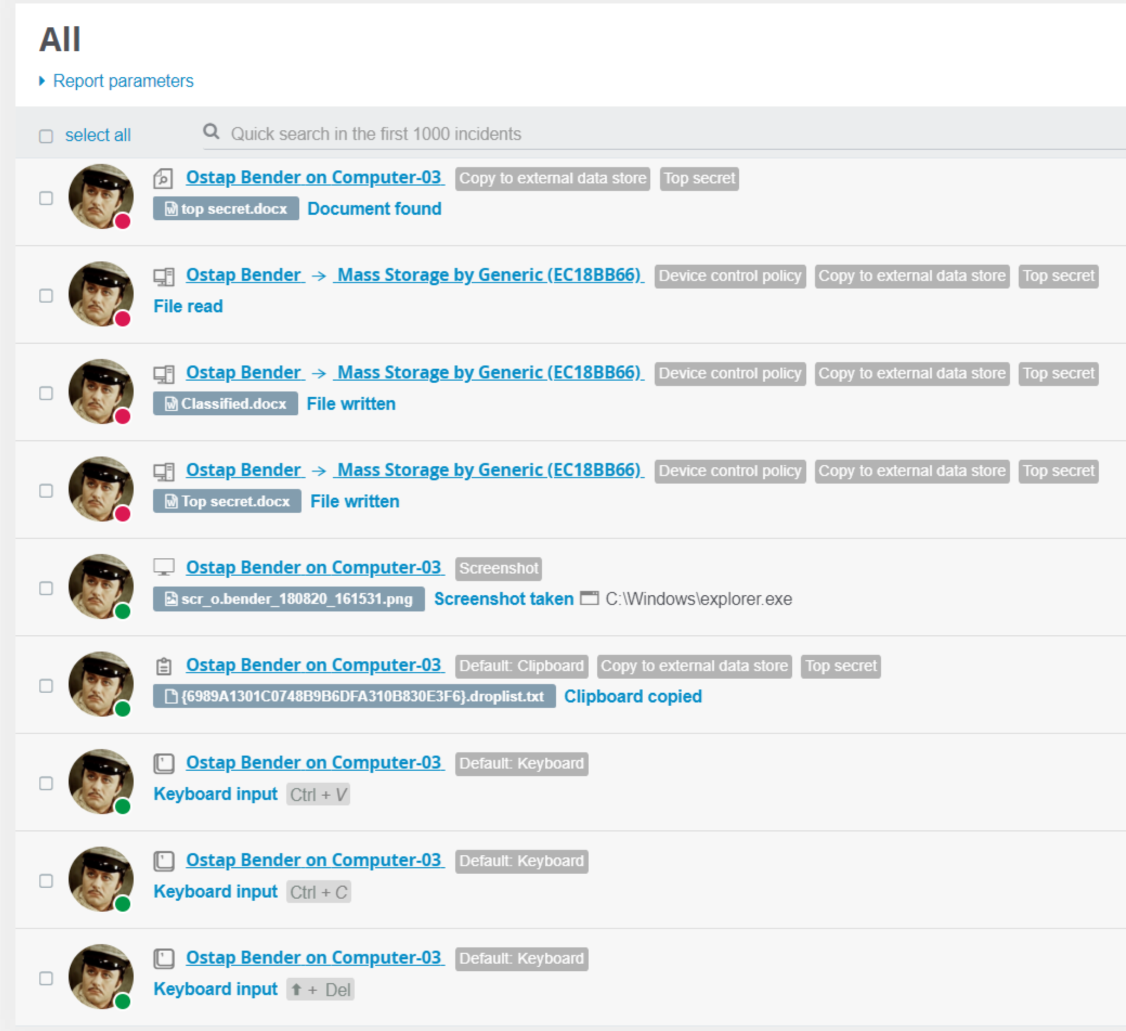
ZECURION

Security Philosophy

- Main purpose – internal control and forensic investigation
- Main driver – security
- Users are malicious
- Signature feature – hide endpoint agent from the user
- Typical scenario – one or more security officers permanently work with the system
- Archive stores all events and files
- Corporate “big brother”

Archive of Files and Events

- Store all files and events in a single database
- Shadow copies of files
- Fast search and reports
- Apply new policy to the archive
- Interactive table and graphic reports
- Pre-installed reports
- Customizable dashboard with widgets



All

▸ Report parameters

□ select all — Quick search in the first 1000 incidents

□ Ostap Bender on Computer-03 | Copy to external data store | Top secret
top secret.docx | Document found

□ Ostap Bender → Mass Storage by Generic (EC18BB66) | Device control policy | Copy to external data store | Top secret
File read

□ Ostap Bender → Mass Storage by Generic (EC18BB66) | Device control policy | Copy to external data store | Top secret
Classified.docx | File written

