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

# Technische Leistungsbeschreibung

## Securepoint Antivirus Pro

## Inhalt

# Securepoint Antivirus Pro

Securepoint Antivirus Pro ist eine zuverlässige Sicherheitssoftware mit cloudbasiertem Management. Sie schützt Windows Systeme und Daten vor bekannter und neuer Malware sowie unerwünschten Programmen

## Securepoint Antivirus Pro Portal

Das Securepoint Antivirus Pro Portal ist ein benutzerfreundliches Cloud-Management Tool für die Administration mehrerer Securepoint Antivirus Pro Installationen an unterschiedlichen Standorten. Damit können Quarantäne, Exklusionen und Einstellungen sowie geplante Scans aller Clients verwaltet werden. Das Portal ist in den Sprachen Deutsch und Englisch verfügbar, die Client-Software am Endgerät (GUI) kann in Deutsch und Englisch angezeigt werden.

### Kernfunktionen von Securepoint Antivirus Pro

- Verhaltensanalysen zur Erkennung von Bedrohungen anhand ihres Verhaltens oder schädlicher Merkmale
- Analysen in mehrstufigen automatisierten Verfahren
- Isolieren von erkannten Bedrohungen in der Quarantäne
- Automatische Benachrichtigungen bei Virenfund

## IKARUS T3 scan.engine

Securepoint Antivirus Pro verwendet die VB100-zertifizierte IKARUS T3 scan.engine mit Multithreading. Sie garantiert eine zuverlässige Erkennung von Malware und potenziell unerwünschten Programmen oder Anwendungen (PUP/PUA).

### Arbeitsweise der IKARUS T3 scan.engine

Jede Datei durchläuft bei der Überprüfung durch die Engine in Antivirus Pro mehrere Prozesse:

- Hashes der Datei werden analysiert
- Abgleich der Hashes mit Black- und Whitelists
  - *Der Wert befindet sich auf der Whitelist:* Die Datei gilt als „sauber“ und ist nicht infiziert
  - *Der Wert befindet sich auf der Blacklist*: Die Datei gilt als „Bedrohung“ und wird sofort unter Quarantäne gestellt
  - *Keine Übereinstimmung mit den Listen:* weitergehende Analysen
- Dateityp wird anhand von Analysen identifiziert
- Verhalten der Datei wird analysiert:

- Der Code wird zuerst statisch und dann dynamisch betrachtet (Sandboxing). Dabei wird analysiert: Was macht die Datei? Auf was zielt es ab? Worauf versucht es zuzugreifen?
- Die extrahierten Informationen werden mit anderen bekannten Bedrohungen abgeglichen
- Für jeden Dateityp sind unterschiedliche Vorgänge definiert:
  - Archive werden entpackt, um jedes Dokument einzeln zu überprüfen
  - Passwortgeschützte Dateien werden zu öffnen versucht, um sie anschließend zu überprüfen

Die Analyse kann drei unterschiedliche Ergebnisse liefern:

- Sauber: Die Datei ist nicht infiziert.
- Malware: Die Datei ist infiziert und wird sofort isoliert (unter Quarantäne gestellt).
- Potentielle unerwünschte Anwendungen/Programme (PUA/PUP): Die Datei / das Programm ist unerwünscht und wird sofort isoliert (unter Quarantäne gestellt).

## Sandboxing

Für die weitergehende Analyse verdächtiger Dateien wird zusätzlich eine eigens entwickelte Sandbox-Umgebung eingesetzt. In diesem virtuellen, vollständig isolierten Umfeld werden bei Bedarf Überprüfungen durchgeführt, indem Verhaltensweisen und andere Merkmale analysiert werden, um mögliches schädliches Verhalten zu erkennen.

## Feedback Loop

Die Scan Engine in Antivirus Pro fungiert als „Feedback loop“. Sie **analysiert** erst, **extrahiert** anschließend die Dateiinformationen und **kontrolliert** diese zuletzt. Dieser Vorgang wird so oft wiederholt, bis:

- Malware/PUA/PUP gefunden wurde.
- alle Informationen der Datei und deren Inhalte (verstecke Dateien, Links etc.) bekannt und überprüft sind, daher nichts mehr geprüft werden kann und sie als „sauber“ gilt.
- die Prüfungszeit abgelaufen ist. Danach wird die geprüfte Datei als „sauber“ markiert.
- nähere Überprüfungen notwendig werden (beispielsweise bei unbekanntem Dokumenttyp) und das das Dokument automatisch an das Analyse-Team Team weitergeleitet wird.

Die Scan Engine in Antivirus Pro analysiert und extrahiert alle benötigten Informationen und gleicht sie laufend mit der Virendatenbank ab. Damit diese immer auf dem aktuellsten Stand ist, erhält sie mehrmals täglich Updates.

## Dateistatus

### Sauber (clean)

In einer sauber“ beziehungsweise „clean“ deklarierten Datei, wurden von Securepoint Antivirus Pro keine Bedrohungen gefunden.

