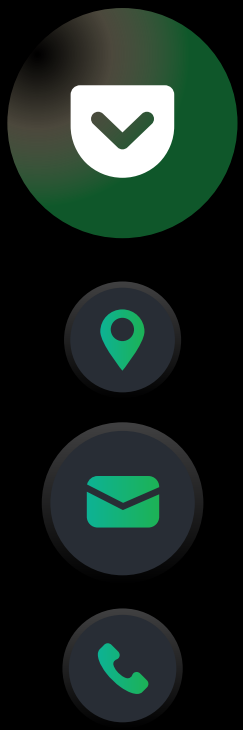
TrustDecision

Global Risk Persona

Know Your Users' Digital Identity to Detect Fraud

IP Address | Email Address | Phone Number

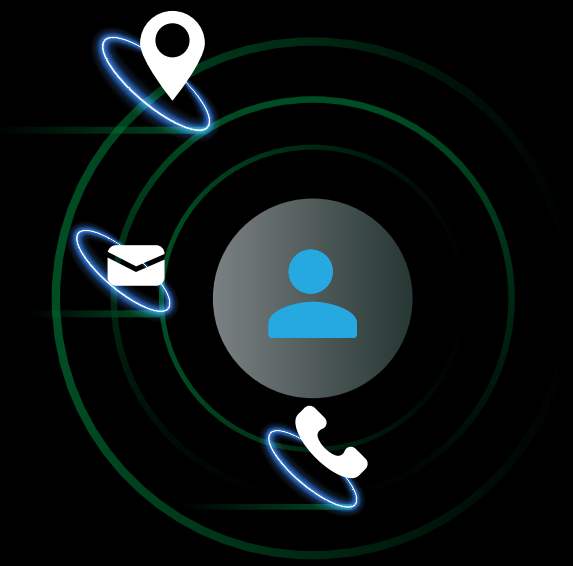


\ Table of Contents \

What is Global Risk Persona?

TrustDecision's global risk persona provides a unified view of an entity's risk by consolidating data from multiple sources, including IP, email, and phone number. It identifies patterns and anomalies across these dimensions to determine a user's legitimacy. By correlating diverse signals into a singular risk profile, a global risk persona reduces false positives and enhances the accuracy of fraud detection.

This approach offers a comprehensive perspective on potential fraud, enabling proactive decision-making. It helps identify coordinated fraud attempts across accounts, geographic regions, and transactions, ensuring robust protection against evolving threats.



What is IP Profiling?

IP profiling evaluates the risk associated with an IP address by analyzing its attributes and behavior. It detects suspicious activity, such as the use of anonymizing tools (proxies, VPNs, or Tor), geolocation mismatches, and high-frequency requests. It is commonly used to reduce risk of bot-driven attacks, account takeovers and identifying fraudulent transactions.

The value of IP profiling lies in its ability to detect hidden threats, ensuring that businesses can block malicious traffic while maintaining seamless access for legitimate users.

What is Email Profiling?

Email address profiling assesses the legitimacy and risk of an email address by evaluating its validity, activity, and behavioral patterns. It detects disposable, abusive, or fake emails commonly used for fraud, including fake account creation, promo abuse, and phishing. It also enhances email campaign effectiveness by targeting only legitimate users.

The key value is its ability to prevent fraud early, reduce operational overhead from false positives, and improve downstream processes like payment validation and engagement tracking.

What is Phone Number Profiling?

Phone number profiling analyzes a number's validity, type, and geographic consistency to assess its risk. It detects disposable, VoIP, or inactive numbers often associated with fraud — adds a layer of security by ensuring the authenticity of users during registration, 2FA, and transactions.

Its value lies in reducing fraud incidents, improving customer trust, and ensuring robust security across all stages of the user journey, particularly in high-value or sensitive transactions.

Knowing Who's Interacting with Your Digital Platform, Where and How.

