Comparison criterion	Comment	SearchInform	ForcePoint (ex WebSense)	Safetica	Symantec	McAfee (Intel Security)
Functional capabilities						
Base of captured data	Database of all the captured data	Available	N/A (incidents)	N/A (incidents)	N/A (incidents)	N/A (incidents)
Visualized user relations	Graphic report on communication of a user with external and internal contacts	Available	Available	N/A	Available	N/A
Visualized data transmission routes	Graphic report on the document movement over network channels	Available	N/A	N/A	Available	Available
Search for unstructured data on local and removable drives	Capability to connect any device for in-depth content analysis	Available	N/A	N/A	N/A	N/A
File activity	Capability of user activity investigation based on file system operations	Available	N/A	N/A	N/A	N/A
Keyboard activity	Capability of user activity investigation based on keyboard input	Available, with capability to disable control of critical data (passwords)	Available	Available	N/A	N/A
Audio recording	Capability of user activity investigation based on the audio recorded at the moment of violation	Available, with capability of automatic disablement outside of controlled objects (not to record audio of conversations with strangers)	N/A	N/A	N/A	N/A

Comparison criterion	Comment	SearchInform	ForcePoint (ex WebSense)	Safetica	Symantec	McAfee (Intel Security)
Video recording	Capability of user activity investigation based on the video recorded at the moment of violation	Available	Available, but in a separate solution	N/A	N/A	N/A
Webcam	Capability of biometric identification of user based on the video recorded with a webcam at the moment of violation	Available	N/A	N/A	N/A	N/A
Audit of activity in software and on websites	Capability of investigation of user activity in software and on websites considering duration	Available	N/A, only event of visiting website	Available	N/A, only event of visiting website	N/A, only event of visiting website
Online monitoring	Viewing screen and listening to speech via microphone in real time	Available	N/A	N/A	N/A	N/A
Corporate e-mail	Common e-mail protocols POP3, SMTP, IMAP, MAPI	Available	Available	Available	Available	Available
Personal e-mail	Personal e-mail in web (Yandex, Gmail, etc.)	Available	Available	Available	Available	Available
Messengers monitoring (w/o end-to-end encryption)	Lync\Skype for business\Web Skype, ICQ, etc.	Available	Available	Available	Only web	Only web
Messengers monitoring (with end-to-end encryption)	Telegram, Viber, WhatsApp	Full-fledged (files, calls, messages – web client and application)	Not full list and only text	N/A	N/A	N/A
Control of portable storage devices	Shadow copying with IS policy applied or access blocking	Available	Available	Available	Available	Available

Comparison criterion	Comment	SearchInform	ForcePoint (ex WebSense)	Safetica	Symantec	McAfee (Intel Security)
Encryption of portable storage devices	Capability to create protected perimeter	Available	Third-party technology	N/A	Available	Available
Shadow copying of data on connected storage devices	Capability to check data on portable device for compliance with IS policies	Available	N/A	N/A	N/A	N/A (but there is available file access blocking)
Audit of printing		Available	Available	Available	Available	Available
Cloud storages control	Dropbox, Yandex.Disk, OneDrive, etc.	Available	Available	Available	Available	Available
HTTP(S) control	Control of search requests, posts, publications, file transfer, etc.	Available	Available	Available	Available	Available
Audit of wireless networks	Restriction of access to wireless networks (including personal, open on smartphone)	Available	Available	N/A	Available	Available
Control of remote access tools	Control (audit, shadow copying) of data transmission via remote access software (RDP, TeamViewer, rAdmin, etc.)	Available	N/A	N/A	N/A	N/A
Monitoring transmission via network folders, clipboard, filesharing hostings, FTP	Control (shadow copying or blocking) of file transfer	Available	Available	Available	Available	Available
Operation in Windows infrastructure (domain and workgroups)	Capability to protect corporate domain or non-domain PCs	Available, full	Available, full	Available, full	Available, full	Available, full

Comparison criterion	Comment	SearchInform	ForcePoint (ex WebSense)	Safetica	Symantec	McAfee (Intel Security)
Operation in Linux infrastructure	Capability to protect corporate PCs and servers on Linux platforms	Available	Available	N/A	N/A, but there is available for MacOS	N/A, but there is available for MacOS
Integration with corporate mail systems	Exchange, PostFix and other corporate mail servers	Available, including cloud solutions of corporate mail	Available, including cloud solutions of corporate mail	N/A	Available, including cloud solutions of corporate mail	Available, including cloud solutions of corporate mail
Integration with document flow systems	SharePoint, etc.	Available	Available	N/A	Available	Available
Integration with corporate cloud storages	Integration with corporate accounts in DropBox, Yandex.Disk, etc.	Available	Available	N/A	Available	Available
Integration with ACS (access control systems)	ACS data can be included in the reports	Available	N/A	N/A	N/A	N/A
Integration with BI systems	Compatibility with other BI systems as additional data source	Available, presets are included in the installation package	N/A	N/A	N/A	N/A
Integration with SIEM	Capability of data transfer to SIEM solutions	Available, seamless integration with own SIEM or transfer to side solutions	Available	Available	Available	Available
Integration with SOC	Capability to transfer IS incidents to SOC solutions	Available	Available	N/A	Available	Available
Attribute search, search by digital fingerprints, search by regular expressions		Available	Available	Available	Available	Available

