TRACKWATCH®

Human insights powered by AI for Enhanced Detection

GATEWATCHER

Detecting Advanced Cyber Threats : The New Challenge for Organizations

The financial consequences of a cyber attack can durably weaken your organization.

The growth in the volume of threats complicates the alert criticity assessment handled by your analysts.

The persistence of an undetected targeted attack can increase the prejudice caused to your information system.

The stealth and complexity of the latest cyber attacks increase the risk of compromise for your IT infrastructure.

3,86M$

Is the average global cost of a data security breach in 2020. [1]

255%

growth in the number of ransomware attacks in France between 2019 and 2020. [2]

207 days

is the average time it takes for a company to detect a security breach. [3]

53%

of successful intrusions are not detected by the cyber detection tools already in place. [4]

Trackwatch® : An intelligent platform to detect and analyze the most advanced threats and intrusions, in real time.

☑ **In-depth files analysis**
Trackwatch® detects all types of malware by scanning through multiple anti-virus engines. The platform can scan up to 6 million files per 24 hours.

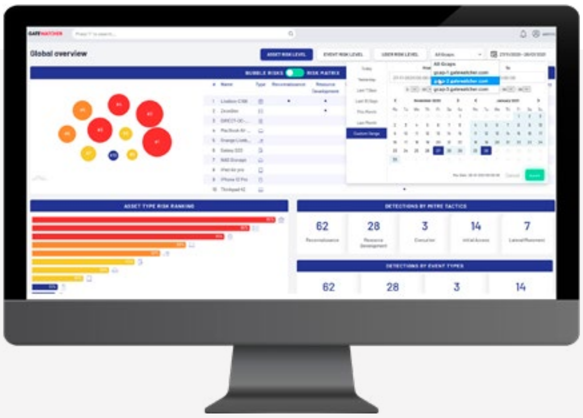
☑ **Payload control**
Trackwatch® performs an advanced protocol analysis on packets in order to compare them to known attack signatures and allows the detection of polymorphic shellcodes, and any encoded payloads.

☑ **Better visibility over hidden threats**
Trackwatch® embeds AI algorithms allowing the detection of complex attacks to be spotted (malicious PowerShell scripts, DGA attacks, SMB flows in ransomware attack scenarios...).

☑ **Alert at the very first sign of an attack**
Trackwatch® detects the weak signals of fileless attacks and advanced threats not yet identified, thanks to a multi-vector analysis of network flows: static, dynamic and by machine learning.

Trackwatch® combines advanced flow analysis with innovative methods to detect abnormal behavior on the network. Its combination of multiple detection technologies allows the platform to continuously adapt to polymorphic threats, guaranteeing a very strong relevance to the ever increasing sophistication of advanced persistent attacks (APTs).

Operational as soon as it is set up, Trackwatch® combines machine learning algorithms that identify unknown activities with various network traffic analysis methods (static, dynamic and heuristic). This approach provides increased visibility on malicious actions in motion and contextualizes each alert.



Sources : [1] Ponemon Institute, [2] ANSSI, [3] IBM, [4] FireEye Mandiant

User benefits

DETECTION TECHNOLOGY QUALIFIED BY ANSSI

Trackwatch® was awarded the elementary qualification from the french ANSSI in 2019. This endorsement certifies the platform software and hardware resilience, and allows its use by OIVs in their compliance with the french LPM.

INSTANTLY FUNCTIONAL PROTECTION

Trackwatch® does not require additional equipment or hidden costs. The solution is easy to set up and detects threats and intrusions immediately.

STRONG INTEROPERABILITY WITH YOUR EQUIPMENT

Trackwatch® offers interconnection possibilities with all SIEMs on the market, as well as with MISP, EPP, EDR, proxies...

A PLATFORM THAT COMBINES SCALABILITY AND PERFORMANCE

Trackwatch® offers a wide range of appliances offering throughputs from 10MBPS to 40 GBPS without any compromise on performance with up to 27000 EPS processable in burst compared to 1200 on average on the market.

A FLEXIBLE SOLUTION

Trackwatch® can operate in connected mode or completely offline for restricted networks. You remain in control of your information. Its TAP bypass position guarantees no impact on your production environment.

OPTIMIZED EFFICIENCY FOR YOUR SOC

Trackwatch®, generates contextual metadata that simplifies the investigation work of SOC analysts and their handling of alerts criticity. It also contribute to shorten the remediation time.

Use cases

Spot a ransomware attack in real time
Trackwatch® is able to detect the specific elements of these attacks: recovery of the key from a C&C, identification of suspicious SMB flows or detection of malicious attachments in an email. The platform gives you the advantage to react as soon as possible.

- Detection of silent movements on the network and obfuscated exploitation techniques.
- Detection of ransomware before it is executed.
- Prevents loss of control of your information system and possible financial or reputational damage.

React at the first signs of a targeted attack
Trackwatch® is the only solution able to cover the entire Kill Chain of an advanced cyber attack and to identify the exploitation techniques used throughout its course.

- Advanced level of detail on the attack: target user, opening of sockets, in-depth analysis of the code.
- Identification of an attacker as soon as he enters the network.

Comply with the French military planning act (LPM)
Integrating software and hardware hardening requirements into its very design, Trackwatch® has the ANSSI's basic qualification and allows you to comply with the french military panning act requirements with a simple deployment in a PDIS type architecture.

- Simple and efficient detection compliance with the MPL.
- Long-term qualified products.

Identify security policy violations
Trackwatch® is the perfect tool for strict enforcement and control of your security policy. It provides a mapping and inventory of all your network traffic useful to your cyber analyst team who can establish the most critical events and develop the appropriate security policy.

- Any attempt to violate your security policy will be immediately flagged with an alert.
- Comprehensive and smooth control of your traffic.

About us

Gatewatcher is a leading european software vendor specialized in the detection of the most advanced cyberthreats and intrusions. Its unique model combines several technologies with A.I. to provide you optimal protection.

Contact us

contact@gatewatcher.com
www.gatewatcher.com