CrowdStrike Store

OPSWAT.

CROWDSTRIKE

Data Sheet

OPSWAT: METADEFENDER CLOUD MALWARE ANALYSIS

Providing real-time hash, IP and domain analysis using advanced threat prevention, detection and binary reputation technologies

CHALLENGES

Malware analysis is a very difficult task that requires state-of-the-art technology and constant updates, but security teams often lack processing and tracking resources. When analyzing a file, many security analysis tools are available, making the selection process difficult.

SOLUTION

OPSWAT MetaDefender Cloud provides real-time hash, IP and domain analysis and reports using advanced threat prevention, detection and binary reputation technologies. This cloud-based cybersecurity threat detection and prevention solution uses 20+ anti-malware engines, easily integrates with the CrowdStrike Falcon® platform and is available in the CrowdStrike Store. Additional engines provide exponential malware detection, increasing your set of heuristic tools and giving you access to the latest artificial intelligence (AI) detection technologies on the market. One easy-to-use platform generates detailed findings and reports with certainty as high as 99.5% within milliseconds.

BUSINESS VALUE

Use Case/Challenges	Solution	Benefits
There is often too much malware to analyze with given resources. Security teams need to track a multitude of data points to identify infections or weaknesses as soon as possible.	OPSWAT provides a scalable solution that includes a summary of multiple anti-malware engines working together to track, analyze and report any risks as they appear.	Quickly and easily multi-scan files for threats using multiple industry-leading anti-malware engines. Process files quickly. Access reputation information for IP and domain requests.
Technical decision makers face a real challenge when evaluating cybersecurity solutions: lack of expertise using all product capabilities; paid on-premises proofs of concept (POCs); forced to purchase first paid POC; and reliance on vendor reputation.	OPSWAT offers a free POC that is available in the CrowdStrike Store — it's fast to integrate and easy to use.	The integration between CrowdStrike and OPSWAT is security-tested and proven. Two teams of malware experts are ready to guide and troubleshoot any problem.

KEY BENEFITS

Content enrichment and effective detection, leveraging threat analysis from 20+ anti-malware engines

World-class threat intelligence database with billions of hash, IP and domain data points

Malware analysis history and evolution of detection trends for easy decision-making during incident investigations

End-to-end secure information handling across Falcon and MetaDefender Cloud platforms

TECHNICAL SOLUTION

The CrowdStrike® Falcon platform uses OPSWAT MetaDefender Cloud to access the hash, IP and domain analysis and history of a file, providing more context enrichment around file reputation. Falcon queries MetaDefender Cloud securely via HTTPS as a request that is processed by multiple anti-malware engines and analyzed using the knowledge base of the OPSWAT threat intelligence community. In return, information such as the number of anti-malware engines that flagged the file, malware type, IP analytics, domain reputation and the hash's history report are sent back to Falcon via HTTPS. Falcon displays this information in the Falcon management console as "intel cards." These cards have links back to the MetaDefender Cloud website, where you can access additional threat intelligence reports about the file. Based on 20+ anti-malware engines, a comprehensive file analysis report is generated to help with deeper event investigation.

ABOUT OPSWAT

OPSWAT is trusted by over 1,500 organizations spanning the globe. OPSWAT is a global leader in critical infrastructure cybersecurity that helps protect the world's mission-critical organizations from malware and zero-day attacks. To minimize the risk of compromise, OPSWAT CIP solutions enable both public and private organizations to implement processes that ensure the secure transfer of files and devices to and from critical networks. More than 1,500 organizations worldwide spanning financial services, defense, manufacturing, energy, aerospace and transportation systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations; and protect their reputations, finances, employees and relationships from cyber-driven disruption.

Learn more: **https://www.opswat.com/**

KEY CAPABILITIES

Generate file hash scan results from multiple anti-malware engines

Access a large dataset of scanned files, IP addresses and domain data points from OPSWAT's global malware intelligence community

View a hash scan history report with trends of malware discovery and global surfacing

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:
https://www.crowdstrike.com/

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
https://www.crowdstrike.com/free-trial-guide/

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**