Avira

APC
AVIRA PROTECTION CLOUD
Zero-Day and Advanced Persistent Threat detection and prevention API

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 third generation machine learning system. The Avira Protection Cloud provides technology partners and service providers a fast, simple and highly effective way to add the industry's leading anti-malware capabilities into their own solution.

Safeguarding Avira's customers from new and previously unclassified malware, the Avira Protection Cloud identifies Zero-Day and Advanced Persistent Threats spreading in a Windows environment. Accessed using a REST API or used in combination with the SAVAPI anti-malware SDK the Avira Protection Cloud invariably delivers 100% detection of malware on devices, appliances and services.

Technology partners access the Avira Protection Cloud using the SAVAPI anti-malware SDK or the REST API. In either case, a hash query can be made and compared with the master hash database. Within tens of milliseconds a response is returned to the endpoint or appliance. If the hash is unrecognized, optionally, the file is sent anonymously to the Avira Protection Cloud for full analysis. Analytical techniques used include a powerful cloud scanning engine, classification by Avira's NightVision machine learning system, and unpacking and detonation by Autodump, Avira's sandbox and emulation technology. As new analytical methods are developed, they can be plugged into the Avira Protection Cloud and brought online without requiring integration by technology partners.

KEY FEATURES:

- Accessible using a REST API and from the SAVAPI SDK, the Avira Protection Cloudoffers support for different platforms.
- Cloud-based service for scalability and security.
- A hash database of over a billion entries providing 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.
- A third generation machine learning system running on thousands of CPU cores and terabytes of memory, capable of comparing thousands of attributes of suspicious files simultaneously.
- Virtualized environments that can sandbox and emulate many key OS systems used to detonate malware that may hide from other analytical techniques.
- A powerful engine tackling highly polymorphic malware samples combined with a self learning approach identifies known threats.

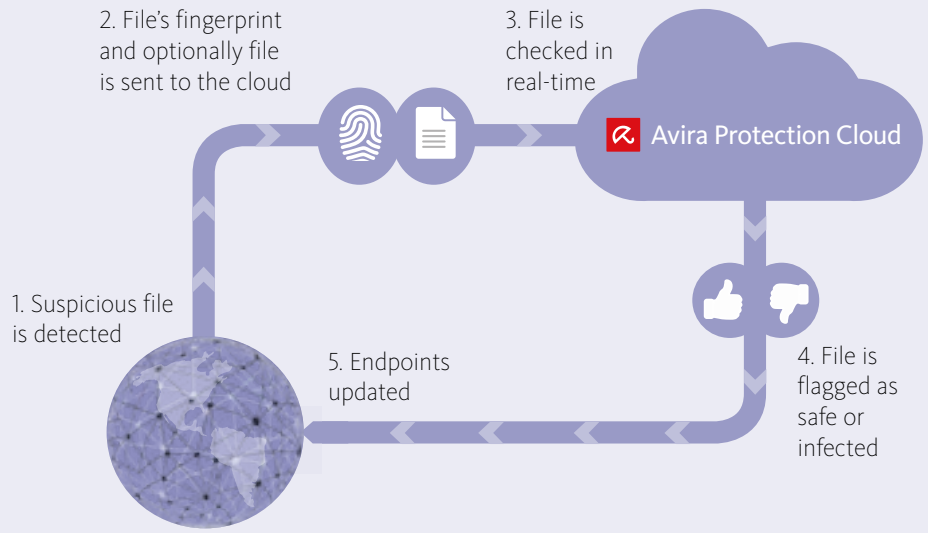
Avira

APC

Integration

The **Avira Protection Cloud** is accessed directly by a REST API, or from Avira's SAVAPI anti-malware SDK that can be embedded within many security systems (eg. Next Generation firewalls, UTM, Security as a Service, Windows client, email or document scanning systems). It can be used as 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 own 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. Secondly, it appears as a 'Black Box' to malware authors. This concept, known as 'Detection Protection' makes it very challenging for malware authors to test their code against the Avira Protection Cloud. As a result of this, the Avira Protection Cloud delivers excellent performance for longer periods compared with approaches to malware detection.



Specifications

- Size:
  > 8TB memory
  ~1000 CPU cores
- Supported OS (SAVAPI):
  Windows, Linux, MacOS, Solaris, FreeBSD, OpenBSD
- Implementation:
  Accessed through a REST API
  File submission and hash query
- Accessed from the SAVAPI SDK
  HTTPS connection.
- Real Time Threat Reporting:
  Windows files and executables, .pdf etc.
- Scan and Detection:
  Malicious Windows executables
- Performance:
  100mS to a target of 60 seconds dependent on threat type
- Relearning time:
  Updates every 15-30 minutes
- File attributes:
  >8600 dimensions available for analysis

Contact Avira

Europe, Middle East, Africa

Avira
Kaplaneiweg 1 | 88069 Tettnang
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

Website:
oem.avira.com

Blog:
insights.oem.avira.com

Social Media:
@AviraInsights