Avira

# REMEDIATION SDK

Avira's Remediation SDK, is the industry's most trusted and reliable solution to eliminate malware from an infected system and restore the system to a stable state.

Remediation is essential for any end-point protection solution. If a system gets infected by malware, users expect a remedy. The objective is to reliably restore the system to the state that existed before infection, allowing the user to regain control and continue normal operations.

Avira's Remediation SDK thoroughly removes all active artifacts of malware, returning the system to a healthy state. In more than 99% of cases a complete system restore is possible if the malware was first detected by an Avira anti-malware SDK.

The Remediation SDK provides the core functionality upon which developers can build a complete EDR/EPP solution. The SDK offers an option to rename, delete or quarantine malicious artefacts. It efficiently kills the active running processes, cleans the system registry, and removes malicious WMI event subscriptions. It can also restore changes for specific content in certain files, if modified by the malware.

## APPLICATION

Many cyber security companies license their anti-malware technologies. However, they rely on the remediation functionality to be developed in-house as it is not offered by their partner. Avira's Remediation SDK enables EDR/EPP providers, MSSPs and AV providers to integrate a mature remediation technology into their security products and services. This reduces the risk of ineffective malware removal or damage to the operating system.

Leveraging Avira's 30 years of industry experience and knowledge of a large diversity of malware families saves cyber security companies from the costs, risks and potential delays associated with in-house development.

## INTEGRATION

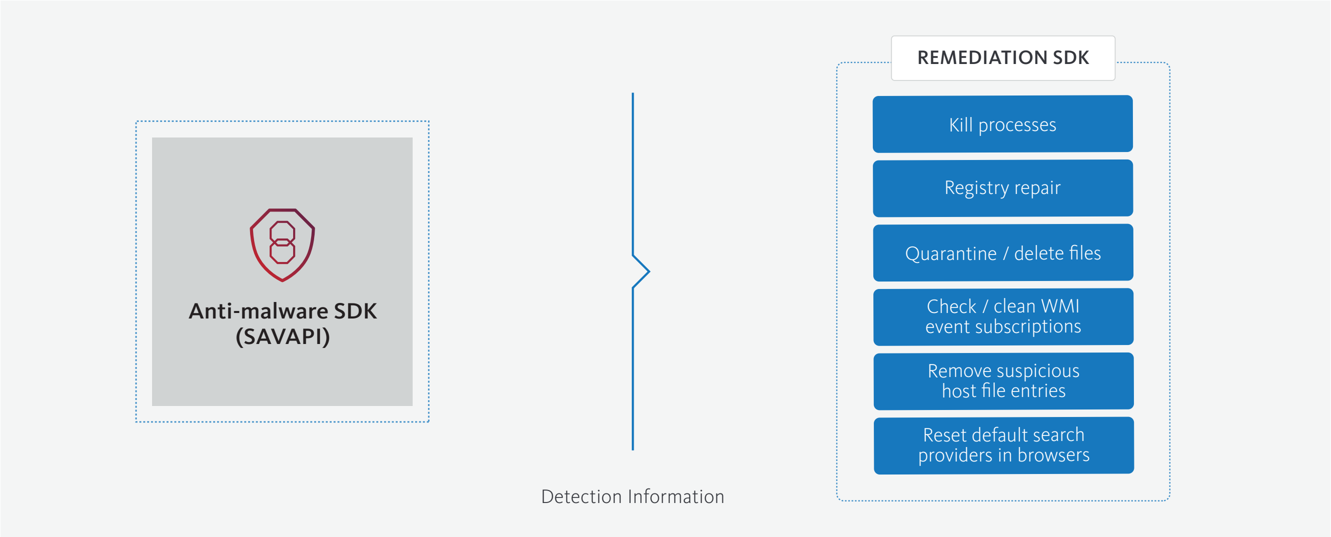
Avira's Remediation SDK is a standalone SDK built around a C++ library with C/C++ interface. It is statically linked against the Microsoft runtime library. The Remediation SDK includes a C#.NET wrapper that enables an easy integration into third-party security solutions. The Remediation SDK uses compressed and secured RDFs (Rule Definition Files) to update data needed for disinfection routines. The RDFs are updated with the newest malware disinfection information several times per day. For effective malware removal the Remediation SDK needs brief detection information from an upstream scanner. This includes detection name (preferably in Avira format), file name detected, filepath and some optional flags.

### Key Features:

- Able to disinfect malware that has re-infection persistence
- Cleans file system and registry artifacts
- Removes malicious WMI events subscriptions
- Cleans the host file from unwanted and malicious entries
- Can reset the default search provider in the browser if it was set to a malicious page
- Able to reboot the system, if the operation is needed to clean the system (e.g. to clean locked files)
- Updater for RDFs (Rule Definition Files)
- Flexible licensing mechanism

Avira

## REMEDIATION SDK



Anti-malware SDK (SAVAPI)

Detection Information

REMEDIATION SDK

- Kill processes
- Registry repair
- Quarantine / delete files
- Check / clean WMI event subscriptions
- Remove suspicious host file entries
- Reset default search providers in browsers

## SPECIFICATIONS

**Supported Platforms:**

Windows OS (Windows 7 and Server 2008 R2 and above), 32 and 64 bits

**Implementation:**

Native shared library

**System Requirements**

- Pentium 4 class CPU 1 GHz or better
- 30 MB free disk space, at least 1 GB RAM
- Library must be run in processes with administrator privileges
- Internet connection required to fetch updates

## 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

© 2020 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: August 2020.