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 scan files locally for malware. It also lets you access real-time classification of unknown files using the Avira Protection Cloud, and is complemented by the Avira URL Cloud which 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 saves you from the cost and delay of in-house development by leveraging the experience and knowledge of Avira's award-winning technologies. The Anti-malware SDK provides key security services, high-performance offline scanning, and an online connection to the Avira Protection Cloud for complete protection against malware.

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

It is employed extensively by endpoint-detection and managed-security service providers; next-generation firewall vendors; mail-gateway, unified threat-management, and software-utility providers; as well as service providers – anyone looking to integrate malware analysis into their product or service.

INTEGRATION

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

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

Library mode: A C library available for Windows (32-bit & 64-bit), Linux, and MacOS, offers complete control of integration with callback support. Using callbacks for file operations (FOPS) means SAVAPI integrates easily into memory backed, virtual, and encrypted file systems.

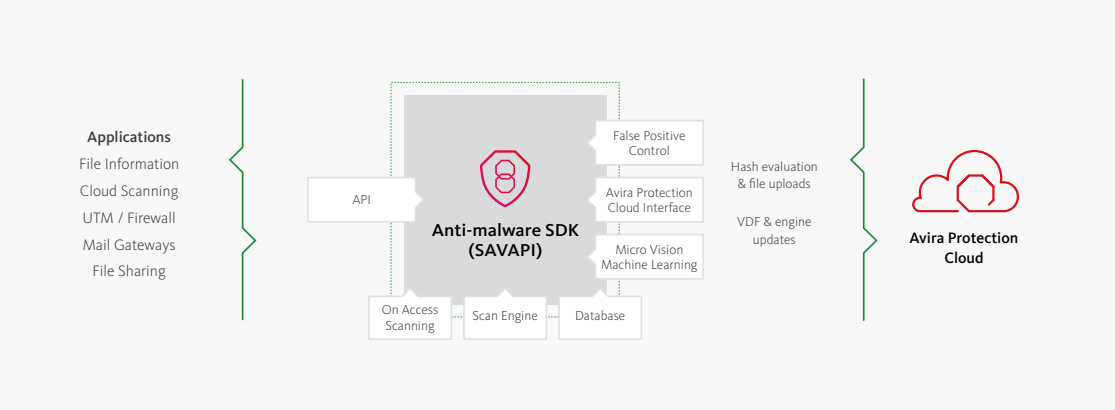
Daemon/service mode: A multi-threaded service or daemon listens to client requests on Unix and network sockets. A variety of integration methods are available including C#, Perl, Python, C, and C++.

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

Avira

ANTI-MALWARE SDK INTEGRATION EXAMPLE



AVIRA PROTECTION CLOUD

Using Avira's Anti-malware SDK with the Avira Protection Cloud allows you to achieve >99.99% 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 AI platform, NightVisionTM – to classify the file in real time and provide feedback to the anti-malware system.

The combination of a lightweight scanning engine with near 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 scan files automatically that are accessed or executed at OS level. On-Access adds an additional layer of security by allowing scanning decisions to be made before other processes and prior to operating-system execution. It is fully configurable and offers multiple filtering capabilities, including 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 prevented from impacting the performance of anti-malware scanning. It is a no-cost option that can be enabled within Avira's Anti-malware SDK (SAVAPI).

Avira

SPECIFICATIONS

Size:
100MB

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

Supported OS:
Windows (32-bit & 62 bit), 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 Scanning
Advanced archive scanner
On-Access extension for Windows
False positive control
Avira Protection Cloud Integration

Scanning and Detection:
Malicious Windows PE EXEs and DLLs
Linux, MacOS, and Android malware
Malicious scripts: 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 viruses DOS Batch MIRC/ IRC
script Shell script (Bash, etc.)
PIF, INI, REG (ASCII)

Viruses (selection):
Encryptors, Polymorphic,
Metamorphic viruses, Stealth viruses,
Boot/File/MultiPartite viruses
Java Applets, file formats exploits
SPR (Security or Privacy Risk e.g.: Jokes)
Backdoors
Trojans (Remote Access Trojans)
Password/Keyloggers/DoS, Droppers etc.)
Macro viruses (MS Office, Embedded
Objects, Excel Formule, MSO/HTML, PDF)

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