### Malware

Malware ist bösartig und versucht über unerwünschte Verhaltensweisen im infizierten System Schaden anzurichten.

Hinweis: Auch Android-, Linux- oder auf andere Systeme optimierte Malware kann auf einem Windows-System Schaden anrichten und wird daher als bösartig erkannt.

### Potentiell unerwünschte Anwendungen/Programme (PUA/PUP)

PUAs/PUPs sind per se nicht schädlich, jedoch meistens unerwünscht. Häufig werden sie automatisch bei einem Download mit heruntergeladen. Die Scan Engine in Antivirus Pro erkennt diese und stellt sie unter Quarantäne.

Beispiele für PUAs/PUPs: Toolbars, Chip Installer, Key Generator

## Das Engine-Ranking-System

Die Scan Engine in Antivirus Pro arbeitet mit einem Engine-Ranking-System, das drei Klassifizierungen aufzeigt:

1. Malware (höchste Stufe)
2. PUA
3. Sauber

Eine Datei kann mehrere Verhaltensweisen aufzeigen. In diesem Fall wählt die Scan Engine automatisch das höchste Ranking.

*Beispiel: Eine von der Scan Engine geprüfte Datei weist Merkmale von PUA und Malware auf. Aufgrund der zwei Klassifizierungen wird automatisch das Ranking-System angewendet. Da Malware im Ranking höher als PUAs liegt, wird die geprüfte Datei als Malware eingestuft.*

## Klassifizierungen der Scan Engine in Antivirus Pro

Unbekannte Dateien können unter Umständen als „false-negativ“ oder „false-positive“ eingestuft werden.

- *Ein false-positive Ergebnis* wird als „*infiziert“* erkannt, obwohl es sich um eine „*saubere“* Datei handelt.

  false-positive Ergebnisse sind sehr selten. Bei Verdacht auf ein false-positive Ergebnis senden Sie die betroffene Datei bitte über die Quarantäne-Funktion an das Analyse-Labor. Dort wird die Datei erneut überprüft und ggf. freigeschalten.

- *Ein false-negative* Ergebnis wird als „*sauber“* klassifiziert, obwohl es sich um eine infizierte Datei handelt.
  False-negative Ergebnisse können bei gänzlich unbekannten Malware-Formen auftreten. Durch die mehrstufigen Analysen der Scan Engine in Antivirus Pro und das erneute Überprüfen aller Files nach jedem Virendatenbankupdate („Re-Analysis“) sind sie jedoch äußerst selten. Werden false-negative Ergebnisse identifiziert,

kommen diese sofort auf die Blacklist, sodass sie keinen Schaden mehr anrichten können.
Bei Verdacht auf ein false-negative Ergebnis senden Sie die betroffene Datei bitte an das Analyse-Labor.

## Die Quarantäne- und Benachrichtigungsfunktion

Wurde eine verdächtige Datei gefunden, wird der Zugriff auf diese blockiert und ein Eintrag in der Quarantäne erfolgt. Über die Quarantäne kann im Management-Portal oder in der Client-Software entschieden werden, was mit der gefundenen Datei geschehen soll (z.B. Datei löschen).

Im Securepoint Antivirus Pro Portal können Sie E-Mail-Benachrichtigungen über definierte Ereignisse wie zum Beispiel einen Virenfund aktivieren.

## Dokumente in der Prüfung von Securepoint Antivirus Pro

Securepoint Antivirus Pro prüft alle Arten von Dateien, Programmen oder Anwendungen aus jeder Quelle (Download, Wechseldatenträger, etc.), vor jedem Öffnen. Dieser automatische Scanvorgang kann im Client oder im Securepoint Antivirus Pro Portal aktiviert oder deaktiviert werden.

### Unterschiedliche Scanarten

Securepoint Antivirus Pro ermöglicht umfassende Scans zu individuellen Zeitpunkten.

- **On-Access Scan**: Überprüft alle Lese- und Schreibvorgänge einer Datei oder eines Prozesses in Echtzeit.
- Geplante **On-Demand Scans** und **Scanprofile**: Der On-Demand Scan ist für definierte und manuelle Scans auf einzelne Dateien, Ordner oder auch Laufwerke zuständig. Standartmäßig sind vier Scanprofile vorhanden, welche individuell im Client oder im Management Portal zu frei definierbaren Zeiten konfiguriert, gestartet und gestoppt werden können.
  *Unser Tipp: Wir empfehlen, ein tägliches Scanprofil zu definieren, das automatisch auf Malware und PUA scannt. Verpasste Scans können über die Funktion „Scan nachholen“ im Scanprofil automatisch nachgeholt werden.*
- **Individuelle Scans:** Über das Kontextmenü können Dateien oder Ordner jederzeit individuell gescannt werden.
  *Klicken Sie vor dem Öffnen der Datei mit der rechten Maustaste auf das Dokument und wählen Sie „Überprüfung durch Securepoint Antivirus Pro“*

### Prüfung von Microsoft Office Dokumenten

In Microsoft Office Dokumenten wird zusätzlich zur Malware auch nach bösartigen Makros gesucht. Auch hier werden das Verhalten **analysiert** sowie Dateiinformationen **extrahiert** und **kontrolliert**.

