

Product overview

Cyber Fraud Intelligence Platform

# Share risk signals securely, stop threats early

Real-time fraud intelligence through privacy-preserving collaboration. Cyber Fraud Intelligence Platform turns isolated suspicions into confident action without exposing customer data.



# Coordinated fraud demands a collective response

Fraud teams have long needed a way to share risk signals securely in real time, across institutions and borders, without violating privacy rules. Yet most organizations still operate in silos, limited to sharing intelligence only after fraud is confirmed. That's finally changing.

Fraud Prevention

APP Fraud

Real-Time Fraud Detection

GDPR Compliance

RegTech

Fraud Intelligence Sharing

Mule Account Detection

APP fraud losses  
projected by 2028

\$7.6 bln

Account takeovers  
missed due to lack  
of shared intelligence

60%

Fraud cases never  
even reported

70%

Losses prevented  
with sharing only  
confirmed cases

<40%

All it takes to shift  
funds within a country

10–40 sec

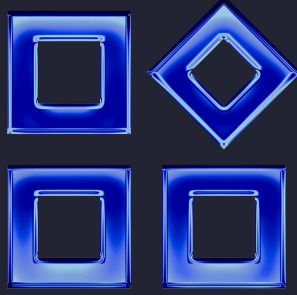


# Intelligence that moves faster than fraud

Privacy and regulatory constraints mean most institutions can only share intelligence after fraud is confirmed, when it's too late. Cyber Fraud Intelligence Platform changes this, enabling organizations to exchange suspicious signals safely in real time and stop fraud before funds are moved, not hours or days after fraudsters have acted


Hashing methods like SHA-256	Cyber Fraud Intelligence Platform
<div>✕ Vulnerable to re-identification</div>	<div>✓ Patented Distributed Tokenization resists re-identification</div>
<div>✕ Not GDPR-compliant for suspicious data</div>	<div>✓ Bureau Veritas-validated GDPR compliance</div>
<div>✕ Limited to confirmed fraud cases</div>	<div>✓ Shares suspicious signals in real time</div>
<div>✕ Responses delayed until funds are gone</div>	<div>✓ Stops fraud before funds transfer</div>
<div>✕ Increases compliance risk</div>	<div>✓ Keeps PII within each participant's environment</div>
<div>✕ Little to no predictive value</div>	<div>✓ Detects emerging threats preemptively</div>

01 Flag in your environment first




The participating member's existing risk platform flags suspicious transactions or account activity based on internal rules. No system replacement needed—build on what you already have.

02 Share using distributed tokenization




Sensitive identifiers (phone, device ID, IBAN) are irreversibly tokenized on-demand inside your firewall using distributed tokenization. Raw PII never leaves your systems – not even platform admins see it.

03 Detect patterns in real time



Tokens are shared instantly across the network. Receive enriched, actionable intelligence to uncover repeat offenders, mule networks, and warm-up activity – 4-8 weeks before funds move.

