SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

INFORMATION SECURITY & RISK MANAGEMENT

[GUIDE FOR PROTECTING YOUR COMPANY AGAINST INSIDER THREATS]

CLOUD DATA PROTECTION: NEW AGE SOLUTION

www.searchinform.com

INTRODUCTION

Companies are increasingly moving IT infrastructure to the clouds: according to Gartner forecasts, by 2025, 90% of the world's companies will fully or partially switch to cloud services. As-a-service model – when customers receive equipment, applications, and even ready-made jobs from a provider – it allows you to speed up business processes and reduce the load on the organization's own resources.

Cloud solutions are safe

Today, many IT products are undergoing a new development in the form of cloud services. Large cloud providers comply with stringent regulatory standards, offer customers access to additional security programs, guarantee the confidentiality of customer data, and as large companies are better able to protect themselves from DDoS attacks than individual customers.

IN THIS BOOK WE:

- Highlight the main risks of cloud services
- Tell you how modern solutions solve the problem of controlling virtual infrastructure
- Give recommendations on how to choose the appropriate protection model depending on the structure of business processes

WHO IS AT RISK?

Cloud services are not necessarily virtual file storages. These include almost any online services that are used in business processes:

- Virtual machines (VMware, etc.)
- Virtual office software (Google Docs, Word Online, etc.)
- Corporate NAS (Synology, HP, QNAP, etc.),
- Corporate storage (SharePoint), cloud storages (Dropbox, Google Drive, Yandex.Disk, OneDrive and CMIS)
- Public web-based email services (gmail.com, etc.)
- Virtual task trackers (Bitrix, Trello, Wrike, etc.)
- Virtual systems of automation and accounting (1C, SAP, etc.)
- Cloud CRM systems
- Corporate and public messengers / telephony (Telegram, Slack, Skype, etc.)
- Other online solutions

The peculiarity of such services is that they process sensitive data outside the corporate perimeter. Therefore, the traditional model, when a business seeks to protect commercially valuable information within the company, is violated. Thus, the risk of confidential data leakage is growing.

HOW DOES IT WORK?

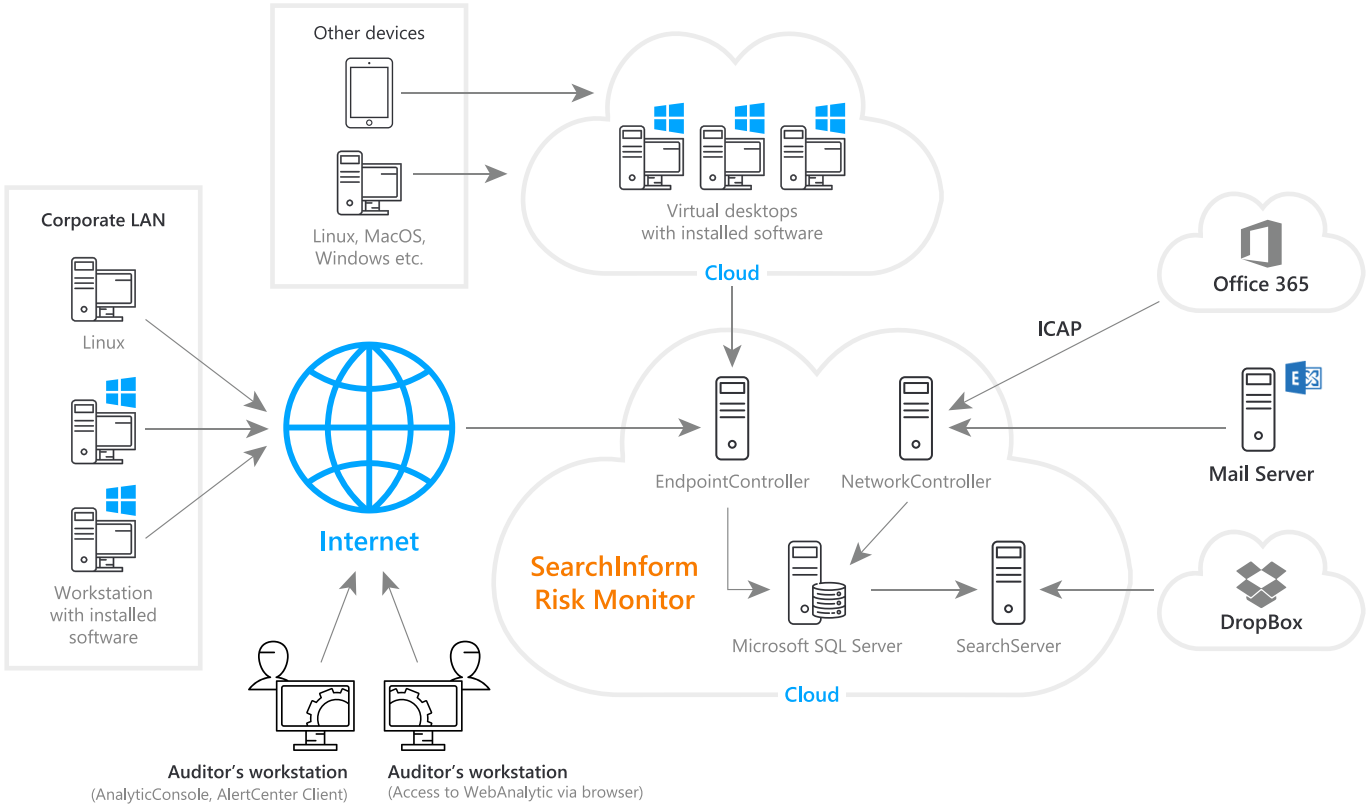
Our solution, SearchInform Risk Monitor supports a cloud-based model. The cloud operation shall mean here the location of server, client or agent parts in a cloud infrastructure.

