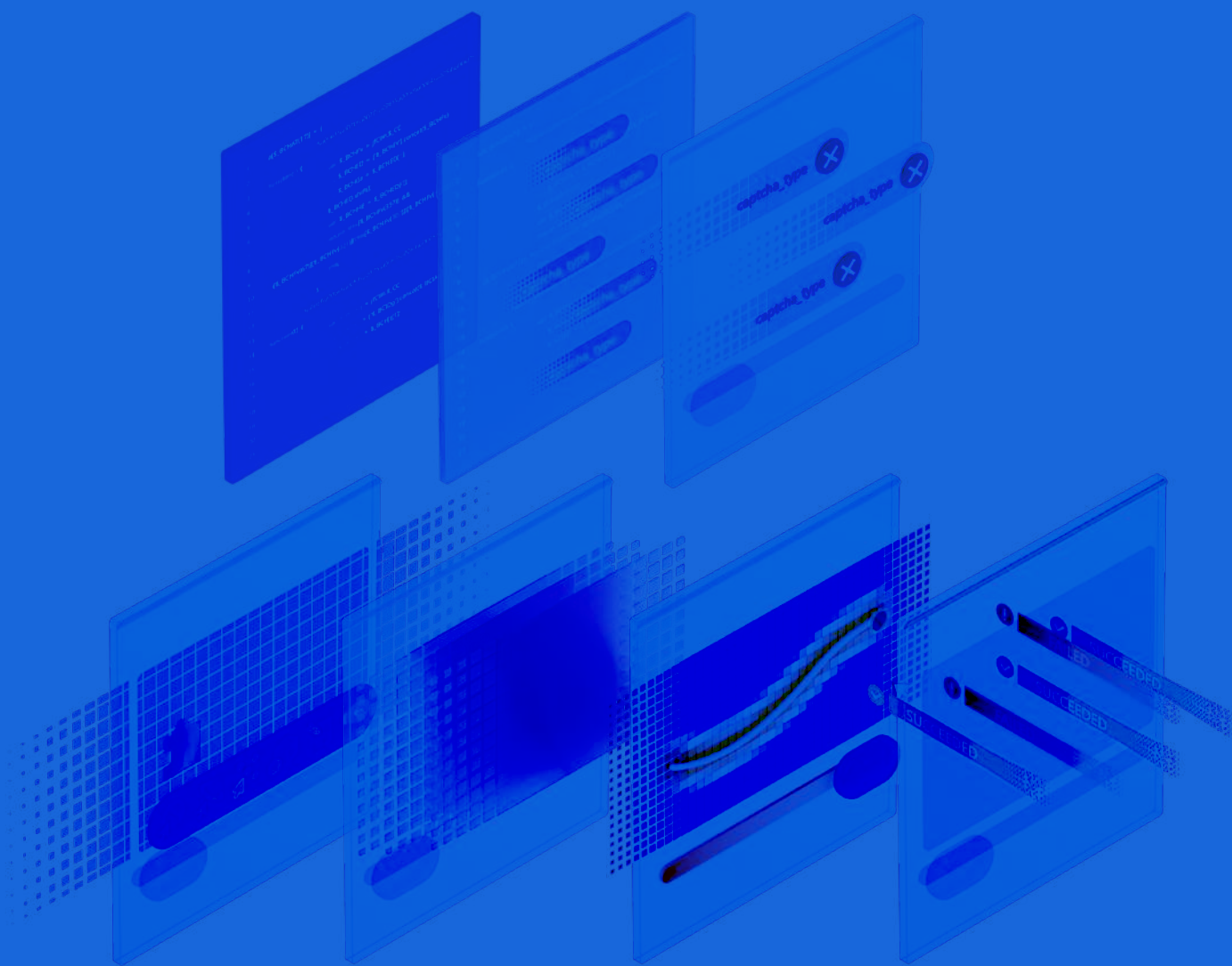


GEETEST

BOT TRAFFIC ANALYSIS DASHBOARD

eBook

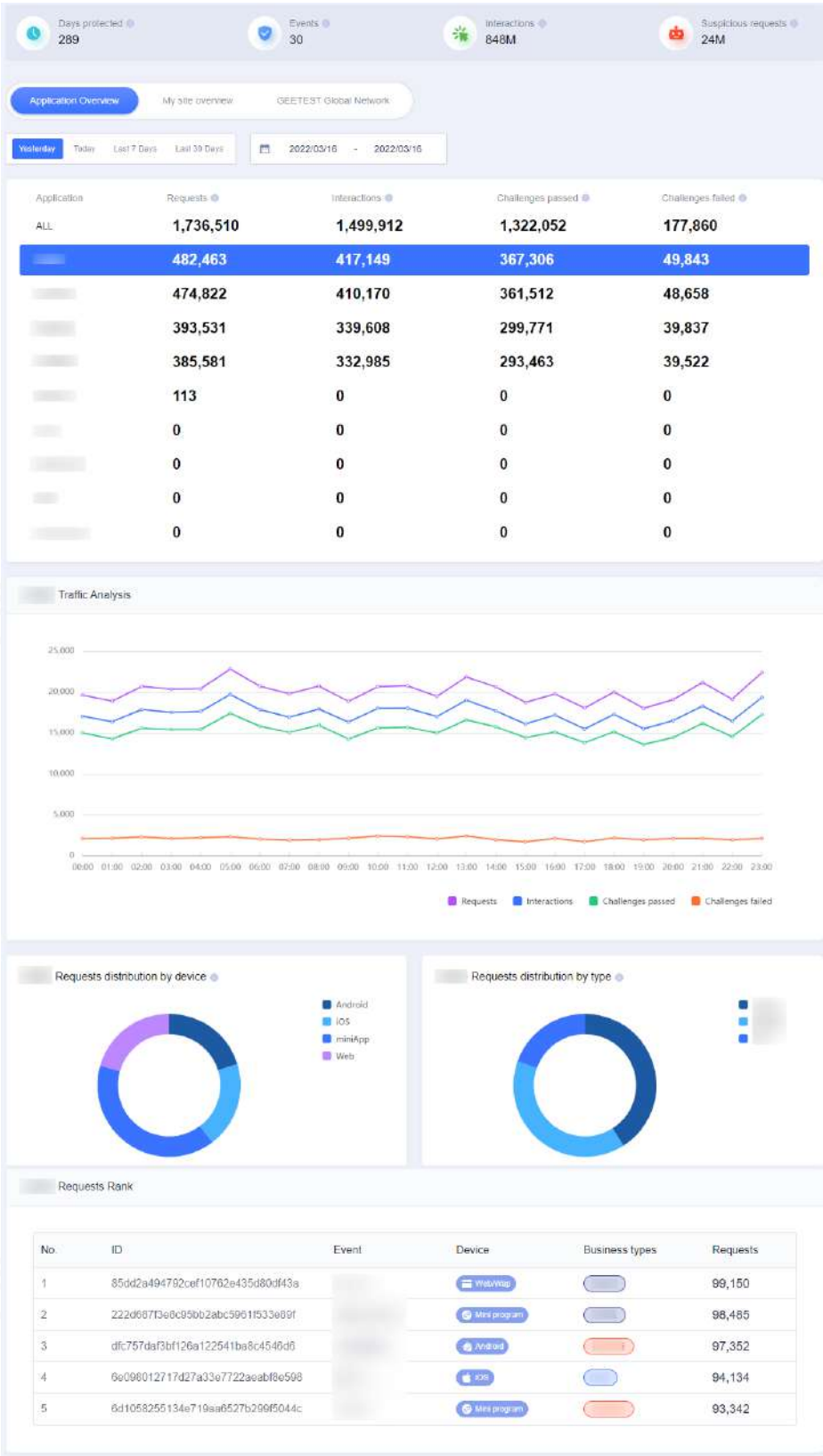


GeeTest Bot Traffic Analysis Dashboard

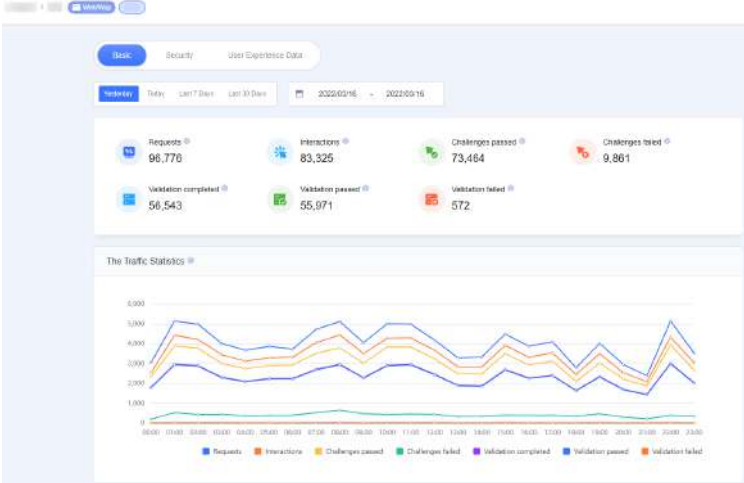
GeeTest Bot Traffic Analysis Dashboard is an all-in-one system that delivers real-time visualized data analysis to help you better understand the attack trend on your business while you use GeeTest Adaptive CAPTCHA, and allows you to make quick changes to system settings, such as security scheme, security strategy, CAPTCHA interface customization, etc. to swiftly adapt to the ever-changing attack and fraud trend.

Inclusive Data Analysis

Manage bot traffic of all your websites, apps, and APIs from one dashboard. Once you deployed GeeTest Adaptive CAPTCHA to your online businesses, no matter they are websites, apps, or APIs, you can get a general sense of the whole situation at one glance.



Multi-dimensional Data Studio



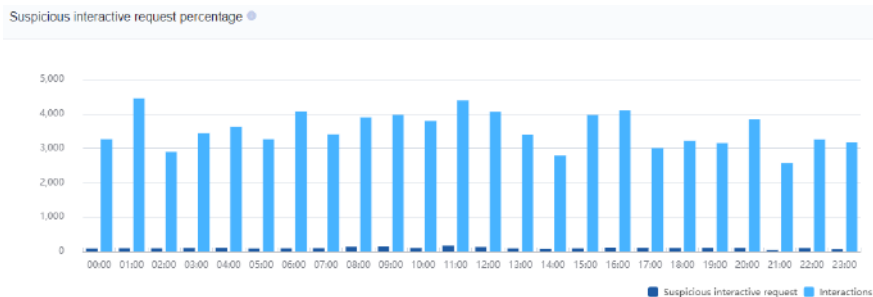