04 Block fraud before losses occur



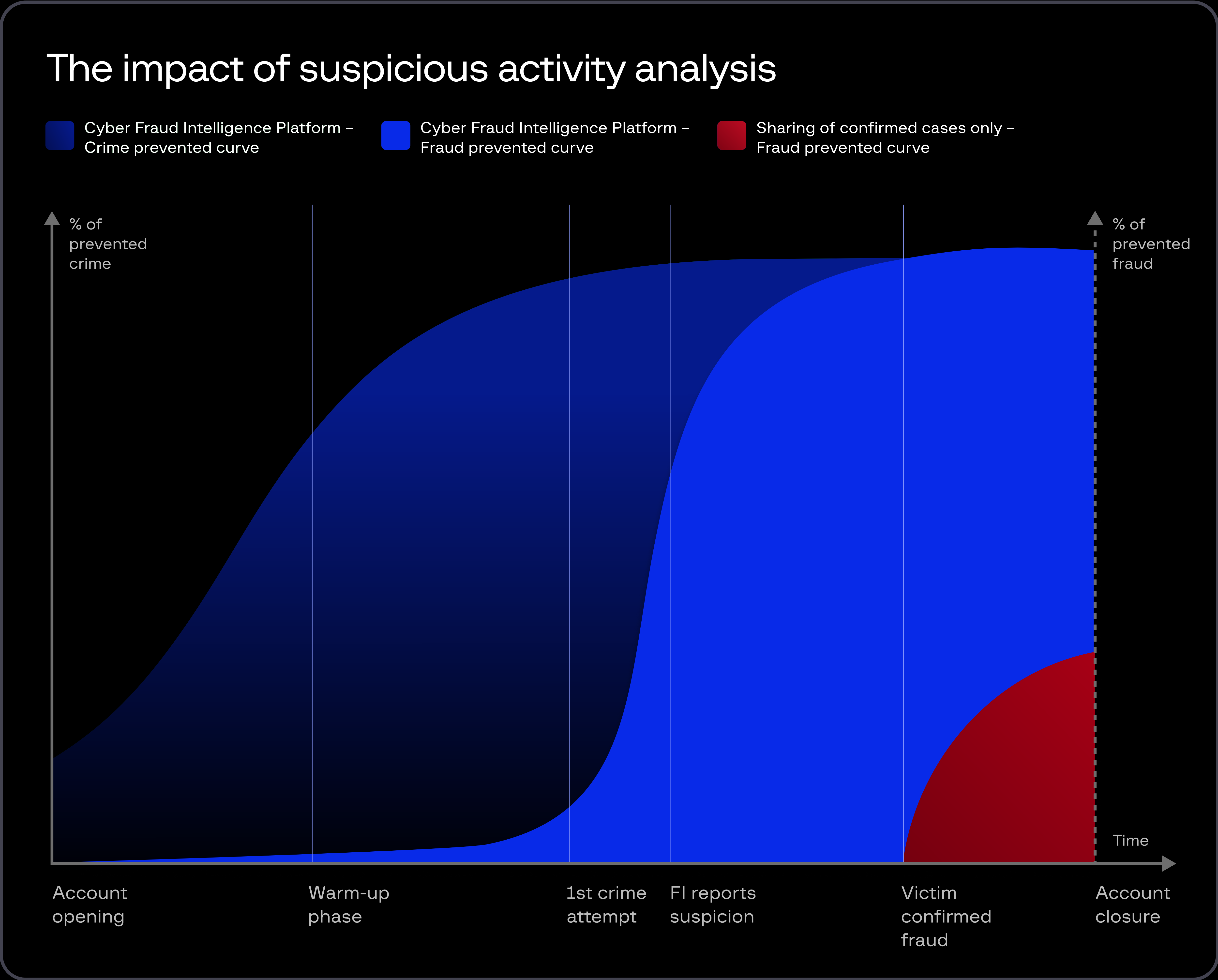
The platform responds within 100 milliseconds, allowing your Risk Engine to decide instantly – block transactions, freeze accounts, or alert customers, with full audit trail and compliance.

Group-IB Cyber Fraud Intelligence Platform enables banks, payment providers, telecom operators, e-commerce, and gaming companies to share fraud intelligence securely across and beyond borders in milliseconds.	Network intelligence exposes coordinated fraud patterns invisible to individual organizations, delivering measurable fraud reduction from day one. Patented Distributed Tokenization ensures data stays within each organization while enabling real-time collaboration that prevents losses.
--	---



# The critical fraud prevention window

CFIP stops fraud already during the critical warm-up phase when suspicious activity first emerges — long before traditional track-and-trace methods can act.



losses prevented

<40%

Sharing confirmed cases only

losses prevented

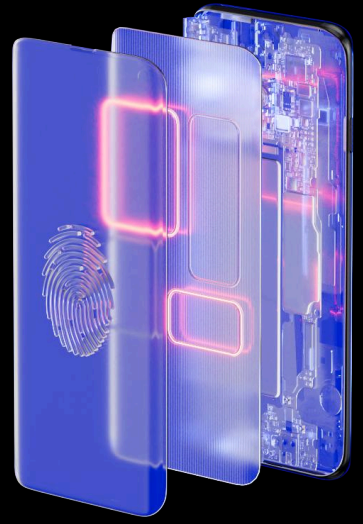
90%+

Cyber Fraud Intelligence Platform

Fraud has a 4–8 week warm-up phase. Traditional methods only react after the attack.



