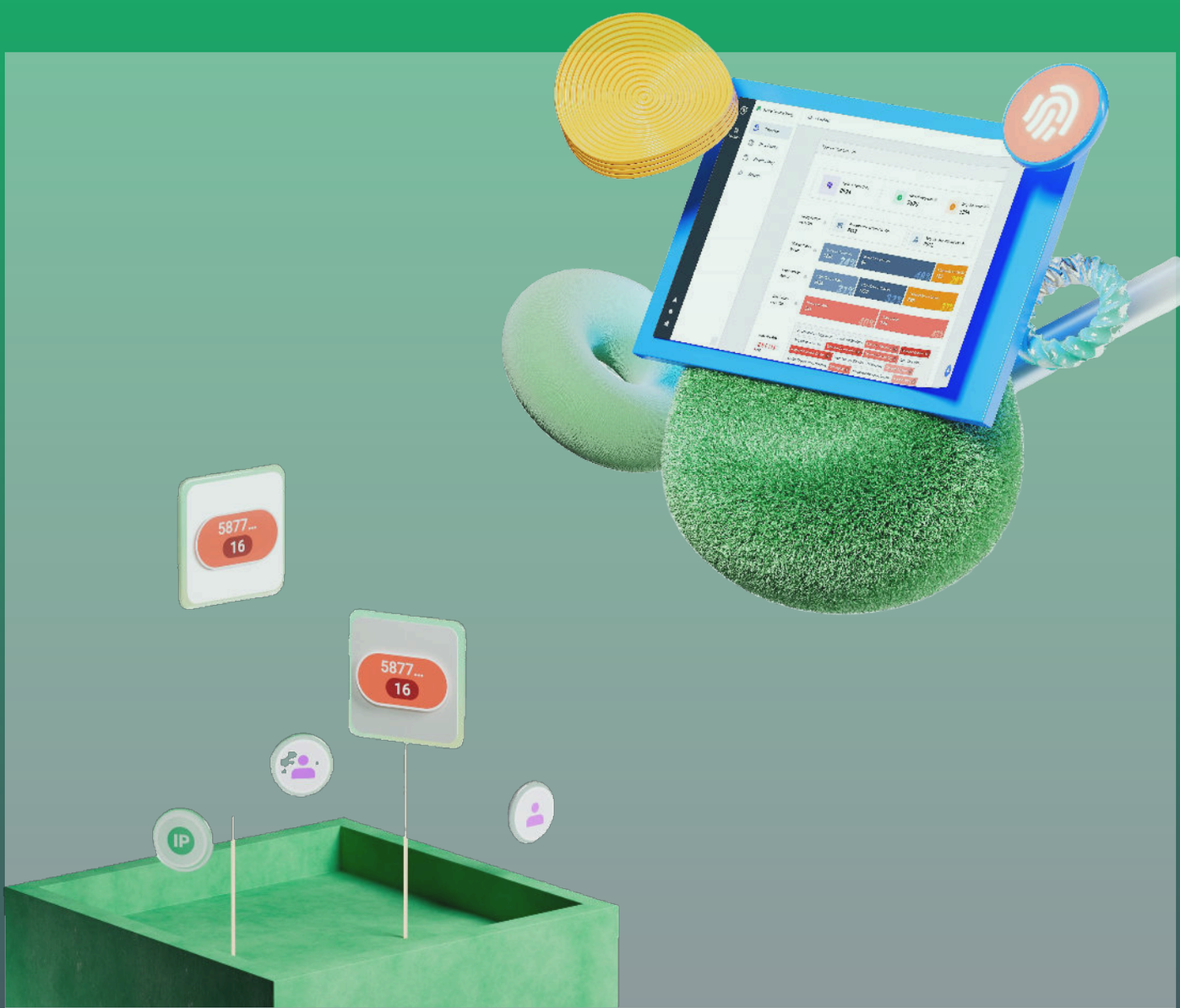
GeeTest

Device Fingerprinting



GEETEST

2026

Precision Profiling, Robust Defense

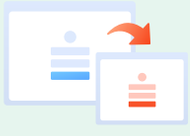
GeeTest Device Fingerprinting is an advanced cybersecurity solution designed to fortify online platforms against evolving digital threats. Leveraging sophisticated algorithms and cutting-edge technology, it intelligently identifies and tracks devices, providing a robust defense mechanism against malicious activities.

