CYREN

Cloud Threat Lookup

Advanced Threat Protection

Get instant evaluation of your file hash queries from Cyren's real-time global security cloud

Cyren's threat lookup service is a 100% cloud-based solution that allows service providers and Cyren solution partners to conduct a file integrity check and get up-to-moment classification of malware threats based on Cyren's global threat intelligence, integrating a powerful security layer via Cyren's Cloud Threat Lookup API for enhanced email protection, web protection, endpoint protection or breach response.

Unmatched detection depth, breadth and speed

Today's malware threats are altering their behavior along numerous dimensions in order to avoid detection by traditional technologies, requiring a new level of sophisticated analysis. Cyren's GlobalView™ security cloud processes 25 billion internet transactions a day and performs rich correlation across multiple detection vectors to block over 300 million threats daily, giving you the ability to categorize billions of malware hashes with an expected response time of just 90 ms per query.

Easily deployed and privacy-law compliant

As a cloud-delivered service, Cyren's Threat Lookup can be quickly deployed, requiring minimal set-up and configuration of the API calls, and it scales easily and automatically utilizing Cyren's highly elastic global cloud infrastructure. The only prerequisites for using the service are connectivity to threatlookup.com via HTTPS and possession of a token API Key.

The service allows the option of utilizing only regionalized infrastructure in the European Union or the United States, guaranteeing compliance with EU laws and legislation (GDPR). Cyren controls all analysis end-to-end, so samples or analysis data are not shared or uploaded to any third parties.

Cloud threat lookup integration points can include:

- In-network or proxy server
- Firewall, NGFW, UTM or appliance
- Email server (MTA)
- Content scanner (email framework such as amavisd)
- Advanced threat protection like sandboxing and queuing

Threat Intelligence

The Cyren Cloud Threat Lookup Difference

Superior Detection

- Cyren's GlobalView™ security cloud provides some of the leading technology and security vendors — including Google, Microsoft, IBM, Check Point and Fortinet — with the fastest and most accurate threat data and detection technologies in the industry.

Unlimited Scalability

- As Cyren's layered threat intelligence stack is purpose-built for cloud computing across Cyren's global infrastructure, it allows us to scale easily, utilizing highly elastic computing power to identify malicious behavior with both greater depth and speed while supporting large query volumes.

Fast Analysis

- With a 90 ms expected response time per query, hash classification is nearly instantaneous.

Google Microsoft Check Point SOFTWARE TECHNOLOGIES LTD. SONICWALL Deutsche Telekom

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

CYREN

CLOUD THREAT LOOKUP

Advanced Threat Protection

Enhanced Threat Lookup

As a service option, Enhanced Threat Lookup provides the ability to upload files and further enhance detection by applying anti-malware heuristics and static code analysis. It consists of three phases: 1) Hash lookup, 2) File upload, and 3) Check hash. If your license includes the "Enhanced Threat Lookup" package, an "upload_sample" URL will be returned which can be used to upload and submit the relevant file for further analysis and processing.

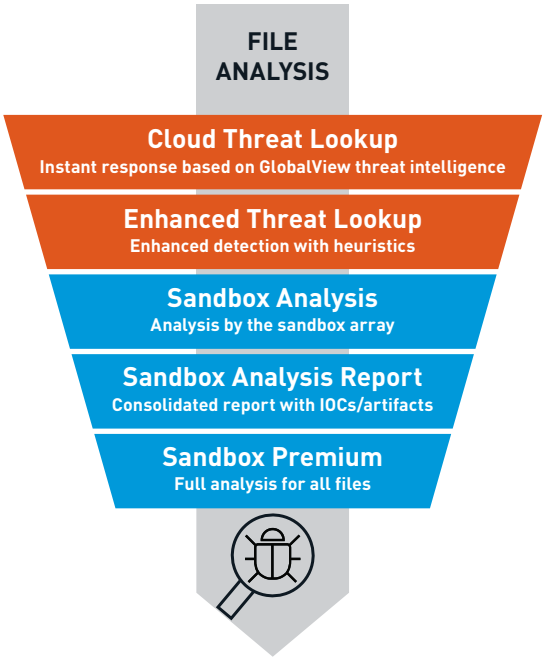
Option for dynamic analysis with sandbox array

Cyren's Cloud Threat Lookup Service is integrated into a full malware analysis stack that includes Cyren's cloud sandbox array, allowing if desired layered treatment of objects uploaded for analysis and giving service providers, ISV's and appliance manufacturers several options in selecting the depth of analysis which best meets their objectives, thus guaranteeing efficiency in the return of results.

How the threat lookup service works

Files or file attachments are presented to the API by computing a hash of the file in SHA-256 format and sending the hash to the cloud. Note that no personally identifiable information goes to the cloud. Upon receiving a valid request, the service responds with information about the provided hash, classifying as malware (and giving the threat name), a potentially unwanted application, or, if a known, clean file, "Confirmed clean."

THREAT LOOKUP SERVICE PACKAGES



SUPPORTED FILE TYPES

Windows executable files, Mac files, Microsoft Office, PDFs, Flash files, Scripts, Archive files

THREAT LOOKUP RESPONSE CODES

Description	response_code	http_status_code	message
When user submits invalid sha256	-1	200	Unsupported checksum type
Sample was already uploaded	1	200	Already uploaded. Process in progress
Non-existent route caught by the routing engine	0	200	API Version x.x, unknown call
When sha256 is missing from the API call	-1	400	Missing or malformed parameters!
Sha256 of the file submitted doesn't match the sha256 submitted through API	-1	400	SHA256 hash mismatch
Empty file was delivered to API.	-1	400	Empty file! Aborted
Sandbox artifact cannot be displayed due to insufficient permission or wrong ownership	-1	401	Access denied!
Sandbox artifact not found on the file system.	-1	404	No such resource found!
Disallowed characters in API call	-1	404	Unknown or malformed call
If any of the backend runs unexpectedly, and was not caught by the API handlers	-1	500	Internal system error. Contact the system administrator