□ Ostap Bender → Mass Storage by Generic (EC18BB66) | Device control policy | Copy to external data store | Top secret
Top secret.docx | File written

□ Ostap Bender on Computer-03 | Screenshot
scr_o.bender_180820_161531.png | Screenshot taken | C:\Windows\explorer.exe

□ Ostap Bender on Computer-03 | Default: Clipboard | Copy to external data store | Top secret
{6989A1301C0748B9B6DFA310B830E3F6}.droplist.txt | Clipboard copied

□ Ostap Bender on Computer-03 | Default: Keyboard
Keyboard input | Ctrl + V

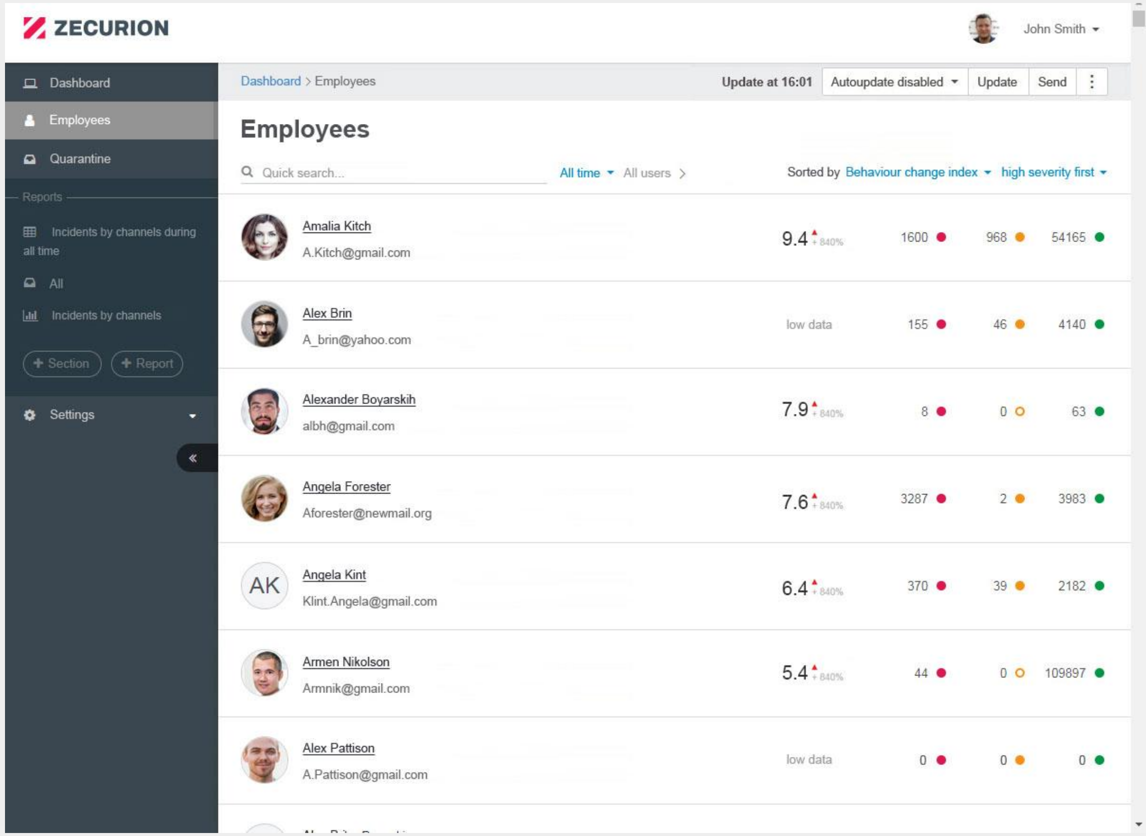
□ Ostap Bender on Computer-03 | Default: Keyboard
Keyboard input | Ctrl + C

□ Ostap Bender on Computer-03 | Default: Keyboard
Keyboard input | ⬆ + Del

ZECURION

User Behavior Analysis

- Calculates User Behavior Analytics (UBA) index for each user
- Displays UBA index dynamics
- Alerts security officer on unexpected deviations
- Proactive protection
- Helps to prevent security incident before it happens



