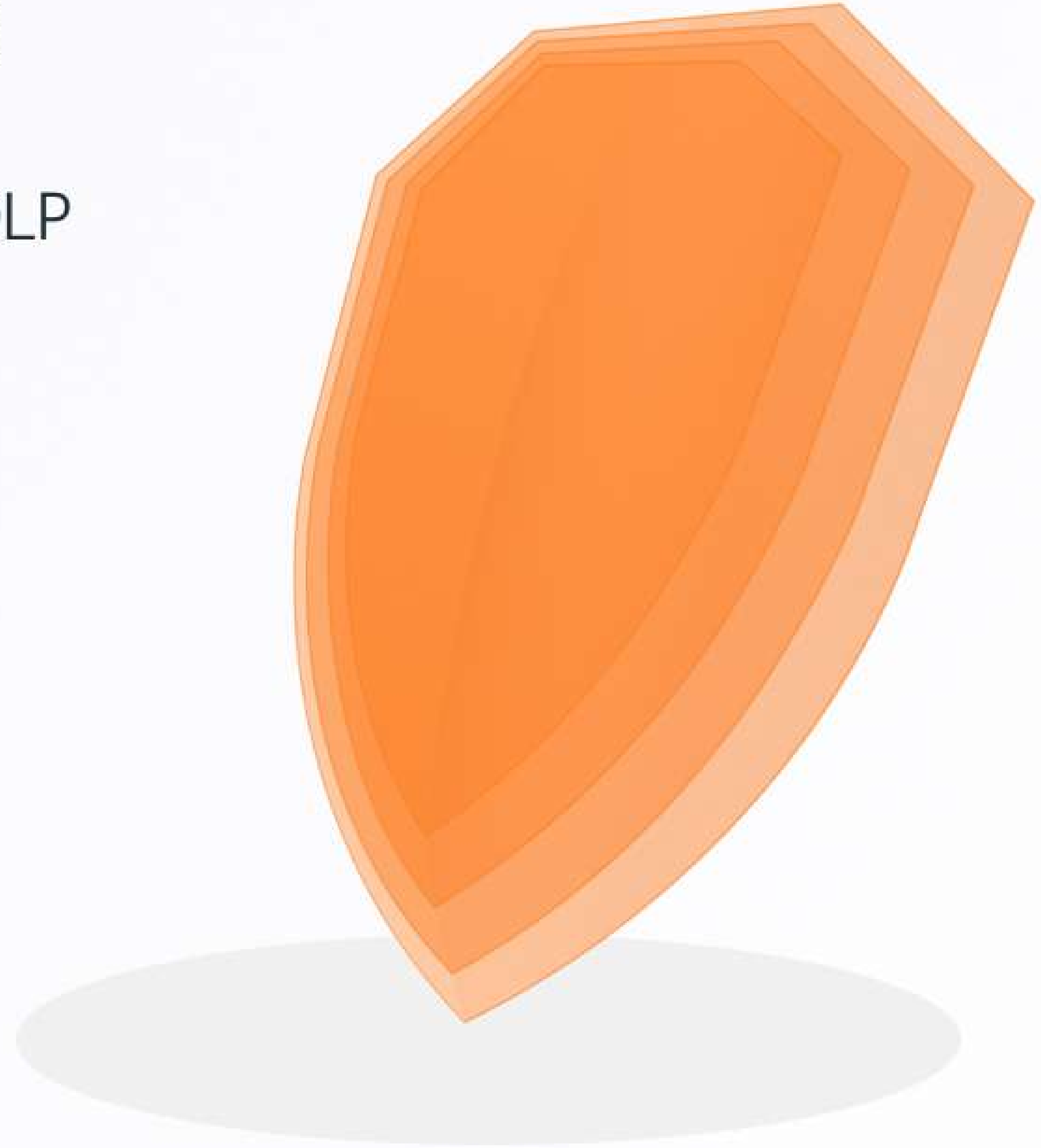
Endpoint Protection DLP: Features and Benefits

Discover, monitor, and protect your sensitive data with Anexet DLP

- Monitoring user activity
- Detection of malicious activity
- Blocking insider activity of employees
- Investigation of incidents
- Easy to configure and use



Multi-OS DLP Endpoint Protection

- In today's diverse IT environments, safeguarding sensitive information across multiple operating systems is crucial. Anexet offers control over devices running on Windows, Linux, and MacOS. Empower your organization with a DLP system that adapts to your diverse technological landscape. Protect your data, maintain compliance, and ensure peace of mind with our robust, multi-OS DLP solution
- The functionality of the product may vary depending on the platform

User Activity Monitoring

Daily Activity

Protection of Confidential Data

The system allows you to control the use, transfer and storage of information. Monitoring and analyzing user activity helps to determine what actions were performed with the data. This allows you to identify the causes of the violation and take measures to prevent similar incidents in the future

User Relations

Monitoring of Communications

The system can be used to detect any suspicious activity, such as attempts to transfer confidential information to third parties or change the terms of transactions without appropriate permission. By monitoring communication traffic and paying attention to deviations from the normal activity of employees, the DLP system can detect and highlight indirect signs of threats that may indicate fraudulent activity

