It's not about me

SPECIAL EDITION

What an employee can do if there's no monitoring?

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

INTERNAL THREAT MITIGATION PLATFORM

In order to discover information security threats, companies need powerful instruments. SearchInform software do it all: control incoming and outbound traffic, IT infrastructure events, ensure confidentiality of critical data on PCs and in databases, track user activity, assess human resources risks and alert to security policies violation.

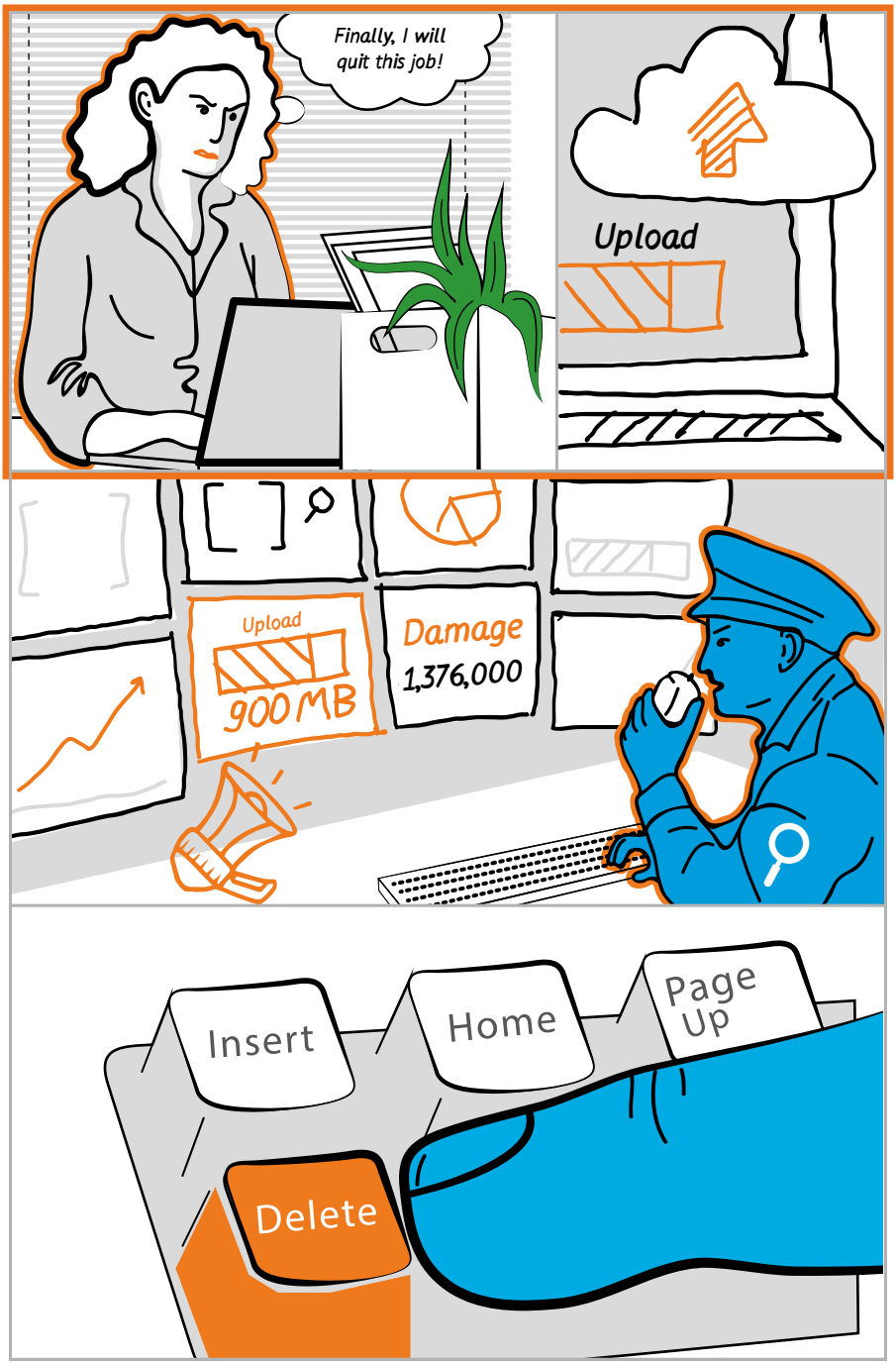
This is not about you

While you are reading these words, 59 records get stolen or lost somewhere around the world. This is the average speed of data breach per second.

You are sure that data loss won't hurt your business, but the average data breach cost is $2,5 million* including commercial and reputational losses.