Fraud vs Legitimate Users

Registration

Fake account creation

According to TrustDecision's data,

40-60% fraud detected started with fake account registration

25-40% detected with invalid/disposable emails, VoIP phone numbers or anonymized IPs

Fraudster Tactics

- **Disposable Emails:** Use temporary or fake email addresses to bypass verification and avoid detection.
- **VoIP or Disposable Phone Numbers:** Exploit non-traceable phone numbers to bypass phone-based authentication.
- **Anonymized IPs:** Utilize VPNs, proxies, or Tor nodes to hide their location and evade detection.
- **Automated Bot Registrations:** Deploy bots to create mass accounts for promo abuse or further fraudulent activities.

Login

Account takeover (ATO)

15-25% ATO caused by weak 2FA triggers

30-40% fraudulent activities were caught using brute-force attacks, IP spoofing or credential stuffing to gain unauthorized access to legitimate accounts.

Fraudster Tactics

- **Credential Stuffing:** Test stolen username-password pairs from data breaches across multiple platforms.
- **Brute-Force Attacks:** Use automation to repeatedly guess login credentials until successful.
- **Session Hijacking:** Intercept user sessions through IP spoofing or malware to gain access without credentials.

Order

Web scraping

Payment

Chargeback

Promotion

Campaign policy abuse

Retention

Skewed engagement metrics

20-30% financial loss caused by web scraping during order placement and payment stage

Scraping and hoarding tickets

- Scrape ticket prices in real-time to identify fluctuations, purchase tickets during price drops and resell them for profit.
- Use bot to scrape ticket inventory and automate bulk purchase, artificially create scarcity by holding a large number of tickets, inflating prices on secondary markets.

Exploitation of payment system

- Fake account creation and anonymized IP made it easier for fraudsters to get away with using stolen card, then initiate chargeback once goods are received.
- Legitimate customers which account was taken over can claim that they didn't authorize the transaction, leading to increase of chargeback rates.

Competitive intelligence and promotion abuse

- Scrape the website available data and pricing for competitive advantage, it can be used for undercutting or price matching.
- Collect promo codes at speed, then perform bulk transaction at discounted price for resale.

Low Marketing ROI due to Bad Quality of Customer Database

Wasted budget on invalid/malicious users, leading to skewed metrics

- Unnecessary channel delivery cost spent on SMS sent to invalid/fake phone numbers and emails sent to disposable or abusive email addresses.
- Giving more opportunities for fraudsters to exploit discounts, claim rewards that leads to drained marketing budgets
- Misleading campaign performance with false sense of growth, potentially causing marketers to over-invest in underperforming campaigns.

What Data You can Get?

Breaking down technical details to layman terms of the information you can gather and what each of it means.

IP Address

206.166.123.45 LOOKUP

Continent Asia	**Country Code** SG	**Country** Singapore	**Province** Central Region	**City** Singapore
Longitude 103.8198	**Latitude** 1.3521	**Owner** Singtel	**Operator** Singtel	**ZIP Code** 048581
Time Zone Asia/Singapore (GMT+8)	**Domain** singtel.com.sg	**ASN** A57473	**AS** Singapore Telecom	**Risk Score** 72
Scenario Mobile Network	**Authenticity Score** 65	**Network Risk** VPN, Dynamic IP	**Behavioral Risk** Tampered Device	

Parameters	Enumeration Value	Description
Risk score	Range from 0-100	Higher score indicates higher risk, based on TrustDecision's multi-factor calculation.
Authenticity score	Range from 0-100	It measures likelihood of real human versus bot.
Behavioral risk based on device anomalies	tampered device	Device attributes are modified.
	fake device	Spoofed or simulated device.
	high risk device	Device previously linked to suspicious activity or identified fraud patterns.
Network risk	proxy	Proxy Server: Intermediary server used to conceal the user's IP address.
	vpn	Virtual Private Network: Secure connection encrypting traffic and masking the IP address.
	idc	Internet Data Center
	dynamic	IP address that changes periodically to enhance anonymity.
	tor	The Onion Router: Privacy network routing traffic through multiple encrypted layers.
	scan	Port scan: Identifying vulnerabilities in systems or networks.
	brute force	Attack method testing all combinations to breach account security.

