

WEGWEISER · AUF EINER SEITE

Softwareüberwachung

Sie findet Software, die niemand freigegeben hat.

Virenschutz ist gut bei Schadsoftware und schweigt bewusst, wenn ein Entwickler einen KI-Programmierassistenten installiert, ein Techniker AnyDesk zurücklässt oder unter einem Benutzerprofil ein Miner läuft. Die Softwareüberwachung prüft jedes betreute Gerät darauf, als Ergänzung zum Virenschutz.

7
Erkennungsgruppen, je ein Schalter

1
Durchlauf am Tag, nichts zu planen

0
Dateien in Quarantäne, Prozesse beendet

Nicht freigegebene Software

Melden

Werkzeuge, die ohne Ihr Zutun auf einem Kundenrechner landen: KI-Assistenten, Entwicklerwerkzeuge und alles, was Anwender selbst installieren.

> Keine Schadsoftware, und genau darum geht es - Ihr Virenschutz schweigt hier bewusst. Es ist die Frage nach Lizenzen, Datenschutz und "wer hat das installiert", und es ist die Frage, die Ihnen gestellt wird.

ZUM BEISPIEL
Claude Code, GitHub Copilot CLI, Gemini CLI, Ollama, LM Studio, ChatGPT Desktop

PRÜFUNGEN
13 im täglichen Durchlauf, 31 im Tiefenscan, davon 18 auf Probe

BISHER GEFUNDEN
280 in Ihrem Bestand

Werkzeuge gezielter Angriffe

Melden

Werkzeuge, die organisierten und staatlich gestützten Angreifergruppen zugeordnet werden.

> Selten, und in dem einen Fall ernst. Wenn das anschlägt, lohnt es sich, alles andere liegen zu lassen.

ZUM BEISPIEL
Cobalt Strike, Mimikatz, known intrusion-set toolkits

PRÜFUNGEN
613 im täglichen Durchlauf, 2,611 im Tiefenscan, davon 1,196 auf Probe

BISHER GEFUNDEN
143 in Ihrem Bestand

Bekannte Schadsoftware und Angriffsbaukästen

Melden

Dateien, die zu bekannter Schadsoftware passen: Ransomware, Banking-Trojaner, Loader und die Baukästen, mit denen sie betrieben werden.

> Ihr Virenschutz sollte das meiste davon finden. Wir schauen ebenfalls hin, weil eine zweite Meinung zu einem gerade übernommenen Rechner ihren Wert hat.

ZUM BEISPIEL
Ransomware families, loaders, credential stealers

PRÜFUNGEN
89 im täglichen Durchlauf, 2,960 im Tiefenscan, davon 2,767 auf Probe

BISHER GEFUNDEN
6 in Ihrem Bestand

Wonach wir suchen: die sieben Gruppen in klaren Worten, wie viele Prüfungen jede enthält, was sie in Ihrem Bestand gefunden hat, und je ein Schalter.

WONACH SIE SUCHT

Sieben Gruppen, jede mit einem Schalter: nicht freigegebene Software, Werkzeuge gezielter Angriffe, bekannte Schadsoftware und Angriffsbaukästen, Spyware und Überwachungssoftware, Angriffscode und Hintertüren, auffällige Muster sowie breite Community-Signaturen (standardmäßig aus). Der Schalter entscheidet, worüber Sie informiert werden; geprüft wird immer alles.

SO FUNKTIONIERT ES

1. Nichts zu planen: Alle paar Minuten werden die am längsten fälligen Geräte geprüft, so wird der Bestand etwa einmal am Tag durchlaufen, ohne Lastspitze. Einmal im Monat kommt pro Gerät ein Tiefendurchlauf mit dem ganzen Katalog dazu.
2. Die Prüfungen stammen aus unseren eigenen Paketen, aus signature-base und aus YARA-Forge (über 45 geprüfte Quellen, jede Woche neu). Jede neue Prüfung läuft zuerst auf Probe und erscheint erst unter Ihren Erkennungen, wenn sie auf genügend Geräten ohne Fehlalarm gelaufen ist.
3. Ein Fund bekommt eine KI-Einschätzung, fließt in den Zustandswert des Geräts ein und erscheint unter Erkennungen. Ihr eigenes Admin-Werkzeug blenden Sie einmal aus, dann bleibt es weg.
4. Eigene Regeln: „Melde mir, wenn Steam auf einem Kundenrechner ist“ legen Sie in einem Assistenten an, über Programm, Dienst, Dateieigenschaften, einen Text oder einen Datei-Hash. Ausprobieren, sehen, wo sie greift, speichern.

WAS SIE NIE TUT

Sie meldet und greift nicht ein: keine Quarantäne, kein beendeter Prozess, kein isoliertes Gerät. Eine ungefragte Quarantäne auf dem Produktivserver eines Kunden ist schlimmer als ein Fund, den Sie selbst beurteilen. Auf den Geräten liegen nur verschlüsselte Regelpakete, und die gedrosselte Prüfung stört weder die Arbeit des Kunden noch seinen Virenschutz.