AI-native NG-EDR

Supports public cloud SaaS **Available for free trial**

Faster security
Boost business

Covers the ATT&CK security framework, cloud-native architecture equipped with kernel-level lightweight sensors, detecting new and concealed attacks quickly.

Traditional security products

SLOW

VS

Our NG-EDR

FAST

How fast is it of capturing new attacks?

Threat detecion Intelligent technology, detection in minutes!

- ✗ AV
  Relying on features like file HASH for detection, making it difficult to discover new attacks without known patterns.
- ✗ Regular EDR
  Generating a large number of detections, making it challenging to distinguish priorities. It requires extensive manual involvement, making the analysis of attacks slow.

- ✓ Behavior-based intelligent detection can accurately identify attacks even as file characteristics (such as HASH) constantly change.
- ✓ Intelligent aggregation of threat events ensures valuable clues are not drowned in a sea of detections, enabling rapid detection of new attacks.

How fast is the threat report output?

Attack traceback Generative AI, instant reporting!

- ✗ The content of reports requires manual investigation and tracing, taking at least several days to complete.

- ✓ Using generative AI can directly generate threat reports with detailed attack information and contextual information.

How fast does the sensor operate?

Data collection Lightweight sensor, no system slowdown!

- ✗ CPU usage exceeding 1% or even 10%, memory usage ranging from tens of megabytes to several hundred megabytes.

- ✓ Endpoint CPU usage typically below 0.1%, memory usage typically below 15M.

How fast is the installation and deployment?

Installation depolyment SaaS deployment, login now to use!

- ✗ Procurement and installation are complex, taking several days or even weeks to start using.

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

Summary of Competitive Analysis

Core index		Ours	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
Endpoint Resource Usage	**CPU usage**	<0.1%	<1%	1%	5%	0.3%
	Memory usage	<15M	227M	70M	30M	15M

Data source: public materials or measured data

How Do We Achieve This?

Outstanding Kernel-Level Lightweight Sensor

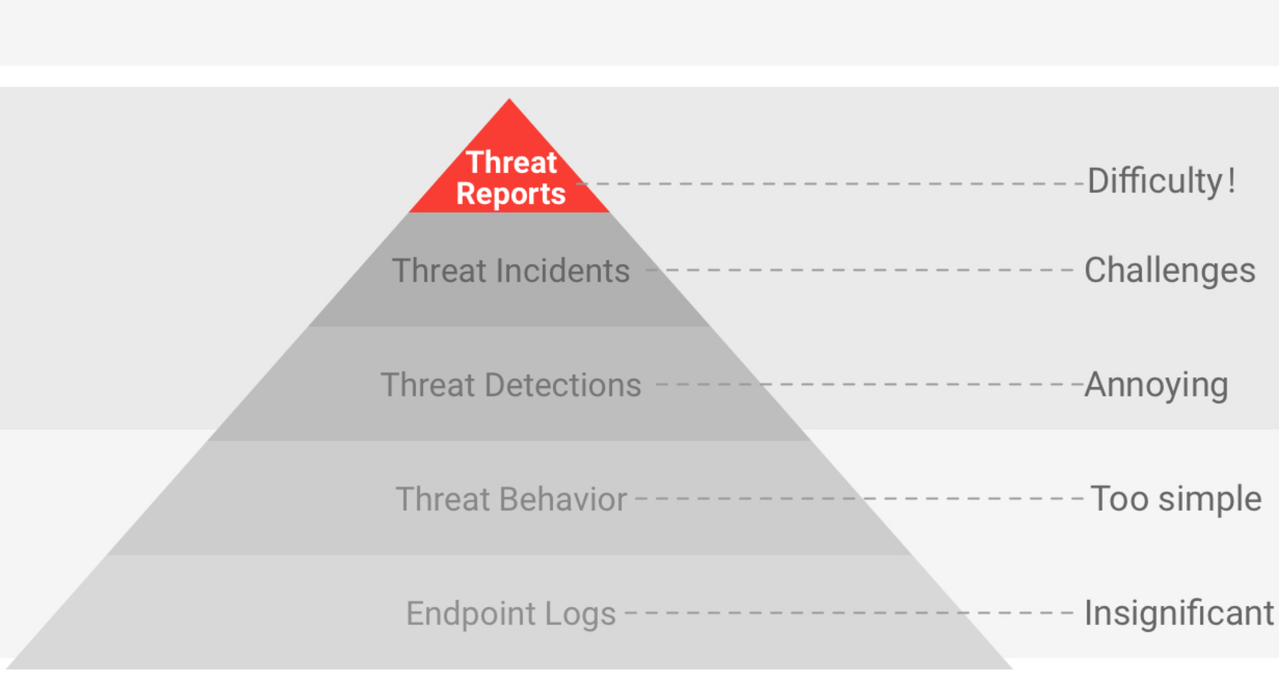
Comprehensively collect endpoint behavioral logs using lightweight sensors and kernel-level data acquisition technology, ensuring no system slowdown.

Powerful Advanced Threat Hunting Capability

Based on massive logs, using our distinctive algorithm to efficiently and intelligently detect threat events, rapidly generates threat reports, reconst acts the attack process, saving time and effort.

Represented Vendors: **ours**, CrowdStrike, etc.

Represented Vendors: Regular EDR vendors.



Pyramid of Threat Insight

Typical Use Cases

Dealing with Ransomware Attacks

Deep detection based on threat behavior, data recovery as a fallback, double protection for peace of mind.

Dealing with Fileless Attacks

Both static memory detection and dynamic behavioral monitoring, leaving no room for fileless attacks.

Dealing with Phishing Attacks

Combining static features and dynamic behavior tracking, accurately detecting new "baits".

Dealing with Mining Attacks

Focusing on threat behavior, effectively discovering mining pools and mining machines.

>400

Covers 400 ATT&CK attack methods

>2000

Supports 2000 detectable attack patterns

<0.1%

<0.1% endpoint CPU usage typically

<15M

<15M endpoint memory usage typically