SEARCHINFORM
INFORMATION SECURITY

Data Protection Solutions by SearchInform: Comprehensive Modules and Detailed Descriptions

**For more details, please refer to the description*	TimeInformer	DLP	RiskMonitor	FileAuditor
Forensic	✗	✗	✓	✗
M365	✗	✓	✓	✓
MailController	✗	✓	✓	✗
IMController	✗	✓	✓	✗
DeviceController	✗	✓	✓	✗
CloudController	✗	✓	✓	✗
HttpController	✗	✓	✓	✗
FtpController	✗	✓	✓	✗
PrintController	✗	✓	✓	✗
MonitorController + Keylogger	✓	✗	✓	✗
Watermarks on screenshots	✓	✗	✓	✗
MicrophoneController	✓	✗	✓	✗
ProgramController	✓	✗	✓	✗
Data Classification	✗	✗	✗	✓
Files activities monitoring	✗	✗	✗	✓
Files access rights audit	✗	✗	✗	✓
Watermarks in files	✗	✗	✗	✓

Description

Forensic DataBase stores all “raw” events, based on which the system detects incidents. E. g. original version of an email, a telegram chat message, a voice message in WhatsApp, a document uploaded to the cloud, etc. Data is kept indefinitely and regardless of whether security policy violations are found in them. Forensic DataBase offers content-dependent information retrieval, as well as the ability to apply security policies to the archive of communications.

M365 is the integration with Microsoft 365 through a proprietary API. For DLP and RM, it enables the protection of communications (attachments, chats, texts) in Teams Online and Exchange Online, irrespective of whether the user engages with the 365 platform via a web browser or desktop application. For FA, the integration facilitates the categorisation of any data uploaded or processed by users.

MailController — collection, categorization and quarantine of emails. Protects corporate and public email (gmail etc.). Protects email clients with classical protocols (IMAP, MAPI, SMTP’s) and email in browser.

IMController — collection, categorization and blocking of messages, calls and files, transmitted in corporate and publicly available messengers, including Whatsapp and Telegram.

DeviceController — collection, categorization, blocking and forced encryption of files, transmitted via input/output ports on data storage devices.

CloudController — collection, categorization and blocking of files, transmitted to cloud services or collaboration software (for example, Zoom).

HttpController — collection, categorization and blocking of any random browser traffic, which isn’t gathered by other controllers.

FtpController — collection, categorization and blocking of FTPs traffic.

PrintController — collection, categorization and blocking of files, sent for printing.

MonitorController + Keylogger — create screenshots and make the recording of user screen, take photos or make video recordings via web-cam, audit keyboard input. Detect monitor photographing and ensure biometric identification of employee by face.

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

MicrophoneController — performs audio recording from PC microphone with ongoing conversion and recognition of audio into text.

ProgramController — estimates time, spent on work in programs and browser. Evaluates productivity and navigates through user activity during corporate investigations.

Data Classification — content-based classification of files, kept on PC, in LAN and in Database Management System. The system adds special labels, which can be used for both audit and as a criteria for blocking of access to files.

File activity monitoring — log of local and network file operation activity, operates on the driver level and doesn’t require activation of embedded into OS logs.

File access rights audit — audit of current access rights, detecting facts of change of access rights to objects on local and network file systems.

Watermarks in files - adds text or symbols to the specific document to designate its confidentiality.