Avira

AVIRA CLOUD SANDBOX API

UNLIMITED-SCALE AND COMPLETELY PRIVATE

The Avira Cloud Sandbox API enables security vendors and service providers to submit files and receive detailed threat intelligence reports containing a complete threat assessment.

It is the security industry's most powerful and scalable malware analysis service. The Avira Cloud Sandbox utilizes the most advanced file analysis, deep inspection and award-winning dynamic detonation technologies to develop detailed threat intelligence.

The cyber-security industry is reliant on accurate and detailed threat intelligence. This intelligence is developed by sophisticated malware analysis systems that range from sandboxes (using emulation or virtualization) through deep content inspection, to AI and machine learning systems.

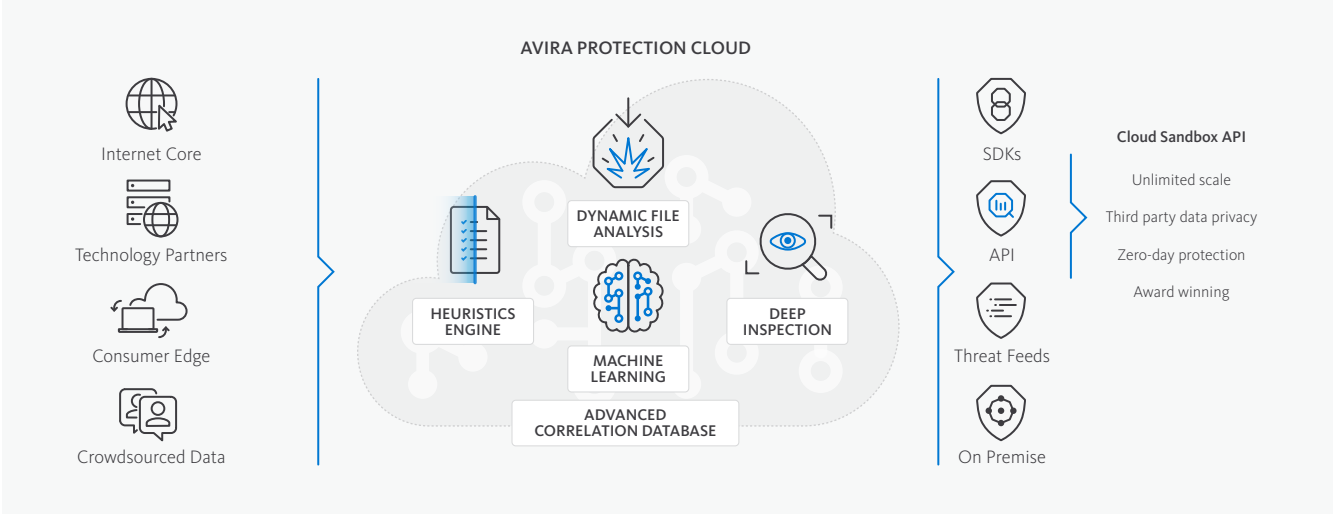
However, such systems are difficult to develop, require skilled engineers to maintain, and are limited in scale. Despite this, cyber-security vendors need to respond to customer demands for protection against the exponential increase in volume and complexity of attacks.

Vendors must have access to malware analysis tools that scale without limitation, meet customer's expectations of cost effectiveness, and work in a world that increasingly demands compliance to a range of new regulations, of which the most important is data privacy.

Avira's Cloud Sandbox API:

- Provides a malware analysis system that scales quickly and economically
- Delivers a malware analysis service that meets the strict data-privacy requirements of enterprises and new regulations such as GDPR
- Ensures zero-day protection and customers are protected from all suspicious traffic

AVIRA PROTECTION CLOUD



Avira

AVIRA CLOUD SANDBOX SERVICE

The Avira Cloud Sandbox is an award-winning, unlimited scale automated malware analysis system. It is the first to deliver a unique combination of affordability, scalability and privacy. It blends multiple advanced analysis technologies to deliver a complete threat intelligence report from an uploaded file.

The sandbox's malware analysis modules build a view of the origin and behavior of a threat. They extract and develop a cascade of valuable information that is used to create the most detailed and accurate threat intelligence. This enables researchers to understand how malware subverts the target system.

The Cloud Sandbox API delivers a detailed file-specific threat report containing valuable actionable intelligence. The report provides a detailed classification of the file, information on the techniques, tactics and procedures (IoCs) present in the threat, and a description of how and why the submitted file was identified as clean, malicious, or suspicious.

If the detonation layer is triggered during analysis of the file, additional information is provided in the report. This details the complete changes seen in the host during the detonation of the file (e.g. external calls or changes to the registry).

The report provides the intelligence required by security teams to understand the nature of a threat.

From inception, the service has been designed to address industry-wide concerns for personal data-privacy and regulation. As a result, GDPR compliance is built-in, addressing a key challenge faced by the cyber-security; how to handle third party personal data.

It is the first automated malware analysis service to address the industry's needs without compromise; scale, accessibility and privacy.

