

ZECURION DLP INTRODUCTION

2022

 Artem Smirnov
Head of Presales Team

 **ZECURION**





About Zecurion

- Established in 2001
- Focused internal security vendor
- 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 Product Line



Zecurion Data Loss Prevention Suite

- Traffic Control capturing module for Mail and Web
- Device Control for endpoints
- Discovery crawler module
- Staff Control user productivity analyzer
- Screen Photo Detection module



Zecurion SWG → New Zecurion NGFW (H2 2022)

New Zecurion solution for network security and Internet user protection



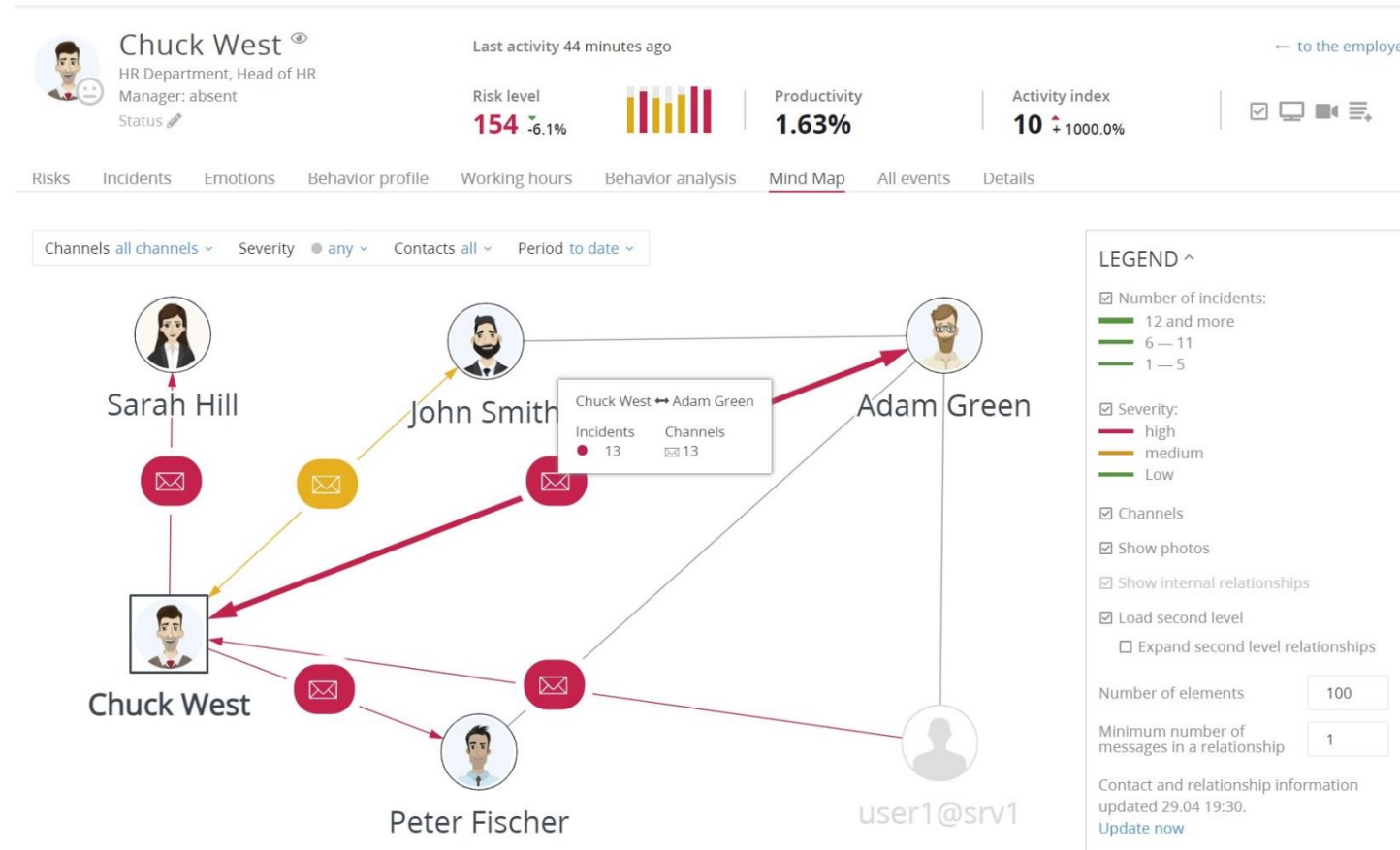
Zecurion PAM — Privileged Access Management

