GROUP-IB

AVO

SUCCESS STORY

GROUP-IB × AVO BANK

Shaping the new era of banking
in Uzbekistan: Digital and Secure

About AVO bank

Industry	Finance
Year founded	2023
Country	Uzbekistan

AVO bank was recognized as a Strategic Partner by Mastercard in Uzbekistan in 2023.

AVO bank is a recently founded bank in Uzbekistan, with its headquarters in Tashkent. Since its launch as a digital bank in 2023, AVO bank has introduced several innovative products, including the AVO Platinum credit card with an interest-free period. A key feature of this service is the accompanying app designed to make banking as easy as possible for every user.

In the first three months, the AVO bank app was downloaded over

1 million times

Background

The number of attack attempts keeps rising. AVO bank continues to grow, but so do the threats it faces. Recently, tens of thousands of threats have been prevented each month, which means that quick and effective responses are more crucial than ever.

The banking sector has always been one of the most appealing targets for cybercriminals. With the recent boom in digital banking, the use of mobile banking malware has soared. Card data leaks and ransomware attacks also remain key attack vectors within the banking industry.

AVO bank faced an ambitious challenge: to rapidly launch digital services while providing comprehensive cybersecurity against emerging threats to both customers and employees. The bank wanted to ensure that the convenience, speed, and quality of its services would not be affected. To meet this challenge, AVO bank was seeking solutions with flexible licensing models that could be deployed in record time.

As Uzbekistan's digital economy expands, so does the focus — at national level — on cybersecurity. Financial institutions like AVO bank must comply with regulatory requirements aimed at enhancing security posture. The bank's choice therefore also depended on the capability of ensuring compliance with regulatory standards by implementing advanced anti-fraud systems and providing detailed reporting on fraudulent activities.

Initial pain points

- Tight deadline for launching the bank
- Building the cybersecurity infrastructure from scratch
- Focus on purchasing SaaS instead of on-premises solutions to fulfill the bank's goals
- Limited in-house resources for complex incident monitoring and response
- Quick deployment and comprehensive protection needs for clients and employees
- Compliance with regulatory requirements

Why Group-IB?

> The AVO bank information security team was familiar with the quality of Group-IB solutions and considered them to be among the best worldwide. The flexible deployment options in SaaS format and Group-IB's partnership with the Central bank of Uzbekistan also served as convincing arguments. Another decisive factor in choosing the company was Group-IB's own Security Operations Center (SOC) team, which would be involved in monitoring incidents and threats faced by our bank.

YEVGENY ARTYUKHIN,

Head of Security at AVO bank

Group-IB has been working closely with Uzbekistan's private and government organizations for many years. It recognizes Central Asia's economic importance and the region's potential to become a global cybersecurity hub. In August 2023, the Central Bank of Uzbekistan signed a memorandum of cooperation with Group-IB to establish interaction between organizations on countering cyber attacks and strengthening cybersecurity. In December 2023, Group-IB established its Digital Crime Resistance Center (DCRC) in Uzbekistan. The center is currently staffed by Group-IB's world-leading threat researchers who gained extensive experience in other regions.

Platform

UNIFIED RISK PLATFORM

Products

- Threat Intelligence
- Fraud Protection
- Managed XDR
- Attack Surface Management
- Digital Risk Protection
- Business Email Protection

Services

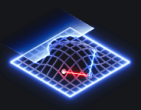
- Audit & Consulting
- Education & Training
- Digital Forensics & Incident Response
- Hi-Tech Crime Investigation

Bank’s stack of choice for countering cybercrime

AVO bank initially implemented three Group-IB solutions: Attack Surface Management, Threat Intelligence, and Managed Extended Detection and Response. At the same time, the bank pilot tested Digital Risk Protection and Fraud Protection, which proved effective and which the bank is now using on a daily basis.

Threat Intelligence

The bank has chosen the industry’s largest adversary-centric threat intelligence system to proactively identify and control industry-specific threats and defend against targeted attacks.



Attack Surface Management

The bank has chosen Attack Surface Management (ASM) to uncover all external IT assets, assess risk using threat intelligence data, and prioritize issues to allow for high-impact remediation efforts. ASM identifies unmanaged assets and new devices added to the infrastructure, strengthens security posture with minimum allocation of resources, and creates a single pane of glass across the entire company.