Dashboard > Employees

Update at 16:01 | Autoupdate disabled | Update | Send

Employees

Quick search... All time All users >

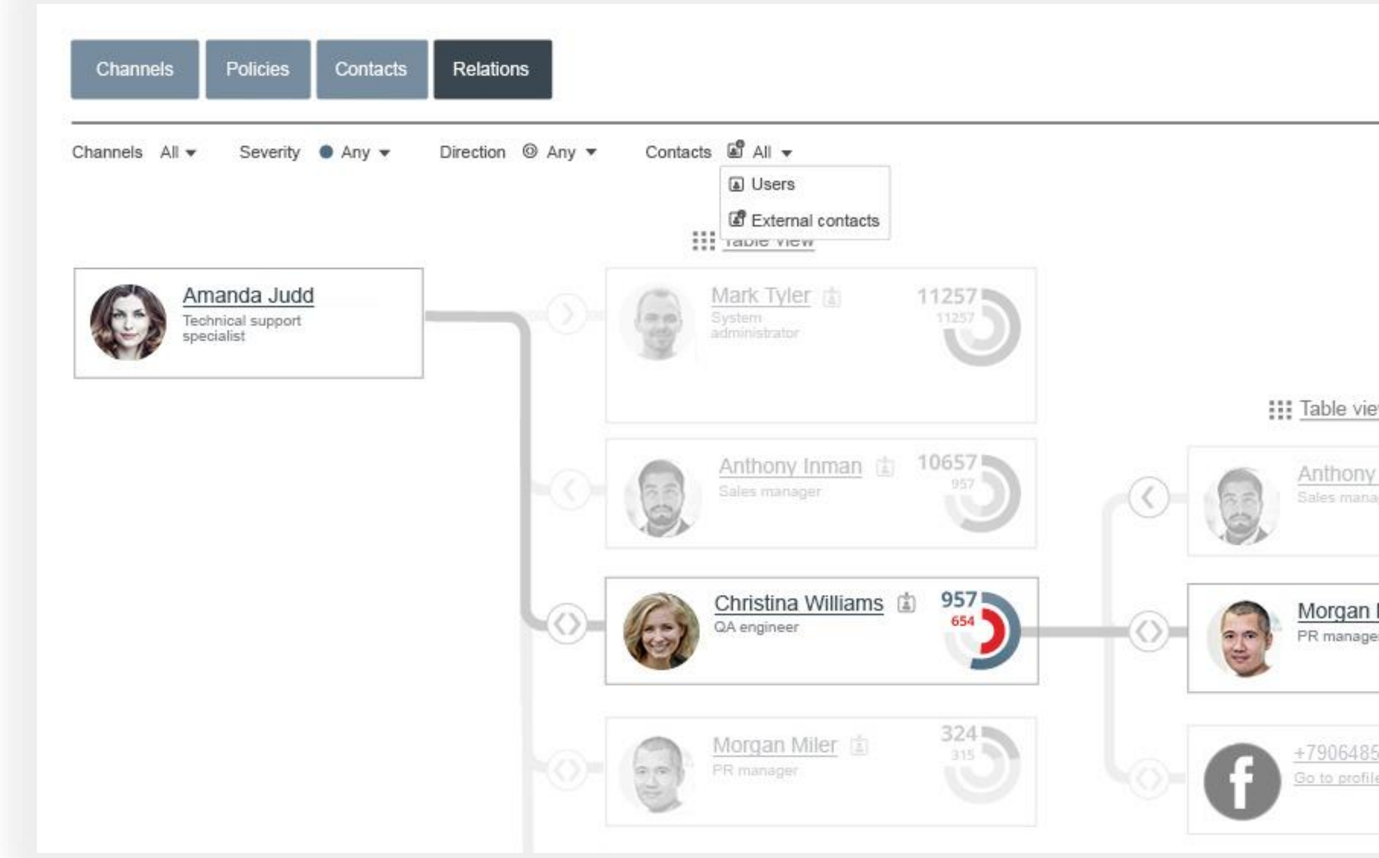
Sorted by Behaviour change index high severity first

Amalia Kitch A.Kitch@gmail.com	9.4 ▲ + 840%	1600 ●	968 ●	54165 ●
Alex Brin A_brin@yahoo.com	low data	155 ●	46 ●	4140 ●
Alexander Boyarskih albh@gmail.com	7.9 ▲ + 840%	8 ●	0 ○	63 ●
Angela Forester Aforester@newmail.org	7.6 ▲ + 840%	3287 ●	2 ●	3983 ●
AK Angela Kint Klint.Angela@gmail.com	6.4 ▲ + 840%	370 ●	39 ●	2182 ●
Armen Nikolson Armnik@gmail.com	5.4 ▲ + 840%	44 ●	0 ○	109897 ●
Alex Pattison A.Pattison@gmail.com	low data	0 ●	0 ●	0 ●