Control and record sessions of privileged users

ZECURION DLP UNIQUE FEATURES

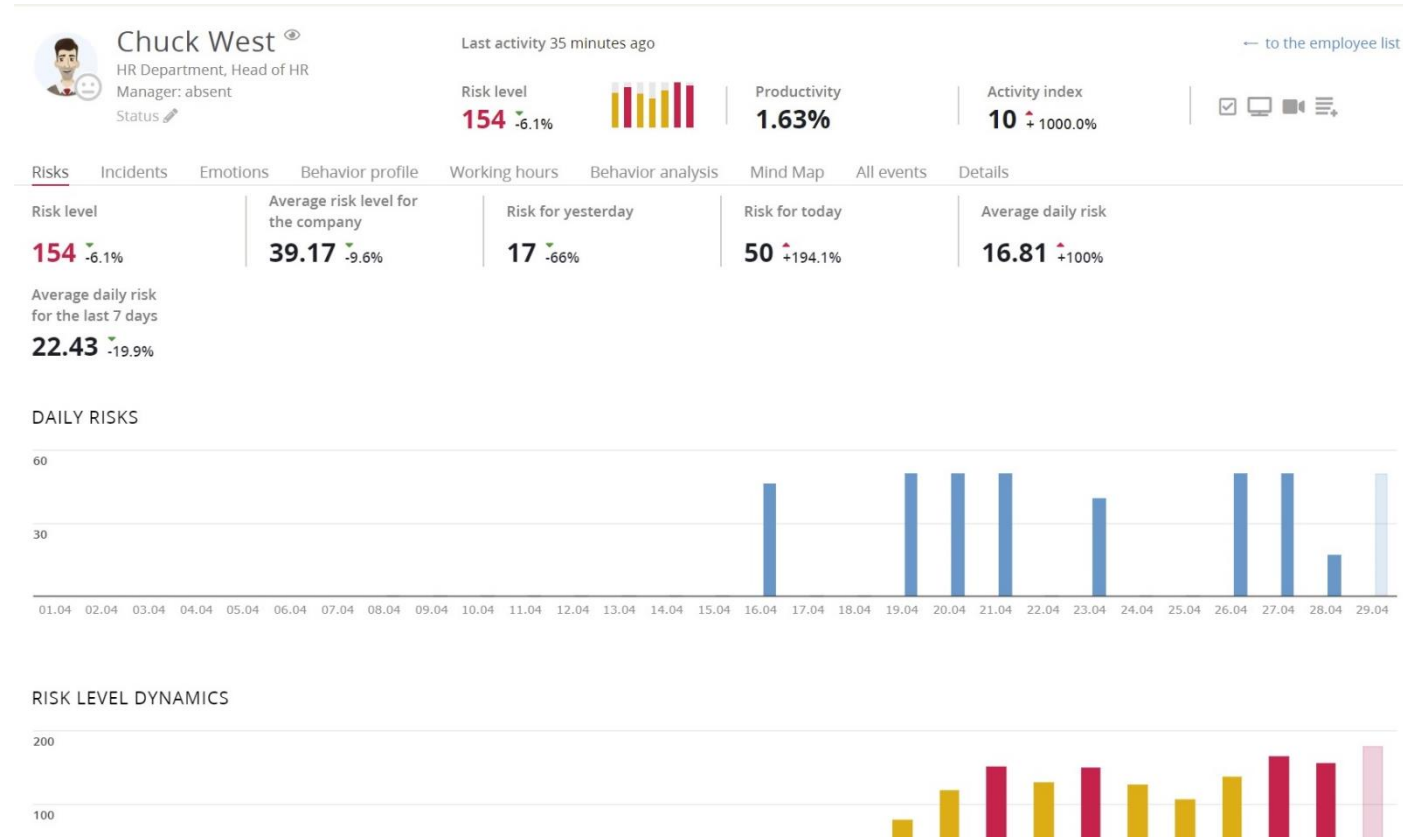
Intelligence Capabilities

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



Advanced UBA tools

- 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.