GeeTest dashboard organizes your use of Adaptive CAPTCHA into applications. Each application represents a website, app, or API where you deployed CAPTCHAs. Within each application, you have different events (IDs), such as login, order, comment, etc. Find the detailed verification data of each event in **Data Studio**. It helps you get a profound observation of the whole custom journey.

Profound Details Explained

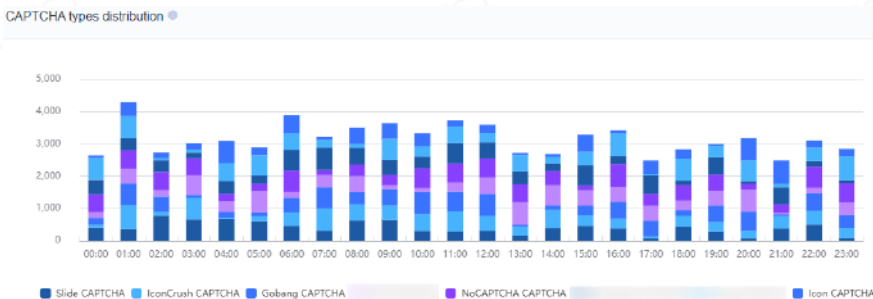
- Suspicious interactive request trend on an hourly basis helps you make accurate security strategy alterations.



- Comparative analysis between suspicious requests and normal requests updated hourly gives you a quick hint of real-time traffic changes in this event.



- CAPTCHA types distribution tells you which type of verification is more popular and which are not among your visitors to help you improve user experience.



Bot Attack Analysis & Configuration

Ways of bot attacks may change over time, but if you looked at the root, there are mainly two types of bypassing CAPTCHA methods: using web simulators and cutting in from APIs. GeeTest dashboard offers a chart of suspicious requests to your websites, apps, or APIs based on the methods of bot attacks.



The chart shows methods of bot attacks.

You can configure the methods of bot attacks that you want to detect from GeeTest dashboard.

CAPTCHA farm detection

Off by default. With settings on, the detection result will be returned to you via API. It is a detecting and labeling strategy that focuses on the features of CAPTCHA farms. We recommend you to turn it on when you on GeeTest invisible mode. Consult your account manager for more details.

☒ On

Web simulator detection

Off by default. With settings on, the detection result will be returned to you via API. It is a detecting and labeling strategy that focuses on the features of web simulators. We recommend you to turn it on when you on GeeTest invisible mode. Consult your account manager for more details.

