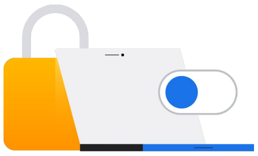
इंटरनेट पर सभी को सुरक्षित अनुभव देने के लिए पार्टनरशिप करना: एपीआई की भूमिका

उपयोगकर्ताओं और अन्य संगठनों को गलत लोगों से बचाने के लिए हम ऐप्लिकेशन प्रोग्रामिंग इंटरफ़ेस (एपीआई) बनाते हैं और उन्हें शेयर करते हैं. ये ऑनलाइन खतरों का पता लगाने और उन्हें ब्लॉक करने में मदद करते हैं. यही नहीं, इंटरनेट को सभी के लिए सुरक्षित बनाने में भी इनसे मदद मिलती है.



एपीआई बनाना

हम तीन मुख्य मामलों में लोगों को सुरक्षित रखने के लिए, सुरक्षा से जुड़े एपीआई बनाते हैं. इन एपीआई के कुछ उदाहरण:

बच्चों की सुरक्षा

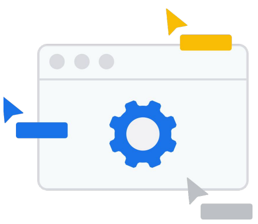
- Content Safety API
- CSAI Match API
- Hash Matching API

मैलवेयर वगैरह से सुरक्षा

- Safe Browsing API
- Project Shield API
- VirusTotal API

जानकारी की क्वालिटी

- Perspective API
- Vision API
- FactCheck API
- Civics Information API
- Text Moderation



पहुंच बढ़ाना

अपने एपीआई की पहुंच बढ़ाने के लिए, हम अपने पार्टनर के साथ सुरक्षा से जुड़े एपीआई शेयर करते हैं:

4.6 करोड़

साल 2022 में, Cloud Armor API ने अब तक का सबसे बड़ा डीडीओएस हमला, यानी कि Layer 7 को ब्लॉक किया. इस हमले के दौरान हर सेकंड 4.6 करोड़ अनुरोध किए जा रहे थे.

2 अरब

Perspective API को एक दिन में 1,000 से ज़्यादा पार्टनर ने तकरीबन 2 अरब बार कॉल किया.

4 अरब

बच्चों की सुरक्षा से जुड़ी टूलकिट (Content Safety API + CSAI Match API) ने पिछले 30 दिनों में 4 अरब से ज़्यादा इमेज और वीडियो प्रोसेस किए हैं.

सीमित ऐक्सेस देना

हम यह पक्का करना चाहते हैं कि सिर्फ़ भरोसेमंद पार्टनर के पास एपीआई का ऐक्सेस रहे. साथ ही, उनका इस्तेमाल नियमों के दायरे में रहकर और सुरक्षित तरीके से किया जाए. इसके लिए, हम तीन सबसे ज़रूरी कदम उठाते हैं:

जांच करना → पाबंदी लगाना → लागू करना

हम अपने सुरक्षा API का ऐक्सेस केवल ऐसे पार्टनर्स को देते हैं जिनकी हमने सावधानी पूर्वक जांच की हो, इन टूल के अनधिकृत इस्तेमाल पर रोक लगाते हैं और हमारी सेवा की शर्तों की नीतियों को सख्ती से लागू करते हैं. सुरक्षा से जुड़े एपीआई के ज़रिए हम अपने भरोसेमंद पार्टनर को एक-साथ मिलकर काम करने के लिए बढ़ावा देते हैं. इससे हमें इंटरनेट पर सभी को सुरक्षित अनुभव देने में मदद मिलती है.

सुरक्षा से जुड़े Google के एपीआई

बच्चों की सुरक्षा से जुड़े एपीआई

बच्चों की सुरक्षा से जुड़ी टूलकिट

Content Safety

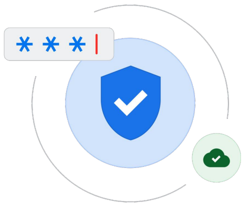
इस मॉडल का मालिकाना हक Google के पास है. यह बच्चों का यौन शोषण दिखाने वाली अरबों इमेज पहचानने और उन पर प्राथमिकता से कार्रवाई करने में मदद करता है. यह मशीन लर्निंग क्लासिफ़ायर का इस्तेमाल करता है, ताकि बच्चों का यौन शोषण दिखाने वाली उन इमेज की पहचान की जा सके जो प्लैटफ़ॉर्म पर पहली बार देखी गई हैं. इससे तुरंत उनकी समीक्षा करने, उन्हें हटाने, और उनकी शिकायत करने में मदद मिलती है.

CSAI Match

इस टेक्नोलॉजी का मालिकाना हक YouTube के पास है. सबसे पहले इसी टेक्नोलॉजी में हैश-मैचिंग का इस्तेमाल किया गया था. बच्चों का यौन शोषण दिखाने वाले वीडियो (सीएसएआई) की पहचान करने और सिस्टमैटिक तौर पर फ़्लैग करने के लिए इसका इस्तेमाल किया जाता है. इससे पार्टनर को उनकी समीक्षा करने, पुष्टि करने, शिकायत करने, और उन पर कार्रवाई करने में मदद मिलती है.

Hash Matching

हम Google का Hash Matching API, एनसीएमईसी के लिए उपलब्ध कराते हैं. इससे उसे CyberTipline पर मिलने वाली शिकायतों पर प्राथमिकता से कार्रवाई करने और उनकी समीक्षा करने में मदद मिलती है. यह उन शिकायतों पर तुरंत कार्रवाई करने में मदद करता है जिनमें बच्चों को तुरंत मदद की ज़रूरत होती है.