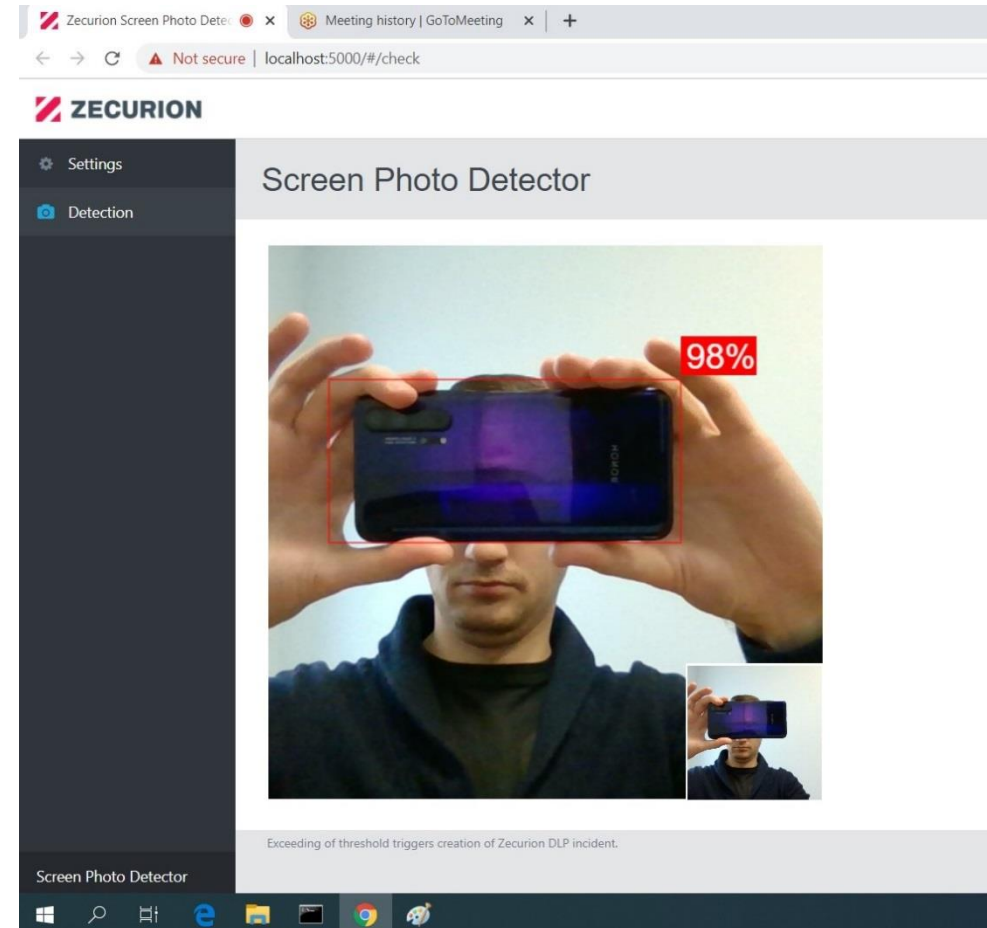
Control Capabilities

- Keyboard recording
- User sessions (screens) recording
- Application control
- Microphone recording
- Webcam recording
- Passwords and accounts

