Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

SECUREPOINT

Technical Description of Service

Securepoint Antivirus Pro

Contents

Securepoint Antivirus Pro

Securepoint Antivirus Pro is reliable security software with cloud-based management that protects Windows systems and data from known and new malware and unwanted programs.

Securepoint Antivirus Pro Portal

The Securepoint Antivirus Pro Portal is a user-friendly cloud management tool for the administration of multiple Securepoint Antivirus Pro installations at multiple sites. This allows for management of quarantines, exclusions, settings and scheduled scans on all clients. The portal is available in German and English, the GUI of the client software on the end-user device may be displayed in German or English.

Core Functions of Securepoint Antivirus Pro

- Behaviour analysis to identify threats on the basis of their behaviour or malicious features
- Multi-level automated analysis process
- Isolation of identified threats in Quarantine
- Automated notification when viruses detected

IKARUS T3 scan.engine

Securepoint Antivirus Pro uses the multi-threading, VB100-certified IKARUS T3 scan.engine. This guarantees reliable identification of malware and potentially unwanted programs or applications (PUP/PUA).

How the IKARUS T3 scan.engine works

Every file checked by the scan engine in Antivirus Pro runs through multiple processes:

- Hashes of the file are analysed
- Hashes are compared with blacklists and whitelists
    - *If the value is on the whitelist:* The document is considered “clean” and is not infected
    - *If the value is on the blacklist:* The document is considered “infected” and is immediately placed in Quarantine
    - *No match with the lists:* ongoing analysis
- File type is determined by analysis
- Behaviour of file is analysed
    - Code is first viewed statically, then dynamically (sandboxing). Analysis here looks at: What does the file do? What is its goal? What does it try to access?
    - The information extracted is compared to known malware

- Various processes are defined for every file type:
  - Archives are unpacked to inspect every file individually
  - Password-protected files are opened where possible so as to inspect them

The analysis may deliver one of three results:

- Clean: The file is not infected.
- Malware: The file is infected and is immediately isolated (placed in Quarantine).
- Potentially Unwanted Application/Program (PUA/PUP): The file/program is unwanted and is immediately isolated (placed in Quarantine).

Sandboxing

Suspicious files earmarked for ongoing analysis are also placed in a specially developed Sandbox environment. Within this virtual, completely isolated environment, tests are carried out as required to analyse behaviour and other features in order to identify possible malicious behaviour.

Feedback Loop

The scan engine in Antivirus Pro works as a “feedback loop”. First, it **analyses**, then it **extracts** file information and finally **examines** the information. This process is repeated as often as necessary, until:

- Malware/PUA/PUP is found.
- All information in the file and all content (hidden files, links, etc.) are identified and checked, so that nothing is left to check and it is considered “clean”.
- The checking time has expired. After this, the file is marked “clean”.
- Further investigation becomes necessary (e.g. unknown document type) and the document is automatically sent to the Analysis Team.

The scan engine analyses and extracts all necesarry information and continually compares it with the virus database. This database is updated several times a day to ensure it is always current.

File Status

Clean

If a file is declared “clean”, Securepoint Antivirus Pro has not found any threat.

Malware:

Malware is malicious software that tries to damage an infected system with unwanted behaviour.

Note: Even malware optimised for Android, Linux or other systems may cause damage to a Windows system and is therefore identified as malicious.

Potentially Unwanted Application/Program (PUA/PUP)

PUAs/PUPs are not malicious as such, but mostly unwanted. They are often automatically downloaded together with another file. The scan engine in Antivirus Pro recognises them and places them in Quarantine.

Examples of PUAs/PUPs: Toolbars, chip installers, key generators

The Engine Ranking System

The scan engine in Antivirus Pro works together with an Engine Ranking System that has three classifications:

1. Malware (highest level)
2. PUA
3. Clean

A file may demonstrate multiple behaviours. In this case, the scan engine automatically assigns the highest ranking.

Example: A file checked by the scan engine shows features of PUA and malware. The ranking system is automatically applied because there are two classifications. As malware is ranked hinger than PUA, the file is categorised as malware.

Classifications of the scan engine in Antivirus Pro

Unrecognised files may, in certain circumstances, be categorised as “false negative” or “false positive”.

- *A false positive result* is identified as “*infected*” although it is a “*clean*” file.

  False positive results are very rare. Where a false positive is suspected, please send the file via the Quarantine function to the Analysis Lab. The file will be checked again there and, where appropriate, cleared.

- A false negative result is identified as “*clean*” although it is an “*infected*” file.
  False negative results can occur in the case of completely unidentified malware types. Thanks to the multi-level analysis of the scan engine and re-checking of all files after every virus database update, however, they are extremely rare. Where false negative results are identified, they are immediately blacklisted to prevent further damage.
  Where a false negative is suspected, please send the file to the Lab.

