

SEARCHINFORM

TOP 3
INTERNAL THREAT PROTECTION
SOLUTIONS

Discover the SearchInform product suite

Arshan Khan
Channel Lead

SEARCHINFORM GLOBALLY

SEARCHINFORM

20+ years
in Information Security

4000+ customers **22+** countries

3 million

PCs protected by
SearchInform solutions

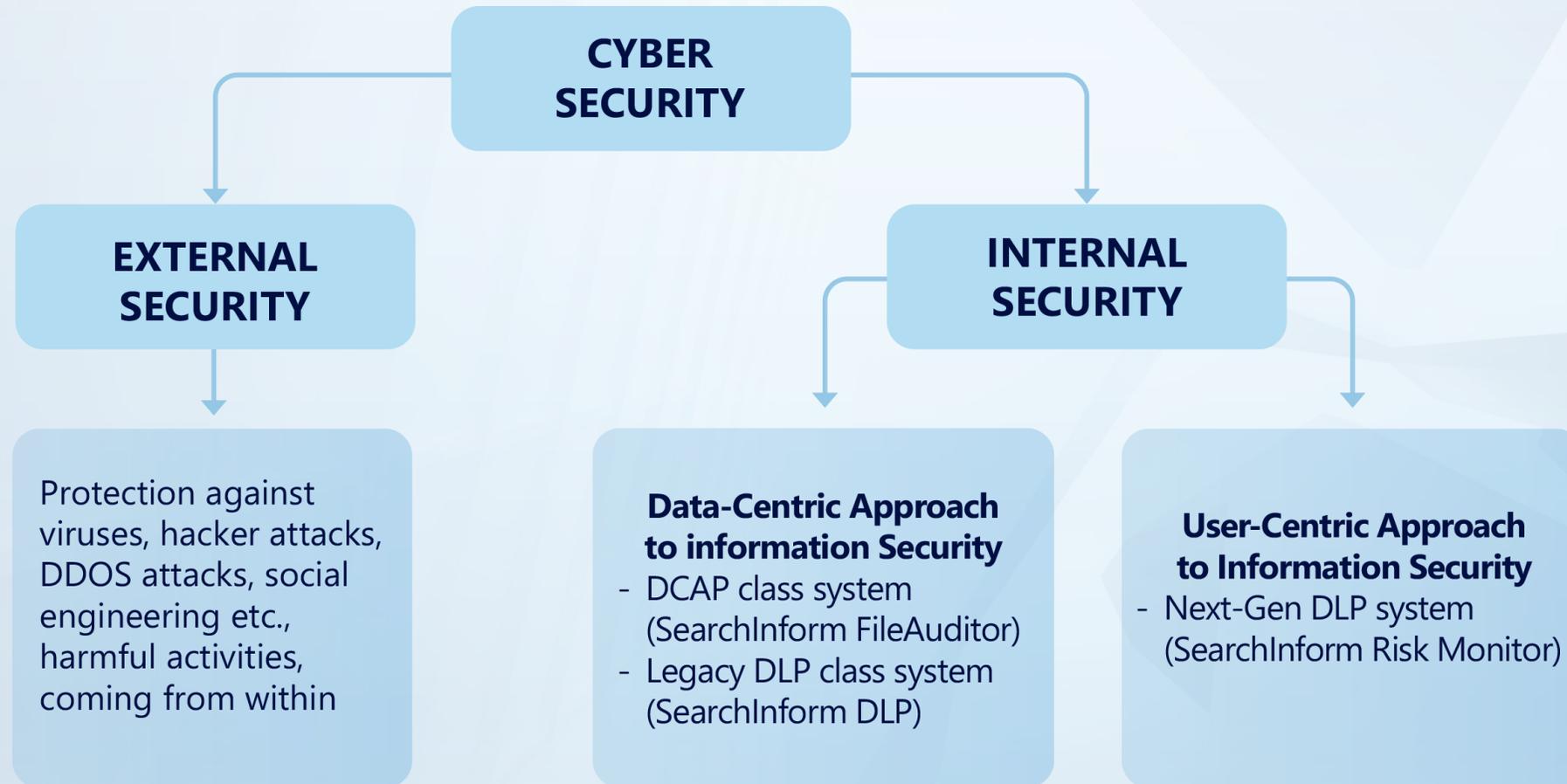
