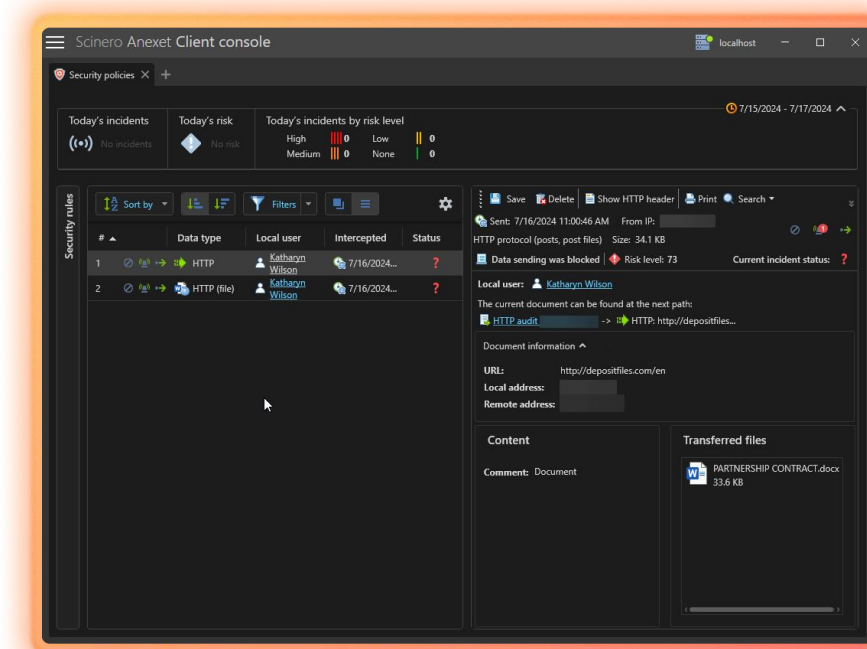
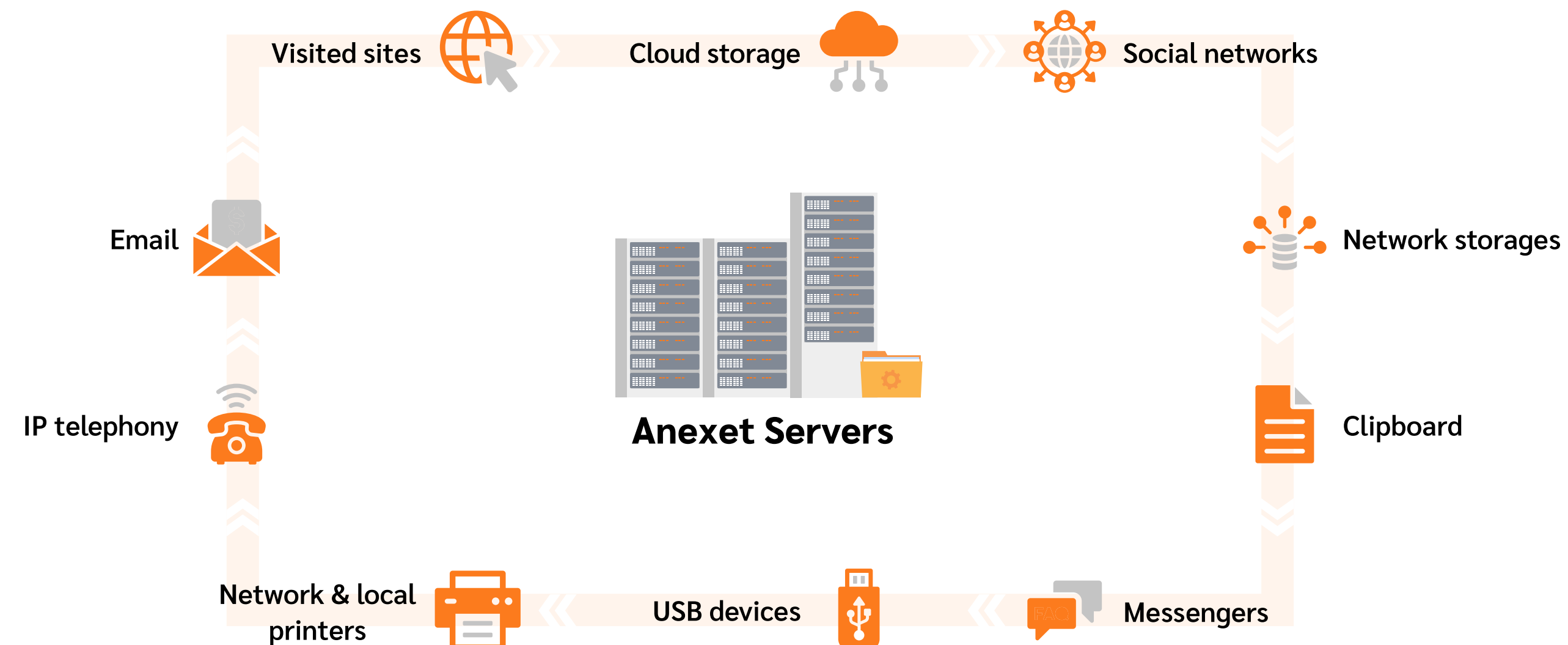


