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.

For more information about use cases, see OWASP Automated Threat Handbook - Web Applications (https://services.google.com/fh/files/misc/owasp_handbook_again.pdf).

How reCAPTCHA Enterprise works

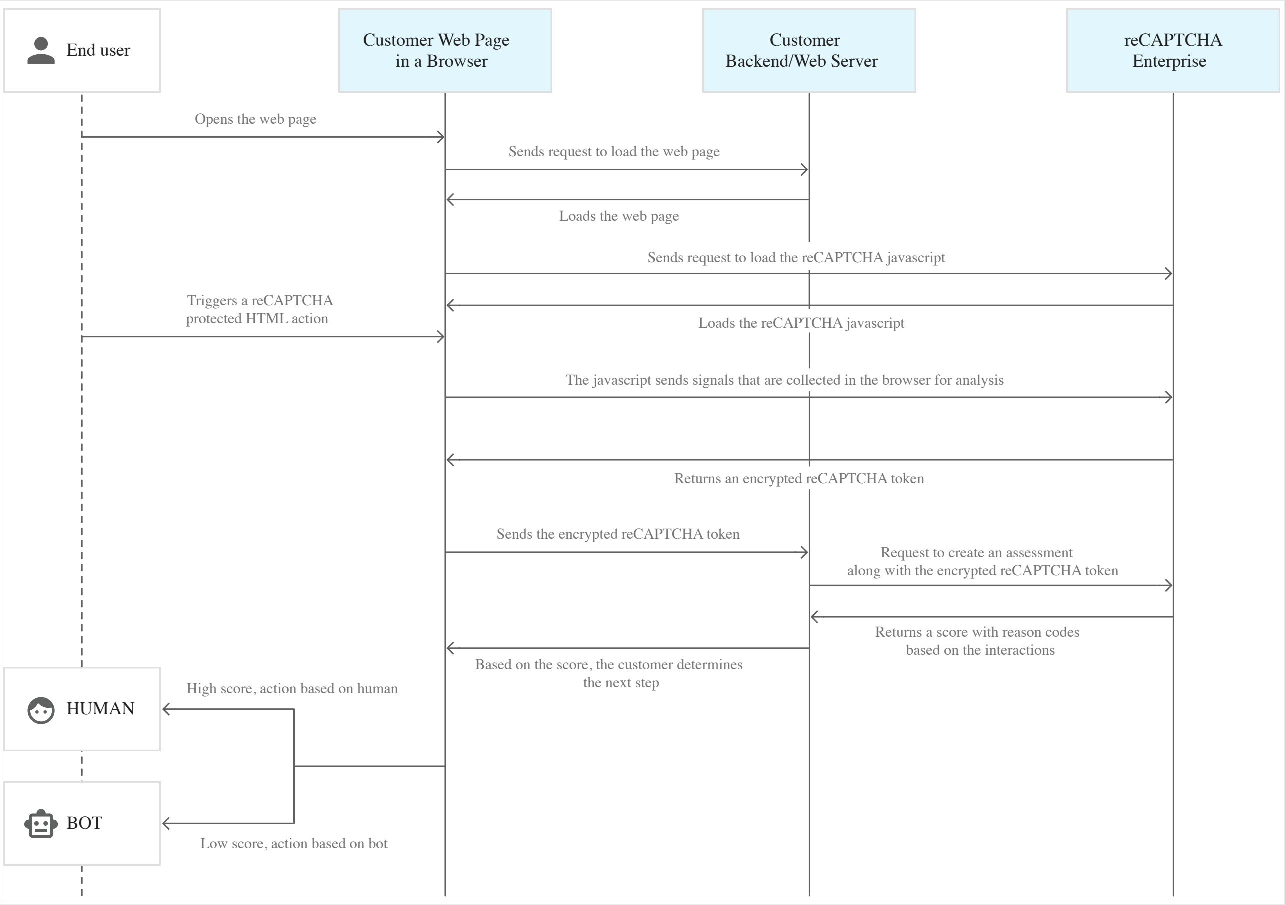
When reCAPTCHA Enterprise is deployed in your environment, it interacts with the customer backend/server and customer web pages.

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:


End user
Customer Web Page in a Browser
Customer Backend/Web Server
reCAPTCHA Enterprise
Opens the web page
Sends request to load the web page
Loads the web page
Sends request to load the reCAPTCHA javascript
Triggers a reCAPTCHA protected HTML action
Loads the reCAPTCHA javascript
The javascript sends signals that are collected in the browser for analysis
Returns an encrypted reCAPTCHA token
Sends the encrypted reCAPTCHA token
Request to create an assessment along with the encrypted reCAPTCHA token
Returns a score with reason codes based on the interactions
Based on the score, the customer determines the next step
HUMAN
High score, action based on human
BOT
Low score, action based on bot

What's next

- Get started with reCAPTCHA Enterprise (/recaptcha-enterprise/docs/getting-started).

Last updated 2022-09-28 UTC.