Quarantine and Notification Function

Should a suspicious file be found, access is blocked and an entry is made in the Quarantine. A decision about what is to be done with the file (e.g. deletion) can be made in the Management Portal or the Client software.

Email notification of defined events, e.g. virus detection, can be activated in the Securepoint Antivirus Pro Portal.

Document Checks by Securepoint Antivirus Pro

Securepoint Antivirus Pro checks all types of file, program and application from every source (download, removable drive, etc.) every time they are opened. This automatic scan procedure can be activated or deactivated in the Client or in the Securepoint Antivirus Pro Portal.

Different Types of Scan

Securepoint Antivirus Pro can conduct comprehensive scans at individual times.

- **On-Access Scan**: Checks all read and write processes on a file or a process, in real time.
- Scheduled **On-Demand Scans** and **Scan Profiles**: The On-Demand Scan is responsible for predefined and manual scans of individual files, folders or drives. Four Scan Profiles are defined by default. These may be individually configured and started/stopped at freely determined times in the Client or the Management Portal.
  Our tip: We recommend defining a daily Scan Profile that automatically checks for malware and PUAs. Missed scans may be automatically caught up on in the function "Catch up on scans" in the Scan Profile.
- **Individual Scans:** Files and folders can be individuall scanned at any time via the context menu.
  Before opening a file, right-click on it and select "Check with Securepoint Antivirus Pro".

Checking Microsoft Office Documents

The software also searches for malicious macros as well as malware in Microsoft Office documents. Here, too, behaviour is **analysed** and file information is **extracted** and **examined**.

Scan Duration

It is not possible to provide exact timing, as this depends on the size and complexity of the file to be scanned. The engine processes, on average, approximate 1,000 files per second in an On-Access Scan at a single node/server. Depending on the hardware, it may be assumed that the time will be between 0.01 milliseconds and five seconds (for special files).

Advantages of Securepoint Antivirus Pro

Resource-efficient Operation with Securepoint Antivirus Pro

The faster antivirus software works, the faster the computer. The scan engine in Antivirus Pro has therefore been developed to achieve scaleability and resource efficiency. Various operating modes (memory or disk optimisation) and an almost linear increase in performance by raising the number of parallel threads means that this is one of the highest performing complete systems on the market. Thanks to the fast functionality of Securepoint Antivirus Pro, it is very energy efficient and achieves longer battery life for laptops and notebooks.

Machine Learning

Based on user behaviour, the scan engine recognises the documents, programs, etc. most frequently used. The are prioritised when canning to optimise system performance.

Analysis Information Via SigQA (Signature Quality Assurance Programm)

SigQA serves to improve signature-based identification. Signatures serve to combine multiple CRCs in a single identification routine. In order to prevent false positives, they are silently sent in the first step, so that only the telemetry data are sent when a threat is identified.

The OPSWAT Interface

Securepoint has OPSWAT Platinum certification. Antivirus Pro uses the IMACI interface. This interface reports to OPSWAT that a current virus database is integrated, the Client is protected and there are no current threats. The scan engine in Antivirus Pro can therefore be integrated with OPSWAT MetaDefender.

Password Protection for Client Settings

Administrators have the option of blocking configuration settings on Clients by requiring a password for changes. All settings and actions are then subject to unified administration via the Securepoint Antivirus Pro Portal. On-Demand Scans and individual scans may still be initiated by users without a password being requested.

ELAM with Securepoint Antivirus Pro

ELAM (Early Launch Anti Malware) is an early start function from Microsoft which launches Securepoint Antivirus Pro at system boot. It protects the process from external attempts to stop it.

Important Contact Data

Securepoint Support

Support hotline:
+49 4131 2401-0

support@securepoint.de

Analysis Lab

probe@ikarus.at

Glossary

GUI / Graphical User Interface

The interface of Securepoint Antivirus Pro directly on the Client computer.

Macros

Macros are automatic functions that execute in the background intended to simplify use of MS Office applications. Micrsofot invented macros to facilitate simpler work for users and process optimisation for companies. Macros are not automatically dangerous, but they can be used to camouflage threats. They are only classified as malicious when a threat is proven.

Example 1: Downloading an image to copy it into a document may be considered malicious but may also be normal behaviour.

Example 2: A macro that is automatically executed when a document is opened is not always desirable, but not necessarily malicious.

OPSWAT

A cybersecurity company focusing on protecting criticial infrastructure. More information can be found at https://www.opswat.com/de/products/metaaccess.