We have collected real life cases shared with us by our clients which prove: there is no company which would be totally protected from information leakage, fraud and malicious insider activity.

**According to the IBM Security global research.*


Finally, I will quit this job!
Upload
Upload
900 MB
Damage
1,376,000
Insert
Home
Page Up
Delete

“Little something” to remember

An employee of a trading company who was denied a raise decided to quit. But before the dismissal she uploaded an archive with about 900 MB of corporate data to an external storage.

The DLP system analysis of the archive showed that the employee stole the company’s research projects which covered all the local market. The overall cost which resulted from document design, lost profit, disclosure of sensitive data regarding clients and production cost amounted to $1,376,000.

The archive was removed from the third-party resource thanks to timely incident detection.

The investigation revealed the fact of accounting document forgery. The disgruntled employee altered financial information which was stored on a file server. Documents could have been restored, and the prompt DLP intervention would have saved time and money which would have been spend on fines when submitting reports to the tax office.

Besides, such a trick could lead to seizure of the company’s accounts, which would paralyse the workflow until everything is sorted and get followed by a bankruptcy.

Investigation tools

SearchInform FileAuditor

SearchInform DLP: CloudController


Copying files...
Clients
sec
Login:
Password:
Copying files...
70%
Clients
elete ?
yes
no
dismissed

Data leakage to the cloud

The DLP system alerted information security specialists to an export of an abnormally large archive to Dropbox. The login and password were instantly found in the cloud, the specialists discovered that the copying was still on.

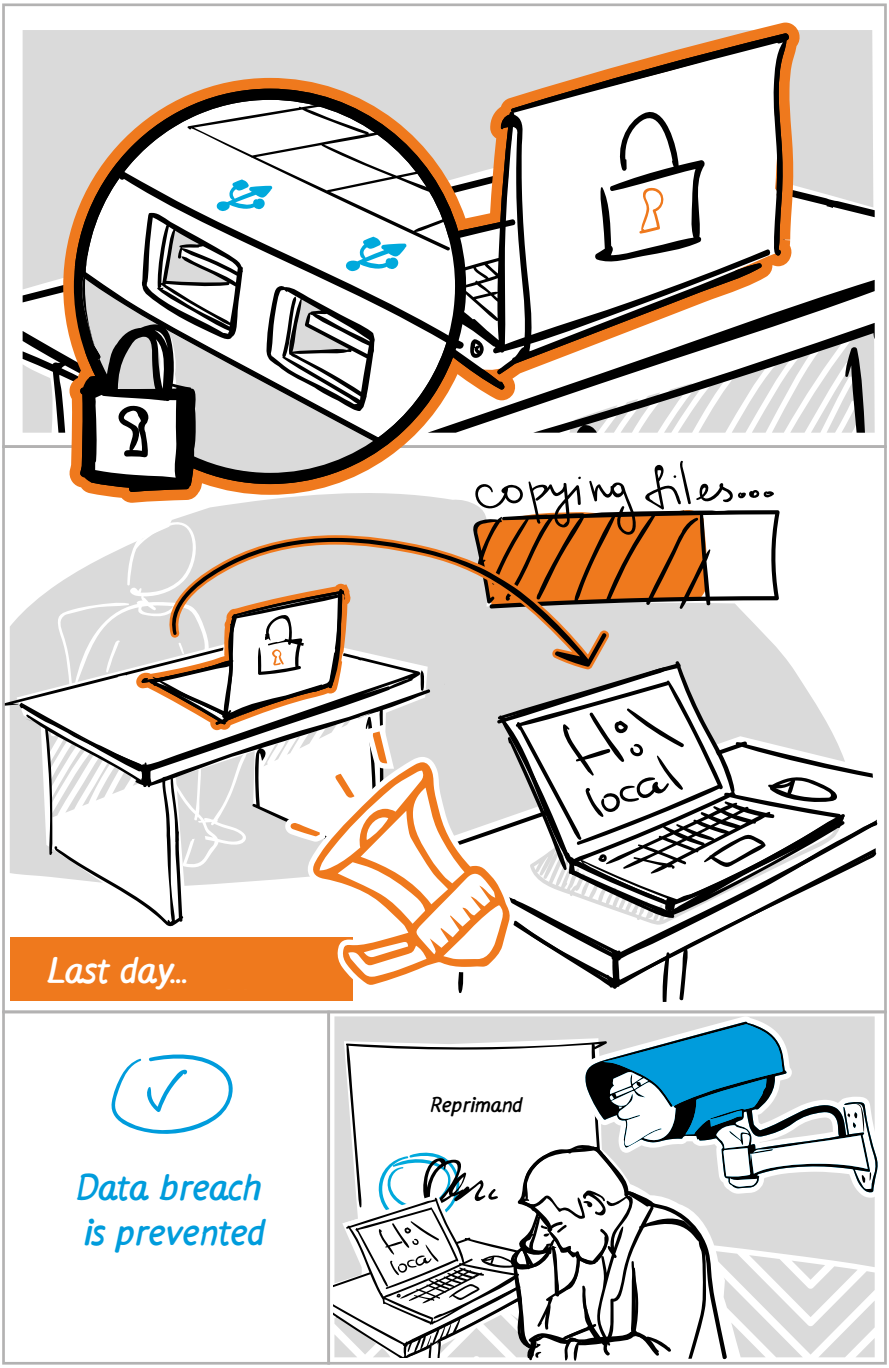
After accessing the employee's PC in a real time mode, information security specialists saw that he was copying the customer base and deleting files on the PC.