Documents and files

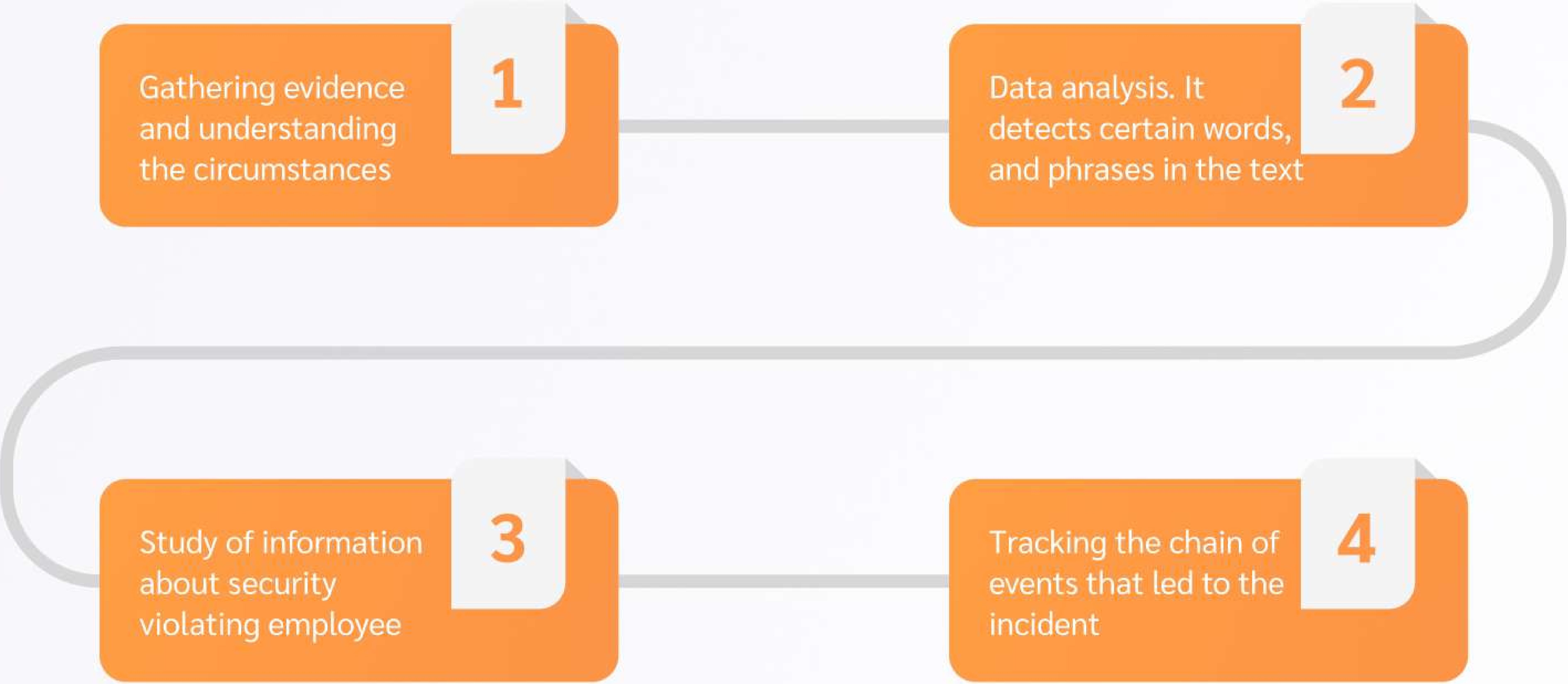
USB devices

Messages

Web and applications

Investigation of Incidents

The investigative function is an important tool to ensure the security of confidential information and prevent data leaks



1 Gathering evidence and understanding the circumstances

2 Data analysis. It detects certain words, and phrases in the text

3 Study of information about security violating employee

4 Tracking the chain of events that led to the incident

Detection of Malicious Activity

Chronology

Files and Messages Content Analysis

Analyzing the contents of files and messages. This allows you to detect and block attempts to transfer confidential data. We use content, statistical, event and attribute analysis of information. We analyze the relationships between employees

File Operations

Files and Messages Content Analysis

Contextual analysis includes checking the access rights of users, applications, or systems trying to access data, and their actions with the data. This method helps to understand how confidential information is used. It evaluates the context of data usage based on its sensitivity and value to the company

Security Rule

Network Traffic Control

Network monitoring and filtering. Network traffic control, identification and blocking of confidential information transmission using network protocols and applications, including e-mail, cloud services, messengers, outgoing and incoming web traffic, employee communications through various communication channels

Blocking Insider Activity of Employees

- Detect real threats using the DLP system, initiate automatic incident management processes, enable alerts for responsible teams or data access blocking
- Identify and evaluate employees at high risk. Get recommendations in case of changing employee behavior in order to prevent incidents
- Identify and block unwanted or redundant applications, hardware, or peripherals