WEGWEISER · 1ページ資料

Software Watch

誰も許可していないソフトウェアを見つける。

ウイルス対策ソフトはマルウェアには強い一方で、開発者が入れたAIのコーディング支援ツール、作業したエンジニアが残していったAnyDesk、ユーザープロファイルの下で動くマイニングについては何も言いません。ITサービス事業者や情シスが聞かれるのは、まさにそうした質問です。Software Watchは、ウイルス対策ソフトを補うものとして、管理しているすべての端末でそれを確認します。

7
検出カテゴリー、それぞれにスイッチ

1
1日1回のスキャン、設定不要

0
隔離したファイル、停止したプロセス

Unsanctioned software — Tell me

Tools installed on a client machine without going through you: AI assistants, developer CLIs, and the things people install for themselves.

> Not malware, and that is the point - your antivirus is deliberately quiet about it. This is the licensing, data governance and "who put that there" question, and it is the one you get asked about.

LOOKS LIKE
Claude Code, GitHub Copilot CLI, Gemini CLI, Ollama, LM Studio, ChatGPT Desktop
CHECKS
13 on the daily sweep, 31 on a deep scan, 18 of them on trial
FOUND SO FAR
280 on your estate

Targeted attack tooling — Tell me

Tools associated with organised and state-backed intrusion groups.

> Rare, and serious the one time it is not. If this fires it is worth stopping what you are doing.

LOOKS LIKE
Cobalt Strike, Mimikatz, known intrusion-set toolkits
CHECKS
613 on the daily sweep, 2,611 on a deep scan, 1,196 of them on trial
FOUND SO FAR
143 on your estate

Known malware and criminal toolkits — Tell me

Files matching known malicious software: ransomware, banking trojans, loaders, and the kits sold to run them.

> Your antivirus should catch most of this. We look as well, because a second opinion on a machine you have just taken over is worth having.

LOOKS LIKE
Ransomware families, loaders, credential stealers
CHECKS
89 on the daily sweep, 2,960 on a deep scan, 2,767 of them on trial
FOUND SO FAR
6 on your estate

What we look for（検出対象）の画面（英語版）。7つのカテゴリーを平易な言葉で示し、それぞれのチェック数、IT環境で見つかったもの、スイッチを1つずつ表示します。

検出するもの

7つのカテゴリーに、それぞれスイッチが1つあります。許可されていないソフトウェア、標的型攻撃のツール、既知のマルウェアと犯罪用ツールキット、スパイウェアと監視ツール、攻撃コードとバックドア、不審なパターン、コミュニティによる幅広い検出（初期設定でオフ）です。スイッチで決まるのは何を知らせるかで、スキャンでは常にすべてを確認します。

仕組み

1. スケジュールの設定は要りません。数分ごとに最も間隔が空いている数台をスキャンし、負荷の山を作らずに全端末をおおむね1日1回確認します。月に1回は、カタログ全体の詳細スキャンも行います。
2. チェックの出所は、当社が手作業で書いたルール、signature-base、45以上の審査済み公開ソースをまとめて毎週更新されるYARA-Forgeです。新しいチェックは試験運用から始まり、十分な数の端末で問題なく動いてからDetections（検出）画面に出ます。
3. 検出結果にはAIの判定が付き、端末の健全性スコアに反映されます。自社の管理ツールなら、一度却下すれば以後も却下されたままです。
4. 独自のルールはウィザードで作れます。「お客様のPCにSteamが入っていたら知らせてほしい」なら、インストール済みプログラム、サービス、ファイルの詳細、テキスト、ハッシュから指定し、どこに一致するかを試してから保存します。

しないこと

報告はしますが、手は出しません。隔離も、プロセスの停止も、端末の切り離しもしません。お客様の本番サーバーで頼まれてもいない隔離が起きるのは、自分で判断できる検出結果よりも悪い結果だからです。端末が受け取るのは暗号化されたルールパックだけで、スキャンは負荷を抑え、大きすぎるファイルは飛ばします。