Avira

SAVAPI

AVIRA ANTI-MALWARE SDK

Embedded scan engine

Avira's SAVAPI SDK provides your customers with the industry's best protection against malware, Zero-Day and Advanced Persistent Threats.

Implementing the SAVAPI SDK on your appliances, endpoints and systems enables you to scan files for malware. It allows you to access real-time classification of unknown files using the Avira Protection Cloud and is complemented by the Avira URL Cloud that delivers URL threat classifications.

SAVAPI provides a simple way for developers and providers of security products and services to get to market quickly, avoiding the costs and delays associated with in-house development by leveraging the experience and knowledge of Avira's award winning technologies. SAVAPI delivers key security services, provides high performance offline scanning, and an online connection to the Avira Protection Cloud that invariably delivers complete protection against malware.

The SAVAPI SDK is widely used by hardware and software vendors looking to implement anti-virus / anti-malware solutions. It is widely used by Next Generation Firewall vendors, Unified Threat Management, software utility providers, service providers – anyone looking to integrate malware analysis into their product or service.

KEY FEATURES:

- Fast integration time, typically within hours
- Daemon updates without service interruption
- Supports scanning of all file types
- Offline scanning including signature based, heuristics and generic analysis
- Integrated machine learning providing local risk evaluation
- Archive unpacking modules
- Integration with Avira Protection Cloud

Integration

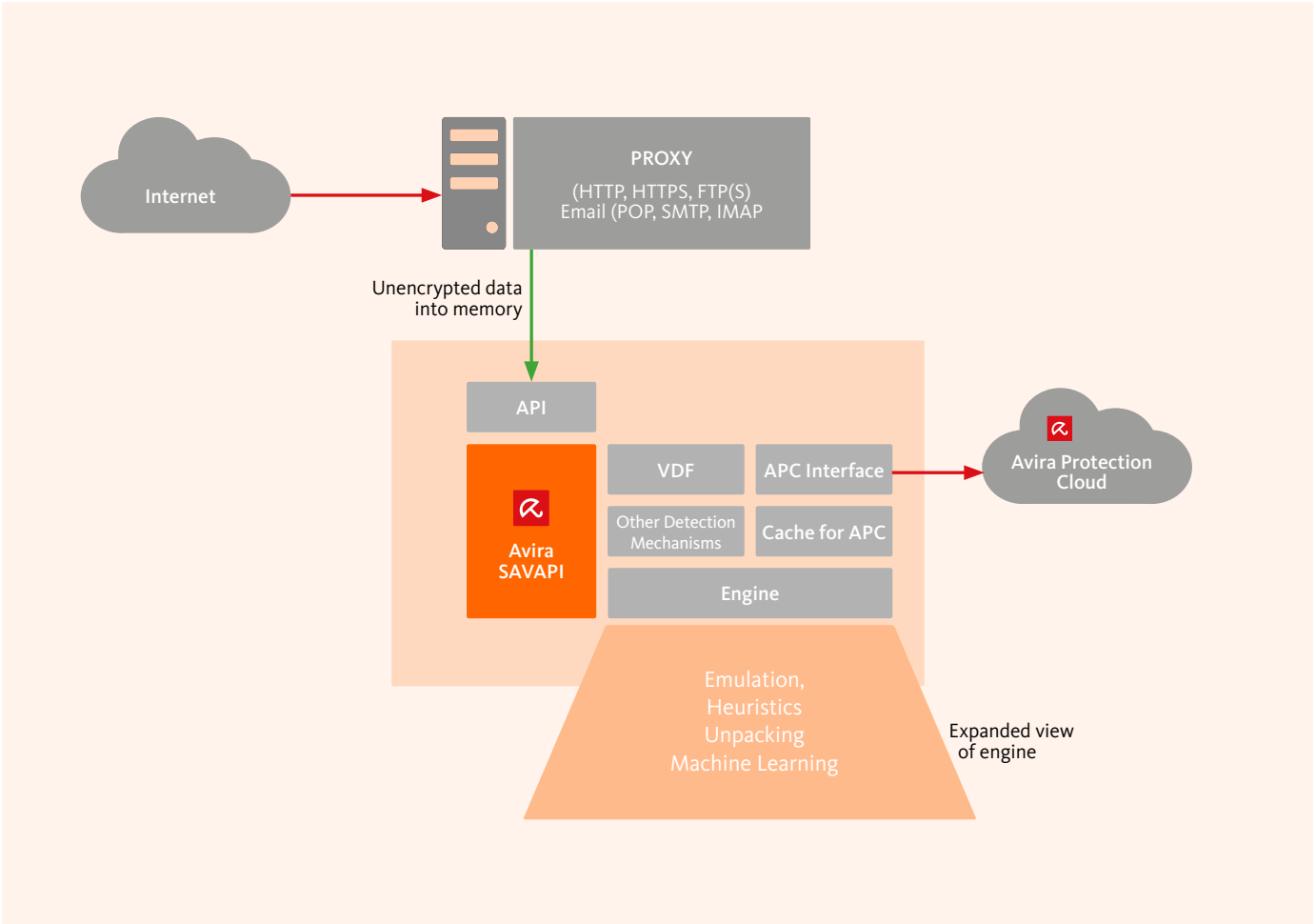
The SAVAPI SDK is written in C and can be used by any common C/C++ compiler.