Offices in Dubai, Riyadh, and Istanbul



NEXT-GEN APPROACH

to Information Security by SEARCHINFORM

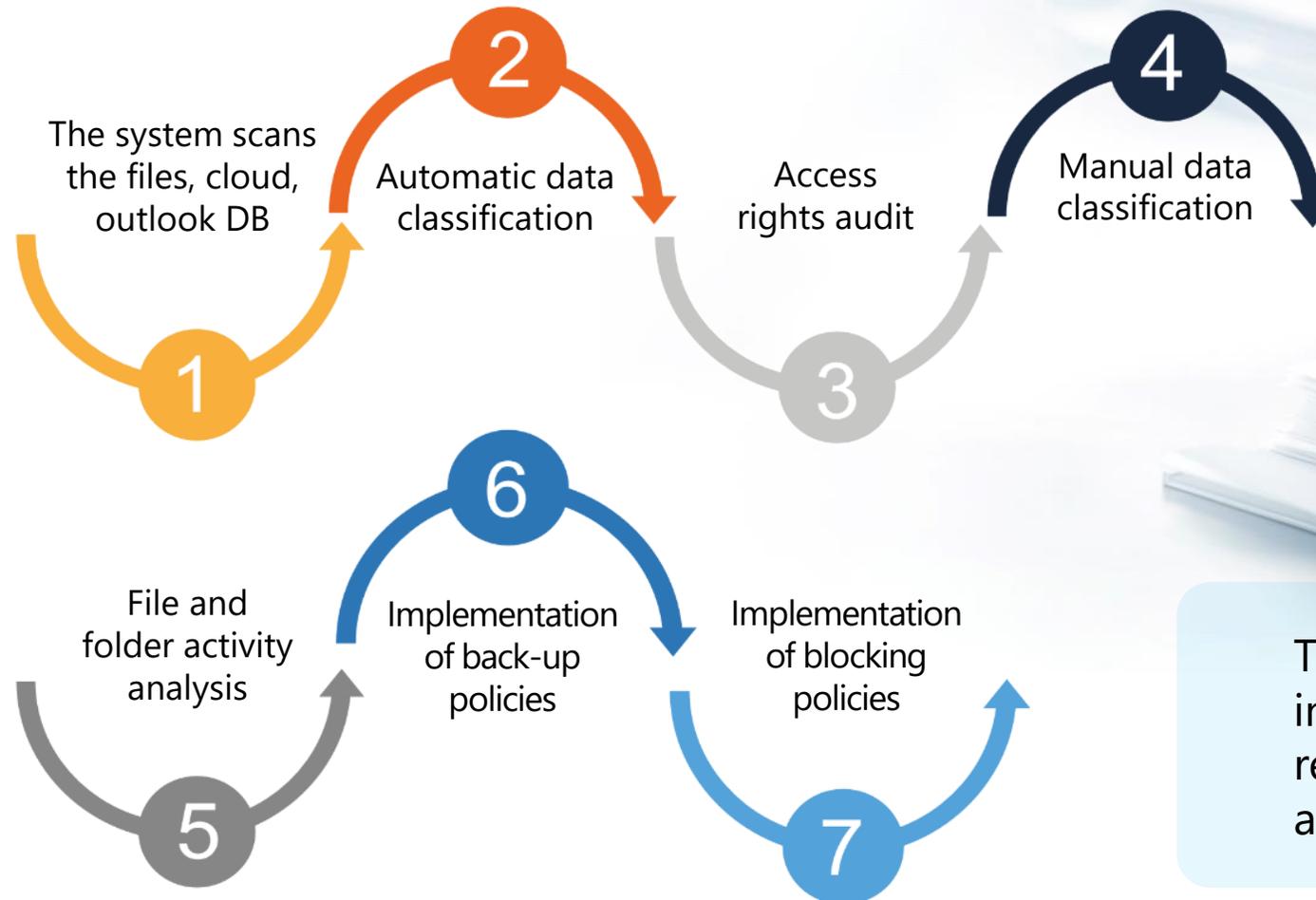
SEARCHINFORM



SEARCHINFORM FILEAUDITOR

SEARCHINFORM

DCAP performs data classification, access rights distribution and protection of data at rest.