Comparison criterion	Comment	SearchInform	ForcePoint (ex WebSense)	Safetica	Symantec	McAfee (Intel Security)
Complex search queries	Capability to combine several simple search queries into a complex query for more precise results	Available	Available	Only attributes + regular expressions	Available	Available
Search for similar texts	Search by document or paragraphs to find documents similar in meaning	Available	N/A	N/A	N/A	N/A (but there is a feature of plagiarism search)
Search for similar images	Capability to detect graphic objects (for example, stamps)	Available	N/A	N/A	N/A	N/A
Text search in audio	Capability to search for words or phrases in an audiorecording	Available	N/A	N/A	N/A	N/A
Synonym search	Capability to use synonyms in search	Available	Available	Available	Available	Available
Stemming	Capability to use stemming in search	Available	Available	N/A	Available	Available
Statistical analysis	Capability to use statistical data in search (for example, the number for particular time)	Available	Available	Available	Available	Available
Report on activity of DLP administrators	Capability to track operations inside the system: installation/uninstallation of agents, viewing of data, change of security policies, etc.	Available	Partially	Partially	Partially	Partially

Comparison criterion	Comment	SearchInform	ForcePoint (ex WebSense)	Safetica	Symantec	McAfee (Intel Security)
Report on violations of data transmission security policies	Capability to visualize security policy violations with details of the incident	Available	Available (including notification of user)	Available	Available (including notification of user)	Available (including notification of user)
Report on violations of data storage security policies	Capability to visualize storage security policy violations with details of operations with a confidential file	Available	Without operations drill down	N/A	Without operations drill down	Without operations drill down
Report on document transmission route	Capability to visualize transmission of a document inside the corporate network over data channels (content route)	Available	Available	N/A	Available	Available
User relations report	Capability to visualize communication of employees inside the company and with external contacts	Available	Available	N/A	Available	Available
Report on working day of user	Capability to generate a summary report on working day, work efficiency, violations of work regulations	Available	N/A	Available	N/A	N/A
Report on installed software		Available	N/A	Available	N/A	N/A
Report on hardware		Available	N/A	Available	N/A	N/A
Summary user data		Available	Available	Available	Available	Available

Comparison criterion	Comment	SearchInform	ForcePoint (ex WebSense)	Safetica	Symantec	McAfee (Intel Security)
Automated categorisation of websites		Available, for any new websites	Available	N/A	Available	N/A
Protection of data in motion (DLP)		Full-fledged implementation	Full-fledged implementation	Conditional (for example, a confidential file, when sent on Skype, can be blocked, but text of the same file, when sent as a Skype message, is not blocked); not all channels are monitored	Full-fledged implementation	Full-fledged implementation
Protection of data at rest in the infrastructure (DLP)		Full-fledged implementation	Only detection, audit of operations and access rights are not available	N/A	Only detection, audit of operations and access rights are not available	Only detection, audit of operations and access rights are available only via DRM integration
Investigation of violations (forensics)	Capability to reconstruct an incident in details (up to video repeat of the violation), detection of the guilty and involved parties	Full-fledged implementation	Partially and in a third-party solution	N/A	N/A	N/A
Unambiguous identification of violator (forensics)	Capability to unambiguously identify an employee by digital (AD, web accounts) or biometric (voice, face) component	Full-fledged implementation	Partially (attributes of traffic or AD)	Partially (AD)	Partially (attributes of traffic or AD)	Partially (attributes of traffic or AD)
Identification of risk groups (preventive security)	Addictions, radical views, deviant interests, proneness to gambling, terrorist activity, etc.	Full-fledged implementation	N/A	N/A	N/A	N/A
Detection of fraud, theft, bribery (economic security)	Detection of obvious or indirect theft of money, abuse of official position or infrastructure for	Full-fledged implementation	N/A	N/A	N/A	N/A

Comparison criterion	Comment	SearchInform	ForcePoint (ex WebSense)	Safetica	Symantec	McAfee (Intel Security)
	personal needs, promotion of affiliated deals and suppliers					
Profiling of employees (preventive security)	Capability of automated profiling (psychological portrait of employee)	Full-fledged implementation, no analogues	N/A	N/A	N/A	N/A
Inventory of IT infrastructure	Capability to get a report on the status of technical components (hardware and software)	Full-fledged implementation	Partially	Full-fledged implementation	N/A	N/A
Detection of violations of work regulations	Inefficient work, outsourcing in work time, absence at workplace, non-major activity (video games, news, social network, etc.)	Full-fledged implementation, activity in IT systems and ACS	N/A	Only at PC	N/A	N/A
Implementation of perimeter of encrypted data transmission	Capability to create safe perimeters of data transmission (when data can be used only inside the network)	Available, implemented for USB storage device	Third-party technology	N/A	Available	Available
Privileged users monitoring (IT administrators)	Capability to control remote connections to servers and workstations over RDP, TeamViewer, rAdmin, etc.	Implemented as shadow copy and restriction both	N/A	N/A	N/A	N/A