The specialists' reaction allowed the company to prevent an incident: the information security department succeeded to promptly access the employee's desktop until he could complete the copying. He was asked to delete the documents from the cloud, and after he was dismissed.

Investigation tools

SearchInform Risk Monitor:

- CloudController
- MonitorController
- Keylogger


copying files...
Hi, local
Last day...
Data breach is prevented
Reprimand
Hi, local

Data breach due to friendship

USB ports were blocked on the PC of an employee who managed the paperwork regarding dismissal and because of that his activity was monitored particularly strict. MonitorController made screenshots on which the specialist responsible for data protection saw that the employee was transferring gygabytes of information to some disk H:\ on the PC of his friend who kept working in the company.

The specialist studied the history of operations and found out that the employee's colleague freed the required space on the disk H:\ beforehand and granted access to the quitting employee right away. He was going to take the documents on his personal flash drive.

The data leakage outside the corporate perimeter was prevented. The worker's friend received a reprimand, the information security department of the company took him under control.

Investigation tools

SearchInform Risk Monitor: MonitorController

SearchInform FileAuditor


$ 100,000
Market research
PURCHASE
One week after
Darknet
Market research
Get
One more week after
Market research down
Market research
download for free
Market research
download for free
Market research
download for free
Access to the research
File Auditor
1
2
99
100
Location:
1
2
~300 PCs
Access denied

Easy access files

A retail company regularly ordered expensive market research (only one would cost $100,000). The information security department of the company noticed a suspicious tendency: one week after obtaining of the results the market research gets found on the darknet, and one more week after that it becomes available for all the Internet users.

The specialists responsible for risk mitigation offered top management to check who had access to the research. In order to learn more the company installed FileAuditor. The access to the documents should be granted to no more than 100 specialists in accordance with the security policies. The audit showed that there actually were 300 employees who could access the data from their PCs.

After the excessive access rights were discovered the access to the data was denied. A retrospective investigation was conducted with the help of DLP to find out who leaked the documents and where to.

Investigation tools

SearchInform FileAuditor


This is your new workplace
downloading...

Undercover

A company hired a sales network manager. As any other new employee, he was taken under control by the information security department.

The control wasn't in vain: an employee appeared to be "in disguise". His main intention was to access the corporate accounting department's system and the following leakage of the data to competitors.

The transfer of the data to the competitors would have affected the company significantly and caused customer churn. This would have cost the company over $164,000 a year.

The employee was fired.

Investigation tools

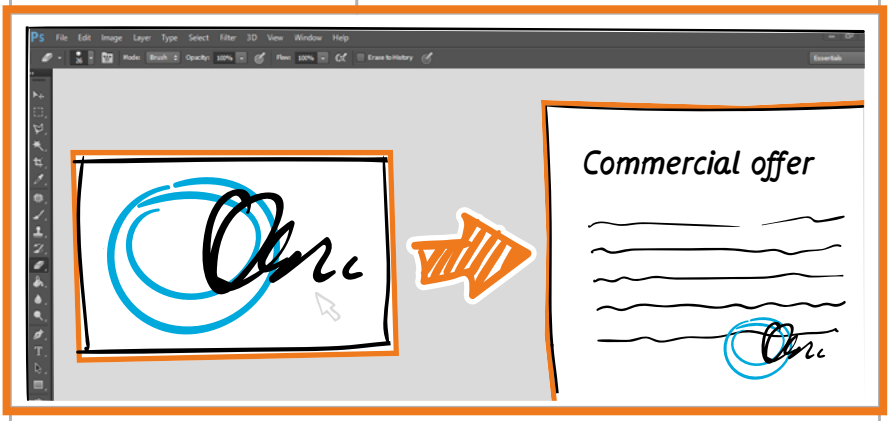
SearchInform DLP:

DeviceController

SearchInform FileAuditor

Commercial department

Report on the total activity of processes



Forged seal

A specialist responsible for information security and risk mitigation paid attention to an employee's computer in the commercial department – Photoshop.exe process was frequently ongoing there. The manager's job wasn't related to the tasks that could be implemented with the help of the graphic design software – he had nothing to do with design, marketing or advertising.

