CLOUDMARK®
Intelligent Network Security

Product Datasheet

Cloudmark Insight Data API

Benefits

Threat Intelligence from Cloudmark's Industry Leading Global Threat Network

Threat data aggregated across 1+ billion active users

Continuously updated threat analysis

Dependable Cloud Service

7x24x365 hardware, software, and performance management

Services hosted in carrier-class SOC 2-certified Data Centers

Continuous capacity monitoring and systems expansion

Key Features

Superior Anti-Abuse Protection

Industry-leading detection of content associated with spam, phishing, and malware activity

Advanced content filtering powered by Cloudmark Authority

Ability to scan multiple content types and call-to-actions

High Performance REST API

Scan performance suitable for integrating real time scanning into your application

Scalable, geo-redundant cloud-based API service

Leading Threat Intelligence for your Business Needs

The Cloudmark Insight Data API provides enhanced visibility into the comprehensive threat intelligence data aggregated by the Cloudmark's Global Threat Network (GTN). The Cloudmark GTN system is the world's largest commercial threat intelligence platform, observing and analyzing the real-time messaging and threat traffic patterns seen by over 1 billion active users. This system also processes spamtrap and end user feedback related to active spam, phishing, ransomware, and malware campaigns.

Cloud-Based Access to Cloudmark Authority Scanning

The Insight Data API provides a cloud-based REST interface to make live queries into Cloudmark Authority threat engine. Current threat categorization results are returned instantaneously by the API, allowing your system to leverage results in live traffic analysis. The following types of queries are supported:

- Textual content (or full email messages)
- Files
- IP addresses
- Domains
- URLs

These requests are analyzed by the Cloudmark Authority engine and a verdict is returned that denotes the current threat classification for the analyzed content. Categories returned include:

- Legitimate – Content does not pose a known threat
- Spam – Matches content used in spam activity
- Phishing – Matches content used in phishing activity
- Virus – Malware content detected
- Compromised – Matches URLs that are hosted on known compromised web sites

Cloudmark Insight Data API Solutions

Over the Top Messaging Providers

While open messaging platforms such as email and SMS have historically been the prime platforms for abuse, attackers are now beginning to explore how to attack users within walled garden messaging platforms. By using the knowledge gained in malicious message campaigns seen in the wild, it becomes possible to quickly identify attackers who are sending the same content and call to actions to users within your messaging platform. Integrate the solution to scan messages as they are originated, enabling blocking of known unwanted or malicious messages before delivery.

Email Service Providers

Integrate the Insight Data API directly into your marketing message sending platform to scan messaging content being sent by your customers. The query result data will be useful to continuously evaluate customer accounts for proper sending practices, potential account credential compromises, and for flagging accounts for sending practice improvement consulting.

Communication Provider as a Service (CPaaS) Providers

Companies that provide API-driven messaging systems are susceptible to being abused by spammers who wish to use those platforms to reach their targets via SMS, mobile app notifications, or other non-email destinations. Attackers who are allowed to sign up accounts will leverage those systems for the sole purpose of sending spam/malware content to their intended targets. The query result data will be useful to continuously evaluate customer accounts to see if they are using the system according to acceptable use policies and for flagging accounts for sending practice improvement consulting.

Web Hosting Providers and Website Builder Sites

Attackers who are allowed to sign up for trials or otherwise free tier accounts will leverage those systems for the sole purpose of hosting spam/malware content, or to support phishing site landing pages. This type of activity leads to site reputation problems and is typically a source for complaints, chargebacks, and takedown requests. To stop these types of abuses, the solution can be used to scan newly posted web site content in an attempt to see if the landing page contains spam, malware, or phishing landing page content.

About Cloudmark

Cloudmark is a trusted leader in intelligent threat protection against known and future attacks, safeguarding 12 percent of the world's inboxes from wide-scale and targeted email threats. With more than a decade of experience protecting the world's largest messaging environments, only Cloudmark combines global threat intelligence from a billion subscribers with local behavioral context tracking to deliver instant and predictive defense against data theft and security breaches that result in financial loss and damage to brand and reputation. Cloudmark protects more than 120 tier-one service providers, including Verizon, Swisscom, Comcast, Cox and NTT, as well as tens of thousands of enterprises.

Americas Headquarters
Cloudmark, Inc.
San Francisco, USA

Europe
Cloudmark Europe Ltd.
London, UK

Paris
Cloudmark Labs
Paris, France

Japan
Cloudmark Japan
Tokyo, Japan