SophosLabs Threat Intelligence

The threat landscape continues to evolve as bad actors engage in targeted and sophisticated tactics, techniques and procedures with common tools and proven attacks. In 2018, SophosLabs observed several advanced trends, which we believe will play a significant role in new cyber-attacks: from the continued adoption of manual attack techniques by ransomware gangs, the steady increase in malicious deployment of cryptocurrency miners, to mobile platform and growing IoT exploits.

Security organizations must often increase the volume of data feeds they purchase as a method to complement their existing data sets. But instead, they are increasing the number of false positives in their security systems through the acquisition of un-curated data. SophosLabs' threat research team and highly automated infrastructure utilizing next-generation tools, has developed high-accuracy, distinctive and often exclusive data sets that are now available commercially and can help improve detection and response capabilities.

The Global Strength of a Tier-1 Lab

With over three decades of advanced malware analysis, SophosLabs threat research lab delivers industry-leading threat intelligence with performance, scalability and flexibility to meet partners' security workflows so they can focus on what they do best.

300,000-plus daily
suspicious URLs analyzed

500,000-plus daily
previously unseen files analyzed

80% of malicious URLs
come from legitimate websites

2,000-plus daily
previously unseen Android apps analyzed

50 million
files for Neural Network genetic similarity comparisons

600 million daily
Live Protection lookup events added to data lake

30,000-plus daily
malware samples added to Live Protection cloud

300 million
files used for Machine Learning model training

SophosLabs worldwide threat research infrastructure tracks malware trends and cyber threats across geographies.

Breadth of Data

- Disparate and complementary data sources with global visibility
- Sophos product telemetry derived from network and endpoint
- Mid-market centric data

Data Science

- Security machine learning
- Deep learning using feed-forward, convolutional, recurrent, and policy gradients
- Transfer learning and domain adaptation

Data Quality

- Data curation process to reduce false positives
- Continuous PE file and URL reputation assessment

SOPHOS

SophosLabs Analysis Platform

Our analysis framework uses layers of analytics to reduce unknowns with the goal

of deriving verdicts and intelligence reports in seconds for most commonly used file types. To achieve this, we use a combination of signature-based detections, granular threat analyzers and AI models in static and dynamic analysis modes. All our analysis output is used in our Sophos products.

The SophosLabs Analysis Platform approach differentiates itself in the industry and offers comprehensive file intelligence and URL analysis with an aggressive roadmap for support of a variety of other types of threat object submissions.

Threat Intelligence is consumed through APIs that securely connect to our cloud platform, or through data feeds.

SophosLabs Data Science Difference

Prevalent anti-malware detection technologies are effective at identifying malware with specific characteristics. In-line products do not have the resources to expediently identify and analyze files outside the blue lines in Figure 2, invariably letting through sophisticated malware. By adding deep learning techniques, such as feed-forward, convolutional, recurrent, and policy gradients we can identify files with suspicious attributes like those found in malware depicted inside the orange lines in Figure 3.

In this way, we expand the efficacy of the anti-malware solution to convict many polymorphic malware variants that would otherwise have gone undetected.

Figure 1: Prevalent anti-malware technologies

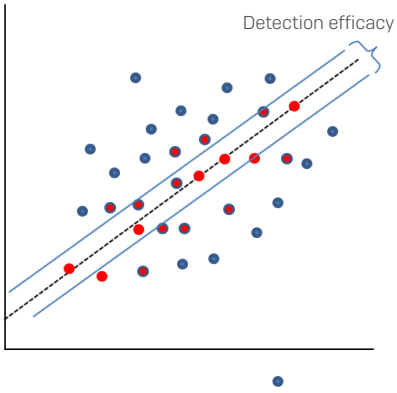
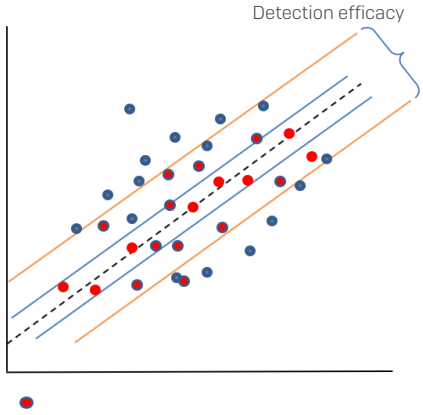


Figure 2: SophosLabs AI assisted detection



- Harness the power of Sophos Labs' 30-plus years of experience in threat analysis and malware reversing
- SophosLabs threat intelligence services are actively used in Sophos products
- SophosLabs submission logic helps you determine suspicious files requiring further analysis
- Receive verdicts quickly to help Web and Email Gateway and cloud products make faster block/pass decisions
- Get detailed intelligence reports for EDR, MDR and IR use cases
- Threat analysis process using progressive analysis techniques with a combination of traditional threat analyzers and neural network modeling

Data Sources and Curation

It all starts with aggregating telemetry from Sophos network, endpoint and mobile products with a variety of complementary data sources to gain global visibility. Our automated curation deduplicates entries, categorizes threat objects, reduces false positives and updates reputations. Conflicting threat data is escalated for review by our threat experts.

