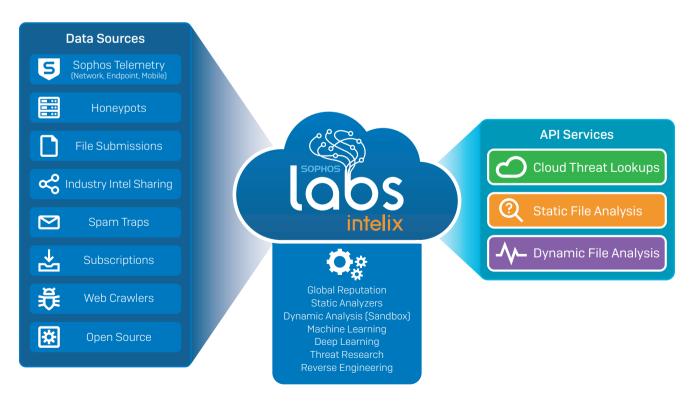**SOPHOS**

SophosLabs Intelix™

RESTful, Integrable, Real-Time Threat Intelligence

Powered by machine learning, decades of threat research, and petabytes of intelligence, SophosLabs Intelix gives your app superpowers to identify, classify, and prevent threats. Designed for easy integration into any application, augmenting your cybersecurity is only an HTTP request away.

SophosLabs Intelix™ Platform

Hosted on the AWS Marketplace, our analysis platform uses layers of analytics across a suite of RESTful APIs to identify known and potential threats, reduce unknowns, and derive verdicts and intelligence reports for the most commonly used file types. To achieve this, we use a combination of AI models in static and dynamic analysis modes, deterministic detections, and an array of granular threat analyzers, underpinned by SophosLabs 24/7/365 global threat research and data science research.

The SophosLabs Intelix™ platform approach differentiates itself in the industry by offering programmatic access to both the vast troves of existing SophosLabs intelligence as well as the ability to conduct analysis in real time and generate new intelligence. Covering a broad range of file formats commonly used in attacks, as well as URLs and Android APKs, SophosLabs Intelix™ enables turn-key cybersecurity threat expertise.

Data Sources

- Sophos Telemetry (Network, Endpoint, Mobile)
- Honeypots
- File Submissions
- Industry Intel Sharing
- Spam Traps
- Subscriptions
- Web Crawlers
- Open Source

SOPHOS labs intelix

Global Reputation
Static Analyzers
Dynamic Analysis (Sandbox)
Machine Learning
Deep Learning
Threat Research
Reverse Engineering

API Services

- Cloud Threat Lookups
- Static File Analysis
- Dynamic File Analysis

SophosLabs Data Sources and Data Curation

Highlights

‣ Harness the power of 30-plus years of SophosLabs experience in threat analysis and research

‣ Leverage SophosLabs threat intelligence services actively used in Sophos products

‣ RESTful APIs, with easily decomposable JSON responses

Breadth of Data

‣ Disparate and complementary data sources with global visibility, consolidated

‣ Sophos product telemetry derived from network and endpoint

Data Quality

‣ Data curation process to reduce false positives

‣ Continuous PE file and URL reputation assessment

Data Science

‣ Powered by industry-leading data science research

‣ Deep learning using feed-forward, convolutional, recurrent, and policy gradients

‣ Transfer learning and domain adaptation

Stand on the Shoulders of Giants

Augment your security by tapping into the intelligence that powers Sophos.

SophosLabs Intelix™ is developed by the critically acclaimed, global Tier-1 threat research lab, SophosLabs, and used in all of Sophos' industry leading cybersecurity solutions.

Never Trade Security for Performance

Triage threats with rapid lookups. Deep dive with granular file analysis.

With our progressive suite of intelligence APIs, quickly identify known threats via Cloud Threat Lookups before moving on to file uploads for detailed analysis with both static or dynamic file analysis.

More Than Just Answers – We Give You Intelligence

Get real-time answers to the hardest to answer questions.

Rich intelligence reports provide you with more than just the good, the bad, and the unknown but also actionable insight into the nature and capabilities of a threat through the use of data science and SophosLabs research.

Three Easy-to-Use Services
Cloud Threat Lookups

Quickly identify known threats via direct access to the latest SophosLabs threat intelligence, queried using suspect malware file hashes, URLs, or Android APKs.

Glean the global reputation and malicious detection for file hashes and Android APKs and reveal the productivity category, security category, and risk level of a URL.

Static File Analysis

Harness the power of multiple machine learning models, global reputation, deep file scanning, and more without needing to execute the file in real time.

These static analyzers generate rich reports, including industry-wide detection coverage, and ensure speedy analysis to determine a verdict or identify files that need further analysis via dynamic file analysis.

Dynamic File Analysis

Detonate malware in real-time in a sandbox utilizing the latest analysis techniques for unmatched visibility into malicious files among the unknown. Every activity and behavior is recorded to reveal the true nature and capabilities of a potential threat.

Advanced anti-evasion technologies thwart malware that attempts to detect if it's in a sandbox or running in a virtual machine, leaving malware with no place to hide.

Try it today:

Search for **SophosLabs Intelix** on the AWS Marketplace

For more information please visit **sophos.com/intelix**

SOPHOS