# Analyzes and Controls Data Flows

Anexet protects the company's internal information from leaks caused by employees



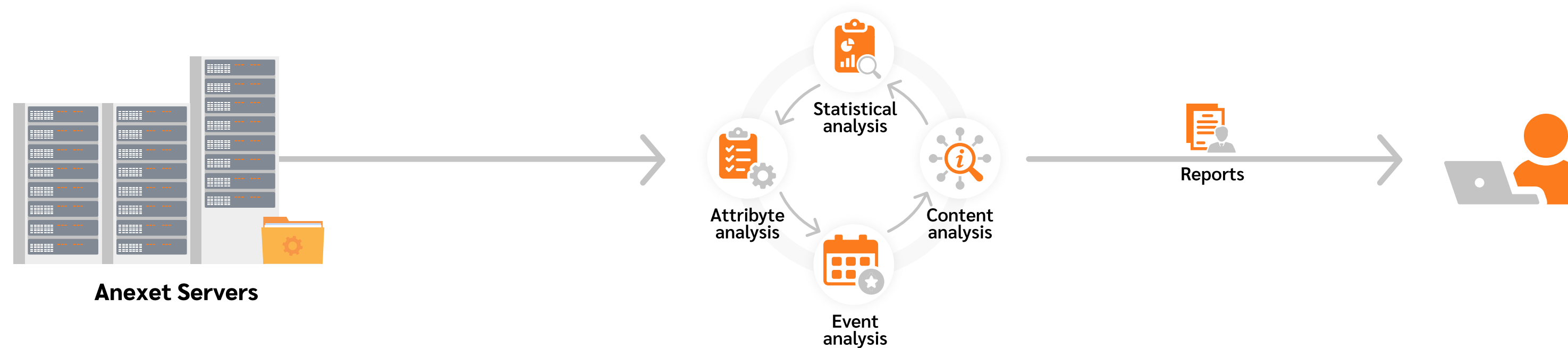
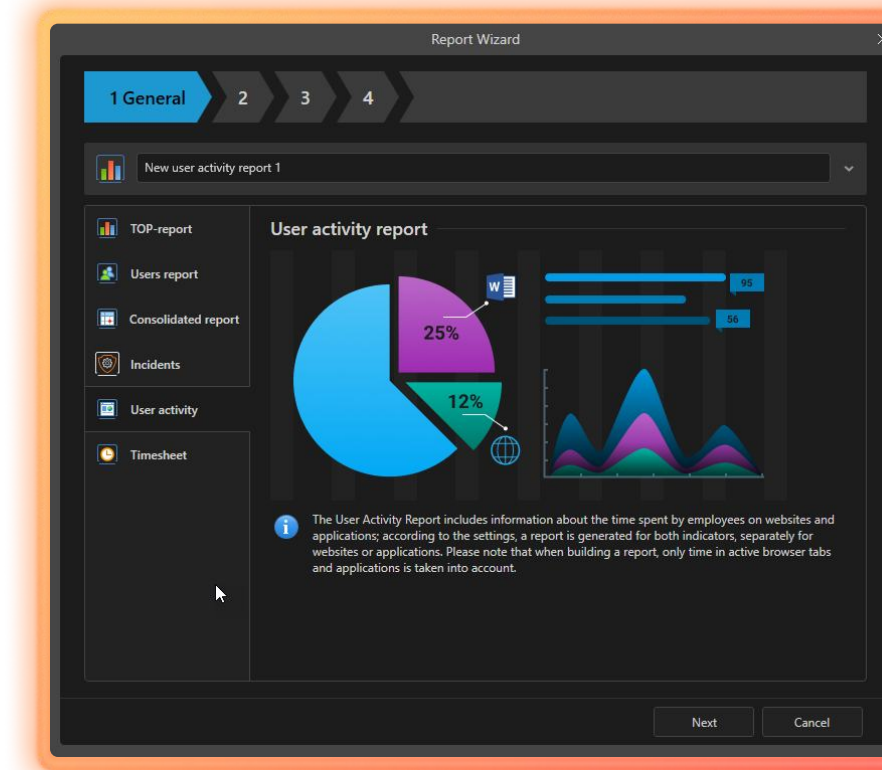
- Control various information streams: cloud storage, social networks, network storage, clipboard, messengers, FTP connections, e-mail, IP telephony
- Control external devices: USB devices, network and local printers, drives, etc
- Monitor employees' actions. System allows to see potential threatening actions with data
- Set the system to detect data transferring via the Internet