☒ On

IP frequency detection

Choose whether returning IP frequency detection result

Off by default. With settings on, the detection result will be returned to you via API. It is for detecting and returning IP frequencies within the period of time you set. We recommend you to turn it on when you on GeeTest invisible mode. Consult your account manager for more details.

☒ On

IP frequency limit alert

Minimum time unit

300

second(s)

Frequency

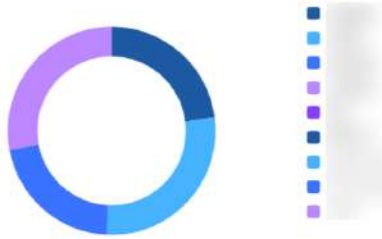
5

time(s)

Quick Security Overview

GeeTest dashboard offers suspicious requests on your applications and events, and types of end devices that generate suspicious requests.

Suspicious interactive requests distribution by applications



Suspicious interactive requests distribution by events

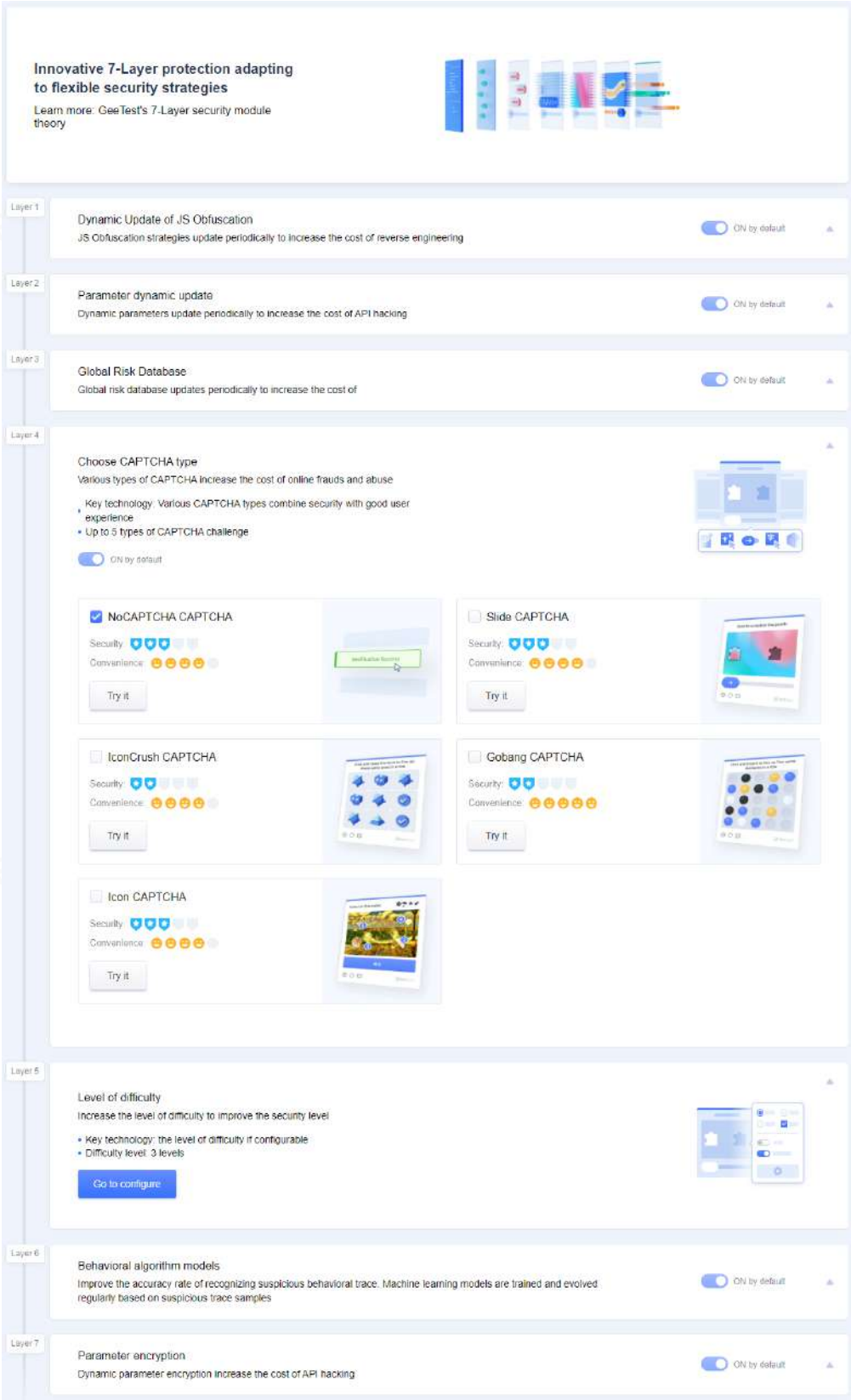


Suspicious interactive requests distribution by devices



Flexible Security Settings for Changing Threats

Apart from data analysis, GeeTest dashboard allows you to make quick changes to system settings, including security schemes and security strategies. You can apply different security settings to different events to sync up with your refining business operation.



Outsmart attackers with 7-layer dynamic protection

It makes GeeTest Adaptive CAPTCHA an evolving solution that does not weaken over time, as it can adapt to the changing data it detects.

7-layer protection changes when you toggle among different security schemes and can combine into 4374 security strategies per defense cycle.

Choose a Security Scheme That Suits You Best

In GeeTest dashboard, you can toggle among 3 security schemes which are designed based on varied scenarios and aims to fill the gap of cybersecurity skill for SMEs, making GeeTest Adaptive CAPTCHA a security solution that suits organizations from large to small.

Set customized security scheme for each event (ID).



☒ **Geetest Intelligent Mode** [Go to configure](#)

Intelligent mode presents suitable CAPTCHA forms based on each request's risk level which is generated by its behavior characteristic, device network environment and so on.

- GeeTest Intelligent Mode: classic security mode of GeeTest CAPTCHA, a soft option for most clients.



☐ **Direct Platform Integration**

Direct platform integration presents suitable CAPTCHA forms based on the risk level generated by your own risk control system.

- Direct Platform Integration: integrate GeeTest CAPTCHA into your current security solution, creating “a whole that is greater than the sum of the parts” solution.



☐ **Geetest Invisible Mode**

Geetest invisible Mode detects the risk level of each request based on its behavior characteristic, device network environment and so on without presenting any CAPTCHA challenges.

- GeeTest Invisible Mode: “NoCAPTCHA” CAPTCHA balances security and user experience to avoid unnecessary interruption to users.

Highly Customizable Interface

GeeTest CAPTCHA dedicates to balance security and user experience of CAPTCHAs. GeeTest Adaptive CAPTCHA provides a high freedom for you to tailor CAPTCHA into not only a security tool, but also a branding spot where your customers will remember. You can customize the CAPTCHA images, interface styles, animation styles, languages, CAPTCHA difficulty, and so on in GeeTest Dashboard.

Interface Style

Style

☒ Shadow

☐ Flat

Theme Color

Customization

Border Radius

NoneSmallDefaultLargeMax

You can customize the interface style by changing theme color, button style, and border-radius. The setting will take effect immediately.

GeeTest Adaptive CAPTCHA supports up to 78 languages, including English, Chinese, Japanese, Indonesian, Korean, Russian, Arabic, Spanish, Portuguese, French, German, Uyghur, etc.

GeeTest supports three animation styles: float, popup, and bind to button. By using [bind to button], your user need to click just one time before the verification.

Multi-Language Configuration

CAPTCHA Animation Style

Float

Popup

Bind to a button

CAPTCHA display form cannot be changed here (this is only a demo). Please visit the Developer docs.

Subaccount Management

GeeTest dashboard supports you and your team in the efficient coordination of several projects. Subaccount management allows the main account authorizes subaccounts with access to creating new applications and events (IDs), and data will sync up with the main account.

Account Info

Manage subaccounts

Manage subaccounts

In use

Not activated

Closed

Search by names/emails

+

Add

Name	Email	Phone number	Creation date	Last login time	Department	Notes	Operation
			2022-01-25	2022-01-25			

<

1

>

Note: Time and date of GeeTest dashboard is Greenwich Mean Time (GMT) if you chose English as the dashboard language.



360,000 Domains Worldwide Choose GeeTest

And You?

imperva

DATA DOME

airbnb

miHoYo

BINANCE

Best Western

NIKE

[I'm ready to talk](#)

[Give Me A Free Trial](#)

[Try Demo Now!](#)



[Adaptive CAPTCHA eBook](#)



www.geetest.com