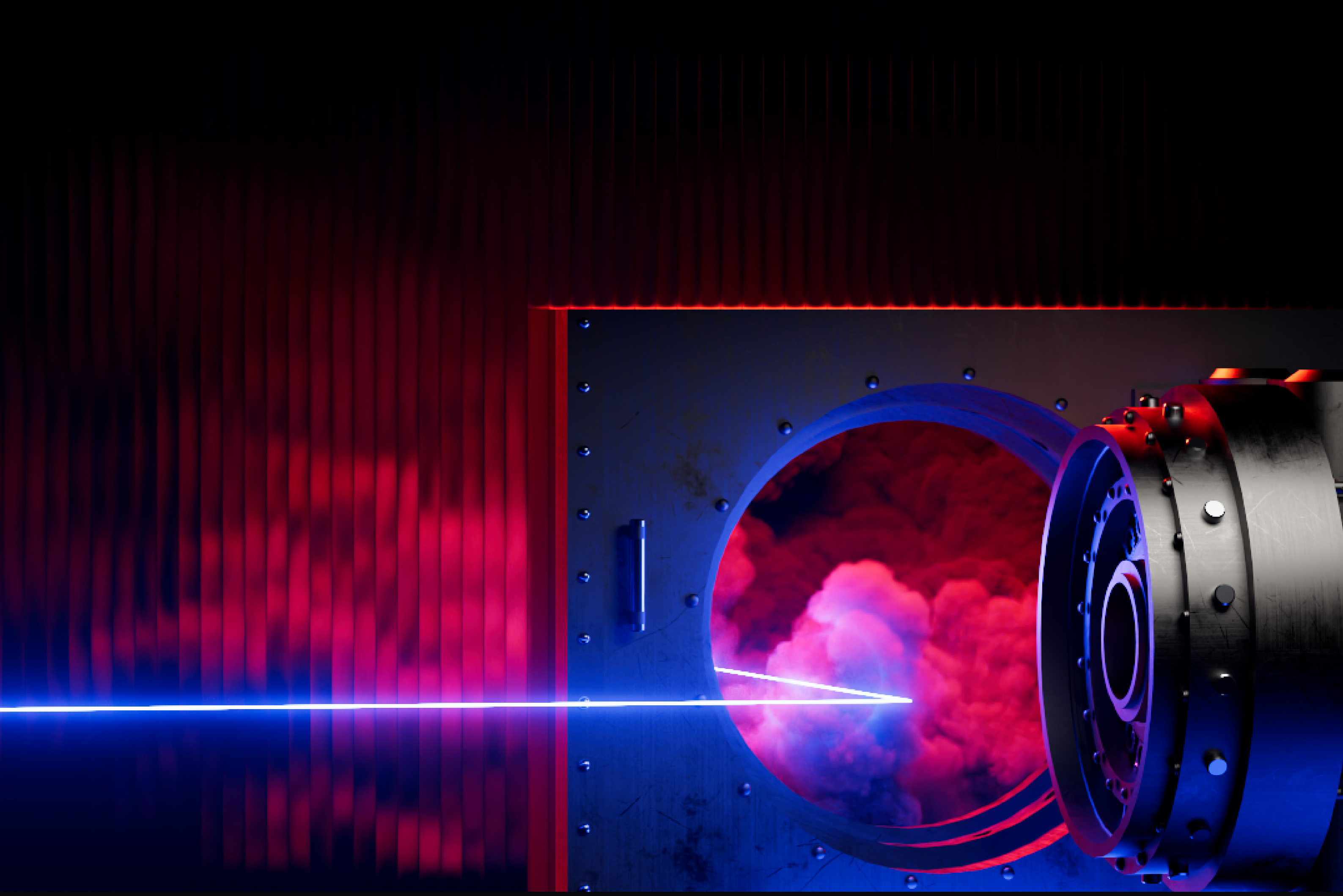


FINANCIAL SECTOR

FRAUD PROTECTION

Client-Side Digital Channel Antifraud

Most Common Industry Threats

Money Laundering

Case #1

Definition

AML involves placing ill-gotten funds into the financial eco-system, Fraudster do this by opening fake accounts or obtaining control of existing accounts

Solution

Fraud Detection Multi-accounting detection will help your team identify mule accounts controlled by fraudsters before they can use the accounts to move funds

Account takeover

Case #2

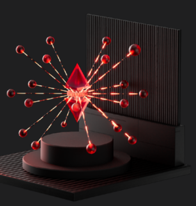
Definition

Cybercriminals take unauthorized ownership of online accounts using stolen usernames and passwords often obtained from data breaches, social engineering, and phishing attacks

Solution

Fraud Detection using advanced device fingerprinting and behavioral profiles, Fraud Protection creates a digital biometric profile for your customers, stopping fraudsters from gaining access to your client's accounts.

