DATASHEET

Group-IB Fraud Hunting Platform /
Preventive Proxy

GROUP-IB FRAUD HUNTING PLATFORM/PREVENTIVE PROXY

Group-IB Fraud Hunting Platform is a unique system designed to proactively protect digital identities and prevent fraud in real time. The product's star module, Preventive Proxy, is a state-of-the-art solution that defends users of both mobile applications and web portals against harmful bot activity. Our protection knows no boundaries, covering financial institutions, government agencies, and e-commerce businesses alike.

Bot detection from Group-IB Fraud Hunting Platform is made possible through the analysis of user behavior and the environment in which the application or portal operates.

Types of bot attacks that Group-IB's solution protects against

Web scraping

Using bots to extract content and data from public and password-protected webpages

Brute force

Gaining access to user accounts by establishing login credentials automatically

Unforeseen costs

Money spent on handling fake requests from bots (sending SMS messages to users, buying additional bandwidth)

Credential stuffing

Using stolen credentials to gain unauthorized access to user accounts automatically

Bot attacks on mobile API

Collecting data and committing fraud through the mobile channel

(D)DoS attacks

Denial-of-service attacks on resources or their elements using bots

Unauthorized use of API

Directing requests to the API and using it from third-party or spoofed mobile applications

Automation tools

Using Selenium, PhantomJS and other tools to automate user actions

How Group-IB's bot protection solution works

In addition to checking headers and how often requests are sent to the customer's servers, the solution does the following:

1

Analyzes user actions for characteristics that are typical for bot activity (e.g. linear mouse movements, program clicks)

2

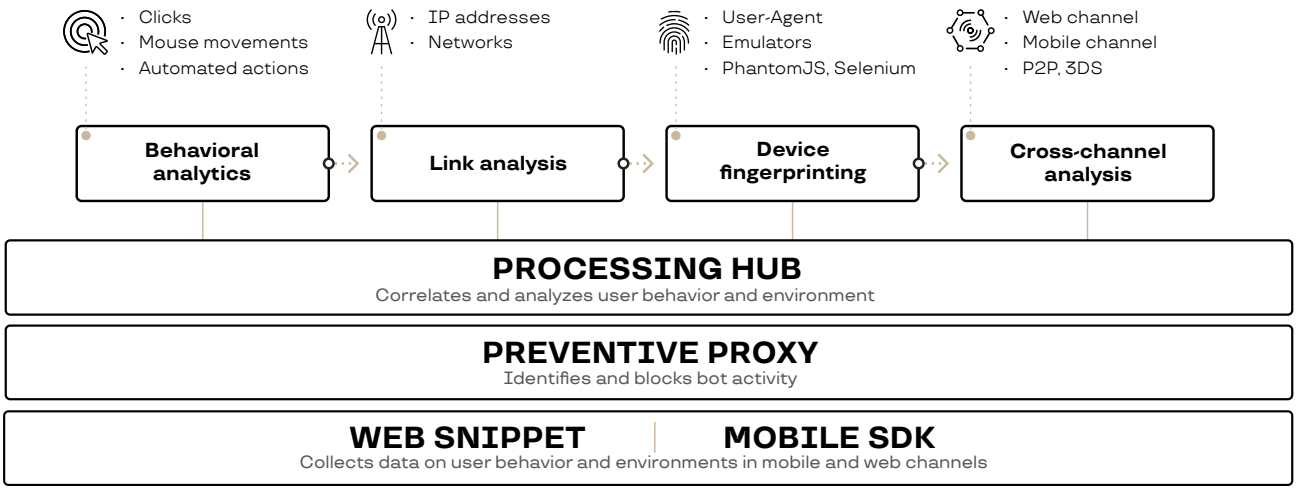
Collects browser, app, and device parameters and checks them for signs of bot activity (e.g. Selenium, PhantomJS, or mobile emulators are deployed)

3

Uses Group-IB's patented technology to protect the parameters of a real user session against being reused by bots

How Group-IB's bot protection solution works

Group-IB Fraud Hunting Platform consists of several modules:



Web Snippet

As soon as the first page of the web resource is loaded, Web Snippet transfers data on user behavior and the environment in which the web application is running to the system server side.

Mobile SDK

Mobile SDK works similarly to Web Snippet, but within a mobile application.

Preventive Proxy

Preventive Proxy checks requests from the user's device for cookies and determines whether they are correct and unique. Based on the findings, Preventive Proxy decides whether fraud or bad bot activity have been identified.

Processing Hub

Processing Hub generates a new server cookie and issues a verdict on whether bot activity has been identified. When requests are sent from a mobile or web application, Mobile SDK or Web Snippet generate a client cookie based on the server cookie and then transmit it.

Depending on the verdict and custom settings, Preventive Proxy:

Marks requests with additional HTTP headers for either further processing on the protected app's servers or integration with other cybersecurity systems

Skips requests from trusted sources or from legitimate bots (e.g. search engines)

Blocks or redirects requests to other pages

This approach enables additional verification only for suspicious requests: from bots or in the event of false positives (less than 1%, according to statistics)

Key advantages

Continuously analyzes session to identify "smart" bots that emulate human behavior, including tracking software clicks, data insertions, and automated navigation between pages

Combats sophisticated bots by detecting device emulators, anonymizers, and automation tools and by analyzing user behavior and the environment

Protects cross-channel APIs for mobile and web applications by counteracting the interception and spoofing of data in requests sent to the application

Unifies protection for both mobile and web applications that can use a common API

Identifies other types of fraud, thereby comprehensively protecting the company's digital identity

Improves user experience by running additional checks for suspicious requests only (e.g. using CAPTCHA)

Increases API security against attacks using various analytical and penetration testing tools

Keeps conversion rates stable by blocking malicious requests rather than IP addresses

Easily integrates with customer cloud and on-premise systems

Detects and prevents attacks accurately with integrated data on cybercriminals, malware, adversary IP addresses, and compromised data obtained from Group-IB Threat Intelligence & Attribution, the Digital Forensics Lab, and anonymized customer feedback

Protects against bot activity throughout the user's session. Attempts to re-use our access tokens or your session cookie will not help threat actors achieve their goal.

Implementing Group-IB's bot protection solution

To enable protection against bots, Web Snippet (for web portals) or Mobile SDK (for mobile apps) must be implemented.

Preventive Proxy can be deployed within the application infrastructure or the Group-IB cloud.

Delivery options:

- Docker container
- Binary executable file
- Group-IB cloud

Traffic can be processed by:

- Proxying requests through Preventive Proxy
- Marking up using auth-request in NGINX

Technical requirements for Preventive Proxy

For a load of 20,000 to 30,000 requests per second (excluding static content), the following minimum server resources are required:

To minimize processing time, requests for static content can be redirected through a proxy module in the application infrastructure.

CPU	4 cores, 2 threads per core
RAM	8 GB