# Performs Automatic Data Analysis

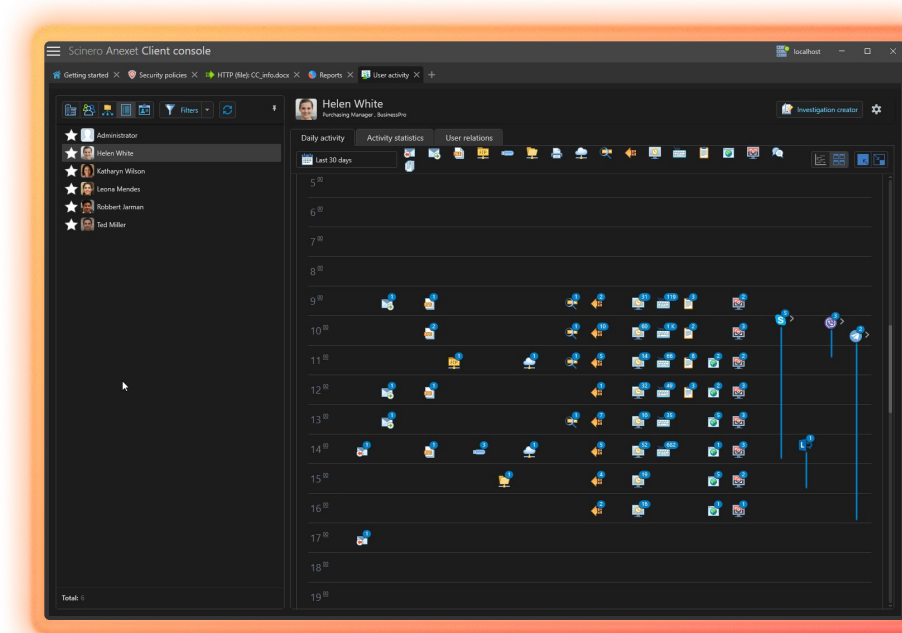
Anexet Activity provides content analysis, statistical analysis, event analysis, and attribute analysis of captured data

- Get a full picture of employee workday: visited sites, applications used, time on browsers, etc
- Detect certain words and phrases in the text, messages, emails
- Set the system to respond to certain events: transferring documents, launching apps, and so on
- Monitor audio from microphones and video from monitors. Take screenshots at any time

