

Threat Intelligence Feed File Reputation

Avira's Threat Intelligence Feeds enhance your own threat intelligence services by giving you access to the data at the heart of Avira's anti-malware solution. They create the opportunity to develop a proactive security position and react to emerging threats before they reach your infrastructure. Avira's Threat Intelligence Feeds provide you with regularly updated file and URL reputation data, delivering the intelligence you need to build powerful and effective threat detection systems.

Threat intelligence feeds deliver 'over-the-horizon' visibility to emerging threats. Avira's file and URL feeds allow you to see what Avira has just detected and enable you to act before you or your customers are impacted by new malware or malicious domains. They bring value to your own business by providing access to the data collected and analyzed by Avira's world-wide sensor network and powerful malware detection engines. Avira's Threat Intelligence Feeds are unique because they provide comprehensive intelligence that has a high degree of relevance to security vendors and service providers.

Avira's Threat Intelligence Feed services include

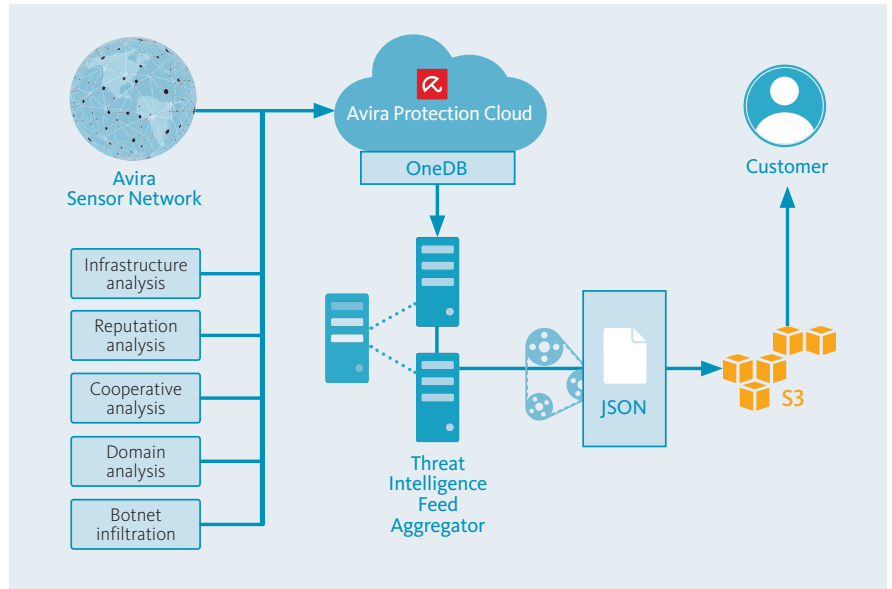
- File reputation
- URL reputation
- Bespoke intelligence feeds

Avira's File Reputation feed delivers a stream of constantly updated threat data drawn from the **Avira Protection Cloud**. The data is delivered as a simple-to-access fixed format JSON hosted in the Amazon S3 cloud and is updated every 60 seconds. It contains over 30 key attributes of clean and malware PE files including: detection, full chain certificates, analysis tags, and

SIMPLE	VALUABLE	SECURE & RELIABLE	BENEFITS
Data delivered in a simple to consume, JSON format	Over 35 file attributes Data drawn from Avira's 500million+ network of businesses and consumers, world-wide	Hosted in a secure Amazon S3 storage	Compliant to data privacy laws; build security without sharing your customers' data
Decoupled, no API or SDK required	Provides near-real time updates covering Zero-day threats	Non-disruptive service updates on a high availability platform	Delivers early warning of threats as they emerge world-wide
Platform agnostic implementation	Dedicated support	Non-intrusive, does not require Avira to have on premise access	Automated feeds minimize integration work
Complete documentation and usage samples			Data set delivered by an award-winning market leader
Simple access and licensing			Leverages Avira's detection technologies in a simple to use way

specific PE attributes, each selected to enable partners to take actionable decisions. The information provided does not contain any personally identifiable data or the file itself. Only meta-data resulting from the analysis is delivered to ensure data privacy.

Avira's Threat Intelligence Feeds are delivered as de-coupled, non-intrusive services: they do not need special code or infrastructure (SDK or API) to be implemented, or require Avira to access customer infrastructure to enable the service.



Specifications table

Field Group	Typical content
Detection	Classification of the file with multiple different values. This has about 50 possible values, including MALWARE, CLEAN, PHISH, RKIT, etc.
	Additional level of confidence for the classification, detection type, time, detection name, additional data
Meta	Multiple file hashes
	File format (MIME)
	Size, first-seen timestamp, submission source
	Tags associated with the file as result of internal analysis (multiple values). This has values from a list of almost 300 tags, with values like: code-hook, obfuscated-calls, unaligned-headers, encrypted, damaged, execryptor, keyhook, etc.
PE	Software product information, file information, company name, version, description, timestamps
	PE format file details and detailed file full-chain certificate validity analysis with revocation check, including upstream certificates up to certificate root

Contact Avira

Europe, Middle East, Africa

Avira
 Kaplaneiweg 1 | 88069 Tettngang
 Germany
 Tel: +49 7542 5000
 Email: oem@avira.com

Americas

Avira, Inc.
 c/o WeWork
 75 E Santa Clara St., Suite 600, 6th floor
 San José | CA 95113 | United States
 Tel: (800) 403-5207 | Email: oem@avira.com

Asia / Pacific and China

Avira Avira Pte Ltd
 50 Raffles Place
 32-01 Singapore Land Tower
 Singapore 048623
 Email: oem@avira.com

blog:

insights.oem.avira.com

www:

oem.avira.com