A key requirement for this infrastructure is the capability to create a full-fledged Windows OS in a cloud infrastructure and install there SearchInform Risk Monitor components. See the diagram below.

All major cloud platforms, for example, Microsoft Azure support this option (for OS virtualization in the cloud).

At the same time, all technical requirements for ports, interaction protocols, network accessibility of monitored PCs, AD accounts and all other formal recommendations remain valid for cloud operation models.

When you monitor a cloud infrastructure, the device (Windows, MacOS, Android, etc.) that a user connects to the cloud infrastructure with does not matter.



General diagram of SearchInform Risk Monitor operation in a cloud infrastructure

DATA PROTECTION IN THE CLOUD

- Scan and detect confidential data: corporate NAS (Synology, HP, QNAP, etc.), corporate storage (SharePoint), cloud storages (Dropbox, Yandex.Disk, OneDrive and CMIS)
- Scan and detect confidential data, take urgent measures in case policies are violated (block): Office 365
- Full functionality for virtual desktops:
  - Capture email correspondence, including email incoming via web browsers
  - Capture chats, calls, SMS, and files on Skype, as well as history tracking
  - Capture chats and attachments on social networks and instant messengers as well as incoming and outgoing messages from other popular sites
  - Capture data sent or received over FTP, including encrypted connection (FTPS)
  - Capture messages (Post/Get requests) sent to web forums, blogs and via browser IM clients
  - Control contents of cloud storages
  - Record employee conversations in the office and on business trips via any detected microphone
  - Record video of onscreen user activity, make screenshots
  - Monitor the content of documents sent to printers
  - Capture data transferred by users to external devices
  - Detect confidential documents, which are stored with violations of security policies in shared folders, computer hard drives, cloud storages and local NAS systems, SharePoint platform
  - Capture key strokes (logins, passwords, etc.) as well as data copied to the clipboard
  - Collect data on applications run by an employee during the day and time spent in them
  - Classify sensitive documents, audit and manage access to files and databases, detect file and folder activities, identify unauthorised use

MODELS OF WORK

We provide our help for SME and large enterprises who:

- Don’t have their own IT infrastructure (email servers, VPN, NAS, etc.) or it is limited
- Have remote branch offices
- Use mainly cloud services for mail, business systems, document management applications, employees communicate via messengers and use a browser for task implementation
- Have domain structure, use enterprise and public email servers, corporate messengers and other popular solutions
- Have all their software available in the cloud or located in the corporate network, employees can work via a terminal server or connect to VDI, corporate software, a browser and messengers are used for performing tasks

SERVICES:

- MSSP (a specialist responsible for risk mitigation is assigned)
- Dedicated DLP server with the Internet access on a provider’s side with or without partial processing on a customer’s side
- DLP server allotted by a provider
- Data storage on a provider’s side or hybrid storage (a large amount of data is stored on a customer’s side)

www.searchinform.com

+44 0 20 3808 4340
order@searchinform.com

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

ABOUT US

SearchInform is the leading developer of risk and compliance software. Our technology secures business against corporate fraud and financial losses, provides for internal risks management, and for human factor control.

Visit our blog to be updated on relevant risk management and data safety issues.

linkedin.com/company/searchinform
facebook.com/SearchInformInternational
twitter.com/SearchinformI