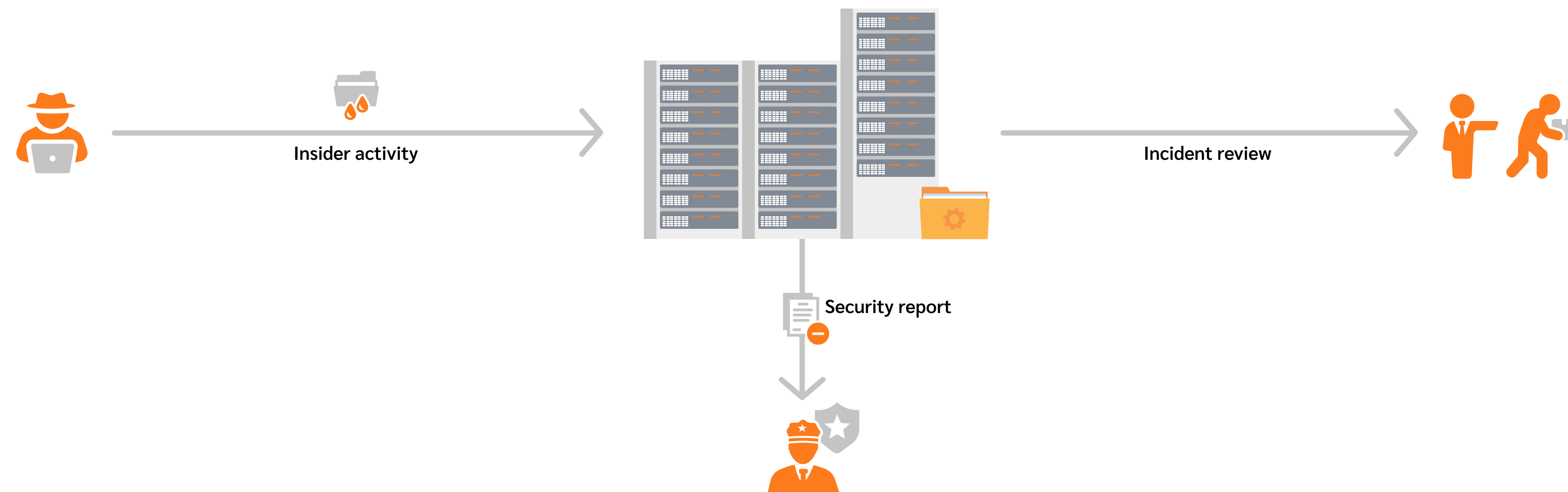


# Identifies Suspicious Actions of Employees

The system helps to detect attempts to spy and transfer confidential information, as well as to establish compromising connections



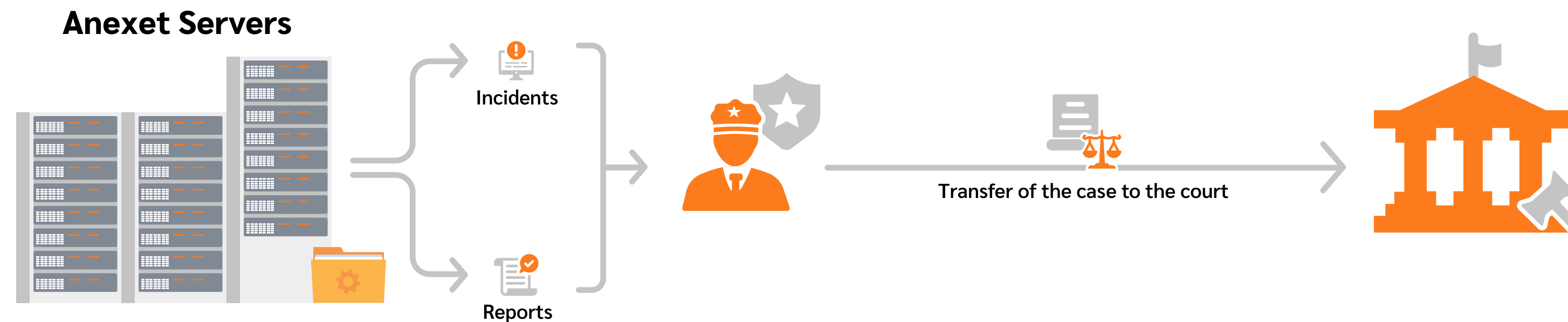
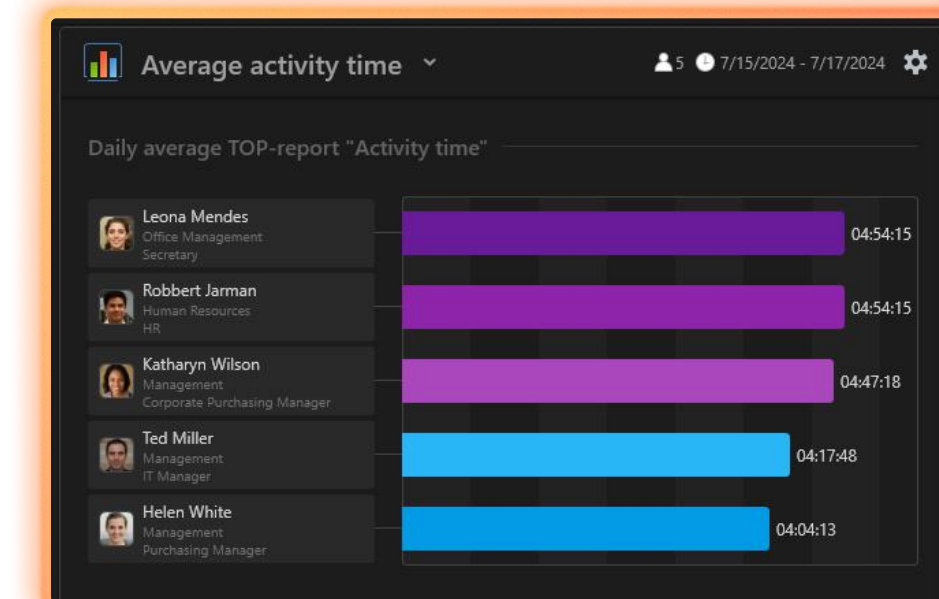
- Visualize connections between all your workers in the graphic model
- Detect insiders. If an employee contacts the third party outside the company contour, you'll get notified
- System analyzes behavioral patterns. If an employee acts suspicious, the system will notice and alarm
- The system can be configured: to protect specific data, to put special attention on employee, to respond to triggers