# Move from autopsy to prediction and prevention



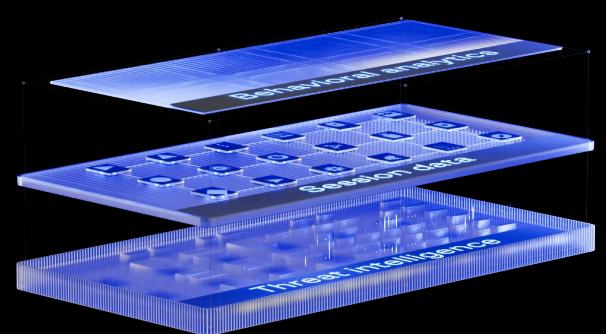
Stop payment fraud before funds move

Real-time risk scoring identifies suspicious recipients and blocks mule transfers instantly. Prevents invoice, CEO, and romance scams at the moment of transaction.



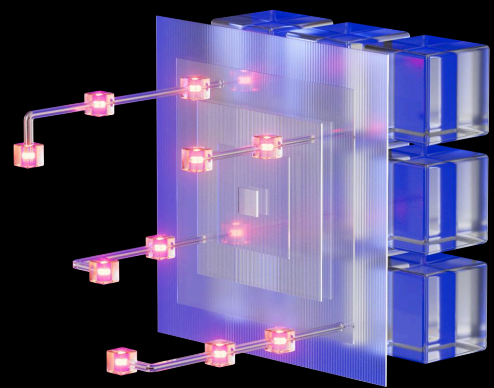
Trace and recover stolen funds faster

Encrypted communication between participants enables immediate tracing and recovery coordination across multiple organizations.



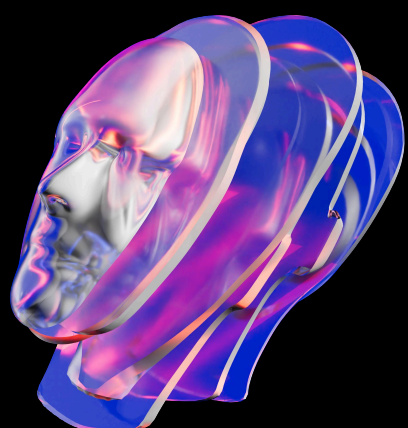
Detect account takeovers early

Behavioral analytics and pseudonymized session data reveal devices linked to high-risk activity at multiple institutions.



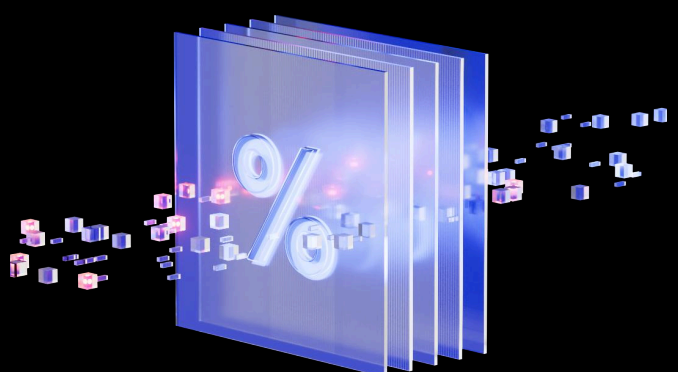
Expose mule networks before activation

Identifies mule accounts during low-value warm-up transactions, uncovering account farming and synthetic identity rings before laundering begins.



Prevent synthetic and deepfake identities

Cross-bank KYC correlation flags inconsistencies and detects fake or reused credentials during account opening.



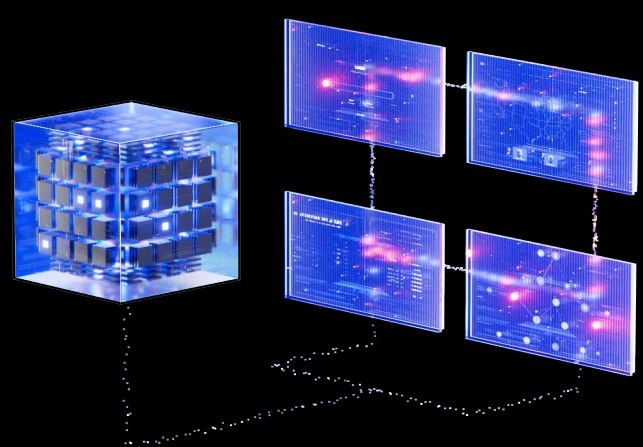
Stop coordinated loan fraud in real time

Cross-lender intelligence identifies velocity patterns and duplicate applications connected to organized bust-out schemes.



