



# FILE REPUTATION API

## ZERO-DAY AND ADVANCED PERSISTENT THREAT DETECTION

At the core of Avira's award-winning security solution lies the Avira Protection Cloud – a global cloud-based security service powered by NightVision™, Avira's advanced machine learning system.

Accessed via the File Reputation API, or used in combination with Avira's Anti-malware SDK (SAVAPI), the Avira Protection Cloud delivers >99.99% malware detection on devices, appliances and services.

The File Reputation API offers technology partners and service providers a fast, simple and highly effective way to add the industry's leading anti-malware capabilities to their own solution.

A REST API enables technology partners to either submit a file hash for evaluation, or upload a file to the Avira Protection Cloud for analysis. Hash inquiries are evaluated, and a result returned within tens of milliseconds. If the hash is unrecognized, the suspicious file can be sent to the Avira Protection Cloud for full analysis. File uploads are assessed and a response containing the classification returned. Analytical techniques used include a powerful cloud scanning engine using unreleased generics and heuristics, classification by Avira's NightVision machine learning system, and unpacking and detonation by innovative Dynamic File Analysis technology. As new analytical methods are developed, they are integrated within the Avira Protection Cloud and brought online without requiring integration by technology partners.

### Key features:

- Accessible using a REST API, the Avira Protection Cloud offers support for different platforms.
- Cloud-based service delivers availability, reliability and scalability
- Powerful hash evaluation technology and a database of over a billion entries provides real-time comparison with known threats.
- Zero-Day and advanced persistent threat detection.
- Avira's Cloud Scanning Engine uses powerful and extensive rules to classify malware within seconds.
- An advanced machine learning system with multiple algorithms based on data containing thousands of attributes of suspicious and clean files simultaneously.
- Virtualized environments that sandbox and emulate many key OS systems used to detonate malware that may hide from other analytical techniques.
- Architected for both premise-to-cloud and cloud-to-cloud integration

## INTEGRATION

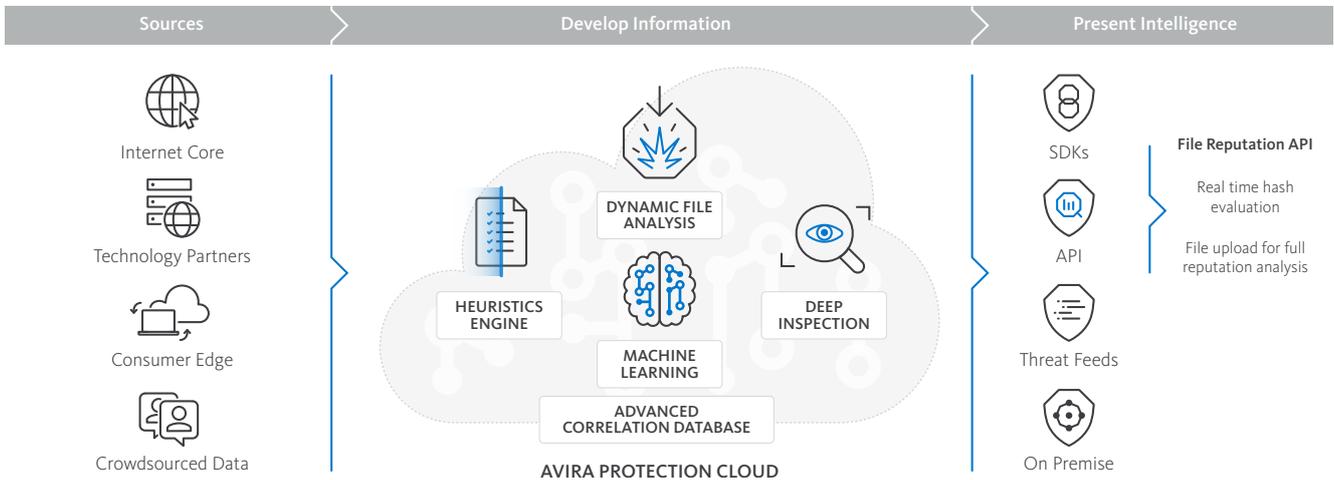
The Avira Protection Cloud is accessed directly via a REST API, or from Avira's Anti-malware SDK (SAVAPI) that can be embedded within many security systems (e.g. next-generation firewalls, as well as UTM, Security as a Service, endpoint detection, IPS/IDS, email gateways or file sharing systems).

It can be used to provide a primary or secondary opinion within a technology partner's or service provider's security cloud, and make a threat decision in real-time.

The Avira Protection Cloud is hosted within Avira's facilities in Germany. This has two key benefits for Avira's technology partners: First, it delivers compliance with some of the strictest data privacy regulations anywhere in the world. Second it appears as a black box to malware authors. This approach, known as 'detection protection' makes it very challenging for malware authors to test their code against the Avira Protection Cloud. As a result, the Avira Protection Cloud delivers excellent performance for longer periods compared to traditional approaches to malware detection.



## AVIRA PROTECTION CLOUD



## SPECIFICATIONS

### Implementation:

Accessed through a REST API for file submission and hash query

### Performance:

Sub 100m to a target of 3 seconds dependent on file size, threat type and network latency

### Real time threat reporting:

Windows files and executables, .pdf etc.

### Scan and detection:

Executables: Windows (PE), Mac, Linux (ELF).  
Documents: Office files, pdf, js, vbs, images, etc

### Relearning time:

Hash and scan updates are continuous  
NightVision updates every 15-30 minutes

### File attributes:

>8600 dimensions available for analysis

## OUR AWARDS



## FIND OUT MORE

Website: [oem.avira.com](http://oem.avira.com)  
Email: [oem@avira.com](mailto:oem@avira.com)  
Blog: [insights.oem.avira.com](http://insights.oem.avira.com)  
LinkedIn: Avira

### Europe Middle East, Africa

**Avira**  
Kaplaneiweg 1  
88069 Tettngang, Germany  
Tel: +49 7542 5000

### Americas

**Avira, inc**  
c/o WeWork, 75 E Santa Clara Street  
Suite 600, 6th floor San José  
CA 95113 United States

### Asia/Pacific and China

**Avira Pte Ltd**  
50 Raffles Place  
32-01 Singapore Land Tower  
Singapore 048623

### Japan

**Avira GK**  
8F Shin-Kokusai Bldg  
3-4-1, Marunouchi Chiyoda-ku  
Tokyo 100-0005, Japan