

WEGWEISER · ON ONE PAGE

Software Watch

It finds software nobody sanctioned.

Antivirus is good at malware and is built to say nothing about a developer installing an AI coding assistant, a technician leaving AnyDesk behind, or a miner running under a user profile. Those are the questions an MSP gets asked. Software Watch checks every managed machine for them, as a complement to your antivirus.

7
detection families, one switch each

1
sweep a day, nothing to schedule

0
files quarantined, processes killed

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: the seven families in plain words, how many checks each carries, what it has found on your estate, and one switch each.

WHAT IT LOOKS FOR

Seven families, each with one switch: unsanctioned software, targeted attack tooling, known malware and criminal toolkits, spyware and monitoring tools, attack code and back doors, suspicious patterns, and broad community detections, which are off by default. The switch decides what you are told about; every scan still checks for everything.

HOW IT WORKS

1. There is nothing to schedule. A few machines are scanned every few minutes, whichever are most overdue, so the fleet is swept about once a day without a load spike. Once a month each machine also gets a deep scan of the whole catalogue.
2. The checks come from our own hand-written packs, from signature-base, and from YARA-Forge, which gathers more than 45 vetted public sources and is refreshed weekly. Every new check starts on trial and reaches your Detections only after it has run cleanly on enough machines.
3. A finding gets an AI verdict, feeds the device's health score and appears in Detections. If it's your own admin tool, dismiss it once and it stays dismissed.
4. Your own rules: "tell me when Steam is on a client machine" is answered in a wizard, by installed program, service, file details, a piece of text or a file hash. Try it, see where it matches, save it. No detection language to learn.

WHAT IT WON'T DO

It reports and doesn't act: no quarantine, no killed process, no isolated machine. An uninvited quarantine on a client's production server is a worse outcome than a finding you get to judge. Machines receive compiled, encrypted rule packs only, scanning is throttled and oversized files are skipped, so it stays out of the way of the client's work and their antivirus.