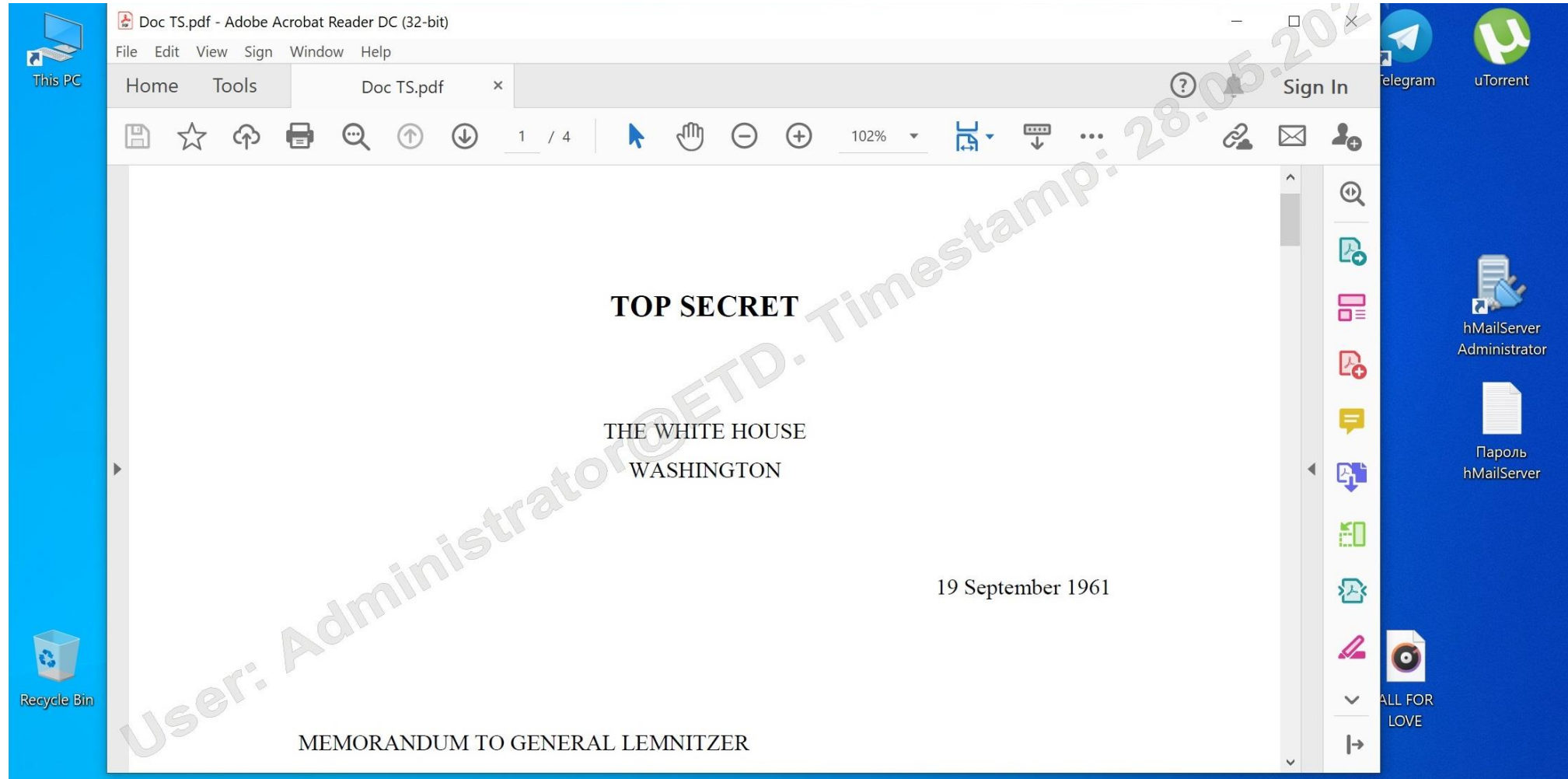
The image displays a screenshot of the Zecurion dashboard interface. The top navigation bar includes 'DLP', 'LOG', 'OCR', 'PAM', and 'REPORTS'. The main content area is divided into two sections: 'Microphone' and 'Web Camera'. The 'Microphone' section shows a report for '20 Aug Administrator' with a file named 'mic_18-08-20-14-55-47.mp3' and a waveform visualization. The 'Web Camera' section shows a report for '23 Jan John Smith' with a file named 'Snapshot_200123_145242.jpg' and a corresponding camera snapshot of a man's face. A sidebar menu on the left lists various system components: DB Main, Dashboard, Employees, Quarantine, Reports (DLP, Staff Control, Web Camera, Microphone, Screenshots, Keyboard), SWG, PAM, Analytics, and Settings. The Zecurion logo is visible in the bottom left corner.