Parameters	Enumeration Value	Description
Scenario	reserved	Typically set aside for specific purposes, and not used for everyday internet access
	unallocated	Not yet assigned or in use by any entity.
	unrouted	Assigned to an entity but not yet been activated for routing on internet.
	unused	Allocated to an entity but not active.
	used	Assigned and being used by a device/network.
	isp	Internet Service Provider
	idc	Internet Data Center
	ixp	Internet Exchange Point
	school	Used by educational institutions
	satellite_comms	Communication using satellite networks.
	enterprise	Used by large enterprise / corporate organizations
	organization	Non-corporate institutions, e.g. government, NGO.
	home_broadband	Assigned to individual users
	mobile_network	Assigned to mobile carriers
	wlan	Wireless Local Area Network (Wi-Fi)
	infra	Underlying physical and virtual systems, networks, and services supporting operations or technology.
	dedicated	Network resources exclusively allocated to a specific client or service.
	anycast	The same IP address is assigned to multiple locations.
	cdn	Content Delivery Network, designed to deliver content quickly to users.

Email Address

alexis@gmail.com

LOOKUP

Risk Score
60

Status
Valid

Risk Label
Suspicious

Parameters	Enumeration Value	Description
Email Status	Valid	Correctly formatted and active.
	Invalid	Incorrectly formatted or inactive.

Parameters	Enumeration Value	Description
Email Status	Abuse	Linked to malicious or spam activity.
	Unknown	Status not verifiable.
Risk labels	Suspicious	Shows signs of potential fraudulent or unusual behavior.
	Temporary	Created for short-term or one-time use.
	Random	Randomly or automatically generated.
	Similar	Address with the same domain but different prefixes, often automated.
Risk Score	Range from 0-100	Higher score indicates higher risk, based on TrustDecision's multi-factor calculation.

Phone Number

+65 9123 4567

LOOKUP

Country ID	Country	Province	City	Operator
SG	Singapore	Central Region	Singapore	Singtel

Phone Type	Risk Score
Mobile	68

Parameters	Enumeration Value	Description
Phone type	fixed_line	Landline number tied to a physical location.
	mobile	Number for a mobile phone with voice and text services
	prepaid	Mobile number linked to a pay-as-you-go account.
	toll_free	Free-to-call number, charges covered by the receiver.
	voip	Voice over IP. Internet-based number for voice communication.
	pager	Beeper
	payphone	Public telephone
	invalid	Non-functional or incorrectly formatted number.
	restricted_premium	Higher-cost number for premium services.
	personal	Number for individual, non-business use.
	voicemail	Phone number recording and retrieving missed call messages.
	others	
Risk Score	Range from 0-100	Higher score indicates higher risk, based on TrustDecision's multi-factor calculation.

Its Role in Fraud Detection

Role in Fraud Detection

IP Assessment	Email Assessment	Phone Number Assessment
Network Risk Analysis: Identifies anonymized IPs used to mask fraudulent activities.	Validation of Authenticity: Verifies whether the email is valid, active, and associated with legitimate domains.	Real-Time Validation: Confirms if the phone number is valid, active, and issued by a legitimate carrier.
Geolocation Verification: Detects inconsistencies between claimed and actual user locations.	Identification of Disposable/ Abusive Emails: Detects temporary or abusive email addresses used for fraudulent activities	Risk Assessment: Flags VoIP, disposable, or high-risk numbers often used by fraudsters.
Behavioral Monitoring: Tracks suspicious IP behavior such as high-frequency requests, geolocation changes, or known malicious activity.	Behavioral Analysis: Monitors patterns such as rapid email creation or association with known fraudulent activities.	Geolocation Matching: Ensures consistency between user-provided information and phone number location.

Key Benefits

Blocks bots and scrapers during account registration or ticketing purchases.	Prevents fake registrations, reducing risks associated with promo abuse and loyalty fraud.	Strengthens account security by enabling reliable 2FA with validated phone numbers
Mitigates risks of account takeover by flagging anomalous login attempts.	Blocks emails linked to phishing schemes or abusive behaviors, ensuring a cleaner user database.	Blocks fraudsters using fake or temporary numbers to exploit promotions or transactions.
Enhances fraud prevention in transactions by detecting high-risk IPs.	Enhances email campaign ROI by targeting legitimate users.	Reduces chargebacks and unauthorized access by identifying high-risk numbers in payment processes.

