



## QI-ANXIN Terminal Threat Detection and Response System

QI-ANXIN Terminal Threat Detection and Response System (EDR) is a new generation of terminal security products driven by threat intelligence. It supplements the deficiency of traditional terminal security products in the defense against advanced threats by continuously monitoring terminal activity behavior, detecting security risks, conducting in-depth investigations of threat risks, and providing remedial responses. It achieves better results and faster efficiency against high-level threats, reduces high-level threats, and ultimately achieves its goals.

### SECURITY CAPABILITIES

#### Collection

- Based on the large data storage technology, the undifferentiated collection of terminal behavior data across the network is achieved.
- Full details of collection can be refined to users, hosts, assets, and processes.

#### Respond

- Based on SkyC2, realize the collaborative linkage between EDR, Skyeye and Skylar, and realize the second level disposal of threat behavior.
- The response mode supports process blackout, terminal isolation, etc.



#### Detection

- Combine threat intelligence, abnormal traffic detection, terminal behavior detection, and other technical means to identify threat clues.

#### Analysis

- Based on the relevance analysis engine and visualization technology, the threat can be presented throughout the network.
- Combined with specific scenarios and other attack processes, further enrich global information such as threats.

### CUSTOMER VALUES

Through the effective integration of terminal big data collection, storage, detection, investigation and other functions with external threat intelligence, QI-ANXIN Terminal Threat Detection and Response System can help users detect and find hidden advanced threat events more quickly, more easily identify abnormal security conditions and restore the truth of the threat, so as to reduce the cost of threat management and the time and cost of risk response.

### PRODUCT FUNCTIONS



#### Collection and storage of terminal safety

It can continuously collect the safety-related data of the terminals of the whole network, and summarize the collected terminal safety data to the big data analysis platform in real-time for unified storage and management.



#### Advanced threat detection and warning

Combined with QI-ANXIN big data threat intelligence, threat hunting and other methods, it can quickly retrieve the terminal behavior of the whole network, accurately locate and generate alarms for advanced threat events.



### Investigation and analysis of threat events

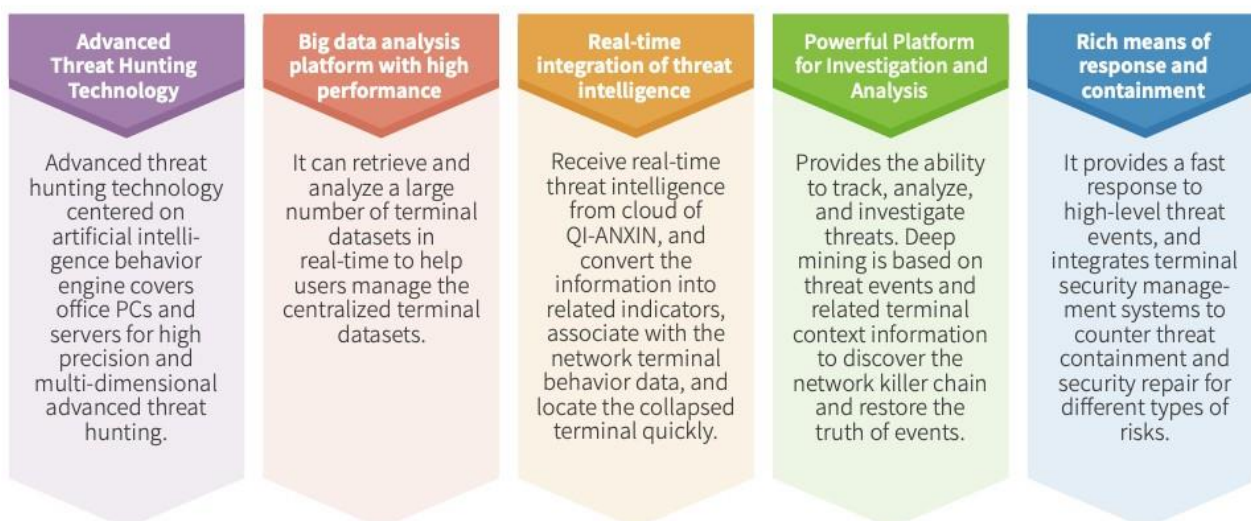
Provides the ability to search large data for terminal security, and can conduct in-depth drill-through analysis of threat events, restore the timeline of threat events. Trace its source, analyze the extent of the impact, damage, and other related information.



### Fast response to threats

Once the scope of impact is determined, the threat event can be quickly responded to, and the local risk terminal can be quickly isolated and disposed of.

## PRODUCT ADVANTAGES



## USE SCENARIOS

