Avira

ENDPOINT PROTECTION SDK

FOR WINDOWS

Bring a Windows endpoint security solution to market more quickly, and with less development risk, using the Avira Endpoint Protection SDK.

Based on an award-winning antivirus solution, the Avira Endpoint Protection SDK for Windows gives you access to the same anti-malware engine, modules and threat intelligence used by Avira, delivered as a simple to integrate and easy-to-use Windows service. It brings together all the detection modules you need to build your own-branded antivirus solution in a fully integrated package optimized to deliver high detection rates and low resource usage.

The Endpoint Protection SDK leverages a multi-layered detection architecture with behavioral analysis powered by our latest machine learning technology. Integration with the Avira Protection Cloud provides access to almost realtime cyberthreat data and helps to protect your customers from cyber threats.

Deployed on millions of endpoints globally, the platform already meets Microsoft's MVI program. This removes the need for separate certification and greatly simplifies your route to market.

INTEGRATION

The Avira Endpoint Protection SDK for Windows is a highlevel software development kit that delivers a Windows service configured through a C#/C++ client library. The service contains the key components needed to create an endpoint protection product for Windows client and server operating systems. It delivers a proven and highly optimized set of security capabilities that integrate with the Avira Protection Cloud to maximize malware detection rates and protect users from malicious content. The Endpoint Protection SDK runs as a Protected Windows Service (Anti-malware PPL). It comes with a set of modules that deliver real time protection, enhanced macro and script protection, and quarantine.

Optional modules add network protection, behavioral analysis, firewall functionality and remediation. The modules add to the detection capabilities of the platform by covering the relevant MITRE ATT&CK tactics and help to protect against file-less attacks, polymorphic malware and zero-day cyberthreats.

MICROSOFT VIRUS INITIATIVE

A major benefit of choosing the Avira Endpoint Protection SDK is that partners are freed from meeting and maintaining compliance to the Microsoft Virus Initiative Program. It means your antivirus product can be the default Windows security solution, and integrates into the Windows Security Center. Avira is responsible for the annual recertification by independent testing authorities required by the MVI program.

Key Features:

- Integrates key anti-virus capabilities into a single, high-level SDK
- Simply integrate and connect to your existing User Interface for a working AV solution
- Supports scanning of all file types
- Built-in machine learning provides local risk evaluation
- Integration with Avira Protection Cloud
- False Positive Control
- Microsoft MVI Program pre-approved platform

Avira

AVIRA PROTECTION CLOUD

Integration with the Avira Protection Cloud enables you to achieve the highest detection rates and helps protect customers from Zero-day and Advanced Persistent Threats.

When the Endpoint Protection SDK detects an unknown or suspicious file, an API query containing a hash of the file is sent to the Avira Protection Cloud. If the Avira Protection Cloud cannot identify the hash, then the file is uploaded for real time analysis.

Within the Avira Protection Cloud the file is analyzed by NightVisionTM, an advanced machine learning system, detonated in a hardened environment to reveal malicious behavior, and scanned by powerful cloud-based engines. Only after the systems classify the file as likely to be safe will the Endpoint Protection SDK forward the file to the client system. Otherwise, the file is blocked and moved to quarantine.

The combination of a lightweight scanning engine with cloud computing power delivers one of the best performing anti-malware solutions available, combined with fast response times.

KEY FEATURES AND CAPABILITIES

The Endpoint Protection SDK can be integrated through a C++ and C# interface and ships with both standard and ptional modules. Standard modules include:

Realtime Protection

A core element of the Endpoint Protection SDK is the Realtime protection module. This enables automatic scanning of files accessed or executed at an operating system level and helps protect against fileless attacks. It is highly configurable and includes an anti-tamper function which helps protect the registry keys, files and processes of the partner's applications. Extensive and flexible filtering capabilities are also built into the module.

On-demand scanning

Triggered through the partner's chosen user interface, the On-demand scanning module comes with multiple scan profiles that include a quick scan, an active process scan, a registry scan, a Windows task scan, and a full system scan. Partners can also define their own scan profiles.

AMSI

The Avira Endpoint Protection SDK uses the Windows Antimalware Scan Interface standard (AMSI), to enhance malware protection for users, applications, scripts and processes. It enables the platform to become the antimalware scanner for applications that support AMSI. This provides enhanced detection of obfuscated script-based malware such as Microsoft Office VBA macros, PowerShell, JavaScript and VBScript.

Quarantine

When malware is detected, it is encrypted and moved to a secure location by the quarantine module. The user can then decide what action to take. The functionality includes copy, remove, and restore.

Remediation

The Avira Remediation module is designed to remove artifacts of identified and known malware, returning the system to a healthy state.

It achieves this by disinfecting malware that has reinfection persistence, cleaning the file system, host file, scheduled tasks, registry artifacts and removing malicious WMI event subscriptions. It can also reset relevant system settings (e.g. proxy), the default search provider in a browser if set to a malicious page, and can reboot the system if required to clean locked files.

Updater

The Endpoint Protection SDK includes a built-in updater module that maintains the platform's entire featureset, reboot-free. It downloads updates directly from the Avira Protection Cloud or mirrored through the partner's proxy server.

Avira

OPTIONAL MODULES INCLUDE:

Network Protection

Avira Network Protection scans all network traffic for malicious content – even if encrypted. It leverages the most up-to-date classification and categorization intelligence available in the Avira Protection Cloud to identify file and web-based cyberthreats and includes a fully configurable whitelist for trusted applications and sites.

Behavioral Analysis

The Behavioral Analysis module leverages both static and dynamic machine learning to constantly monitor the endpoint for new anomalous or malicious activity. When malicious processes are identified, it is designed to move the file reference to quarantine and remove all traces of the malware activity. It is a key element in defeating both polymorphic and zero-day cyberthreats to the system.

Firewall

The Avira Firewall complements, enhances, and integrates with the Windows system firewall, extending functionality to include application layer filtering. It works closely with the Behavioral Analysis module to deliver a lightweight but effective intrusion detection and protection capability. Application inspection firewall rules are automatically managed and kernel-mode level enforced and intrusion attempts blocked.

Avira Protection Cloud

The Avira Protection Cloud uses powerful advanced heuristics, machine learning and dynamic file analysis systems to develop the threat intelligence used by the Endpoint Protection SDK.

SPECIFICATIONS

Minimum hardware requirements:
Dual Core with 1.6 GHz
2GB free RAM (4GB recommended)
2GB free HDD (4GB recommended)
Intel x86 32-Bit and 64-Bit
ARM 64Bit (future release)

APJ & EMEA

AviraOEM sales office
NortonLifeLock Ireland Ltd

Ballycoolin Business Park,
Dublin 15, Ireland

Americas

AviraOEM sales office
Avira Inc.

487 E. Middlefield Rd.
Mountain View
CA 94043, USA

FIND OUT MORE

Website: oem.avira.com
Email: oem@avira.com
LinkedIn: Avira