Managed Extended Detection and Response

The bank has opted for Managed Extended Detection and Response (Managed XDR) to help it identify threats in real time and respond to incidents immediately. Managed XDR hunts for threats in infrastructure, correlates and analyzes alerts, and promptly isolates infected hosts to eliminate malicious activity. Group-IB's CERT-trained SOC analysts offer 24/7 threat triage and take down phishing and non-phishing resources to protect the client’s brand and cash flow.

Digital Risk Protection

The bank has chosen Digital Risk Protection (DRP) to protect its customers and employees against brand-related scams by monitoring the bank’s digital footprint, detecting violations, and prioritizing and initiating appropriate takedown tactics.

Fraud Protection

The bank has adopted this AI-fused and patented technology to protect its clients against fraud and to meet regulatory anti-fraud requirements. Group-IB Fraud Protection provides client-side fraud prevention and digital identity protection across sessions, platforms, and devices in real time for online portals and mobile apps.

Outcomes

30
fraudulent resources
imitating the bank's brand identified by DRP in the first week of use

1,700+
alerts
of medium and high severity detected by MXDR in 10 months

30,000
subscribers
of a clone Telegram channel protected against fraud

1
minute
is the average threat response time

0
phishing emails
now reach the bank's employees

In March 2024, partly as a result of implementing Group-IB solutions, AVO bank successfully completed the certification procedure for compliance with the Payment Card Industry Data Security Standard (PCI DSS).

> Group-IB products protect us from various types of threats, from phishing, scams, and malware to sophisticated ransomware attacks. By analyzing information through their solution interfaces, we not only keep our clients safe but also manage in-house resources, redistributing workload among staff and preventing burnout. All this enhances the quality of our work and ensures peace of mind for our clients.

YEVGENY ARTYUKHIN,
Head of Security at AVO bank

Group-IB's solutions met all of AVO bank's expectations. Rapid integration ensured comprehensive protection for both the bank's infrastructure and customers in a short period. The bank emphasized several noteworthy outcomes:

Enhanced monitoring and detection capabilities

Having a dedicated SOC team strengthened the bank's ability to monitor and respond to cybersecurity incidents. Group-IB's Managed Detection and Response (MXDR) detects and blocks all identified malicious files before they can reach the bank's internal systems. This not only enhances security but also reduces costs relating to anti-virus systems and other conventional solutions that do not provide the required level of protection.

Instant response

Group-IB's MXDR allows for rapid threat response, isolating infected hosts and eliminating all traces of malicious activity. The time between detecting a threat and responding to it is only one minute.

Proactive threat tracking

Using Group-IB's Threat Intelligence (TI), AVO bank can learn about emerging attacks targeting the industry, the region, and its clients. Integrating the MITRE ATT&CK® matrix has made it possible for the bank's cybersecurity team to track and analyze all relevant threats within a single interface, providing immediate insights into the techniques, tactics, and procedures used by attackers. Additionally, TI enables AVO bank to analyze leaked banking card data and monitor mentions of the bank on underground forums.

Fewer internal risks

While the human factor cannot be eliminated completely, MXDR helps minimize such threats. Even if a bank employee accidentally downloads a malicious file or runs a malware program received via email, the files are blocked before any damage is done.

Real-time attack surface scanning

Attack Surface Management (ASM) reduces the burden on the cybersecurity team by serving as the first line of defense. The bank monitors all new digital assets and shadow IT, continuously tracking external resources and quickly mitigating critical risks.

Phishing and scam mitigation

With MXDR, the number of phishing emails has dropped to zero. Additionally, with Digital Risk Protection (DRP), AVO bank identifies and takes down **90%** of fraudulent resources. Group-IB's solutions help the bank detect and eliminate threats that were previously going unnoticed, such as fraudulent Telegram channels. The bank can now also quickly identify and block phishing attacks targeting top management.

Protection of customer funds and data

Fraud Protection has enabled AVO bank to more effectively detect session fraud and prevent the theft of customer funds in real time.

Success highlights

- Quick deployment of a comprehensive cybersecurity stack
- Customer security, trust and confidence ensured
- Continuous monitoring for complex threats such as ransomware
- 90% of fraudulent resources taken down at an early stage

About Group-IB

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

1,550+
Successful investigations of high-tech cybercrime cases

400+
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®
Aité Novarica
kuppingercole ANALYSTS
Gartner
IDC
FROST & SULLIVAN

Fight against cybercrime

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

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785