Problem Statement

As cyber threats continue to rise in frequency and sophistication, businesses face a critical need for robust cybersecurity solutions. Traditional measures are falling short, highlighting the demand for innovative tools. Device fingerprinting is pivotal in addressing challenges such as unauthorized access and fraudulent activities. The challenge lies in implementing an adaptive and seamlessly integrable device fingerprinting solution that effectively combats evolving cyber threats.

Use Cases

Finance and Banking



Phishing Attacks
Account Takeovers
Fraudulent Transactions

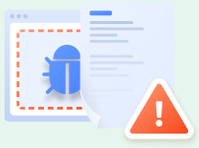
Device fingerprinting aids in risk assessment by analyzing the device's unique characteristics. Unusual patterns or multiple accounts associated with the same device may indicate fraudulent activity, prompting additional scrutiny or authentication steps.

E-commerce

Payment Fraud
Account Compromise
Identity Theft

Device fingerprinting plays a crucial role in fraud prevention by analyzing various device attributes like IP address, browser type, and screen resolution. It helps identify anomalies and patterns associated with fraudulent transactions, enabling e-commerce platforms to block suspicious activities in real-time.

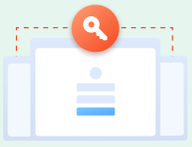
Gaming



Account Hijacking
Cheating and Hacking

In multiplayer games, device fingerprinting can detect patterns associated with cheating, such as the use of hacks or unauthorized software. By identifying and blocking devices exhibiting suspicious behavior, it contributes to maintaining a fair and secure gaming environment.

Cryptocurrency



Phishing Attacks
Identity Theft

Device fingerprinting verifies the legitimacy of cryptocurrency transactions by examining the device characteristics associated with the transaction. This adds an additional layer of confirmation to ensure the transaction is genuine and not initiated by malicious actors.

How it works for you

Behavioral Analytics

Uncover anomalies and potential security breaches through continuous monitoring of device activities.

Real-Time Alerts

Receive instant notifications on suspicious activities, enabling proactive responses.

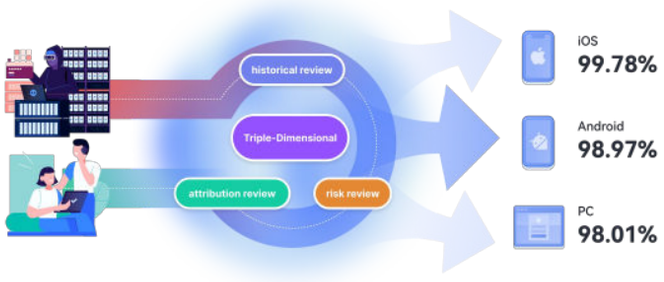
User-Friendly Interface

Intuitive interface for easy management and customization of security settings.

Key Technologies

Triple-Dimensional Review Technology

Triple-Dimensional Review Technology incorporates Historical Review, Attribution Review, and Risk Review to comprehensively assess and analyze data.



