

QAX Endpoint Detection & Response (EDR)

Empowering Cybersecurity with Cutting-Edge Innovations

Cyber-attacks continue to be increasingly sophisticated and widespread, posing significant threats to organizations. Cyber attackers are leveraging a wide range of tactics, techniques, and procedures to breach organizations' defenses, steal sensitive data, and disrupt critical systems. This has led to a growing need for attack lifecycle management.

Attack lifecycle management helps organizations to proactively detect and respond to cyber-attacks, reduce their impact, and minimize the risk of future attacks. By managing the entire attack lifecycle, organizations can better protect themselves against the evolving threat landscape and safeguard their digital assets.

QAX EDR

QAX EDR helps organizations detect and mitigate advanced threats quickly. Security teams can replay attack chain and identify the source of the incident with combined signals. Empowered by comprehensive threat intelligence, QAX EDR incorporates latest threat knowledge to disrupt attack, understand threat actor intent and behavior.

QAX EDR collects data from across entire organizations and integrates various hunting toolkits. Analysts get a holistic view of security infrastructure and perform investigations within just one platform.

Response to incidents needs to be performed quickly to limit the exposure. QAX EDR is designed to help you detect, understand, and stop sophisticated attacks before damage occurs.

“As a long-time user of QAX Endpoint Security, I can’t help but express my utmost satisfaction with this cutting-edge security solution. The platform has consistently delivered top-notch threat protection, detection, response with great ease of use, all of which safeguard our journey to digital transformation.”

“Long Qian - Senior Director of SOC, China Energy”

Benefits

Advanced Threat Detection

Blend of techniques such as anomaly detection, process Chain, APT intelligence, Behavior Analysis

Limit Exposure

Visibility across multiple attack vectors in one solution.

Faster Analysis

With visualization tools and streamlined search and query to fast act on incidents.

How It Works



Collection

Trillions of signals collected in real-time from over thousands customers to gain insights into attacker Tactics, Techniques and Procedures (TTPs).



Detection

Combining live threat intelligence, endpoint and cloud signals, runtime behavior detection and protection techniques, provides holistic view of the attack lifecycle.



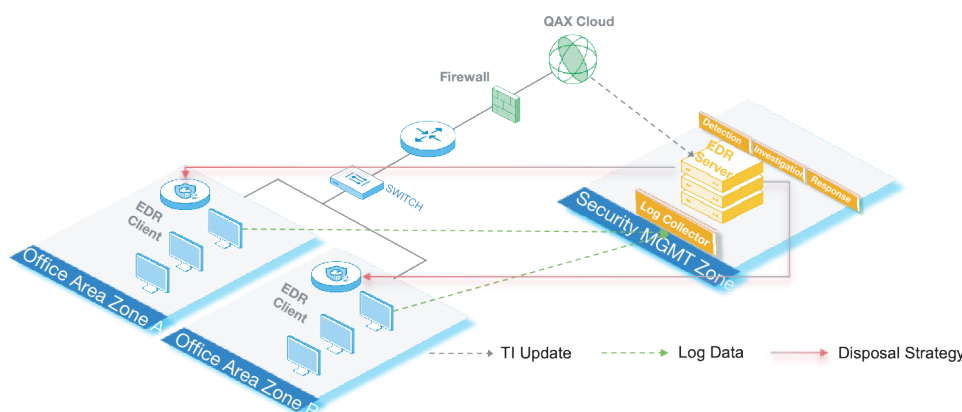
Investigation

Reduce investigation time by searching all the endpoint, network and cloud signal collected and identified. Integrate with QAX other products for broader SecOps to use case analytics.



Response

The integrated console provides collaborative between QAX EDR, NDR and EPP to respond and mitigate incidents by process blackout or isolation.



QAX Advantages

Comprehensive Threat Hunting

Security teams can quickly investigate and identify anomalies across multiple threat vectors for physical and virtual environments.

Live Threat Intelligence Integration

Real-time threat intelligence from QAX cloud for the creation of indicators to identify suspicious or malicious intent on endpoints to act quickly.

Streamlined Investigation and Analysis

Analysts have deep mining capabilities at their fingertips to perform role with visualization capabilities like process tree, cyber kill chain, context info, streamlined search & query experience, community based threat investigation experience and threat intel sharing.

About QAX

QAX, the largest cybersecurity company in China, is a leader in global cybersecurity industry, offering next-generation enterprise and national-level solutions. As the official cybersecurity and antivirus software sponsor for the Beijing 2022 Olympic and Paralympic Winter Games, QAX successfully ensured the event's security with unprecedented "Zero Incident" record.

System Requirements

Supported Systems QAX EDR Agent

Microsoft Windows:

Windows 10,11

Windows Server 2016, 2019 and 2022

macOS:

MacOS 10.15,11,12,13,14

Big Sur 11

Monterey 12(+M1)

Linux:

CentOS7.5-7.9

RedHat 7.6-7.9

BC-Linux el7.8

OpenEuler20.03(LTS-SP3)

OpenEuler22.03

RockyLinux 8