Several deployment scenarios offer a wide range of integration possibilities, from the simplest to more complex scenarios. These include:

Library Mode: A C-Library available for all 32- and 64-bit versions of Windows, Linux and MacOS, offers complete control of the integration with support for call-backs. Using call backs for file operations (FOPS) means SAVAPI can easily integrate with memory-backed and virtual file systems

Daemon / Service Mode: A multi-threaded service or daemon that listens to client requests on Unix and network sockets. A variety of integration methods are available including Perl, Python, C and C++

SAVAPI Service Diagram



Avira

SAVAPI

SAVAPI with Avira Protection Cloud

Implementing SAVAPI in conjunction with the Avira Protection Cloud offers the opportunity to reach 100% detection rates and protect customers from Zero-Day and Advanced Persistent Threats.

When SAVAPI detects an unknown, unclassified, suspicious file, it sends a hash query to the Avira Protection Cloud. If the hash is reported as unknown (possibly Zero-Day malware) the file can be uploaded to the Avira Protection Cloud for analysis. The Avira Protection Cloud uses innovative systems and algorithms, including Avira's third generation Artificial Intelligence, NightVision, to classify the file in real-time and provide feedback to SAVAPI.

The combination of a lightweight scan engine with almost unlimited cloud computing available to power complex detection modules delivers the best performing anti-malware solution available, providing the most reliable virus protection available combined with a very fast response time.

Specifications

- Size:
  76MB
- Platform requirements:
  Min 1.6Gbps CPU
  512MB RAM exclusive use
  1GB Disk space for unpacking
- Supported OS:
  Windows 64 & 32, Linux, MacOS, FreeBSD, OpenBSD
- Implementation:
  C-Library, Daemon, C-Library and Daemon/Service Mode
- Functionality:
  99.9% Detection rate
  Generic and heuristic
  Advanced archive scanner
  Interfaces with Avira Protection Cloud
- Scan and Detection:
  Malicious Windows PE Exe and DLL
  Linux, MacOS and Android malware
  Malicious script: JavaScript, VBScript etc
  Office docs and embedded macros
- Unarchiving
  Zip, zoo, arj, arc, rar
  Flag password protected archives
- Decoders
  MBOX, MIME attachments
- Adware and Spyware *(selection)*
  Worms, mailers
  Web-based malware (HTML, JavaScript, VBS)
  Script virus DOS Batch MIRC/ IRC script Shell script (Bash etc.)
  PIF, INI, REG (ASCII)
- Viruses *(selection)*
  Encrypters, Polymorphic & Metamorphic viruses,
  Stealth viruses,
  Boot /File/MultiPartite
  Java Applets, Exploits in file formats.
  SPR (Security Privacy Risk e.g.: Jokes),
  Backdoors,
  Trojans (Remote Access Trojans),
  Password/Keylogger/DoS,
  Droppers etc.),
  Macro viruses (MS Office, Embedded Objects, Excel Formula, MSO/HTML, PDF)

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

© 2018 Avira Operations GmbH & Co. KG | All rights reserved | Avira | Kaplaneiweg 1 | 88069 Tettnang | Germany | oem.avira.com | Product and company names mentioned herein are registered trademarks of their respective companies
Our general terms and conditions of business and license terms can be found online: www.avira.com | May be subject to errors and technical changes | As of: March 2018