Unified Fraud Detection Through Combines Assessment

When email, phone, and IP assessments are used together, they provide a **multi-dimensional view** of user risk:

Cross-Validation

Anomalies in one channel (e.g., mismatched IP and email geolocation) can trigger fraud alerts.

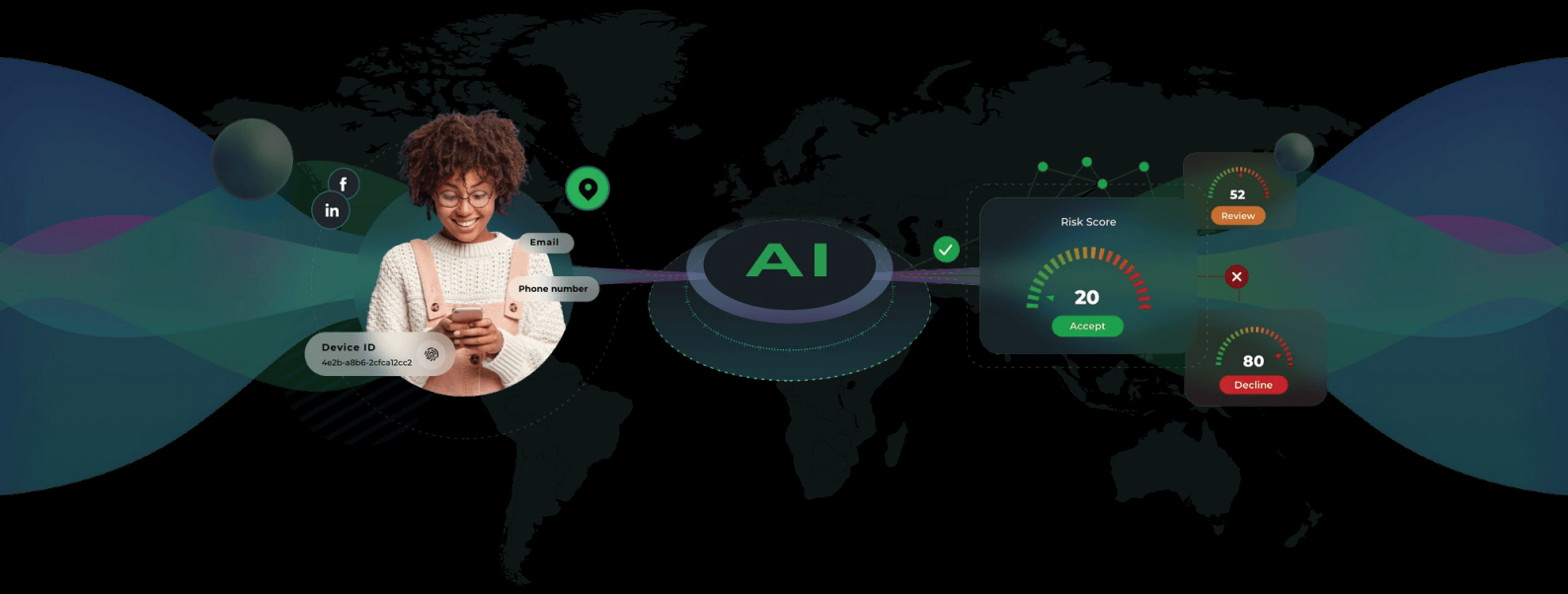
Comprehensive Risk Scoring

Consolidates signals from all three data points to assign a holistic fraud risk score.

Real-Time Action

Automates decisions (e.g., reject, review, accept) based on unified insights.

What Sets TrustDecision Apart from the Rest?



Multi-Dimension Risk Assessment

TrustDecision's Global Risk Persona combines data from multiple dimensions — IP, email and phone number — alongside behavioral signals into a unified risk profile. This comprehensive view enables the correlation of insights across touchpoints, effectively identifying sophisticated and coordinated fraud attempts.