The collected information is stored in a database, important documents remain accessible even after they are deleted on users' computers.

DATA-CENTRIC APPROACH TO SECURITY

WHAT THREATENS SECURITY OF FILES?

3 scenarios, against which you need to ensure protection from:



File can be leaked.



Blocking policies



File can be affected or destroyed (ransomware, malicious employee).



Back-up policies



File can be modified (*e.g. via Chat GPT-powered script to affect file content*).



Back-up policies

Traditional IS (Legacy DLP) vs. Next-Gen approach, implemented in SearchInform Risk Monitor



RISK MONITOR

SEARCHINFORM

Comprehensive platform approach for internal security and business growth.

Risk Monitor is the representation of Next-Gen approach by SearchInform to ensuring comprehensive internal threat protection. Risk Monitor is the DLP-based platform, ensuring 360° protection of corporate assets.



Data Protection & Incident prevention



Continuous monitoring & detection of violations



Quality control of work (correctness of communication with clients, business process chains)



Incident investigation (advanced e-forensics)

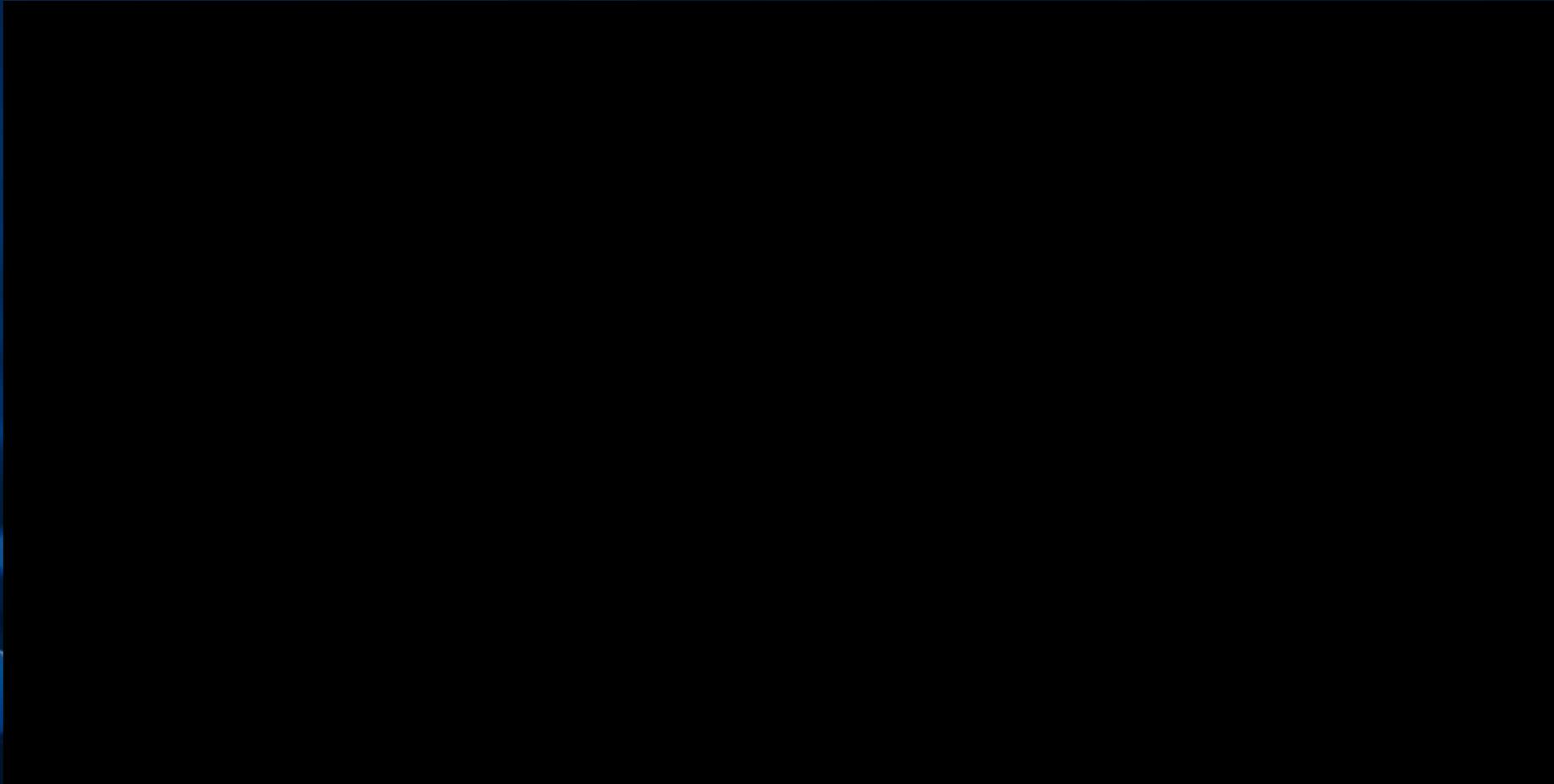


Detection of internal violations (theft, kickbacks, moonlighting)



DETAILED INCIDENT INVESTIGATION

SEARCHINFORM



COMBATING FRAUD WITH **RISK MONITOR**

Management of user access rights