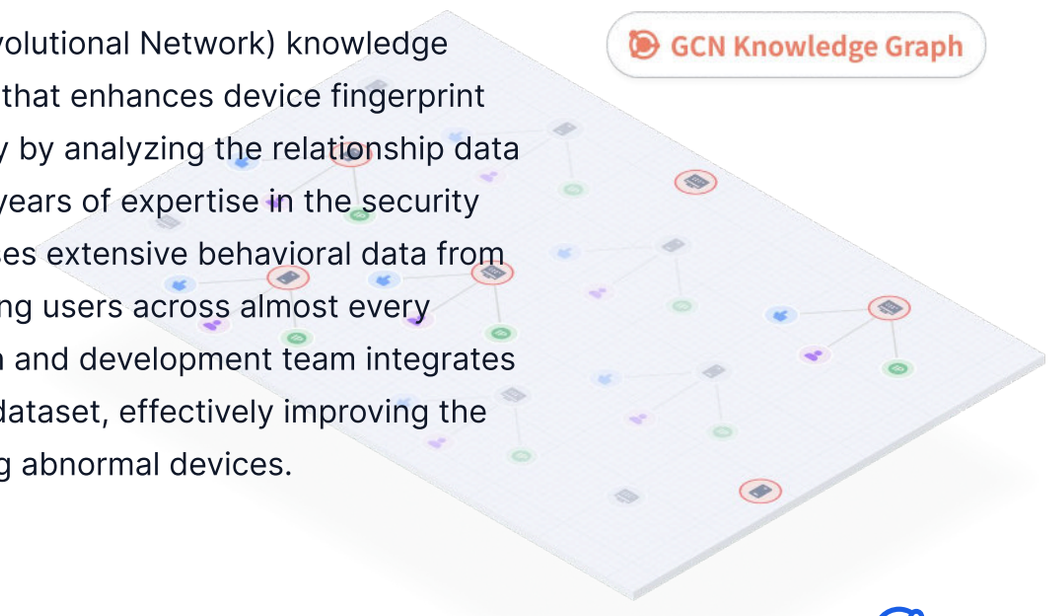
Historical Review: The process of offline collision comparison. By associating device fingerprints with the database, devices with a history of risk are assigned higher risk scores.

Attribution Review: The real-time analysis and identification process. It involves collecting data through an SDK, combining it with device-side detection, and comprehensively analyzing whether the device associated with the current request poses a risk, such as triggering emulator detection, multiple instances, or jailbreaking.

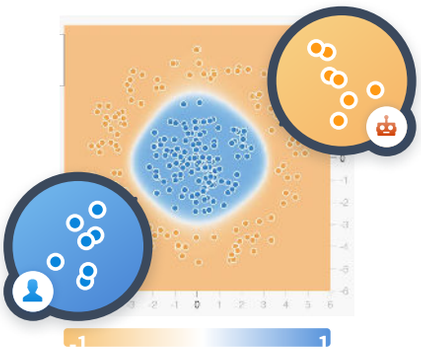
Risk Review: The process of real-time analysis and identification. It involves comprehensive risk assessment based on various dimensions of data, including the current IP address in use, account information, and other business rules.

GCN Knowledge Graph

The GCN (Graph Convolutional Network) knowledge graph is a technology that enhances device fingerprint identification accuracy by analyzing the relationship data among devices. With years of expertise in the security field, Geetest possesses extensive behavioral data from illicit activities, spanning users across almost every industry. The research and development team integrates and models this vast dataset, effectively improving the accuracy of identifying abnormal devices.



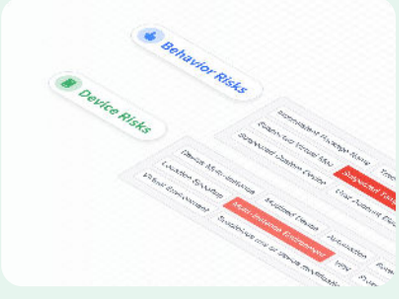
Weak Feature Identification Technology for Devices



- Prioritizing user privacy and compliance by reducing dependency on sensitive information like IMEI/IDFA.
- Expanding Risk Detection Scope with Weak Feature Detection Technology. Highlighting specific risk factors to make abnormal signals from devices more noticeable.