ZECURION

User Connection Map

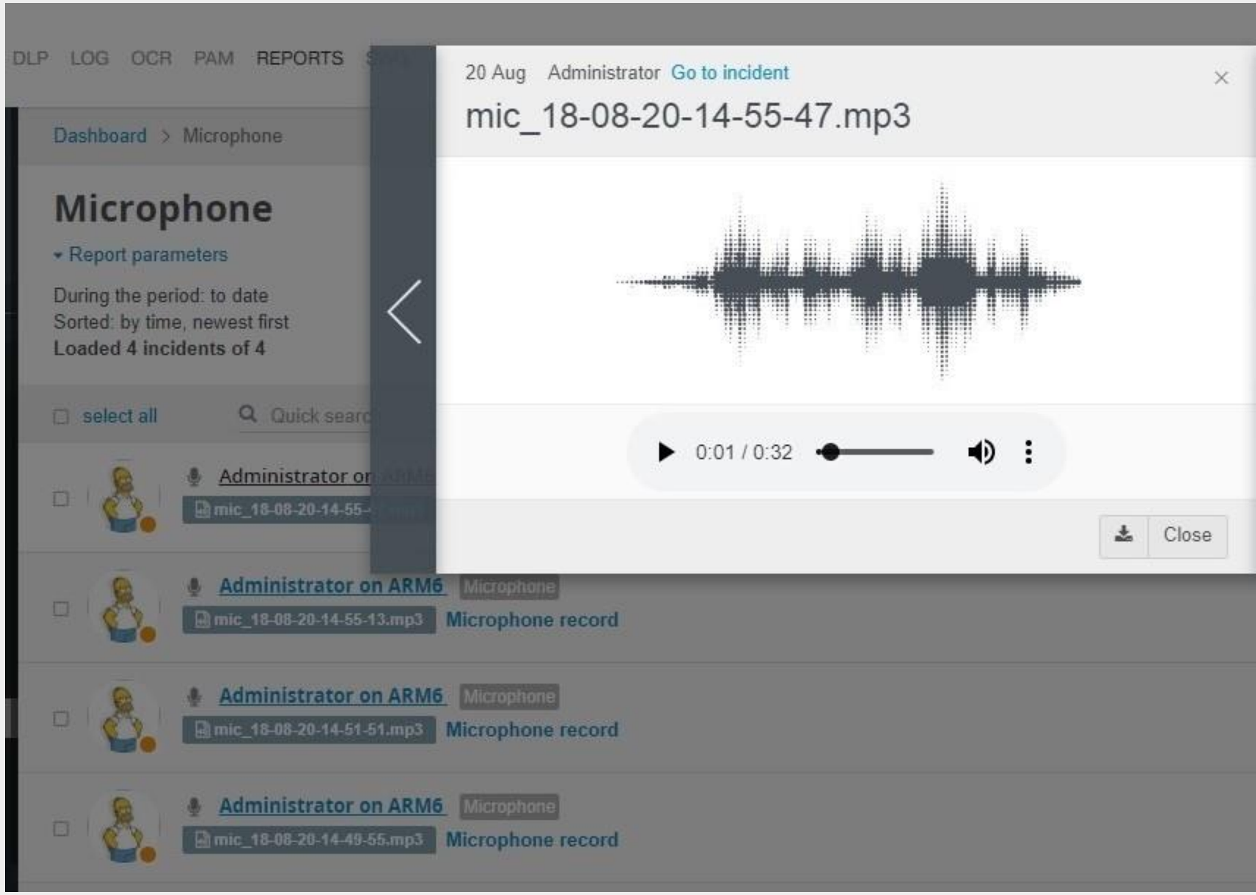
- Interactive connection map (objects and links are clickable)
- Count all channels
- Show internal users and external contacts
- Dramatically decrease investigation effort and time



Channels All ▾ Severity ● Any ▾ Direction Any ▾ Contacts All ▾

Microphone Recording

- Turn on the microphone and start recording on any computer at any given time
- Any computer becomes audio surveillance device
- Records are stored in the archive
- Potential integration of speech-to-text