Screen Photo Detection

- 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



Screen Watermarks



Incident Response Workflow

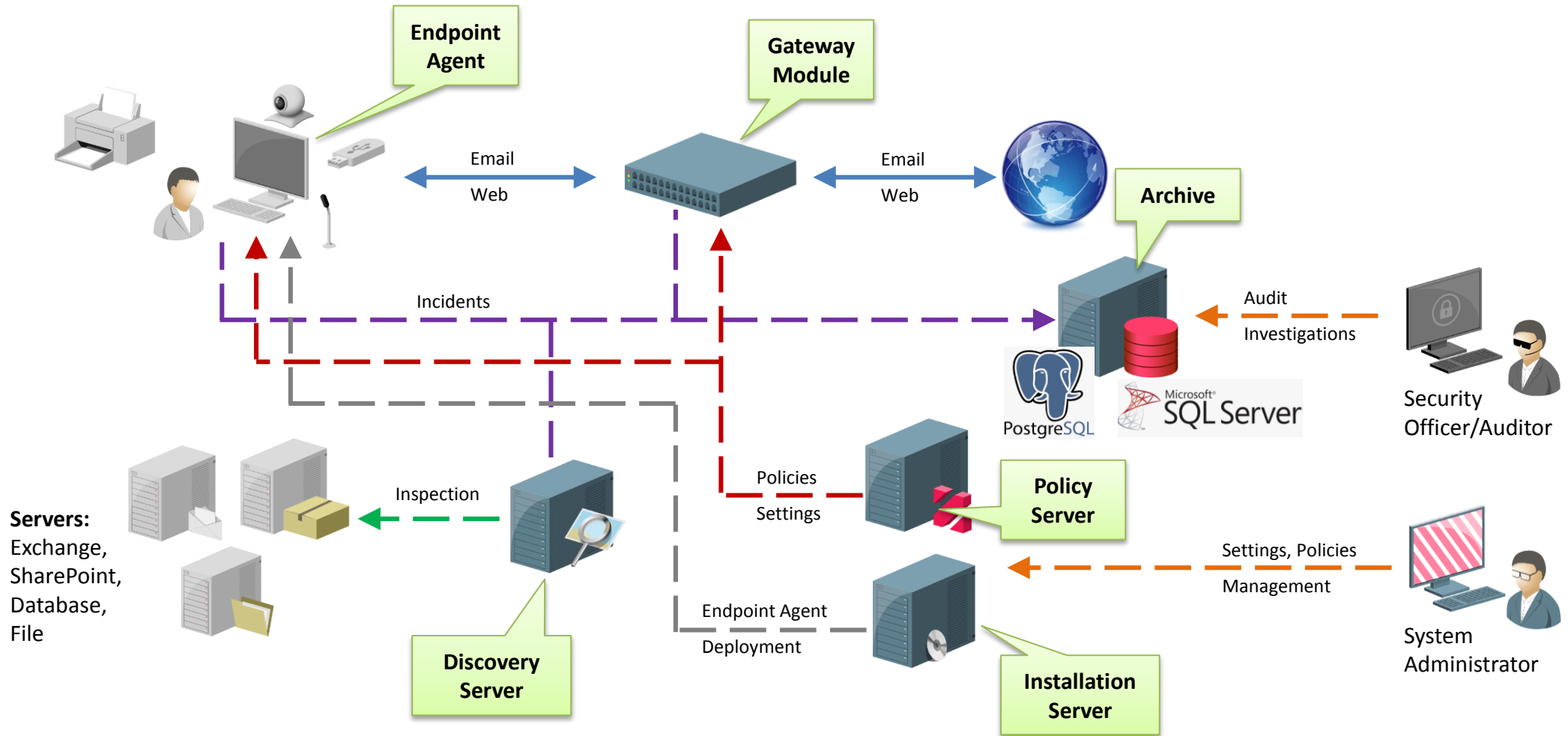
- Incident investigation workflow automation
- Jira-like task tracker
- Create new investigation, assign tasks to subordinate security officers, control execution
- Attach incidents and files from DLP archive
- Write comments

