Avira

File Reputation API

Zero-Day and Advanced Persistent Threat detection and prevention with the Avira Protection Cloud

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 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.

Safeguarding Avira's customers from new and previously unclassified malware, the Avira Protection Cloud identifies Zero-Day and Advanced Persistent Threats. Accessed using the **File Reputation API** or used in combination with Avira's Anti-malware SDK, SAVAPI, the Avira Protection Cloud delivers >99.99% detection of malware on devices, appliances and services.

The 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 enquiries 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 typically within seconds. 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 Autodump, Avira's sandbox and emulation technology. As new analytical methods are developed, they are integrated within the Avira Protection Cloud and brought online without requiring integration by technology partners.

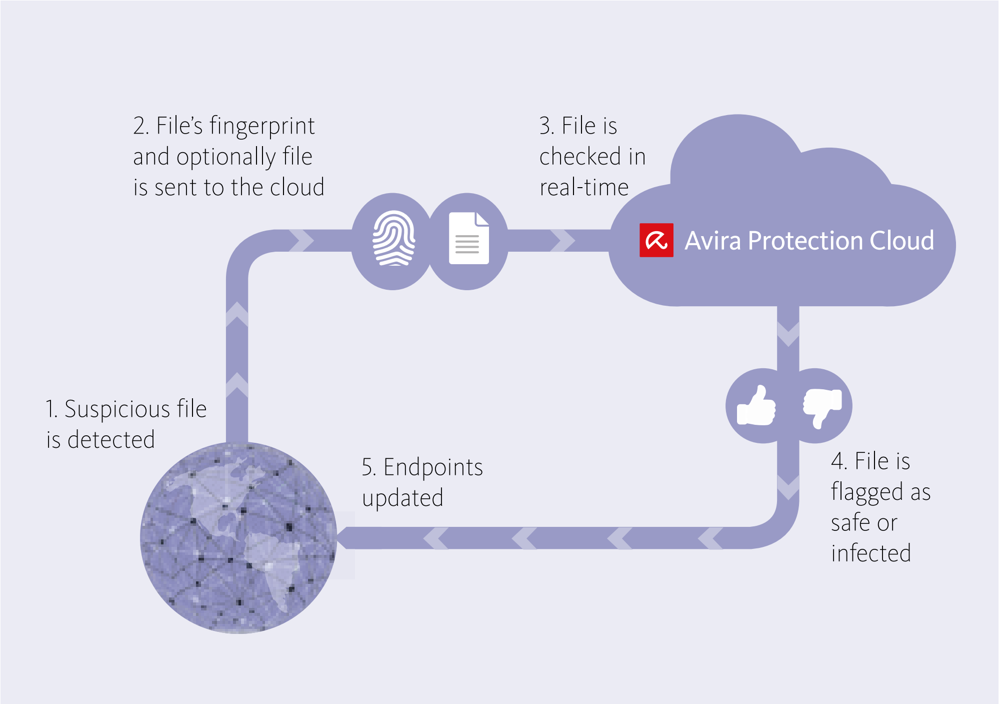
KEY FEATURES:

- 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 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 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 (eg. Next Generation firewalls, UTM, Security as a Service, Endpoint Detection, IPS/IDS, email gateways or file sharing 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 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 classical approaches to malware detection.


2. File's fingerprint and optionally file is sent to the cloud
3. File is checked in real-time
Avira Protection Cloud
1. Suspicious file is detected
5. Endpoints updated
4. File is flagged as safe or infected

Specifications

- **Implementation:**
  Accessed through a REST API
  File submission and hash query
- **Performance:**
  Sub 100mS 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, HTML, 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

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 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