Real-Time Risk Scoring for Automated Actions

Every interaction involving an IP, email, or phone number is dynamically analyzed, generating real-time risk scores based on each user activity. This empowers you to automated critical decisions instantly, such as blocking or flagging high-risk identities /transactions. Unlike batch processing or lagging data approaches, Global Risk Persona delivers immediate responses (300ms response time on average), ensuring fraud detection is always proactive and timely.

Extensive Global Threat Intelligence

With over 120 billion risks intercepted and $10 billion in fraud losses prevented annually, TrustDecision's database spans industries including financial services, e-commerce, gaming, airlines, ticketing and live streaming. Our continually updated global threat network ensures you to quickly identify and respond to known fraud patterns. Real-time updates on new and historical fraudulent digital identities keep your system equipped with the most accurate and actionable data available.

Frequently Asked Questions (FAQs)

1. Does Global Risk Persona comply with data privacy and security regulation?

We don't collect or store any IP/Email/Phone number information of your users. So no worries about the data privacy and security issues.

2. Which industries can benefit from using Global Risk Persona?

E-commerce: Verify customer information to reduce promotion fraud, fraudulent transactions, and chargebacks by identifying fake accounts and suspicious behavior.

Financial services: Support AML and KYC compliance, ensure data validity, and mitigate financial risks.

Online Marketing: Verify email and IP authenticity to improve campaign effectiveness and reduce fake clicks and spams.

Airlines: Help airlines prevent fraudulent registrations and bulk login attempts, enhancing security for email-based services such as booking and customer management.

3. Is Global Risk Persona suitable for MSMEs and large enterprise?

Sure, whether you're a small business or a large enterprise, Global Risk Persona can be tailored to fit your needs.

4. Can I customize the risk scoring and thresholds for my business?

Yes, you can. While we provide recommended risk thresholds for low, medium, and high-risk levels, you have the flexibility to adjust them according to what works best for your business.

5. Is there a trial period or demo available to test each product?

Yes, we provide a testing phase for each product. You can request offline testing with our team or try online testing yourself. And if you'd like to see how things work before jumping in, demos for our IP and email products are available on our website.

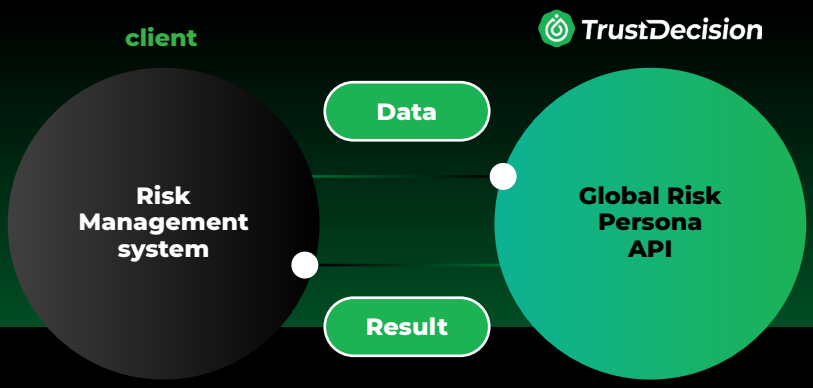
6. What is the pricing model for Global Risk Persona?

Our pricing is based on a per-API call model, so you only pay for what you use.

How to Get Started?

Plug-and-Play API integration

We ensure seamless functionality, scalability and team support throughout your integration process.



Ease of Integration

- Clear and developer-friendly documentation
  Well-organized API documentation, clearly specifying parameters, status codes, request/response formats and examples.
- Multiple Testing Methods Supported
  Both offline and online testing options available.
- Quick Setup
  Get integrated within one day. The integration process is simplified to just a few steps. API keys are generated instantly, and the necessary configurations are lightweight.

	IP Address	Email Address	Phone Number
	20,000 API Calls First 3 months	20,000 API Calls First 3 months	1,000 API Calls First 3 months
Response time	200ms	200ms/5-40s Pro Version	300-500ms
QPS	200	10	20

Get a Free Trial **Talk to us**

Up to 20,000 API calls in the first 3 months

Strengthen User Risk Assessment with IP, Email, and Phone Number Profiling

Request a demo

mkt@trustdecision.com

+60182002123

TrustDecision