Unlimited-scale

Leveraging the power of Amazon Web Services (AWS), it is the first sandbox system designed to scale beyond the needs of a single enterprise and to meet the scale and cost needs of security vendors

Data-privacy

Avira Cloud Sandbox is built to protect customers' data. It is specifically designed to meet customers' demands for third party data privacy and meet the requirements for GDPR compliance

Zero-day protection

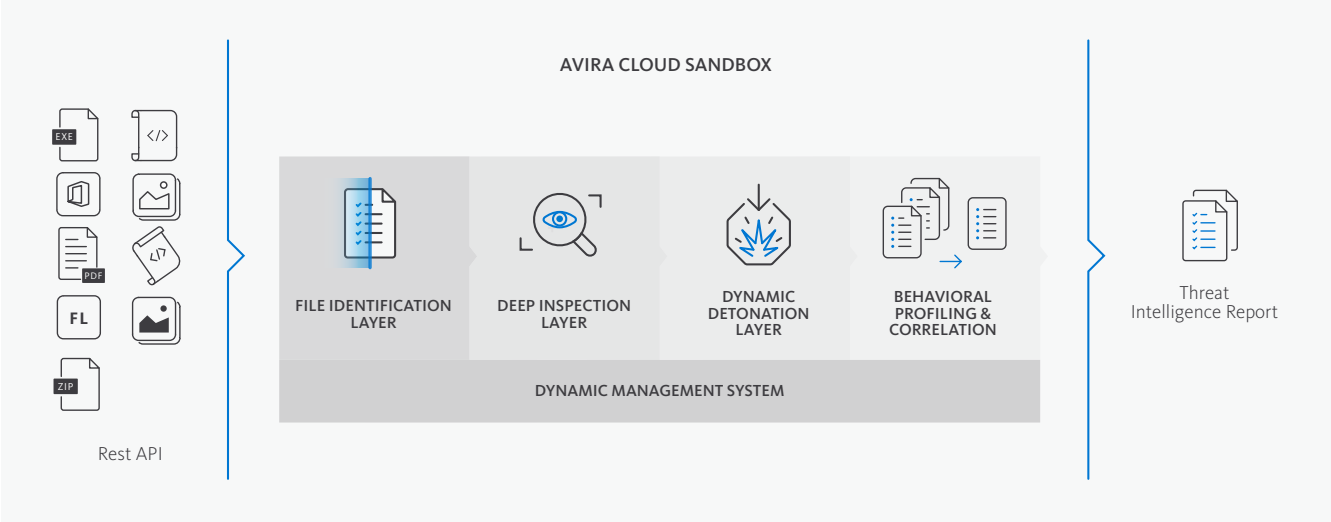
The service provides protection against unknown threats using the most advanced cloud-based analysis modules in the industry

Secure & award winning

Avira's dynamic detonation technology is the first to meet the strict security requirements of Amazon Web Services. Customers' data remains private, and the AWS network is protected from harm

Avira

CLOUD SANDBOX FRAMEWORK



ARCHITECTURE

The Cloud Sandbox leverages the technologies developed within Avira's cloud security system, the Avira Protection Cloud. The Avira Protection Cloud underpins the anti-malware and threat intelligence solutions of Avira, and through OEM partnerships, many of the world's leading cyber-security vendors, ultimately protecting nearly a billion people world-wide.

Built on an Amazon Web Services (AWS) infrastructure, the award-wining Dynamic Detonation Layer enables the Cloud Sandbox to manage the time-sensitive nature of partners' requests at scale and speed. Access to the service, and flexible integration, is enabled through a secure RestAPI.

The system is designed and constantly maintained by the experienced cyber-security engineering team at Avira. The Cloud Sandbox's Deep Inspection and Dynamic Analysis System delivers the highest levels of protection and performance against constantly evolving unknown threats.

ANALYSIS MODULES

Avira's Cloud Sandbox uses a flexible multi-layered automated malware analysis service that delivers deep inspection and reporting to the cyber-security industry. Key modules include:

A **File Identification** layer that evaluates uploaded files, to make an initial assessment. The assessment and tagging systems contained within this layer enable the **Dynamic Management System** to optimize the file's interaction with the deep inspection, dynamic analysis and behavioral profiling layers. This ensures the most accurate analysis and a cost-effective service.

The **Deep Inspection** layer provides unmatched visibility into malware behavior. It leverages Avira's powerful and proprietary heuristics, the NightVision™ machine learning system, and file specific analysis modules. This layer also includes advanced detonation techniques that simulate the entire host with methods that go beyond the first layers of a threat. Behavioral analysis, profiling and machine learning address previously concealed memory artifacts and hidden code layers, while intelligent code transformation defeats evasion and delivers near real-time classification.

A **Dynamic Detonation Analysis** layer uses an isolated detonation platform running within an unlimited-scale AWS environment. The modules in this layer employ a range of advanced sandboxing techniques in order to ensure that the sample targeted by the analysis behaves as it would in a real-customer situation. Analysis of traces within the system are leveraged to identify suspicious or malicious behavior.

The **Behavioral profiling and contextual analysis** layer correlates the cascade of information developed by the system modules and provides context to the data. It identifies novel families of malware, reveals hidden threat patterns, and delivers highly sophisticated behavioral profiling of malware.

The intelligence developed is then delivered to the user through a dedicated reporting module.

Avira

Key features:

- Complete monitoring of all system activities during the analysis delivers full attack chain visibility:
  - Full external network connections monitoring (FTP, TCP, HTTP and DNS requests, etc)
  - Mutex operations and created/modified services
  - Registry keys and their associated values operations
  - Files and folders creation, modification and deletion
  - Dropped/downloaded files execution analysis
  - Memory dump analysis
  - Complete execution chain based on processes, code injections and API calls
- Dynamic code modification to accelerate code deobfuscation and unpacking
- Actionable Intelligence containing reputation, indicators of compromise
- Reporting available in multiple formats from data interchange formats and documents to current industry standard formats
- Supports MITRE ATT&CK™ adversary tactics and techniques
- Advanced machine learning methods included in all analysis layers
- Deep code analysis, from dormant to hidden code, identifies code blocks even if they do not execute or are not visible
- Code similarity clustering and classification
- Hardened analysis environment undetected by evasive threats

OUR AWARDS

FIND OUT MORE

Website: oem.avira.com
Email: oem@avira.com
Blog: insights.oem.avira.com
LinkedIn: Avira

Europe
Middle East, Africa

Avira
Kaplaneiweg 1
88069 Tettnang, 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