The information security specialist decided to review screenshots and desktop activity recording to discover what is going on when Photoshop.exe is launched.

The manager appeared to have been forging price in the offers. He altered the details and literally drew seals on the documents of other providers in order to lobby his partners. As a result, instead of getting "dividends" he got fired.

Investigation tools

SearchInform Risk Monitor:


MonitorController


ProgramController


Tax office
Company registration certificate
S.C.A.M.
Branch
You should sign an agreement with S.C.A.M.
Branch
Branch

Illegal selling

The equipment manufacturer discovered suspicious connection among three employees at the stage of the SearchInform solution testing. During workdays these workers didn't communicate with each other, didn't go to lunch together and were in different offices. But all of them used one email box registered on one of the free services.

The detailed analysis of the captured data allowed the information security specialists to reveal that there had been a draft created in the email box where the employees discussed selling schemes of the manufactured equipment bypassing the manufacturer. The damage caused by the employees' fraud amounted to nearly $55,000.

Two employees were dismissed. The third employee stayed at the company, but corresponding measures were taken.

Investigation tools

SearchInform DLP: MailController


I'll sell confidential data and will finally quit!
Login during non-working hours
Cisco
Login via TeamViewer
Password guessing
VIOLATOR IS DISMISSED
Deny usage of remote admin software
OK

Fraudulent activity with accounts

SearchInform SIEM has detected suspicious chain of events in the IT infrastructure of a company: password guessing and successful logging into the system via TeamViewer during off-hours.

Information security specialists monitored the incident with the help of the DLP system as well – the solution detected the transfer of confidential data via TeamViewer.

The violator was found. It appeared to be one of the managers who wasn't satisfied with the work terms recently and was going to quit.

As a result, the employee was fired, and the usage of remote desktop software was forbidden in the company.

Investigation tools

SearchInform SIEM

SearchInform DLP: CloudController


No bonuses!
I will take revenge on them...
BOSS
Downloading...
Database

Employee's revenge

During a scheduled user activity monitoring there was an employee discovered who couldn't get used to work after a long holiday: besides, being late everyday he would play online poker instead of working and other card games. The reaction of the management was clear: a reprimand and loss of bonuses.

The employee took it his own way and decided to take revenge on his management. One of the security policies of the DLP system aimed at search for negative attitudes and moods helped to discover the correspondence between the worker and his friends where he was very explicit about the top management's actions and promised to "stir up some trouble".

He began to act shortly after. The next day the information security department detected copying a lot of data by the employee to an external storage: there were details about providers, sales, clients as well as the number of financial documents.

The employee couldn't leave the building with the stolen data thanks to the timely actions taken by the specialists responsible for risk management. If the data got stolen it would cost the company nearly $100,000.

Investigation tools

SearchInform DLP:

DeviceController

IMController


Could you please double-check these documents? They will form part of the annual financial report.
Report
Yes, I will do it myself...
SATURDAY
3:26 PM

Employees, who overwork, pose risks to their organization

Quite often workload is distributed unequally. Executives delegate even more tasks to employees, who work hard and more efficient than other staff members do.

However, this may lead to overload and burnout. Employees' morale and discipline may be affected badly.

What's more, if employees work overtime, they are more likely to accidentally commit an information security incident because of fatigue (accidental data leaks and inability to respond adequately to phishing attacks are among most common incidents).

The DLP system helped information security department to detect these tendencies. Basing on this information, employees in charge managed to redistribute workload on other employees. This enabled not to fire a few valuable specialists who regularly worked late hours and didn't have breaks.

The system also enabled to reveal the most efficient employees. The company started to take this information into account when making plans of bonus pay and building a talent pool.

Investigation tools

SearchInform DLP:

IMController

HTTPController

Tutorial for cybersecurity specialist. Explaining the information security in 4 steps
https://searchinform.com/tutorial/

Find recommendations on managing internal security risks in our HOWTOs and White Papers
https://searchinform.com/practice-and-analytics/

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT