reCAPTCHA Enterprise

Help protect your website from fraudulent activity, spam, and abuse without creating friction.

reCAPTCHA Enterprise is a service that protects your site from spam and abuse.

Defend your website with frictionless security

Fraudulent web activities cost enterprises billions of dollars each year. Security teams need to keep attackers out of their websites and ensure that their customers can always get in. reCAPTCHA has over a decade of experience defending the internet and data for its network of more than 5 million sites. reCAPTCHA Enterprise builds on this technology with capabilities, such as two-factor authentication and mobile application support, designed specifically for enterprise security concerns. With reCAPTCHA Enterprise, you can defend your website against common web-based attacks like credential stuffing, account takeovers, and scraping and help prevent costly exploits from malicious human and automated actors. And, just like reCAPTCHA v3, reCAPTCHA Enterprise will never interrupt your users with a challenge, so you can run it on all webpages where your customers interact with your services.

Protect your site with trusted security technology

reCAPTCHA Enterprise uses an adaptive risk analysis engine to keep automated software from engaging in abusive activities on your site. With technology that has helped defend millions of websites for over a decade, reCAPTCHA Enterprise is built to help mitigate fraudulent online activity for your enterprise.

Let your valid users in seamlessly

The reCAPTCHA Enterprise service helps you detect abusive traffic on your website without any user friction. Using a score-based detection system, you can rest assured that your countermeasures rely on detailed data about online activity in order to stop bots and other automated attacks while letting valid users in.

Built for the enterprise

This service offers unique capabilities built specifically for the enterprise. Security teams benefit from enhanced detection such as extra granular scores, reason codes for high-risk scores, and the ability to tune the risk analysis engine to your site's specific needs.

Features

View scores

reCAPTCHA Enterprise returns a score based on interactions with your websites, with 1.0 being a likely good interaction and 0.0 being a likely abusive action.

Take action

Based on the reCAPTCHA Enterprise score, you can take action in the context of your site. For example, with a low score, you can require two-factor authentication or email verification in order to allow a user to continue.

Tune the service to your website's needs

Using reCAPTCHA Enterprise, you can tune your site specific model by sending reCAPTCHA IDs back to Google labeled as false positives or false negatives. And reCAPTCHAs adaptive risk analysis engine will adapt future scores to fit your site.

Flexible API

You can easily integrate reCAPTCHA Enterprise on your site or mobile application using an API-based service.

Overview of reCAPTCHA Enterprise

Google has been defending millions of sites with reCAPTCHA for over a decade. reCAPTCHA Enterprise is built on the existing reCAPTCHA API and it uses advanced risk analysis techniques to distinguish between humans and bots. With reCAPTCHA Enterprise, you can protect your site from spam and abuse, and detect other types of fraudulent activities on the sites, such as credential stuffing, account takeover (ATO), and automated account creation. reCAPTCHA Enterprise offers enhanced detection with more granular scores, reason codes for risky events, mobile app SDKs, password breach/leak detection, Multi-factor authentication (MFA), and the ability to tune your site-specific model to protect enterprise businesses.

When to use reCAPTCHA Enterprise

reCAPTCHA Enterprise is useful when you want to detect automated attacks or threats against your website. These threats typically originate from scripts, mobile emulators, bot software, or humans.

How reCAPTCHA Enterprise works

When reCAPTCHA Enterprise is deployed in your environment, it interacts with the customer backend/server and customer web pages.

When an end user visits the web page, the following events are triggered in a sequence:

1. The browser loads the customer web page stored on the backend/web server, and then loads the reCAPTCHA JavaScript from reCAPTCHA Enterprise.
2. When the end user triggers an HTML action protected by reCAPTCHA such as login, the web page sends signals that are collected in the browser to reCAPTCHA Enterprise for analysis.
3. reCAPTCHA Enterprise sends an encrypted reCAPTCHA token to the web page for later use.
4. The web page sends the encrypted reCAPTCHA token to the backend/web server for assessment.
5. The backend/web server sends the create assessment (`assessments.create`) request and the encrypted reCAPTCHA token to reCAPTCHA Enterprise.
6. After assessing, reCAPTCHA Enterprise returns a score (from 0.0 through 1.0) and reason code (based on the interactions) to the backend/web server.
7. Depending on the score, you (developer) can determine the next steps to take action on the user.

The following sequence diagram shows the graphical representation of the reCAPTCHA Enterprise workflow: