reCAPTCHA Enterprise

Comprehensive online fraud protection platform

Growing sophistication and cost of online fraud

Enterprise security has historically been focused primarily on threats that exploit infrastructure vulnerabilities. However, a rapidly growing risk to the ever-expanding online footprint of organizations stems from automated attacks that emulate web users rather than targeting deeper infrastructure vulnerabilities. In fact, malicious and sophisticated bot-based fraud already exacts a huge socioeconomic toll that ranges from disinformation and loss of customer trust to billions of dollars in lost revenues globally. Some of the most common bot-based threats are highlighted below.

Scraping	Content pilfering for ad revenue diversion or competitive use
Fraudulent Transactions	Purchase of goods or gift cards with stolen credit cards
Account Takeovers (ATO)	Credential stuffing to validate stolen accounts
Synthetic Accounts	Creation of new accounts for promotion value or future misuse
False Posts	Posting of malicious links or misinformation propagation
Money Laundering	Bot-generated ad click revenue on fraudulent websites

300%

Increase in account takeovers in 2017[1]

30 Billion

Credential stuffing attacks in 2018[2]

29%

Breaches involving stolen credentials[3]

[1] Javelin – 2019 Identity Fraud Study
[2] Akamai – State of Internet/Security, Vol. 5, 2019
[3] Verizon – 2019 Data Breach Investigations Report

Google Cloud

Regardless of the threat vector and objective, bot-mitigation technologies have primarily relied on challenge-response systems that require manual text inputs or image-based puzzles to be solved. However, off-the-shelf image processing tools and low-cost offshore labor have enabled threat actors to circumvent such detection. Additionally, high user friction inherent in image-ba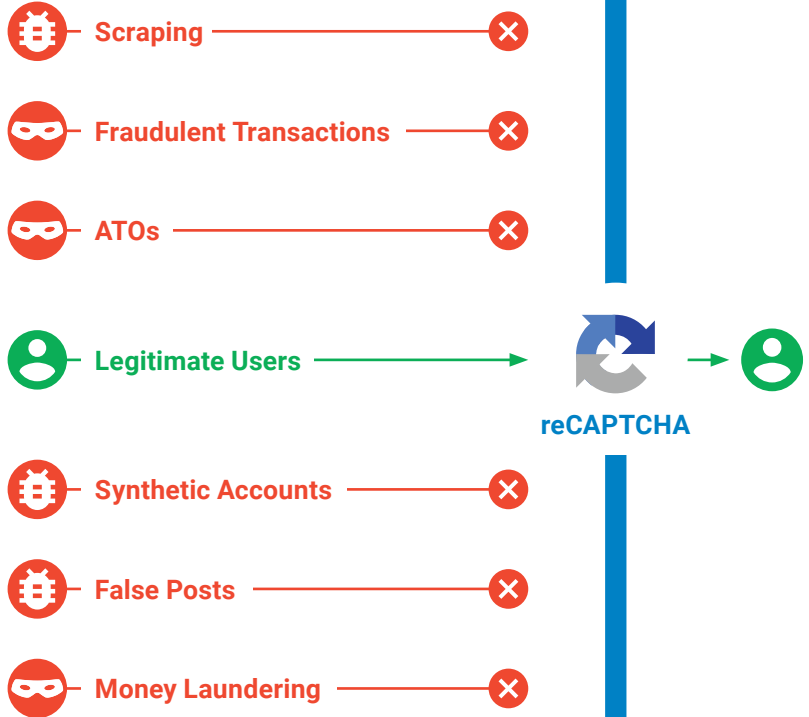sed challenge-response bot detection limits coverage to a few key pages such as login, account creation, shopping cart, and payment. In fact, the risk of bot-based threats like scraping and false posts warrants far more comprehensive protection across websites. Also, false positives and user errors increase the risk of customer churn and transaction abandonment rates. And once initially bypassed, this binary approach clears the path for site-wide attacks by a bot.

reCAPTCHA Enterprise

reCAPTCHA Enterprise is a User Protection Service from Google Cloud that provides comprehensive protection against bot-based online fraud attacks while enabling real web user interactions to proceed seamlessly.

reCAPTCHA has been at the forefront of bot mitigation for over a decade and actively protects 3.4 million websites. Continuing that trend, the reCAPTCHA API has introduced adaptive risk scoring as the primary detection approach, thereby shifting image-based challenges to an optional escalation path role.

Scraping ✗
Fraudulent Transactions ✗
ATOs ✗
Legitimate Users →
Synthetic Accounts ✗
False Posts ✗
Money Laundering ✗

reCAPTCHA

Google Cloud

With frictionless user experience, fraud protection is now easily extended across websites rather than being limited to select pages. Additionally, reCAPTCHA's risk-based bot algorithms apply continuous machine learning that factors in every customer and bot interaction to overcome the binary heuristic logic of traditional challenge-based bot detection technologies. The reCAPTCHA admin console provides statistical detail to help quickly identify pages being targeted by bots and the magnitude of associated risk.

Risk scores can be used to:

Make decisions on the need for additional verification (2FA, phone, email)

Enrich analysis by merging scores with user profiles and transaction history data

Train and provide feedback to underlying machine learning models

New with reCAPTCHA Enterprise:

1. Greater granularity in risk scoring

2. Increased customizability of risk algorithms to organization and page-specific risk profiles

3. Market-leading Google Cloud terms of service, availability, and support for mission-critical web applications

Google Cloud

reCAPTCHA Enterprise highlights

Proven

3.4M sites protected

Customer-friendly

Zero user friction

Customizable

Company-specific risk models
Risk-based escalation (2FA)

Adaptive

ML Model Tuning API

Comprehensive

Site-wide coverage
Mobile App SDK (Android/iOS)

Enterprise-ready

Easy API-based integration
Google Cloud (SLAs/SLOs)

Availability and pricing

reCAPTCHA Enterprise is generally available and is priced based on API calls consumed.
For pricing and sales information, please contact **userprotection@google.com**.

Google Cloud