20 Aug Administrator Go to incident

mic_18-08-20-14-55-47.mp3

During the period: to date
Sorted: by time, newest first
Loaded 4 incidents of 4

Administrator on ARM6
mic_18-08-20-14-55-

Administrator on ARM6 Microphone
mic_18-08-20-14-55-13.mp3 Microphone record

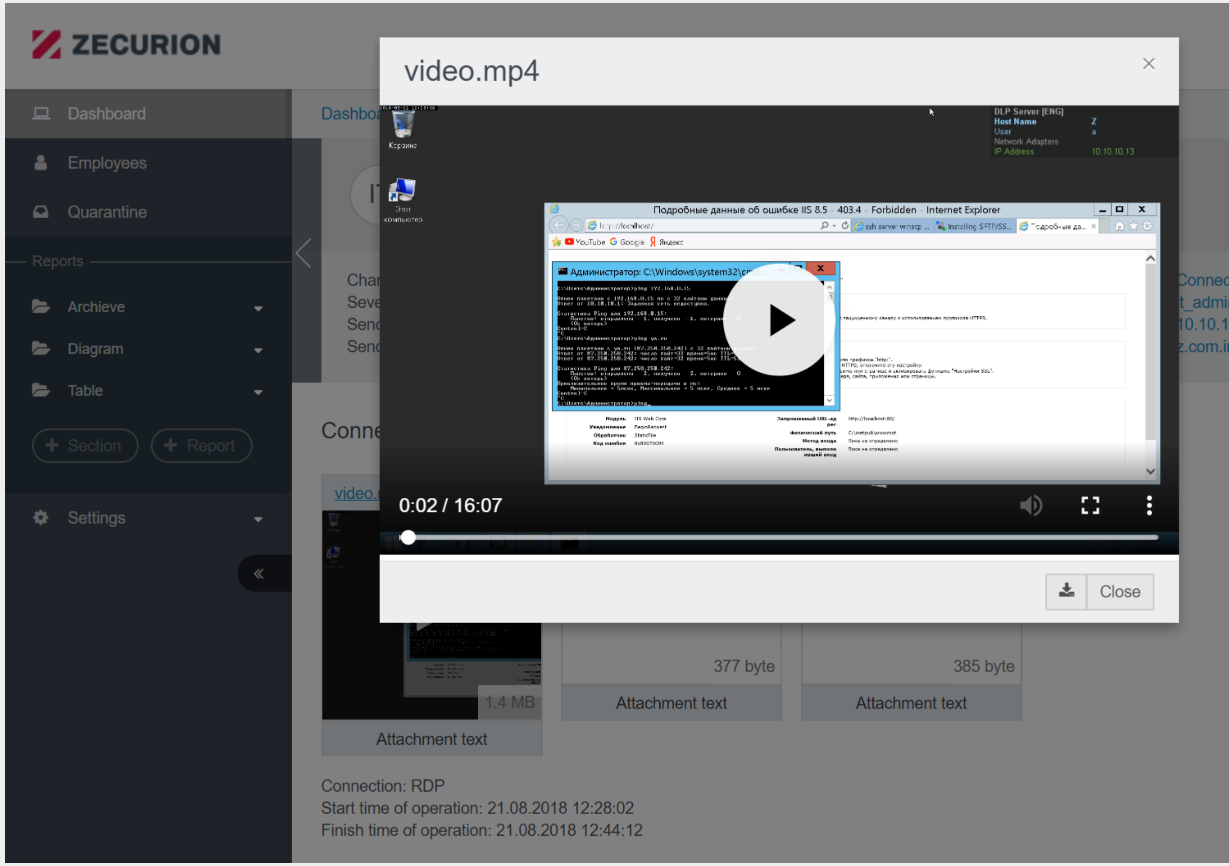
Administrator on ARM6 Microphone
mic_18-08-20-14-51-51.mp3 Microphone record

Administrator on ARM6 Microphone
mic_18-08-20-14-49-55.mp3 Microphone record

ZECURION

User Session Recording

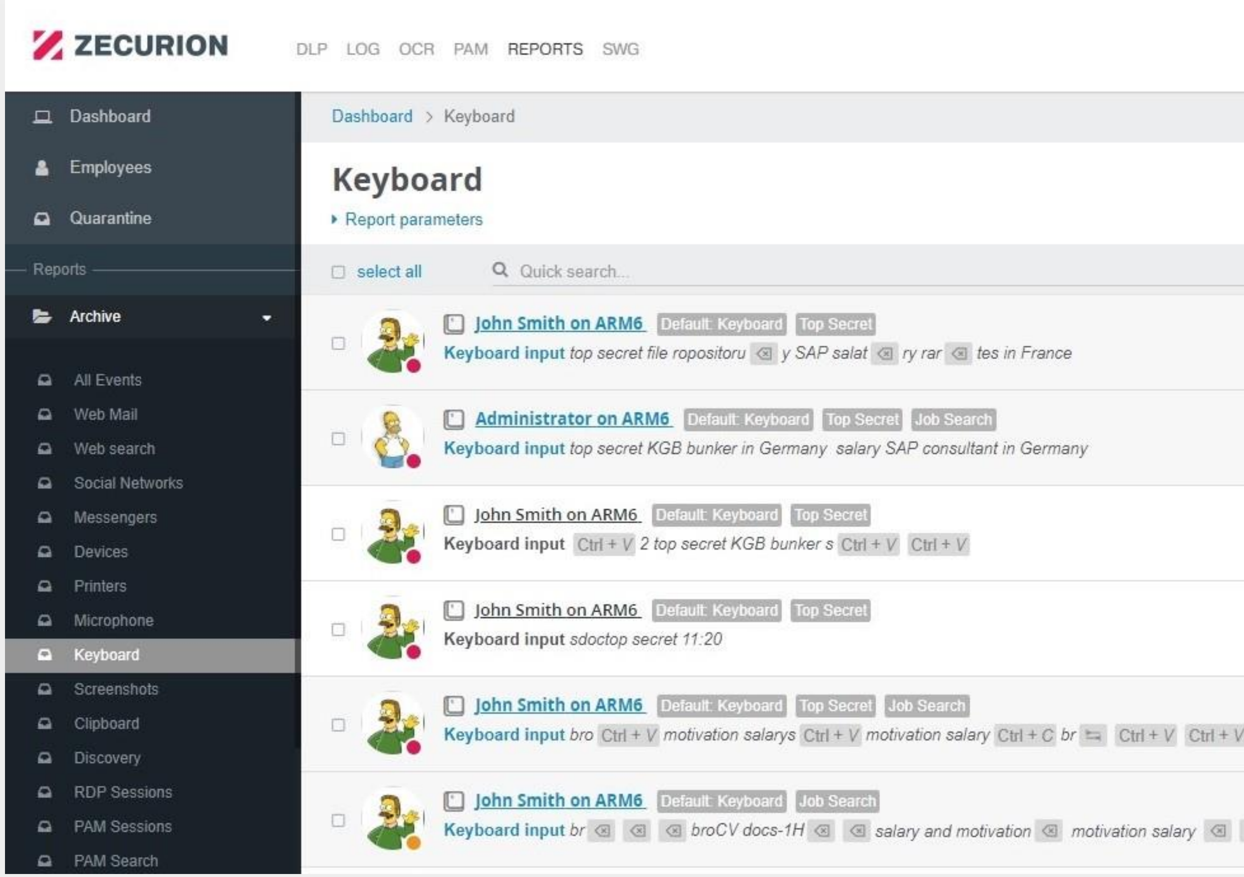
- Sessions are saved as screenshots or video
- Live monitoring of users’ sessions
- Can detect dangerous operations that typical DLP does not control: destroy of data, change logs and settings etc.
- Collect evidence base for legal actions



Connection: RDP
Start time of operation: 21.08.2018 12:28:02
Finish time of operation: 21.08.2018 12:44:12

Keyboard Recording

- Recording of all keystrokes
- Control of employees even when they do not send anything outside
- Possible to obtain passwords for encrypted files



Keyboard

John Smith on ARM6 Default: Keyboard Top Secret
Keyboard input *top secret file repositoru* ⌫ *y SAP salat* ⌫ *ry rar* ⌫ *tes in France*

Administrator on ARM6 Default: Keyboard Top Secret Job Search
Keyboard input *top secret KGB bunker in Germany salary SAP consultant in Germany*

John Smith on ARM6 Default: Keyboard Top Secret
Keyboard input Ctrl + V *2 top secret KGB bunker s* Ctrl + V Ctrl + V

John Smith on ARM6 Default: Keyboard Top Secret
Keyboard input *sdoctop secret 11:20*

John Smith on ARM6 Default: Keyboard Top Secret Job Search
Keyboard input *bro* Ctrl + V *motivation salarys* Ctrl + V *motivation salary* Ctrl + C *br* ⭾ Ctrl + V Ctrl + V

John Smith on ARM6 Default: Keyboard Job Search
Keyboard input *br* ⌫ ⌫ ⌫ *broCV docs-1H* ⌫ ⌫ *salary and motivation* ⌫ *motivation salary* ⌫

Application Control

- Black list (or white list) of applications for certain users or groups
- Control application by hash of executable file
- Eliminates the risk of using dangerous applications: torrent, TOR, anonymizers, messengers, games

ZECURION DLP DETAILS

Components

Traffic Control

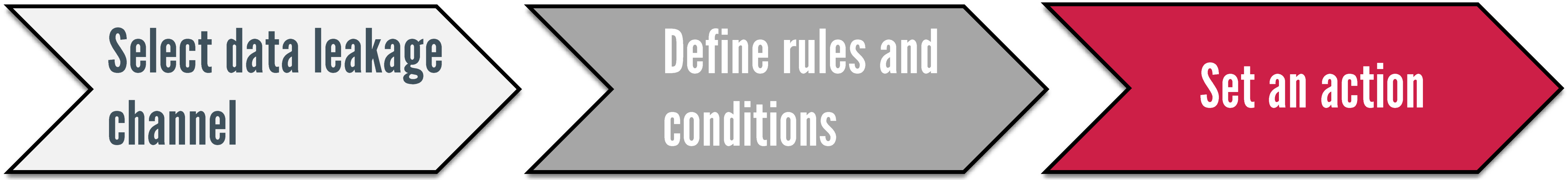
Device Control

Discovery

Key features

- Control all possible data leak channels
- Single policy for all channels
- File content extraction and analysis
- Single web console with customizable dashboard
- Full archive for investigation and retrospective analysis
- Powerful reports with easy drill-down capability and flexible access control
- Flexible deployment – 13 options
- REST API for automation

