Avira

ANTI-MALWARE SDK

CROSS PLATFORM

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

Implementing the Anti-malware SDK on your appliances, endpoints and systems enables you to locally scan files for malware. It also 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. The Anti-malware SDK provides a simple way for developers and providers of security products and services to get to market quickly. It avoids the costs and delays associated with in-house development by leveraging the experience and knowledge of Avira's award winning technologies. The Anti-malware SDK delivers key security services, provides high performance offline scanning, and an online connection to the Avira Protection Cloud that regularly delivers complete protection against malware.

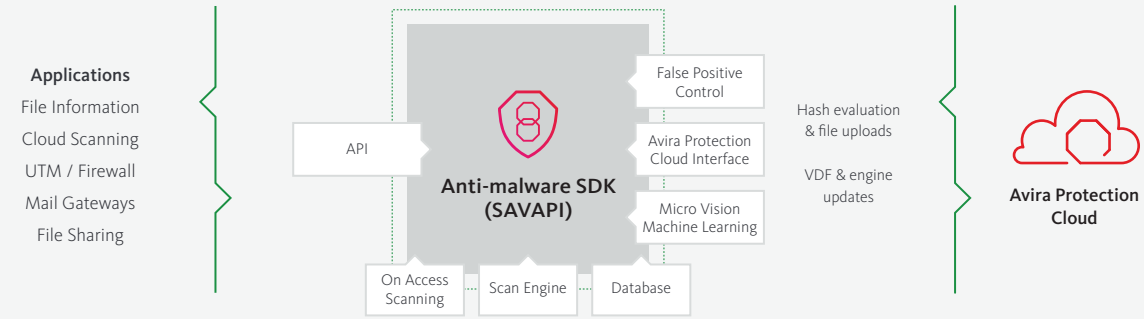
Avira's Anti-malware SDK Anti-malware is widely used by hardware and software vendors looking to implement anti-virus/anti-malware solutions.

It is widely used by Endpoint Detection, Managed Security Service Providers, Next Generation Firewall vendors, Mail Gateways, 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
- Integration with Avira Protection Cloud
- Real-time scanner extension providing enhanced detection
- False Positive Control

SAVAPI INTEGRATION EXAMPLE



Avira

AVIRA PROTECTION CLOUD

Using Avira's Anti-malware SDK with the Avira Protection Cloud offers the opportunity to reach 100% detection rates and protect customers from Zero-Day and Advanced Persistent Threats.

When the Anti-malware SDK 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 anti-malware.

The combination of a lightweight scan engine with almost unlimited cloud computing power, delivers the best performing anti-malware solution available combined with a very fast response time.

ON-ACCESS EXTENSION

On-Access is a real-time scanning extension. It enables Avira's Anti-malware SDK to perform automatic scanning of files accessed or executed at the operating system level. On-Access adds an additional level of security by allowing scanning decisions to occur before other processes and operating system execution. It is fully configurable and offers multiple filtering capabilities, inspection of file-access and file-execution events.

FALSE POSITIVE CONTROL

False Positive Control is Avira's mechanism to ensure exceptional false positive detections are identified in real-time and are prevented from impacting the performance of antimalware scanning. It is a no-cost option that can be enabled within Avira's Anti-malware SDK (SAVAPI).

SPECIFICATIONS

Size:
100MB

Platform requirements:
Min 1.6GHz CPU
512MB RAM exclusive use
1GB Disk space for unpacking

Supported OS:
Windows 64 & 32 bits, Linux, MacOS, FreeBSD, OpenBSD

Implementation:
Pure Library Mode or
Pure Daemon/Service Mode or ClientLibrary & Daemon/Service Mode

Functionality:
>99.99% Detection rate
Generic and heuristic
Advanced archive scanner
On-Access extension for Windows
False positive control
Integration 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)

OUR AWARDS

FIND OUT MORE

Website: oem.avira.com
Email: oem@avira.com
Blog: insights.oem.avira.com
Social Media: @AviraInsights

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