# Web Risk for enterprises

## Growing Risk of Threats Targeting User Generated Content

Over the years, organizations have made significant security investments to protect their corporate users and networks from a variety of security threats. Today, inbound and outbound email, internet traffic and other content types are commonly monitored by firewalls, gateways, DLP and other security tools. However, most organizations are also experiencing a growing footprint of customer or user generated content in the form of blogs, forums, support sites and more which significantly expands the surface area of attack along a new dimension.

For social media companies the problem is particularly pronounced as the size of the network and level of user engagement correlate directly not just with revenues and brand value but also with malware reach and propagation value. Meanwhile, constantly evolving malware artifacts (domains and URLs) used in social engineering campaigns evade content filtering and other security technologies which unwittingly end up propagating malware as users access and share content. Eventually, the presence of malware may erode site ratings, usage, revenues and brand value. To combat this growing risk, organizations need comprehensive and continuous visibility into threats targeting user generated content.

Attacks that start with phishing:
**90%**

Social media cybercrime revenues:
**$3.25B**

Increase in social media phishing:
**500%**

Google Cloud

# Web Risk

Web Risk is a User Protection Service from Google Cloud designed to reduce the risk of threats targeting user generated content. Web Risk lets organizations compare URLs in their environment against a repository of over 1 million unsafe URLs. This includes social engineering sites associated with phishing attacks as well as sites that host malicious or other unwanted software.

The underlying repository is constantly updated by scanning billions of URLs daily and is powered by the same technology that underpins Google Safe Browsing. Initially launched in 2007 to protect users from phishing attacks, Safe Browsing has evolved and expanded protection to web-based threats like malware, unwanted software, and social engineering across desktop and mobile platforms. Today, Safe Browsing works across numerous Google and 3rd party products and protects over four billion devices on a daily basis.

Web Risk extends Safe Browsing API capabilities to organizations that want to use the APIs at higher volumes and have access to new enterprise grade features, such as risk scoring, confidence levels, file/attachment reputation coverage and integration with GCP security (CSCC) and analytics (BigQuery) tools as they are developed and released.

## Comprehensive:

1B+ URLs scanned daily,
1M+ known bad URLs

## High Fidelity:

high verdict accuracy
and low false positive rates

## Proven Technology:

built on Safe Browsing technology
which protects 4B+ devices

Google Cloud

## Flexible API Options

Web Risk offers three methods to check whether a URL is on any of its lists.

- The Lookup API is a very simple method that lets client applications send URLs to the Web Risk server as HTTP requests and receive a verdict and type in response.
- Web Risk also offers an Update API which lets client applications download and periodically update hashed versions of Safe Browser lists to a local database for client-side URL verdict checks.
- Web Risk provides a Submission API (EAP) so you can submit URLs that you suspect are unsafe to Safe Browsing for analysis. Any URLs that are confirmed to match the Safe Browsing Policies will be added to the Safe Browsing service. This enables you to protect your users from known malicious URLs and scale protection across billions of devices.

Collectively, these APIs offer deployment simplicity and support security and latency goals. To reduce client bandwidth usage and protect the server side from traffic spikes, the APIs also leverage client side caching and support compression.

### Update API Sample Request

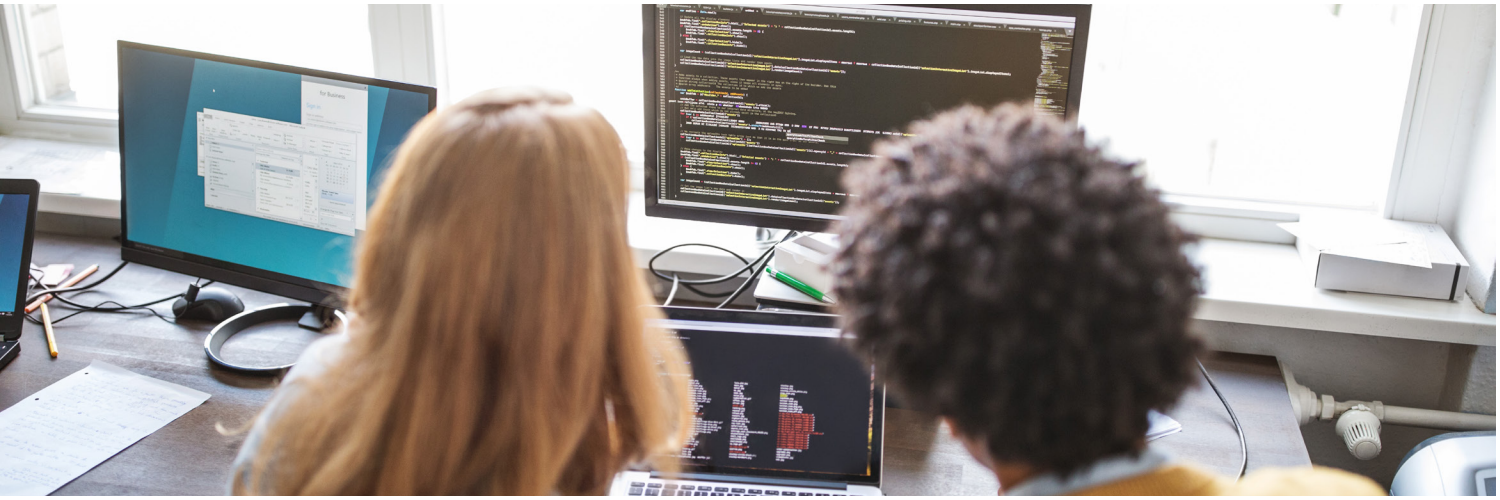
```
Curl

-H "Content-Type: application/json"

"https://webrisk.googleapis.com/v1beta1/hashes.
search?key=YOUR_API_KEY

&threatTypes=MALWARE
&threatTypes=SOCIAL_ENGINEERING

&hashPrefix=WwuJdQ%3D%3D"
```

### Update API Sample Response

```
"threats": [{
    "threatTypes": ["MALWARE"],
    "hash": "WwuJdQx48jP-4lxr4y2RDSk1PC9Rf-4="
    "expireTime": "2019-07-17T15:01:23.0451"
  },{
    "threatTypes": ["MALWARE",
SOCIAL_ENGINEERING"],
    "hash": "WwuJdQxaCSH453-uytERCE23F7-hnfD="
    "expireTime": "2019-07-17T15:01:23.04"
  },}],
"negativeExpireTime": "2019-07-17T15:01:23.04"
```

## Use Cases

Numerous organizations with significant user generated content already use Safe Browsing APIs as a tool to protect their users and their brand.



## High Growth Social Media Network

A fast growing social media network focused on crowdsourced reviews of local services in major cities was experiencing increased incidence of malware and phishing URLs propagating through its site and mobile app. In some cases fake accounts were being used to drive users to click malicious links in what seemed to be legitimate reviews. In other cases, malvertising links were offering up prizes for surveys and promotions.

User complaints and negative online reviews were starting to impact business and network growth. After adopting Web Risk to validate all URLs posted within user generated content across its applications, the social media company was able to curb successful phishing of its users and malware propagation on its sites up to 99%.

## Availability and Pricing

Web Risk is now Generally Available. A trial license that supports free usage up to 100,000 API calls per month is available at **https://cloud.google.com/web-risk/.** For enterprises already using the free API and looking to expand coverage, please contact **userprotection@google.com** for pricing details.