# Instant Notifications to the Security Service in the Case of a Violation

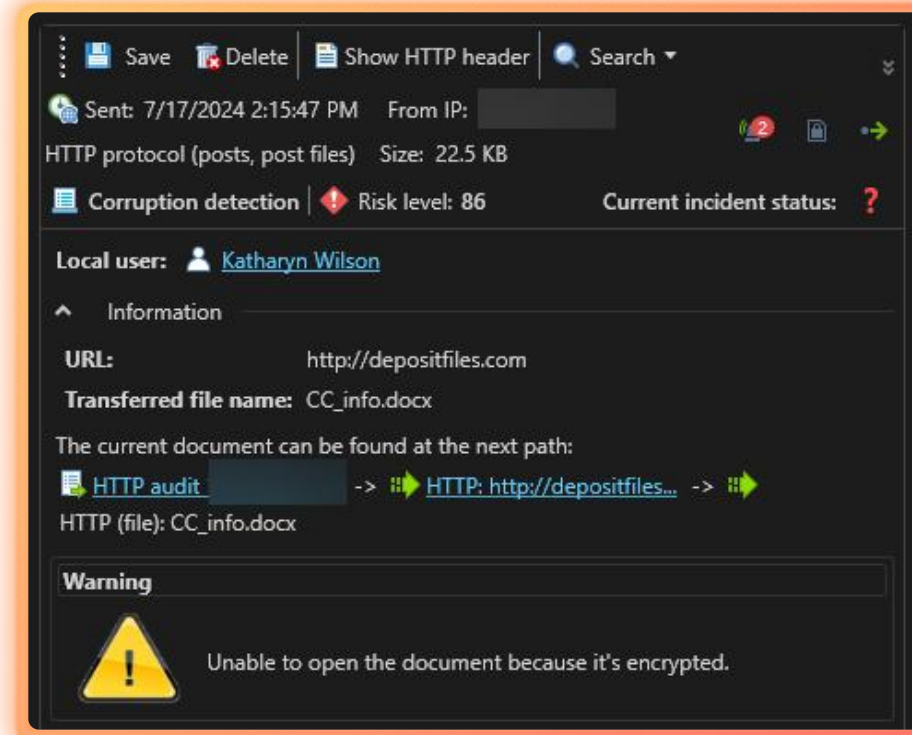
This helps to identify those responsible for leaking corporate information faster and easier and investigate incidents quickly

- In the case of breach, the system notifies the security officer. Management can quickly take responsive actions
- The system helps to find perpetrators and build the whole picture of the breach from the very beginning
- The system provides reports on the breach. It shows vulnerabilities, so it will be possible to remove them
- Reports may be used in the court in the case of judicial proceedings



# Optimization of the Work Environment

The DLP system analyzes employees access to the data and helps managers optimize working processes and eliminate redundant privileges, which can improve workers performance and reduce unnecessary use of the company's resources



- Prevent theft or unnecessary personal use of company's resources (workstation, devices, etc)
- Control employees' efficiency and adapt business processes to reach maximum productivity
- Detect devices that are not the part of the configuration and non-functional devices
- Optimize access levels. Control data access levels and create a robust security framework