The solution distributes user access rights, preventing illicit operations with confidential docs

Track user operations with data in specific apps

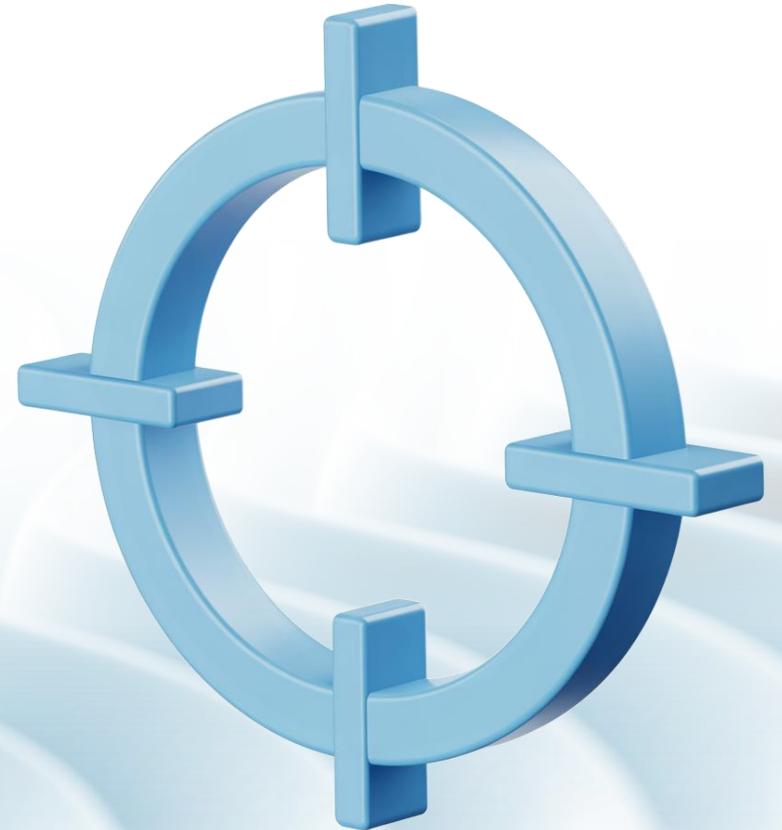
The DLP system tracks all data changes and user activity in applications like Photoshop

Creates shadow copies of important files

This feature helps track the history of file changes and allows documents to be restored if they are altered.

Advanced analytical capabilities

Advanced analytical capabilities, such as content route, provide visibility into fraud rings, detecting all individuals involved in fraudulent activities



PREVENTION OF EMIRATES ID (PERSONAL DATA) LEAK

SEARCHINFORM

EndpointController Console (v. 6.7.5.3) - Victor@Internal.ISC

Journal of requests from agents

Interception on agents | Network interception | Mail servers integration | SMTP integration | Program settings

Pending lists on server | Data flows of agents | Pending lists on agents | FileAuditor scanning

KIB-SERVER-ENG

- Interception on agents
 - Blocking and interception
 - Files by classification (FileAuditor)
 - Messengers (DLP)
 - Printed data (DLP)
 - Websites by content (DLP)
 - HTTP websites (DLP)
 - Bluetooth (DLP)
 - Processes (DLP)
 - Network folders (DLP)
 - Advanced
 - FileAuditor
 - Network interception
 - Mail servers integration
 - SMTP integration
 - Notifications
 - Search Server
 - License