Web injection



Case #3

Definition

Once activated, a web injection Trojan can intercept and manipulate any information a user submits and manipulate anything the user submits online in real-time.

Solution

Fraud Detection constantly monitors the protected resources and detects any attempt to modify them.

Fraud on 3DS pages

Case #4

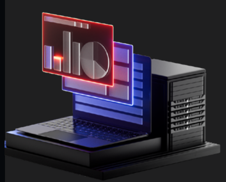
Definition

The threat actors replace a 3DS page with a fake one that asks users to enter their payment data. Users risk losing all their money and having their payment data leaked.

Solution

Fraud Detection will prevent the fraudster from using the stolen credentials. Using the combination of user behavior and Fingerprinting, we will identify the fraudulent login attempt.

Banking malware



Case #5

Definition

Malware is malicious software designed to damage devices and collect sensitive data. It can infect both computers and smartphones. Mobile malware tend to have the same goals: to obtain authorizations to manage the device and intercept login credentials and other important information (SMS, OTPs, etc.).

Solution

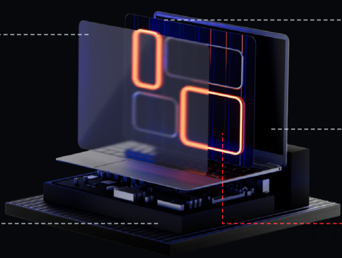
Fraud Detection uses a combination of threat intelligence signatures for known malware, suspicious permissions, and behavioral analysis to detect new malware, such as deviation from typical behavior.

Know Your Users

By creating an accurate digital profile of your legitimate clients, Fraud Protection allows you to protect your organization while providing an excellent user experience. Using advanced device fingerprinting and behavioral profiles, Fraud Protection creates a digital biometric profile for your customers. Our Threat Intelligence and Attribution solution and the Fraud Protection provide us with the latest intelligence on compromised accounts allowing you to require 2FA or the user to change their passwords proactively when their account has been compromised.

Anonymised Advance
Digital Biometrics
Behavioral Analysis

Device Technical Specifications



Device Graphic and
Display Configuration

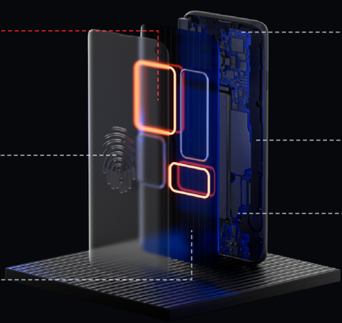
Browser Configuration ISP data

Malware, Bot and RAT Detection

Malware, Jailbreak, Emulator and RAT Detection, SIM Swap

Anonymised User data Advance Digital BiometricsBehavioral Analysis

Android or IOS Operating System Configuration Monitoring



Mobile Operator Characteristic Monitoring

Device Technical Specifications

Device Sensor Monitoring, Accelerometer, Proximity Sensors, Touch Sensors, Gyro-Sensors GPS

Market Recognition

Download the study here

20% Reduction in false positives	**10-20%** More Fraud attempts blocked	**30%** Fewer OTP (formally SMS) for 2FA purposes
REDUCED↓ Workload of fraud analysts and call center operators	**30%** Higher costs of legacy solution than FP	**$288K** In 6 month is the cost savings

Key metrics

- Fraud protection stopped **70% to 80%** of fraud attempts
- Switches from a legacy anti-fraud solution to deploying **Fraud Protection on its web portal**

- **10 million** online customers
- Over **6 million** monthly transactions
- Generating **$7 billion** in annual revenues
- **130% ROI** in 6 months

About Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,400+ Successful investigations of high-tech cybercrime cases	**300+** employees	**600+** enterprise customers	**60** countries
$1 bln saved by our client companies through our technologies	**#1*** Incident Response Retainer vendor	**120+** patents and applications	**7** Unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- FORRESTER®
- Aite Novarica
- KuppingerCole ANALYSTS
- Gartner®
- IDC
- FROST & SULLIVAN

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785