Reduce chargebacks from compromised cards

Checks transactions against a global database of over 300 million compromised cards to block recurring fraud.



Identify zero-day fraud before it spreads

Correlates early anomalies across participants to expose new attack patterns with no historical footprint.

## Bureau Veritas Attestation



Group-IB's Distributed Tokenization technology has undergone an independent technical design and GDPR compliance review by Bureau Veritas. According to our assessment, Group-IB's tokenization technique is designed to align with GDPR principles, including data minimisation and pseudonymisation.





# Scale collaboration on your terms

### Industry Association Consortia

A trusted body like a banking association hosts the processing hub for its members, for sector-wide protection. Group-IB provides the technology and support. Where required, regulators can participate in governance while members maintain operational control.

### Cross-Sector Collaboration

The platform enables networks hosted by industry associations to connect across sectors – finance, telecom, gaming, and e-commerce – for enhanced interoperability and fraud detection.

### Enterprise-Wide Deployment

Global organizations can deploy internally across subsidiaries and business units, enabling world-wide fraud pattern detection while maintaining regional regulatory compliance.

### Individual Institution Participation

Any bank, payment provider, telecom operator, e-commerce platform, or gaming company can join immediately and benefit from day one. No consortium membership required.

# Achieve measurable impact

For all industries

### Stop fraud early and prevent losses

Detect mule networks, APP fraud, and synthetic identities during the critical warm-up phase — before criminals execute and funds are lost.

### Integrate seamlessly

System-agnostic architecture connects to your existing fraud protection tools and systems without costly replacement.

### Reduce false positives

Network intelligence provides richer context, enabling confident decisions that protect legitimate customers while blocking genuine threats.


### Strengthen market position

Early adopters gain immediate access to intelligence from 60+ global fraud sources, positioning your organization as an industry leader in collaborative defense.




## For banks and payment providers

### Detect faster




Identify mule accounts, APP fraud rings, and loan fraud schemes during the 4-8 week warm-up phase before execution.

### Meet regulatory requirements




Align with emerging mandates for fraud intelligence sharing (UK PSR, Singapore MAS COSMIC, EU PSD3) while maintaining full GDPR compliance

### Decide with confidence



Rich network context reduces false positives and enables real-time blocking of genuine threats without impacting customer experience.

### Build customer trust



Enhanced onboarding accuracy prevents mule accounts from entering your system while legitimate customers experience faster, frictionless service.

## For supervisory authorities and industry governance

### Systemic visibility without data access



Gain aggregated insights into fraud trends and cross-border patterns for evidence-based policy development—without accessing raw customer data.

### Custodianship model



Where required, participate in governance of industry-hosted hubs while operational fraud prevention remains in the hands of participating institutions.


### Support market development



Help foster collaborative fraud defense that strengthens financial stability and protects consumers, while respecting institutional autonomy and competitive dynamics.


## For industry associations

### Enable member value




Provide sector-wide fraud protection as a core membership benefit, demonstrating tangible ROI and strengthening member engagement.

### Drive standards



Shape industry best practices for fraud prevention and intelligence sharing, positioning your association as a leader in financial crime defense.

### Facilitate flexible collaboration



Create a trusted environment where members control their participation levels, data-sharing preferences, and integration timelines.



**1,550+**

Successful investigations of high-tech crime cases

**500+**

Employees

**60**

Countries

**\$1 bln+**

Saved by our client companies through our technologies

**#1\***

Incident Response Retainer vendor

\*According to Cybersecurity Excellence Awards

**11**

Unique Digital Crime Resistance Centers

Global partnerships

**INTERPOL**

**EUROPOL**

**AFRIPOL**

Recognized by top industry experts

**FORRESTER®**

**Aite Novarica**

**kuppingercoie ANALYSTS**

**Gartner®**

**IDC**

**FROST & SULLIVAN**

Fight against cybercrime

