Avira

Threat Intelligence Feed File Reputation

Avira's Threat Intelligence Feeds enhance your 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, reacting to new and emerging threats before your customers encounter them. Avira's Threat Intelligence Feeds provide you with file and URL reputation data, updated regularly, delivering the intelligence you need to build powerful and effective threat detection systems.

Threat Intelligence Feeds deliver 'over-the-horizon' visibility to emerging threats. They allow you to see what Avira has just detected, and enable you to take action before you or your customers are impacted by new malware. They add value by improving detection efficacy, and reducing the time taken to collect, organize, collate and analyze threat data. Avira's Threat Intelligence Feeds leverage the world-wide coverage and powerful malware detection engines that deliver Avira's award winning services.

Avira's Threat Intelligence Feed services include

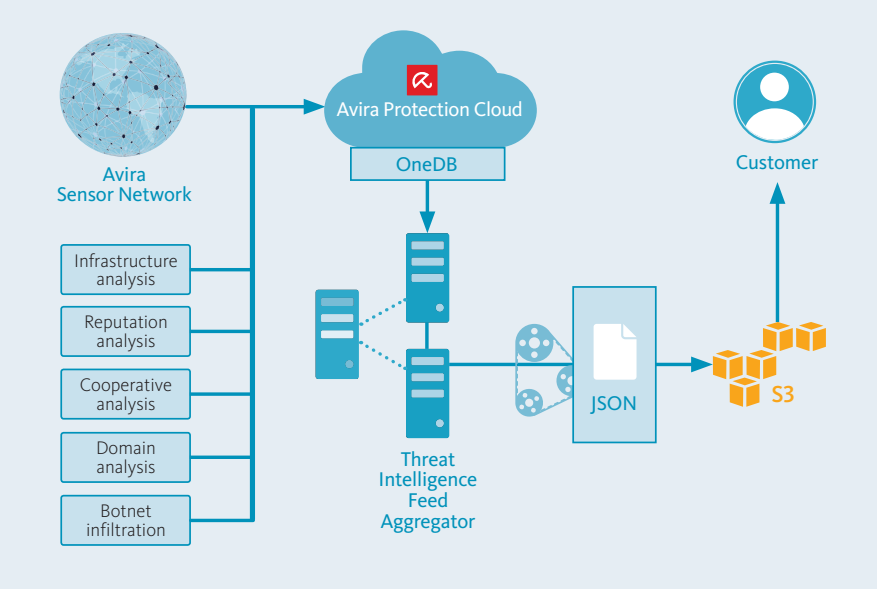
- File reputation
- URL reputation
- Bespoke intelligence feeds

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 30 file attributes	Hosted in a secure Amazon S3 storage	Delivers early warning of threats as they emerge world-wide
Decoupled, no API or SDK required	Data drawn from Avira's 100million+ network of businesses and consumers, world-wide	Non-disruptive service updates on a high availability platform	Automated feeds minimize integration work
Platform agnostic implementation	Provides near-real time updates covering Zero-day threats	Non-intrusive, does not require Avira to have on premise access	Data set delivered by an award-winning market leader
Complete documentation	Dedicated support		Leverages Avira's detection technologies in a simple to use way
Simple licensing			

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
Meta	Multiple hash types of the file
	MIME type
	Size, timestamp, 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.
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
PE	Software Product name version, description
	PE format file details and associated certificates

Contact Avira

Europe, Middle East, Africa

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

Americas

Avira, Inc.
330 Primrose Rd. | Suite 610
Burlingame | CA 94010 | USA
Tel: (800) 403-5207
Email: oem@avira.com

Asia / Pacific and China

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