

Rooma X-WING **AI-native** NG-EDR

Supports public cloud SaaS Free trial available

# Faster security Boost business

Covering the MITRE ATT&CK Framework, and coupling cloud-native architecture with kernel-level lightweight sensors, detects stealthy, new types of attacks fastly.

Traditional endpoint security products  
**SLOW**

**VS** Rooma X-WING AI-native NG-EDR  
**FAST**

How quickly to catch new types of attacks?

**Threat detection Intelligent technology, detects in minutes!**

- ✗ AV  
Relies on characteristics such as file HASH for detection, making it difficult to discover new attacks without known patterns.
- ✗ Ordinary EDR  
Generates a large number of detections, making it challenging to get priorities straight. It requires both heavy manual involvement and a huge amount of time, leading to slow analysis of attacks.

- ✓ Behavior-based intelligent detection technology can accurately identify attacks even if file characteristics such as HASH keep changing.
- ✓ Intelligent aggregation of threat incident ensures valuable clues are not in floods of alerts, allowing rapid detection of new attacks.

How fast to generate threat report?

**Attack traceback Generative AI, instant reporting!**

- ✗ It will take experts days to investigate and tracks different security-related events before complete a report.

- ✓ Leverages generative AI, and threat reports can be directly generated or exported from the display showing attack details and contexts.

How rapid does the sensor run?

**Data collection Kernel-level lightweight sensor, no system slowdown!**

- ✗ CPU usage exceeds 1% or even 10%, and memory usage ranges from tens of megabytes to several hundred megabytes.

- ✓ Typically, endpoint CPU usage is less than 0.1%, and memory usage is under 15M.

How fast is the installation and deployment?

**Installation and deployment SaaS deployment, just login and use!**

- ✗ Both procurement and installation are complex. It usually takes days or even weeks before users can use the product.

- ✓ Supports public cloud SaaS deployment, allowing users to start using by downloading and installing lightweight sensors from the cloud.

**>400**

Covers 400+ ATT&CK techniques

**>2000**

Supports 2000+ detectable attack patterns

**<0.1%**


typical endpoint CPU usage < 0.1%

**<15M**

typical endpoint memory usage <15M



# Summary of Competitive Analysis

Core index		 Rooma X-WING	CrowdStrike	Microsoft ATP	An EDR enterprise in China	Sysmon
Event collection capability	ATT&CK DataSource coverage	>100%	100%	100%	90%	10%
	Event type	48	46	21	40+	27
	Event number	500	482	-	90+	27
Sensor Resources Consumption	-CPU usage	<0.1%	<1%	1%	5%	0.3%
	-Memory usage	<15M	227M	70M	30M	15M

Data source: public materials or measured data

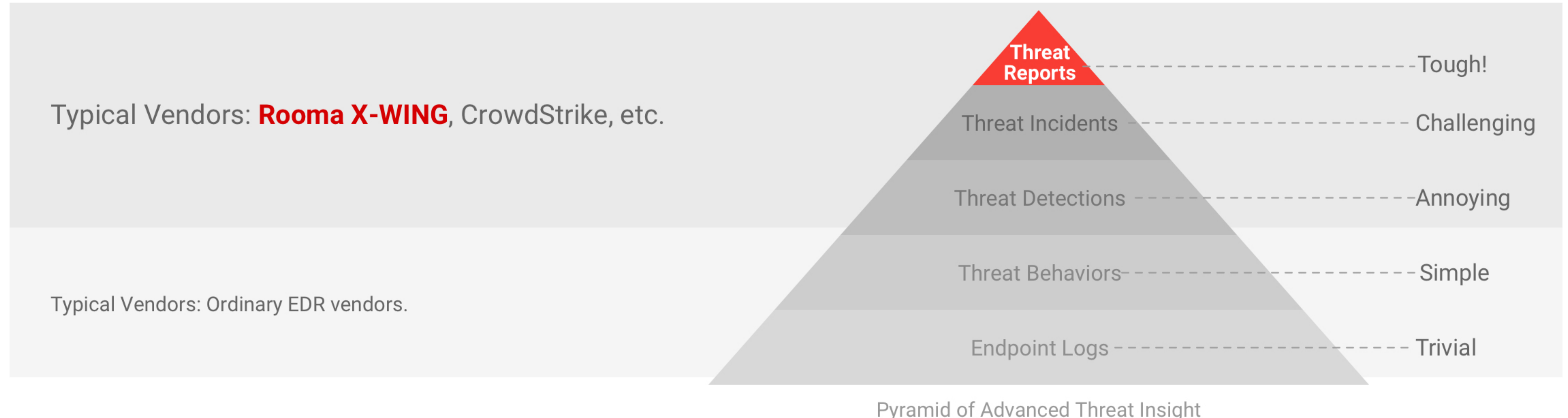
## How Does Rooma Achieve This?

### Superior Kernel-Level Lightweight Sensor

Leverages kernel-level data collection technology, collecting endpoint behavior logs and ensuring no system slowdown.

### Powerful Advanced Threat Hunting Capability

Based on massive logs, efficiently and intelligently detects threat incidents using Rooma's distinctive algorithms and rapidly generates threat reports restoring the attack process, which saves time and effort.



## Typical Application Scenarios

### Against Ransomware Attacks

In-depth detection based on threat behavior and data recovery guarantee provide dual protection.

### Against Fileless Attacks

Combining static memory detection and dynamic behavior monitoring, makes fileless attacks have nowhere to hide.

### Against Phishing Attacks

Coupling static characteristics with dynamic behavior tracking, ensures no new bait is missed.

### Against Mining Attacks

Focusing on threat behaviors, accurately discovers mining pools and machines.

## About Rooma Faster security Boost business

Established in 2021, the founding team members of Rooma Technology (Beijing) Co., Ltd. come from well-known security companies and have more than ten years of experience in the cybersecurity industry. Rooma, takes the actual combat effect of offense and defense as the gold standard for evaluating products, and is committed to solving the problem of undetectable and slow detection of advanced threats in the industry. The self-developed Rooma X-WING AI-native NG-EDR adopts a cloud-native architecture, equipped with a kernel-level lightweight sensor, and the intelligent threat behavior detection mode covers the ATT&CK security framework, which can quickly identify advanced, complex, and new attacks with strong concealment. Leveraging generative AI, X-WING can quickly output attack analysis and traceability reports, saving users valuable time to focus on their business.

✉ support@xrooma.com

For a free trial, please visit Rooma's official website: xrooma.com © 2024 Rooma Sec. All Rights Reserved.