hCaptcha vs reCAPTCHA

Why Organizations are Choosing hCaptcha over reCAPTCHA v2 and reCAPTCHA v3.

As more of our life moves online, new incentives are created for both good and bad actors. Bots are a great example of this dynamic.

Bots now comprise over half of all internet traffic. Both bad and good bots have become more sophisticated, and many legacy solutions designed to mitigate the problems they generate no longer work.

Because of the dramatic increase in automated threats and the level of investment by threat actors in overcoming legacy defenses, stronger and more customizable approaches are needed to secure online properties.

One example of this phenomenon has been the rapid growth in popularity of hCaptcha, which has now taken more than 15% of global market share from Google due to their failure to deliver robust bot mitigation with their reCAPTCHA products.

hCaptcha Enterprise

The Leading Security ML Platform for Fraud and Abuse

Background: Why show challenges?

Bot protection first requires being able to reliably distinguish between real people and machines. At hCaptcha, we have always recognized that reliable humanity verification means occasionally asking people to answer a question. We work hard to reduce how often anyone needs to be challenged, but there is a huge difference between "a few" and zero questions when detecting spam, fraud, and abuse.

As long as people can answer simple questions that machines cannot, posing a question means increasing the cost to attackers of all kinds, and makes many attacks economically infeasible.

Over the years other methods have been tried, but ultimately the trade off is simple. If we want to preserve our privacy online, we need ways to verify a person is interacting with online services without trying to link that to anyone's real identity.

Proposed alternatives are rapidly broken, and always end up putting one or two companies (i.e. Google and Apple) in the gatekeeper's seat, making them responsible for knowing who you are and approving every website you log into or comment you post online.

That is not a world we want to live in.

Online services can trade away your privacy only once, and it will buy them nothing: bad actors have no difficulty circumventing naive approaches when there is any incentive to do so.

This is why we are so focused on privacy-first security, and why asking occasional questions is so useful.

Google reCAPTCHA: An Outdated Legacy Product

reCAPTCHA has been handicapped from the beginning. Google is primarily an advertising business, and every bot reCAPTCHA finds can reduce Google's revenue. This is not a recipe for success.

Perhaps for this reason, Google has failed to invest in reCAPTCHA for many years. This leaves it nearly useless against more sophisticated attacks.

However, Google eventually saw an opportunity to collect even more user data from outside sites, and released reCAPTCHA v3 with the recommendation to embed it on every page of a site. This is nearly useless for security, but quite helpful for tracking user behavior, for example to sell ads.

Due to Google's ad focus, reCAPTCHA v3's model looks very much like ad tracking. It builds a history of the user's online activity, ties this to their Google cookie, and then attempts to figure out if the overall behavior looks normal. This is quite easy to fake, and was broken shortly after v3 was released.

The store-everything approach also harms the user experience, violates privacy, and ends up punishing real people who have not opted into the Google ecosystem, for example by using Firefox. If you've ever noticed an overwhelming number of challenges when using incognito mode or a browser like Safari or Firefox, now you know why!

Similarly, Google's attempt to eliminate interactive challenges in reCAPTCHA v3 inevitably failed, forcing users to attempt to cobble together an awkward mix of v2 and v3 on their own. hCaptcha Enterprise instead offers a completely integrated solution, greatly simplifying use.
Bot protection is an arms race between threat actors and developers, and Google has consistently failed to keep up. reCAPTCHA has hardly changed over 15 years, and has been consistently broken by software attacks. hCaptcha continuously evolves in real-time, providing a much higher level of protection.

Today's advanced threats use sophisticated techniques to penetrate online defenses. reCAPTCHA lacks customizability, with very limited ability to modify or employ different threat models to handle ongoing threats. hCaptcha Enterprise focuses on combining a self- and semi-supervised learning approach to automatically detect new and evolving threats, and provides advanced tools and dashboards to completely customize system behavior.

To keep pace with the ever-evolving threat that bots pose, many organizations are demanding a more robust approach than legacy solutions like reCAPTCHA.

hCaptcha: Today's Leader in Bot Detection

hCaptcha delivers a better end-user experience, stronger security, and a superior suite of advanced features. Driven by privacy-preserving machine learning and a novel approach to humanity verification, hCaptcha rapidly adapts to new and emerging threats to ensure comprehensive protection for your online properties. The unique edge-focused design eliminates data retention, simplifying compliance with privacy regulations around the world.

The Leading Security ML Platform for Fraud and Abuse

Finally, switching from reCAPTCHA to hCaptcha is easy, due to hCaptcha's compatibility features, generally requiring only three lines of code.

Let's compare hCaptcha and reCAPTCHA head-to-head:

Advantages: hCaptcha vs. reCAPTCHA

Here are a few of the many reasons why organizations are selecting hCaptcha as their preferred bot mitigation provider:

- Superior Design: In the battle against malicious bots, hCaptcha takes an entirely different approach, designed from day one for scale, accuracy, and performance without relying on historic data or the personal information of users.

- Adapts to New Threats Automatically: hCaptcha's advanced machine learning capabilities automatically adapt to new threats. This dramatically reduces your workload while offering a higher degree of protection.

- Advanced Features: hCaptcha offers a suite of advanced features to protect your organization against the most sophisticated threat actors. From advanced persistent threat mitigation to private learning, hCaptcha can address your most challenging use cases.

- Privacy Compliance: Privacy laws are proliferating around the world. hCaptcha was specifically designed to protect user privacy and complies with GDPR, CCPA, LGPD, PIPL, and other mandates.

- Works Globally: hCaptcha works in every country and supports 110 different languages. This is critical for organizations that serve a global audience.

- Great User Experience: To provide a low-friction end-user experience, reCAPTCHA requires the presence of Google cookies, personal PII, and tracks historic interactions with the user. Because of its heavy reliance on this information, it will often penalize legitimate users if they are not logged into a Google account. hCaptcha, on the other hand, is device and browser agnostic, providing an equitable, low friction experience to all end-users.

- Comprehensive Accessibility: hCaptcha offers the most robust accessibility on the market, with options like text-based challenges that do not discriminate against those with auditory processing disorders, as audio challenges do. To ensure accessibility, hCaptcha is fully WCAG 2.1 and Section 508 compliant.

- Customization: hCaptcha is highly customizable to meet the needs of your organization You can easily launch on-brand custom challenge content, adjust difficulty levels, manage threat responses, and more.

- Easy Implementation: hCaptcha only needs to be integrated on pages you want to protect, not on every page of your site like reCAPTCHA v3. It can be implemented with just three lines of code.

Moving Beyond Legacy Features

As organizations upgrade their defenses against new threats, outperforming legacy systems like Google's reCAPTCHA is critical to maintain security while preserving a positive user experience.

These solutions must ultimately be evaluated based on the security level they can deliver without compromising user experience, commitment to privacy, and accessibility.

Don't Just Take Our Word For It

Because hCaptcha Enterprise is so effective and simple to implement, we offer a no-obligation pilot to put us to the test.

Many of the world's largest online services have done their own comparisons against legacy alternatives before switching to hCaptcha Enterprise. Compare us side-by-side and the answer will be obvious.

Click to ***start a pilot of hCaptcha Enterprise*** to see for yourself.

hCaptcha Enterprise

The Leading Security ML Platform for Fraud and Abuse