DLP Policy



- Network channels and internet services

- Local devices and ports

- System utilizes 10+ content-detection technologies
- Scans the data inside of files and archives
- Determines encrypted and camouflaged files
- Use context attributes (user, host IP, …)
- Create composite rules with AND, OR and NOT logical operators

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

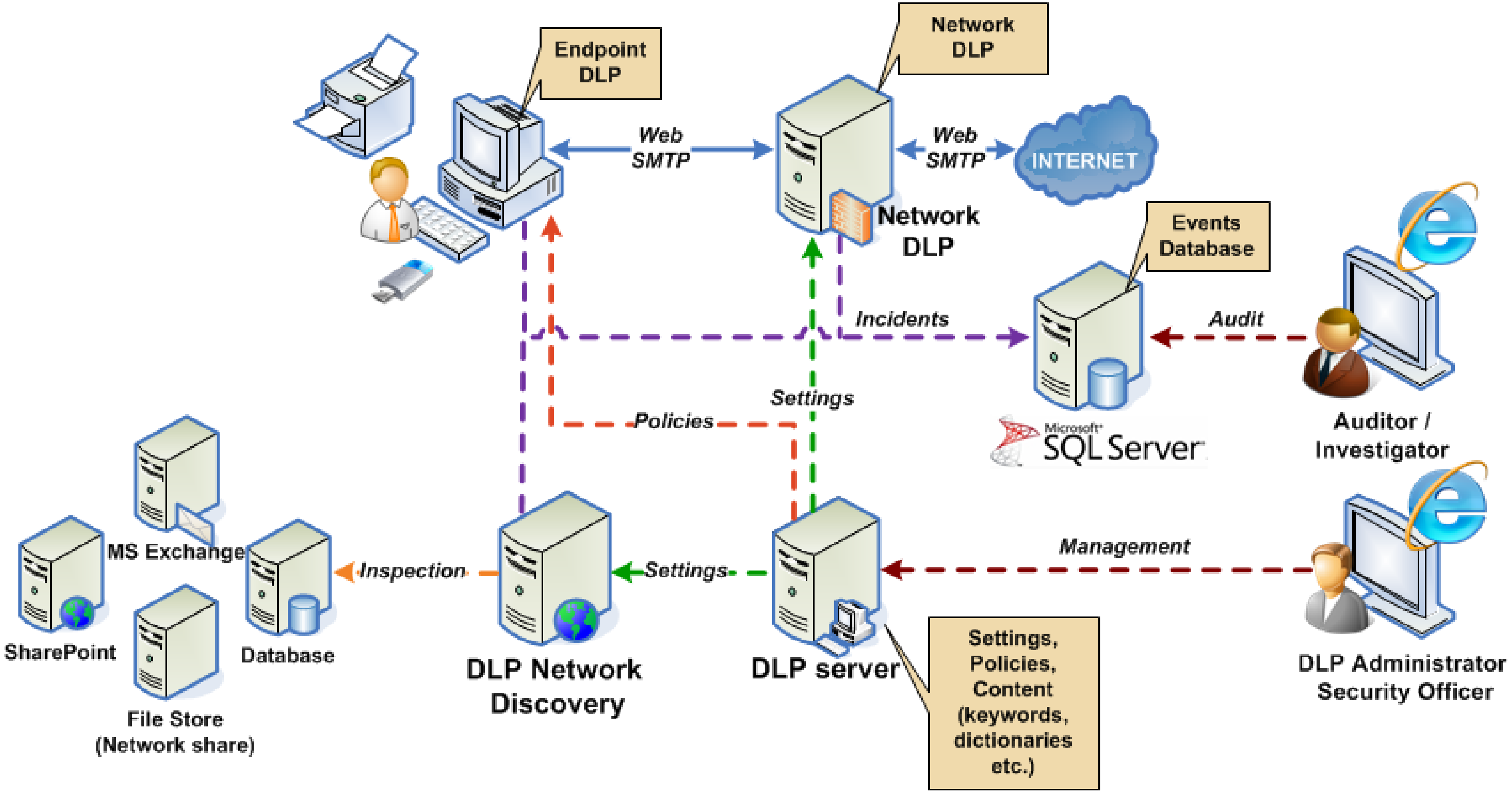
ZECURION

Detection Technologies

- Keywords and dictionaries
- Morphology
- Templates
- Regular expressions
- Digital fingerprints

- Machine learning: Bayes
- Machine learning: SVM
- Image templates
- OCR
- Manual inspection

DLP Architecture



ZECURION

Zecurion Traffic Control

- Total control of internet channels: email, webmail, social networks, messengers etc
- Analysis of SSL-encrypted traffic
- Email quarantine
- Two operation modes: active and passive
- Notification of user and/or security officer

Zecurion Device Control

- 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 request
- Tamper-proof agent

Zecurion Discovery

- Detect improperly stored sensitive data
- Scan of all possible data storage locations: local/network drives, MS Exchange and SharePoint, any database
- Flexible scan parameters – daily/weekly/monthly for selected computers/OUs
- Real-time discovery – scan file on close
- Use of all available content detection rules

Zecurion DLP Benefits

- Prevent data leakage
- Reduce cost of investigation and damage to reputation
- Facilitate early risk detection and mitigation
- Increase comfort level of senior management

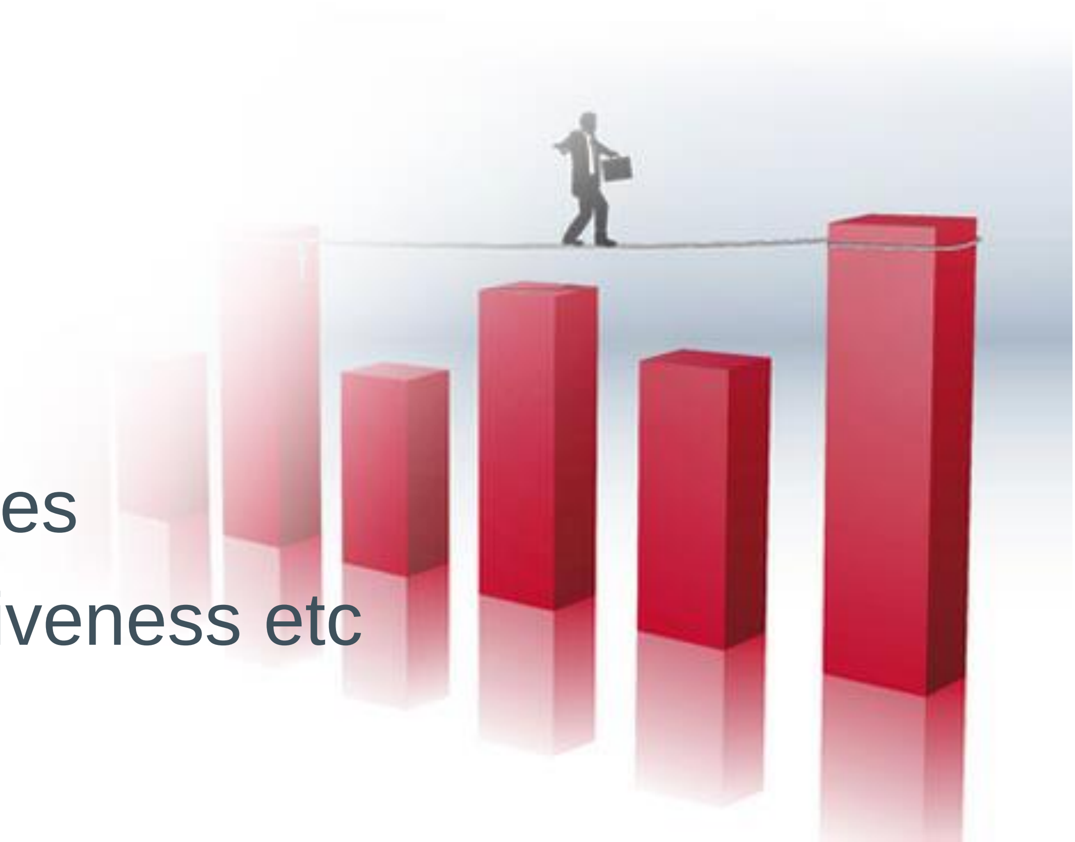
IMPLEMENTATION TIPS & TRICKS

Prepare for Implementation

- Define incidents handling process
- Define initial priorities and process model (Quick Wins vs. Full Deployment, Detect vs. Prevent)
- Map your environment (network, endpoints, storage, cloud)
- Pilot and PoC

DLP Implementation Process

- Define deployment architecture
- Network/endpoint/storage deployment
- Define policies and reports
- Deploy to a subset
- Analyze and tune
- Add channel/component
- Manage incidents and policies
- Analyze trends, risks, effectiveness etc



Zecurion Use Case

Allianz

Insurance

Zecurion Device Control 7500 licenses

«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»

Zecurion Use Case

IDGC OF CENTRE

Electric Grid company

Traffic Control, Device Control, Discovery
15,000 licenses in 11 regions of Central Russia

«Security Department received a powerful and convenient tool for data protection in the Company»

Questions

Contacts

ZECURION

info@zecurion.com

www.zecurion.com