CLOUDMARK®
Intelligent Network Security

Product Datasheet

Cloudmark Insight Crawler 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

Insightful Data for Your Business

Compromised systems are blind spots in the network that continue to be the safe haven for cyber criminals. Threat analysis for emerging threats need the in depth insight into the abuse to identify the bad actors and effectively mitigate them. One of the biggest challenges today is managing all of this unstructured data to provide some useful insights. Emerging and sophisticated techniques make breaches even harder to be detected, leaving IT teams striving to protect their public facing digital assets against fraud and abuse

Most compromised web sites for recent spam outbreaks, were used to redirect users to destinations with malicious contents. Short URLS are commonly leveraged for abuse to redirect users to malicious websites.

Increased spam complaints, reduced open rates and email visits could result in a failed email marketing campaign even if it was legitimate, if the contents indicate spam or phish. Email marketers for top brands loose their sending reputation due to such contents which results in a significant loss of opportunities and a negative return on investment.

Hosting providers and cloud service providers incur huge costs dealing with abuse such as spam, spamvertising, phishing, hacked websites, malicious signups etc. which result in complaints, tear down requests and a malicious site reputation.

Cloudmark Insight API for URL Scanning

The Insight Crawler API provides a cloud-based REST interface for your anti abuse solutions to make live queries into Cloudmark Global Threat Network. The Cloudmark Crawler API transforms unstructured data to structured data for creating an actionable intelligence for your applications to make granular policies based on the scanned results and reputation scores. Cloudmark URL scanning provides the in depth analysis of the url and all the redirects within the landing web page ensuring a complete scan of the contents for the requested URL than just a top level domain analysis.

Smarter Approach to Abuse

Email Service Providers

Delivery, click through and open rates are immensely impacted if the recipient senses an abuse in the campaign. While this could be a legitimate engagement, it can be marked as spam due to spam or phish contents or weblinks to malicious sites. Why compromise on the ROI and reputation with all your subscribers. Insight Web Crawler API solves the problem by using the knowledge gained in malicious message

campaigns seen globally through our threat network. Integrate the Insight URL Crawler API directly into your marketing message sending platform to scan messages for malware or links to malicious websites being sent by your customers. The query result data will be useful for your spam testing tools to identify if there are any malicious/spam/phish URLs present in the contents, thus improving your deliverability rate and reputation.

Communication Provider as a Service (CPaaS) Providers

The need for contextual communication to improve the overall customer experience has driven the CPaaS market which aligns well with the emerging trends of customer engagements. Companies that provide API-driven messaging systems are susceptible to being abused by spammers who use these platforms to reach their targets via SMS, mobile app notifications, or other non-email destinations. The query result data will be useful to identify short URLs that could redirect to malicious web sites or links to some botnets.

Web Hosting Providers and Website Owners

Attackers who are allowed to sign up trials or otherwise free tier accounts, will leverage those systems for the sole purpose of hosting spam/phish/malicious websites, or to support redirects to phishing sites via the 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 websites in an attempt to see if the landing page contains spam, malware, or phishing contents. Insight Web Crawler API can integrate with your anti-abuse platforms to identify redirects on your web pages or if it is compromised. Identify masquerading web sites that might be hosted on your systems or masquerading your website for reporting abuse and add granular policy controls to deter redirections to these sites.

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