सुरक्षा से जुड़े एपीआई

वेब ऐप्लिकेशन और एपीआई सुरक्षा के लिए Google का टूल

Cloud Armor

यह एपीआई खतरनाक हमलों और डिस्ट्रिब्यूटेड डिनायल ऑफ़ सर्विस (डीडीओएस) वाले ऑटोमेटेड हमलों से वेबसाइट, उनकी सेवाओं, और एपीआई को सुरक्षित रखने में मदद करता है.

reCAPTCHA

यह वेबसाइट को धोखाधड़ी वाली गतिविधि, स्पैम, और गलत इस्तेमाल से सुरक्षित रखने में मदद करता है. reCAPTCHA Enterprise खतरों का आकलन करने के लिए अडैप्टिव इंजन का इस्तेमाल करता है. इससे ऑटोमेटेड सॉफ़्टवेयर को गलत इस्तेमाल से जुड़ी गतिविधियों में शामिल होने से रोकने में मदद मिलती है.

Apigee

एपीआई के लिए हर समय मैनेजमेंट की सुविधा उपलब्ध कराने वाला Google Cloud प्लैटफ़ॉर्म, कारोबारों को एपीआई बनाने, उन्हें सुरक्षित रखने, उन्हें इस्तेमाल के लिए उपलब्ध कराने, उन पर नज़र बनाए रखने, और उनकी पहुंच बढ़ाने में मदद करता है.

Safe Browsing

हमारा Safe Browsing API, क्लाइंट ऐप्लिकेशन को यह अनुमति देता है कि वे असुरक्षित वेब रिसॉर्स की लगातार अपडेट होने वाली सूची के हिसाब से यूआरएल की जांच करते रहें. यह टूल हर दिन पांच अरब डिवाइसों की सुरक्षा करता है. इसके लिए, यह लोगों को उन साइटों के बारे में चेतावनी देता है जो मैलवेयर या अनचाहे सॉफ़्टवेयर को होस्ट करती हैं.

VirusTotal

इससे डेवलपर, विश्लेषण के लिए फ़ाइलें या यूआरएल सबमिट कर पाते हैं. साथ ही, डेवलपर को इस बारे में एक रिपोर्ट भी मिलती है कि क्या मैलवेयर के हमले से उनकी वेबसाइट पर कोई असर पड़ा है.

जानकारी की क्वालिटी से जुड़े एपीआई

Perspective

यह एक ओपन-सोर्स एपीआई है. इसमें मशीन लर्निंग टेक्नोलॉजी का इस्तेमाल किया जाता है. इससे "नफ़रत फ़ैलाने" वाली टिप्पणियों की पहचान करने में मदद मिलती है. इसका इस्तेमाल इंसानों के बीच इंटरैक्शन को आसान बनाने के लिए ही नहीं किया जाता, बल्कि लार्ज लैंग्वेज मॉडल और जनरेटिव एआई के साथ इंसानों के बेहतर इंटरैक्शन को भी बढ़ावा दिया जाता है.

Vision

इससे डेवलपर, अपने ऐप्लिकेशन में विज़न डिटेक्ट करने की सुविधाओं को आसानी से इंटिग्रेट कर पाते हैं. जैसे, इमेज लेबल करने, चेहरे और लैंडमार्क की पहचान करने, ऑप्टिकल कैरेक्टर रिकग्निशन (ओसीआर), और अश्लील कॉन्टेंट को टैग करने की सुविधा.

FactCheck

इसे तथ्यों की जांच करने वाले लोगों, पत्रकारों, और शोधकर्ताओं की मदद करने के लिए बनाया गया है. इससे उन्हें यह पता लगाने में मदद मिलती है कि दुनिया भर में कौन-कौनसे तथ्य गलत साबित हुए हैं और कौन-कौनसे नहीं. इस टूल के ज़रिए लोग ऐसे तीन लाख तथ्यों से जुड़े दावे खोज सकते हैं जिनकी जांच जाने-माने पब्लिशर ने की है.

Civic Information

Civic Information API के ज़रिए डेवलपर ऐसे ऐप्लिकेशन बना सकते हैं जिनसे अमेरिका के नागरिकों और मतदाताओं को, राजनैतिक मामलों में उनकी भागीदारी, बैलेट से जुड़ी जानकारी, और मतदान की जगह के बारे पता चलता है. इन ऐप्लिकेशन में जिन चुनावों की जानकारी दी जाती है उनके दौरान, मतदाता पोलिंग बूथ, जल्दी वोट करने, वोट डालने की जगह, और उम्मीदवार की जानकारी हासिल कर सकते हैं.

Text Moderation

Google का टेक्स्ट मॉडरेशन टूल, Cloud Natural Language API के ज़रिए उपलब्ध होता है. इससे संगठन, संवेदनशील या नुकसान पहुंचाने वाले कॉन्टेंट को स्कैन कर पाते हैं. यह नुकसान पहुंचाने वाले अलग-अलग तरह के कॉन्टेंट की पहचान करने में सक्षम है. जैसे, यह नफ़रत फैलाने वाली भाषा, यौन शोषण, धमकाने से जुड़े कॉन्टेंट की पहचान करने में मदद करता है.

Google के साथ, आप हैं हर दिन सुरक्षित

हम ऐसे API बनाने और शेयर करने में निवेश करते हैं जो इंटरनेट पर मिलने वाली धमकियों की पहचान करके उन्हें ब्लॉक कर सकें. इससे यह सुनिश्चित किया जा सकता है कि **Google के साथ, आप हर दिन ज़्यादा सुरक्षित रहें.** हमारे सुरक्षा केंद्र पर जाकर और जानकारी पाएं कि हम बाकियों के मुकाबले ज़्यादा लोगों को इंटरनेट पर सुरक्षित कैसे रखते हैं.