Blocking and interception. Messengers (DLP)

Settings of blocking of files and messages with confidential data sent via messengers

Use blocking rules "Messengers (DLP)"

Enable OCR for images Files check timeout, sec:

Rules	Action	Objects	Files	Processes	Users and groups	Computers
-------	--------	---------	-------	-----------	------------------	-----------

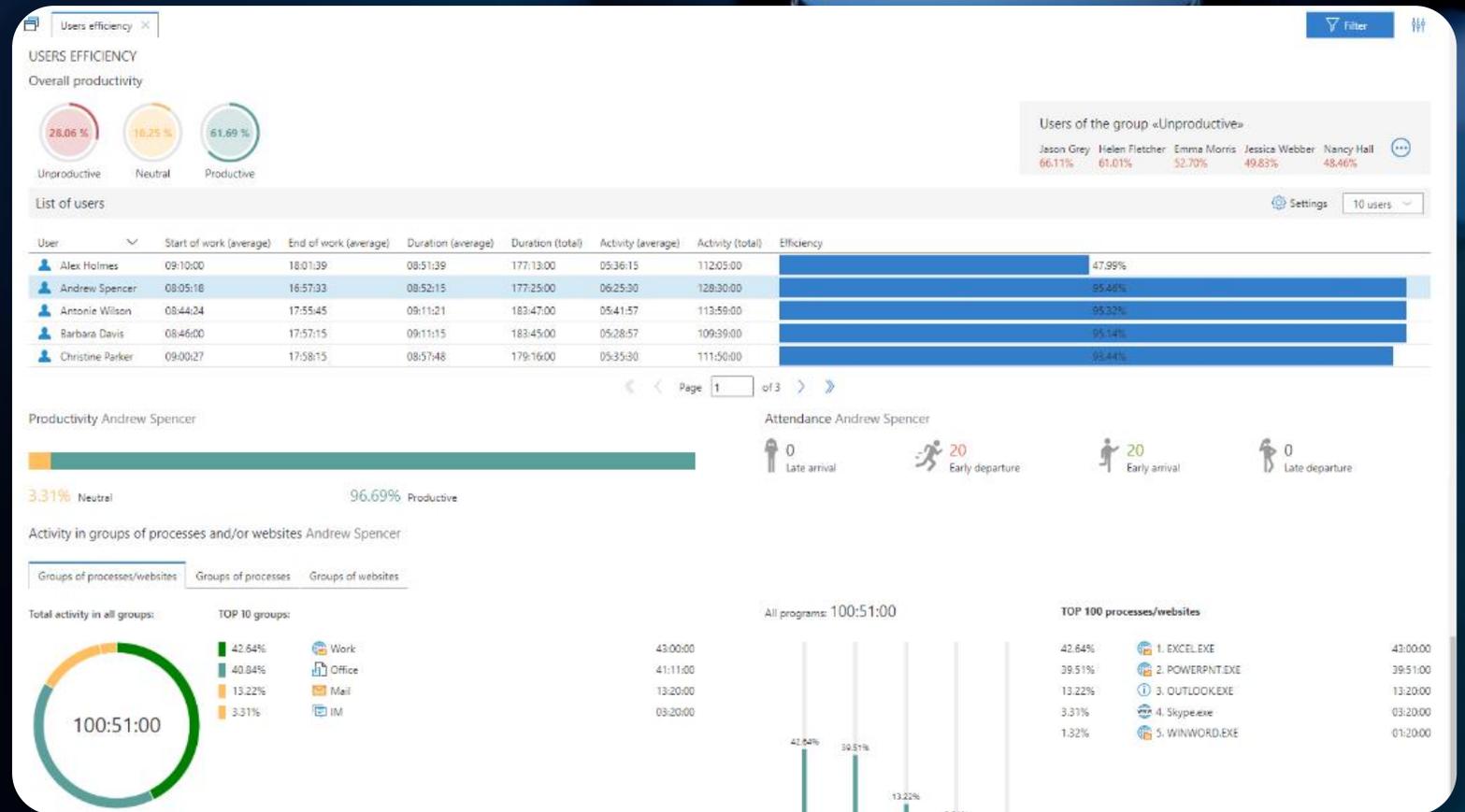
Note! The order of rules is important.

<Microsoft SQL Server> KIB-SERVER-ENG.company.com; endpoint (Version: 0360) 11:07 AM 6/27/2024

CONTROL OF PRODUCTIVITY

Reports of Productivity & current activity.

The system analyzes user activity, detects employees, working extra hours and provides total transparency on what's actually happening in the organization with the help of illustrative reports.



WATERMARKS

FOR PROACTIVE PROTECTION

SEARCHINFORM

Watermarks in files

adds text or symbols to the specific document to designate its confidentiality.

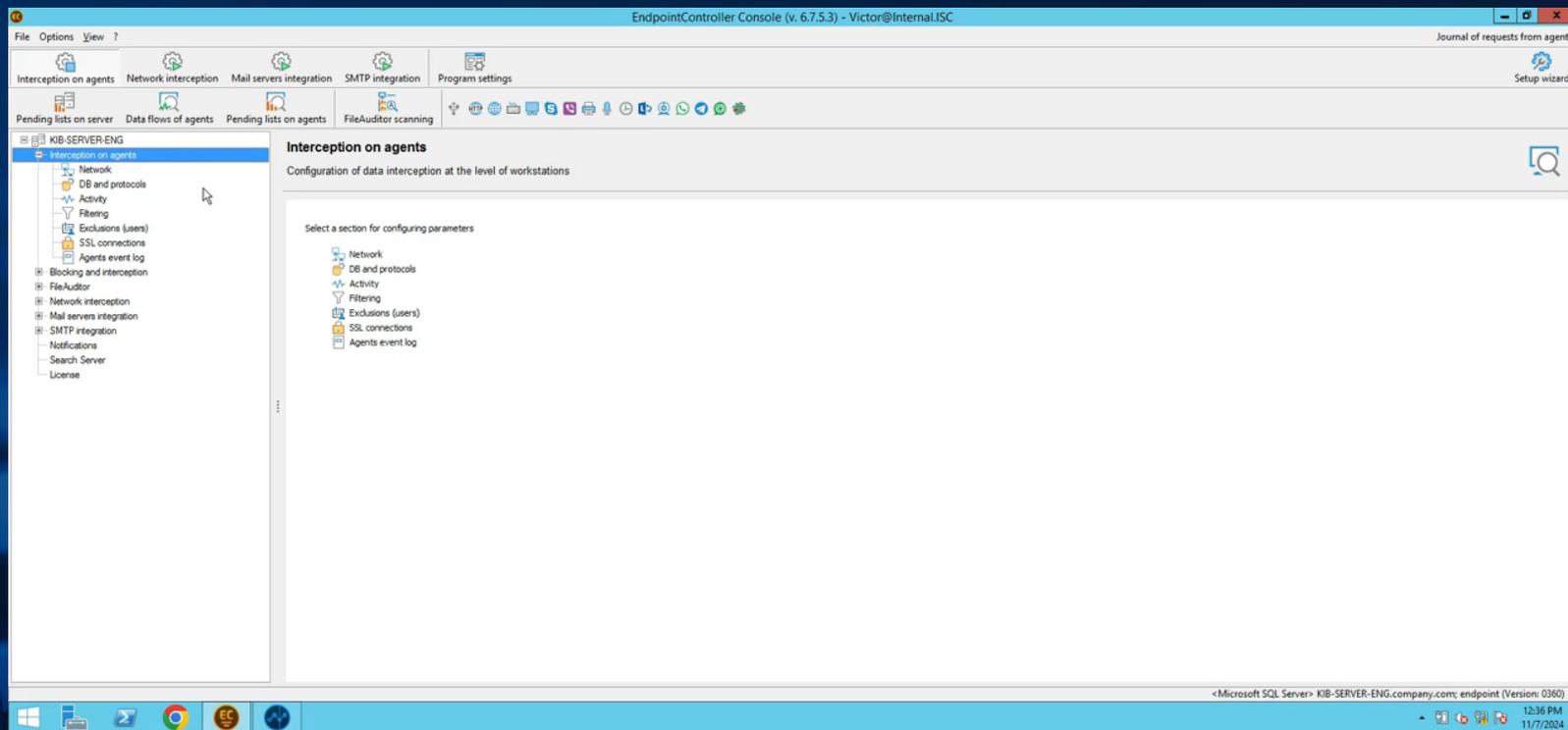
Watermarks on screenshots

displays information on the monitor for protection against taking screenshots or monitor photographing.

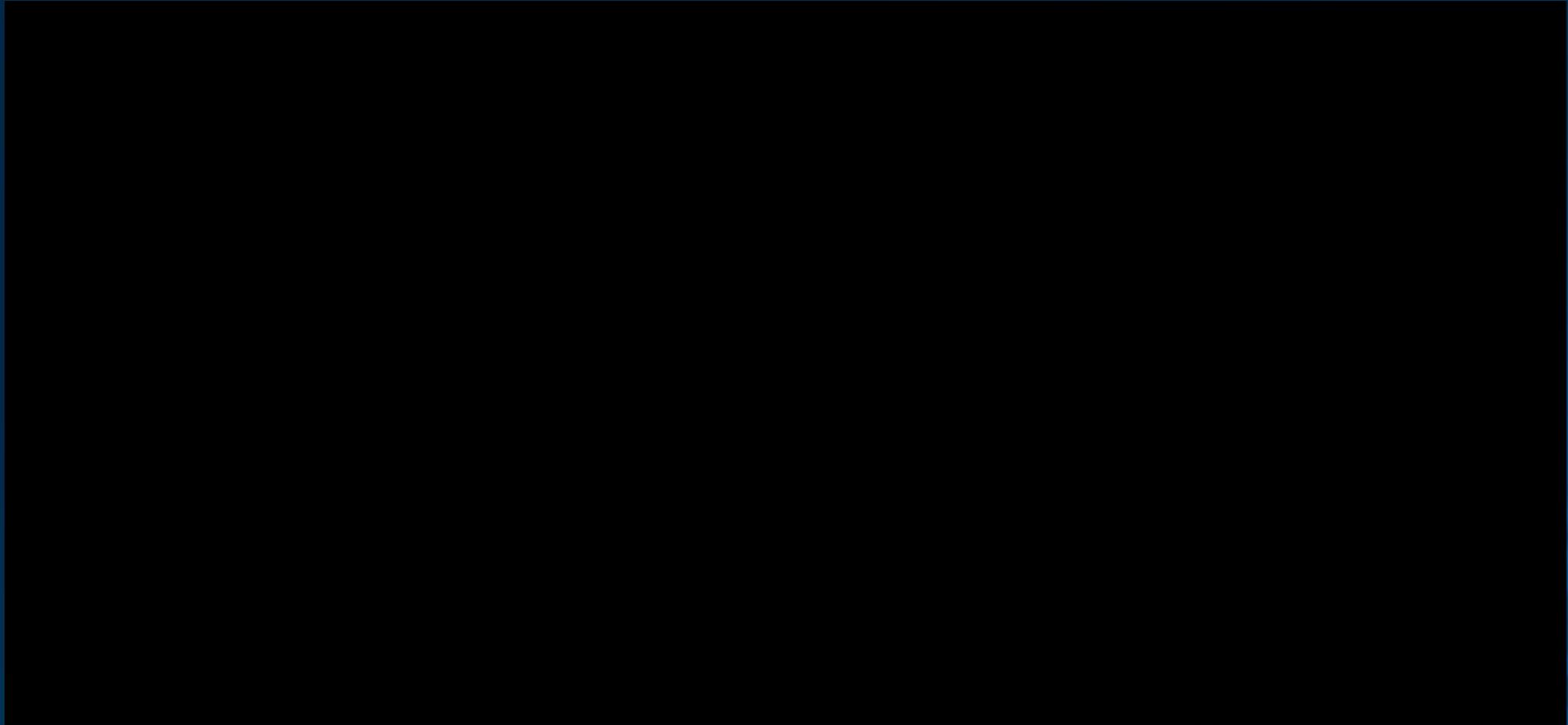
The solution provides proactive protection against malicious actions and prevents leaks of confidential information via cameras, smartphones, and screen capture software. It also blocks screen capture tools, protects the clipboard, providing an additional security layer.