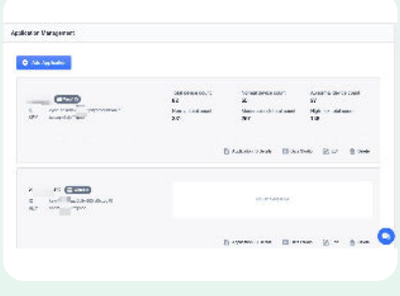
Key Features

Risk Labels



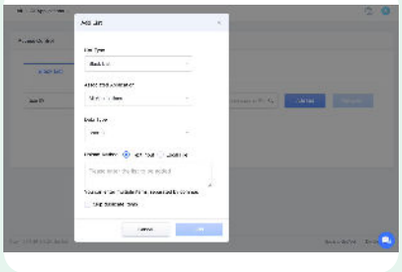
Monitor traffic credibility from both behavioral and device dimensions, providing up to 34 black industry risk labels for reference. It facilitates the identification of devices with similar risk labels, offering optimization references for your security and business strategies.

Application Management



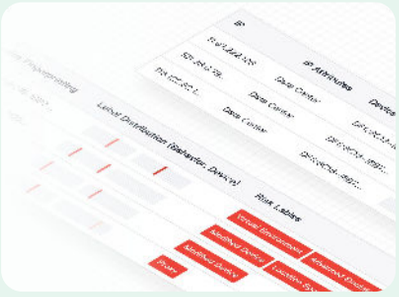
You can add as many applications as you need. Each application's data is distinguished through unique IDs and keys, facilitating secure data analysis for different modules of the business.

Access Control



According to your needs, you can manually add blacklists or whitelists to facilitate the management of access permissions to specific objects or resources.

Data Studio



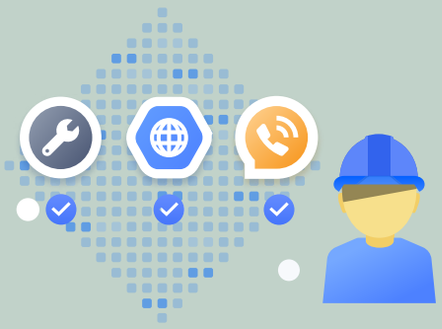
Our Device Fingerprinting product includes a robust Data Studio feature, offering users an intuitive analytics dashboard for comprehensive insights. It enables informed decisions, pattern detection, and effective security strategy optimization.

About GeeTest

Founded in 2012, GeeTest is a leading cybersecurity company that offers international anti-fraud solution and services, including CAPTCHAs, Device Fingerprinting and Business Rules Engine, with advanced AI and ML models. The company protects over 360,000 websites and apps worldwide including Airbnb, Agoda, and GOG, etc, With 7 global service nodes and support for 78 languages, we continue to expand our reach and safeguard businesses worldwide.

Client Support & Service

- Comprehensive support 24/7 service for clients, ensuring a smooth experience.
- Global distributed servers and clusters quickly respond to client requests.



GeeTest Device Fingerprinting

Pioneering Protection, Boosting Business Performance

Take Action Now

Awards

CSS Future Power 50 Club 2018
Deloitte - 2019 Optics Valley Technology Fast 20
Venture50 - 2020 Enterprise Service
Gartner - Representative Vendors in OFD: Bot Mitigation 2020
Forrester -Selected Vendor in Forrester Now Tech: Bot Management, Q4 2021
Deloitte - 2021 Optics Valley Technology Fast 20 & Rising Star
APAC CIO Outlook - the Top Cyber Security Vendors 2022
Startup Stash - Top Bot Detection and Mitigation Tools in 2022
BRICS Industrial Innovation Contest 2022 - GeeTest won the third prize
The Silicon Review - the “50 most admired companies of the year 2022
Capterra - the Ease of Use Badge in Network Security 2022
TechTimes - the Top 5 Best Bot Mitigation Companies in 2023
Gartner Digital Markets - theBest Ease of Use and Best Value badges in 2024

Investors

tisiwi 天使湾创投 | IDG Capital | SEQUOIA | Volcanics Venture 火山石投资 | HUAYU 华宇资本 CAPITAL