### Die Dauer eines Scans

Genaue Zeitangaben können nicht gegeben werden, da es unter anderem auf die Größe und die Komplexität der gescannten Datei ankommt. Die Engine überarbeitet und überprüft im Durchschnitt an einem Endpunkt / Client ca. 1.000 Dateien pro Sekunde im On-Access Scan. Abhängig von der Hardware kann davon ausgegangen werden, dass die Zeit zwischen 0,01 Millisekunden und fünf Sekunden (für spezielle Dateien) liegt.

## Vorteile von Securepoint Antivirus Pro

### Ressourcenschonender Betrieb mit Securepoint Antivirus Pro

Je schneller eine Antivirus-Software arbeitet, desto schneller ist der Rechner. Darum wurde die Scan Engine in Antivirus Pro von Grund auf in Richtung Skalierbarkeit und Ressourcenschonung entwickelt. Verschiedene Betriebsarten (Speicher oder Disc-optimiert) sowie eine nahezu lineare Steigerung der Leistungsfähigkeit durch Erhöhung der parallelen Threads resultieren in einem der leistungsfähigsten Gesamtsysteme am Markt. Dank der schnellen Arbeitsweise von Securepoint Antivirus Pro ist es sehr energieeffizient und sorgt daher für längere Akkulaufzeiten bei Laptops oder Notebooks.

### Maschinelles Lernen

Die Scan Engine in Antivirus Pro erkennt anhand des Benutzerverhaltens, welche Dokumente, Programme, etc. am häufigsten benutzt werden. Diese werden beim Scan priorisiert, um die Leistung des Systems zu optimieren.

### Analyseinformationen über die SigQA (Signature Quality Assurance Programm)

SigQA, dient dazu die auf Signatur basierende Erkennung zu verbessern. Signaturen dienen dazu, viele CRCs auf eine einzelne Erkennungsroutine zusammenzufassen. Um eine false-positive Erkennung zu verhindern, werden diese im ersten Schritt stumm mitgeschickt so dass diese bei einer Erkennung nur die Telemetrie-Daten senden.

### Die OPSWAT Schnittstelle

Securepoint ist OPSWAT Platin zertifiziert. Diese Schnittstelle übermittelt via IMACI die Informationen an OPSWAT, dass eine aktuelle Virendatenbank integriert und der Client geschützt ist sowie keine Bedrohungen vorliegen. Daher kann die Scan Engine in Antivirus Pro in den OPSWAT MetaDefender miteingebunden werden

### Passwort-Schutz für Einstellungen am Client

Administratoren haben die Möglichkeit, alle Einstellungsmöglichkeiten für Clients zu sperren, indem ein Passwort für Änderungen abgefragt wird. Alle Einstellungen und Aktionen werden damit einheitlich über das Securepoint Antivirus Pro Portal oder lokal mit der Eingabe eines Passworts verwaltet. On-Demand-Scans und individuelle Scans können weiterhin ohne Passwortabfrage von den Usern gestartet werden.

## ELAM bei Securepoint Antivirus Pro

ELAM (Early Launch Anti Malware) ist eine Frühstartfunktion von Microsoft, die Securepoint Antivirus Pro schon beim Boot startet. Außerdem schützt sie den Prozess vor Fremdzugriffen, die ihn stoppen wollen.

# Wichtige Kontaktdaten:

## Securepoint Support

Support-Hotline:
04131/2401-0
support@securepoint.de

## Analyse-Labor

probe@ikarus.at

# Glossar

### Bedrohungen

„Bedrohungen“ beinhaltet sowohl Malware als auch PUA/PUP.

### GUI / Graphical User Interface

Interface von Securepoint Antivirus Pro direkt am Client (Computer)

### Makros

Makros sind automatisierte im Hintergrund ablaufende Funktionen, die das Arbeiten in den MS Office Anwendungen erleichtern sollen. Makros wurden von Microsoft erfunden, um Anwendenden ein einfacheres Arbeiten und Unternehmen Prozessoptimierungen zu ermöglichen. Markos sind nicht automatisch gefährlich, sie können jedoch Bedrohungen als Tarnung dienen. Sie werden erst als bösartig klassifiziert, wenn eine Bedrohung nachgewiesen wurde.

*Beispiel 1: Das Herunterladen eines Bildes, um es in ein Dokument zu kopieren, kann als bösartiges, aber auch als normales Verhalten betrachtet werden.*

*Beispiel 2: Ein Makro, das automatisch ausgeführt wird, nachdem das Dokument geöffnet wurde, ist nicht immer wünschenswert, aber auch nicht zwangsläufig bösartig*.

### OPSWAT

Ist ein Cybersecurity-Unternehmen mit Schwerpunkt auf dem Schutz kritischer Infrastrukturen. Nähere Informationen finden Sie unter https://www.opswat.com/de/products/metaaccess.