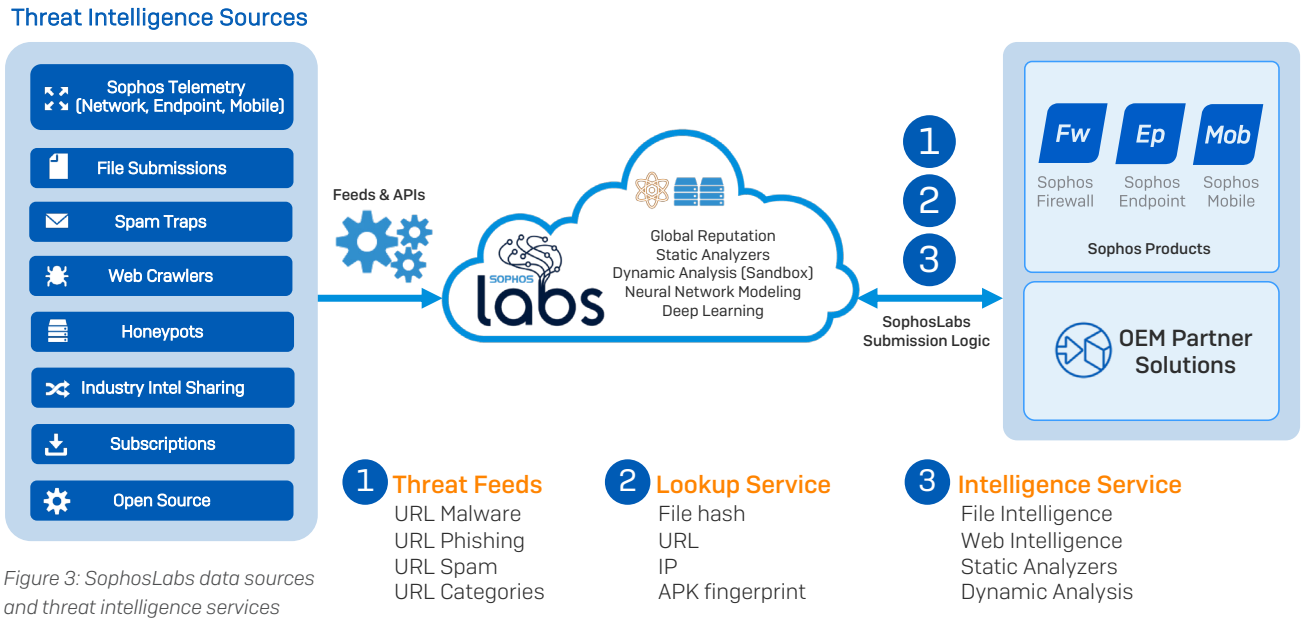


Figure 3: SophosLabs data sources and threat intelligence services

Feeds

Malicious URLs

The malicious URL feed from SophosLabs offers a significant percentage of unique/complementary data to others in the industry. Instead of large volumes of raw data, our goal is to provide accurate threat intelligence with curated malicious URLs to improve uniqueness and quality.

Prevalent Categories	Domain	URI	Description
Malware Repositories	3 million+	60 million+	Known bad sites designed to spread malware
Malware Command and Control	670,000	160,000	Known bad sites
Infected Sites with Malicious Redirects	16,000	27,000	Previously clean sites that are found to contain malware redirects
Potentially Unwanted Apps (PUAs)	19,000	2 million+	Links with suspicious apps
Phishing Sites	560,000	2 million	Known and zero-day phishing sites and links
Email Spam Websites	1 million+	52,000	Known and zero-day spam sites

Web Categorization – Productivity and Compliance

The URL database is populated by hundreds of millions of daily searches through Sophos' customers and partners. It is comprised of 80-plus categories and supports any language.

For optimization, hundreds of URI paths belonging to the same website may be rolled up under one domain/subdomain entity, except for URI paths that are classified under a different category than their parent domain. This organization makes the database much smaller than classifying each unique URI path, more efficient, and very fast.

Use Cases

Web Filtering, Auditing, Policy, Compliance

Common Products and Services

Gateway and Cloud: NGFW, UTM, Email Security

Benefits

- Audit and enforce web usage corporate policy requirements
- Filter potentially unwanted apps (PUA)
- Optimize query speed with a local database of productivity URLs

Cloud Lookup Services

File Malware, Malicious URLs, Productivity URLs and Android (APK) Fingerprints

This service complements real time anti-malware solutions with the latest threat data which may have not yet been updated locally for real-time protection. By initiating a lookup for unknown file hashes, URLs, and APKs, your solution will mitigate protection gaps.

