CLOUDMARK®
Intelligent Network Security

Product Datasheet

Cloudmark Insight Features 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's core threat cataloging systems

Ability to analyze and return data associated with pre-calculated Cloudmark Authority fingerprints

High Performance REST API

Scan performance suitable for integrating real time scanning into your application

Scalable, geo-redundant cloud-based API service

A Direct Line into Industry-Leading Threat Intelligence

The Cloudmark Insight Features 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.

The Insight Features API is intended to be leveraged by customers who run the Cloudmark Authority Engine, or process feedback loops that include analysis headers inserted by remote systems that run Cloudmark Authority. The service is offered as a cloud-based REST API that offers a direct query capability into Cloudmark's core threat intelligence systems, enabling programmatic analysis of these previous calculated fingerprints.

Visibility into Cloudmark's Current and Past Threat History

Previously calculated Cloudmark Authority analysis strings and individual fingerprints can be queried via the straightforward REST API, providing both a current and historical overview of the fingerprint status and granular categorization. Categories exposed include:

- Legitimate – Content represents clean messaging campaigns
- Spam – Matches content used in spam campaigns
- Phishing – Matches content used in phishing campaigns
- Virus – Malware attachment detections
- Compromised – Matches URLs hosted on known compromised web sites

Spamtrap and End User Feedback Statistics

In addition to verdict and categorization information, summary information regarding the queried signature data, the times and dates associated with initial false positive or false negative reports, most recent traffic reports, and changes in state are also accessible. This data can provide insight into spamtrap hits for specific mailings, relative volumes, and the count of Cloudmark customer organizations reporting traffic. Result data includes the rate of block reports from the Cloudmark community, as well as the percentage of reports collected by spamtraps.

Cloudmark Insight Features API Solutions

Mailbox Service Providers

Providing support for email issues can account for a significant amount of support tickets. To decrease support resolution times, it must be possible to quickly review the problem and evaluate what the issue might be. By integrating the Insight Features API directly into helpdesk tools used by customer service representatives (CSR) for live troubleshooting during customer support calls, it will be possible to integrate email troubleshooting into the CSR workflow. This enables the CSR team to provide immediate feedback on message categorization questions the caller, enabling issues to be addressed on the first call.

Hosting Providers

Hosting providers deal with significant abuse issues due to fraudulent signups which attackers leverage to send abuse traffic out from the provider's environment. These attacks result in abuse reports that are forwarded from remote systems. Gain valuable insight into the types of content being sent by analyzing Authority fingerprints contained within feedback loop traffic. Leverage data to investigate fraudulent or compromised account behavior. Data provided by the Insight Features API is helpful to provide backing evidence for fraudulent account shutdowns.

Marketing Email Service Providers

Evaluate reasons for content being rejected or tagged as spam at remote service provider delivery destinations that run Cloudmark Authority software by processing Cloudmark header data contained within feedback loop (FBL) data. The query result data can be used to continuously evaluate local marketing customer accounts for proper sending practices, sending account credential compromises, and for flagging accounts for sending practice improvement consulting.

Security Providers

Use Cloudmark Threat Intelligence to increase the confidence of their automated decision making process and obtain historical information on abuse resources from the email domain. Leverage Cloudmark's data as another dimension of threat analysis within your threat analysis investigations.

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