EMBEDDED WATERMARKS WITH PROACTIVE FUNCTIONALITY

SEARCHINFORM

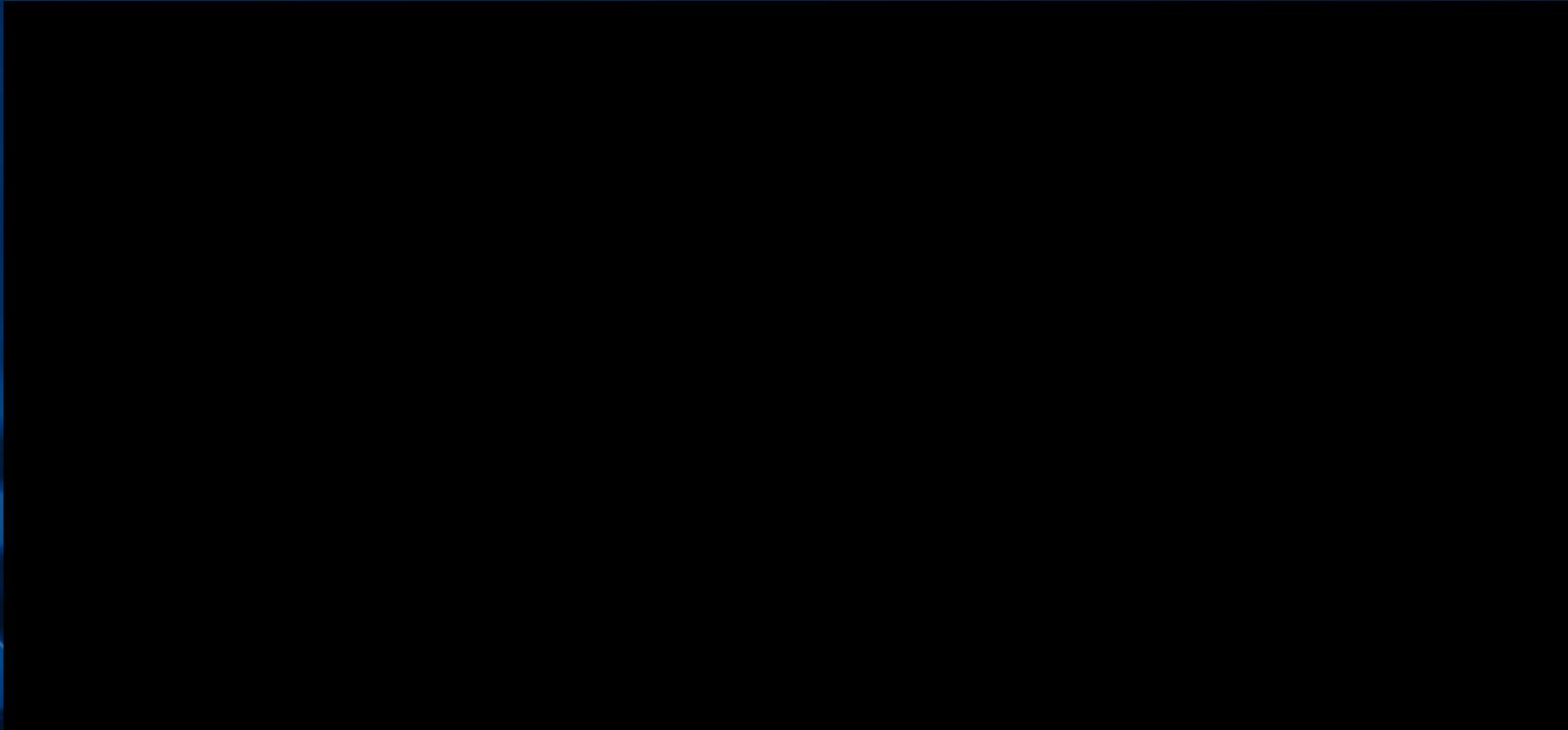


AI-POWERED CAPABILITIES FOR COMPREHENSIVE DATA LEAK PREVENTION



AI-FUNCTIONALITY FOR DETECTION OF CORPORATE FRAUD

SEARCHINFORM



**THANK YOU
FOR YOUR ATTENTION!**

SEARCHINFORM