The screenshot shows a web application interface for incident response workflow management. At the top, there are navigation links: INSTALLER, LOG, OCR, REPORTS, STATUS, and SWG. On the right, there are user controls: DB Main (dropdown) and Adam Gr (profile icon). Below the navigation is a breadcrumb trail: Dashboard > Tasks. A status bar indicates 'Updated 12:33', 'Autoupdate disabled', and 'Update' buttons. The main section is titled 'Tasks' and includes a 'select all' checkbox, a search bar, and filters for Executor, Initiator, Status, Due date, and Sort. The task list contains the following entries:

Task	Assignee	Status	Due Date
Investigation in Tender process	JSmith	new	28.05.2021
Investigation in Sales Team APJ	PFischer	in progress	28.05.2021
Request from IT Department	JSmith	new	05.04.2021
Urgent Case (5-April)	CWest	in progress	05.04.2021

ZECURION DLP DETAILS

DLP Architecture



Data Classification Engine

Keywords and dictionaries ●

Templates ●

Regular expressions ●

Digital fingerprints ●



● Machine learning: Bayes

● Machine learning: SVM

● AI-based image templates

● OCR

Zecurion Traffic Control

- Total control of internet channels: SMTP email, webmail, social networks, messengers, cloud etc.
- Support of messengers: Skype, MS Teams, Viber, WhatsApp and Telegram, MS Lync
- Analysis of SSL-encrypted traffic both on endpoint and gateway levels
- Support of modern cloud services such as Office 365 and Google Docs
- Integration with Check Point, Cisco over ICAP protocol



Zecurion Device Control

- Content-based policies and data classification
- Granular access control for peripheral devices
- Shadow copy of files being written to external drive or printed
- Encryption of copied files on removable media drives
- Centralized deployment and management
- Grant device access by email or phone request
- Fully autonomous mode for policies implementation
- **Advanced channels: keyboard, clipboard, screenshots etc.**
- Company-wide device catalog for easy policy creation



Zecurion Discovery Crawler

- Detect improperly stored sensitive data
- Scan of all possible data storage locations:
 - Local HDD/network share folder drives
 - MS Exchange and SharePoint
 - Database instances
- Flexible scan parameters – daily/weekly/monthly for selected computers/OUs
- Real-time discovery – scan file on close
- File flow tracking inside the LAN network
- **Violated files removal from workstations HDDs**