SophosLabs maintains a significant, global database of all known-bad threat objects it has identified using a combination of threat analytics and machine learning. This threat data is available here before it finds its way on the threat database resident on the product.

All lookups to the service are accessible using a single Protobuf API, which is published in our Cloud Lookup Service SDK. Sophos OEM technical experts assist partners with API integration, testing, and ongoing support.

	File Malware	Malicious URLs	Productivity URLs	APK Fingerprints
Size (2018)	One billion-plus	60 million	28 million	19 million
Updates	2,500	800	1,500	100
Frequency	One minute	Six minutes	One day	10 minutes

Supported file types:
.exe, .dll, .doc, .docx, .docm, .xls, .xlsx, or .xlsm, .ppt, .pptx, .pptm, .rtf

Use Cases

Blocking, Threat Hunting

Common Security Products and Services

- Gateway and Cloud: NGFW, UTM, Email Security, EDR
- SOCaaS, MDR

Benefits

- Access to the latest available SophosLabs threat intelligence
- Immediate response times
- API consumes low on-device resources
- No need to maintain a local threat database

Cloud File Intelligence

SophosLabs performs extensive analysis on over 500,000 unique files daily.

File types are verified using True File Type (TFT), a Sophos file scanning technology, to determine what the file is regardless of its extension.

All file submissions to the service are accessible using a single RESTful API, which is published in our Cloud File Intelligence Service SDK. Sophos OEM technical experts assist partners with API integration, testing, and ongoing support.

Static Analysis

SophosLabs provides granular static analyzers to drastically speed up verdict outcomes and deliver rich intelligence reports. Through the combination of traditional threat analysis techniques and heavy use of machine learning models, SophosLabs can deliver verdicts in seconds for common file types.

Key Features

Machine Learning Models	Malware Detection and Reputation	Advance File Information
‣ Genetic Similarity ‣ File Path Similarity ‣ Malicious Attributes	‣ PE File Reputation ‣ Deep file scanning – yara, antivirus ‣ Industry detection coverage	‣ File properties and metadata ‣ Author, Date, Locales, Languages, File format version, Size, page count, Presence of links, Presence of active content (macros, forms, etc.), OLE objects, signatures

Supported file types:
.exe, .dll, .doc, .docx, .docm, .xls, .xlsx, or .xlsm, .ppt, .pptx, .pptm, .rtf

Supported file types:
.exe, .dll, .doc, .docx, .docm, .rtf, .xls, .xlsx, .xlsm, .ppt, .pptx, .pptm, .pdf, .xml, .mso, .zip, .bzip, .gzip, .rar, .tar, .lha/.lzh, .xz

Use Cases

Blocking, Intelligence/Reporting

Common Security Products and Services

- Gateway and Cloud: NGFW, UTM, Email Security, EDR
- SOCaaS, MDR, IR/Investigations

Benefits

- Advanced detection of never-before-seen files, including Office docs, PDF, PE, XML, Archives, etc.
- Derive verdicts and intelligence in seconds (when possible)
- SophosLabs smart logic helps you identify suspicious files to programmatically submit for further analysis
- Scalable to secure any size network

Dynamic Analysis (Cloud Sandbox)

SophosLabs Cloud Sandbox utilizes the latest analysis techniques to identify malicious files for unmatched visibility into unknown files.

Key Features

Malware and Potentially Unwanted Apps (PUA) detections	Known Malware Families	Other Malicious Behaviors
‣ Sophos antivirus file and memory detections ‣ Sophos Intercept X machine learning, CryptoGuard, and WipeGuard technologies	‣ Yara patterns deep memory scans ‣ Behavior patterns – IOCs attributed to malware	‣ Evasion – anti-sandbox and anti-virtual machine tactics ‣ Cryptomining ‣ Deception technology

Supported file types:
.exe, .dll, .doc, .docx, .docm, .rtf, .xls, .xlsx, .xlsm, .ppt, .pptx, .pptm, .pdf, .xml, .mso, .zip, .bzip, .gzip, .rar, .tar, .lha/.lzh, .xz

SophosLabs Data Privacy and Retention

- Customer data submissions to SophosLabs are stored and processed in three regional data processing units in Europe, North America, and Asia Pacific, so that customers can keep their data within their region
- These regional units are built as sealed units to ensure we have clear PII boundaries for customer data
- SophosLabs may check the hash of a customer-submitted file with external threat intelligence sources, but we do not share the actual file with third parties
- SophosLabs retains all classified malicious files and deletes cleans files in a timely manner

For more information about our security policy visit
https://www.sophos.com/en-us/legal/sophoslabs-information-security-policy.aspx

For more information
Please visit Sophos.com/oem

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

22-03-15 DS-NA (MP)

SOPHOS