Zecurion Staff Control

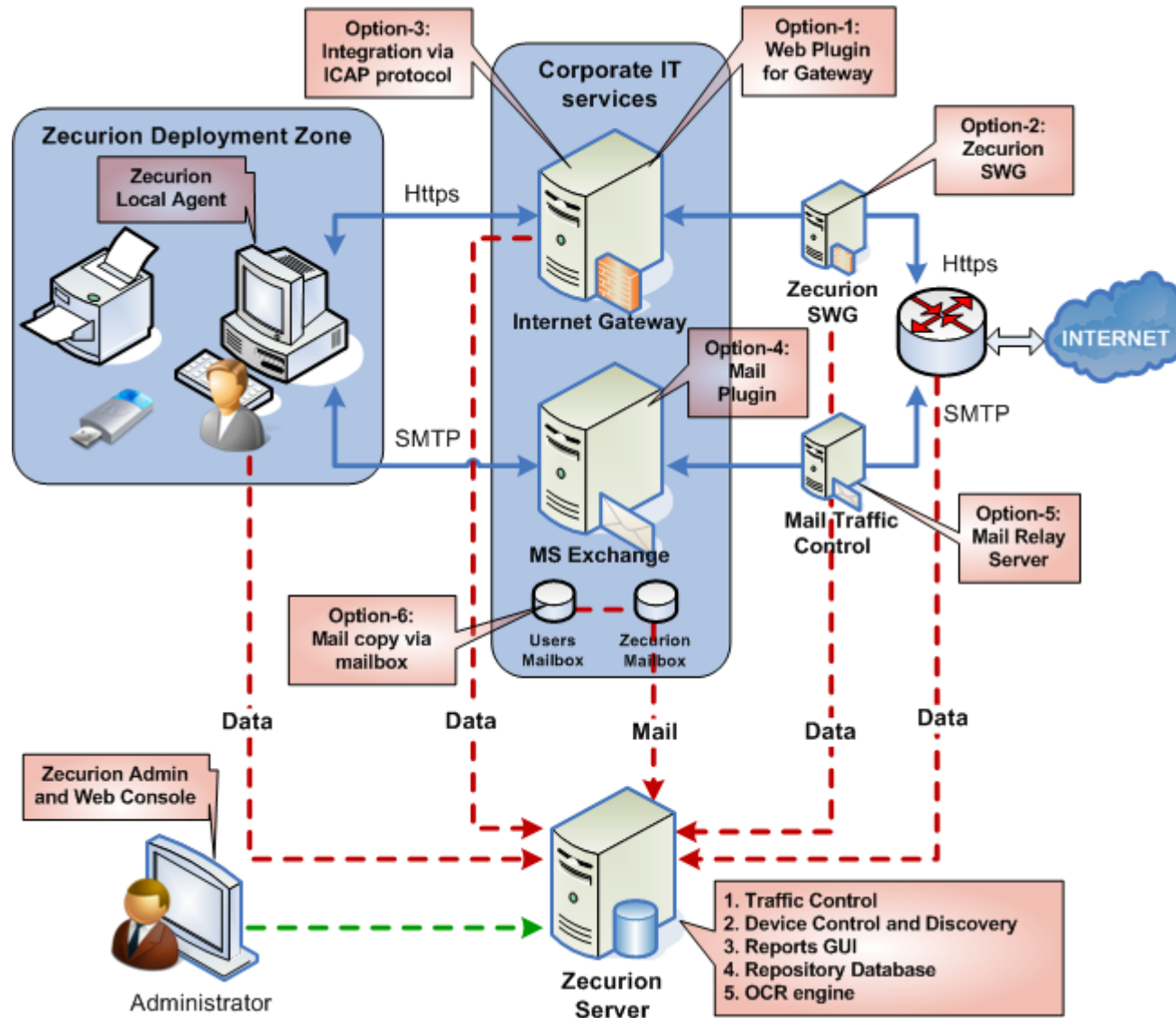
- Employees discipline supervision, both in office and in remote environment
- Workplace monitoring: logon/logoff, websites and application usage, activity
- Websites and application categories
- Discipline reports: late arrivals, early leaving, breaks, time at work, overtime work
- Overall productivity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

WEBSITES AND CATEGORIES			
Website categories ▾	time	%	increase
■ Search Engines	00:00:19	3	+100%
■ Undefined	00:10:02	97	+887%

DISCIPLINE						
date	Arrival to work		Departure from work		Time at work	
15.09	10:57	+57min	17:00	-1hr	6:03	-1hr 57min
13.09	11:32	+1hr 32min	16:46	-1hr 13min	5:14	-2hr 46min
10.09	10:00		13:16	-4hr 43min	3:16	-4hr 44min
09.09	13:04	+3hr 4min	15:17	-2hr 42min	2:13	-5hr 47min
06.09	09:58	-2min	10:09	-7hr 50min	00:11	-7hr 49min
03.09	00:00	-10hr	18:00		18:00	+10hr
02.09	00:00	-10hr	00:00	+6hr	24:00	+16hr

APPLICATIONS AND CATEGORIES				
Application categories ▾	time	%	increase	
■ Entertainment	00:03:03	4	+100%	
■ Office	00:03:01	4	+100%	
■ Undefined	01:12:01	92	+1948%	

How to deploy



Key tech aspects of Zecurion DLP

- Controlling all possible data leak channels on gateways and endpoints
- File content extraction and data classification tools onboard
- Full archive for investigation with retrospective analysis and data mining
- Unified Policy Server with omni-channel policies
- Single web console with customizable dashboard
- Powerful reports builder and IRP engine
- 13 deployment options: fits any IT infrastructure
- Integration: TITUS, SIEM, REST API

