

# REAQTA HIVE

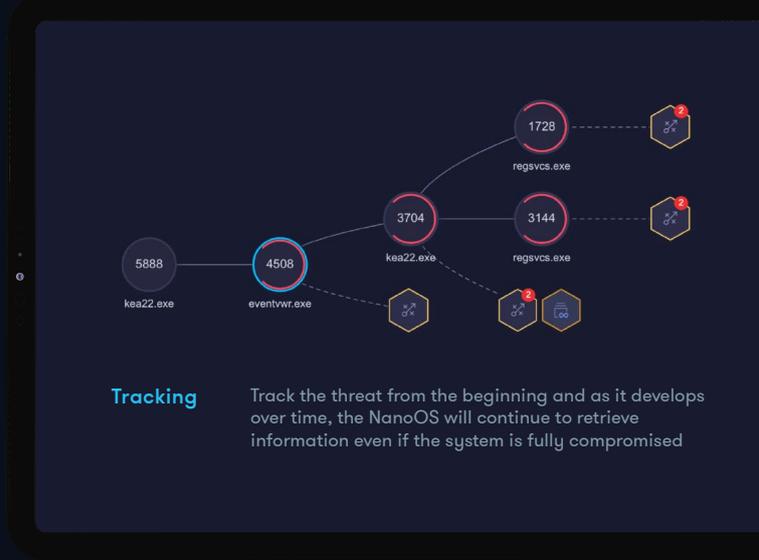


## Active Defense Intelligence Platform

Securing success

# STAY AHEAD OF THE ATTACKERS

With complete visibility, advanced detection and threat hunting



### Tracking

Track the threat from the beginning and as it develops over time, the NanoOS will continue to retrieve information even if the system is fully compromised



### Complete Visibility from Endpoint to Infrastructure

ReaQta-Hive is an Active Defense Intelligence Platform capable of monitoring endpoints from outside the operating system using the world's first NanoOS. The platform offers full visibility over the infrastructure, allowing real-time queries to endpoints, extended searches for both behavioral indicators and IOCs, and advanced data-mining for discovery of dormant threats, lateral movements and supply-chain attacks. The NanoOS remains effective even after a breach, making ReaQta-Hive the ideal solution, even for post-breach analysis.



### MITRE ATT&CK™ Integration & Real-Time Hunting

Unleash the full power of ReaQta-Hive threat hunting engines by searching your whole infrastructure in real-time for the presence of specific Indicators of Compromise (IOC), binaries and behaviors. ReaQta-Hive comes with a complete mapping of MITRE Tactics & Techniques, as well as 100+ searchable parameters. Finding threats is not just simple, but incredibly fast and effective.



### Advanced Threat Detection with a Dual A.I. Engine

A dual-A.I. engine ensures that no threat goes undetected. The first engine runs at the endpoint level, looking for malicious activity targeting a specific device. The second engine runs at the infrastructural level, looking for suspicious activity across the infrastructure. These two engines work in concert to provide multiple points of detection, leaving no stone unturned.



### Compliance Ready

ReaQta-Hive helps auditors identify gaps in compliance by scanning and analysing endpoints. With real-time information on non-compliant endpoints, auditors can quickly remediate compliance issues as soon as they come up.



### Protection Beyond Legacy Solutions and Automated Threat Alerts

The flexibility provided by continuous learning A.I. allows for the detection of new techniques and previously unknown threats, like file-less malware, that would otherwise escape detection from legacy and signature based solutions. A comprehensive early-warning system automatically identifies emerging threats, allowing security teams to perform a full security assessment before a breach happens.



### Anti-Ransomware

Protection from Ransomware is guaranteed by a dedicated dynamic behavioral analysis engine, capable of detecting ransomware and crypto-based attacks without interrupting business continuity. ReaQta-Hive automatically detects and blocks ransomware without requiring any human interaction, preventing data loss and saving valuable time for security teams.



## REAQTA-HIVE ADVANTAGE:

1.	Real-time visibility and insights
2.	NanoOS makes it resilient and invisible to attackers
3.	Early detection of new and unknown threats
4.	Zero business downtime
5.	Single easy-to-use platform
6.	Comprehensive threat response capabilities
7.	Ultra-lightweight agent
8.	Minimum infrastructure requirements
9.	Minimum impact to endpoint performance
10.	Highly customizable solution
11.	Remote remediation of threats
12.	Reduced response time
13.	Support for major platforms and OS's--Windows, Linux, MacOS, Android
14.	Open APIs for easy integration with existing security stack
15.	Effortless security for cloud instances



## REAQTA: CREATED TO SECURE YOUR ENDPOINTS AND DEVICES

### Ease of Use

- Deployment is easy, doesn't interrupt your activities, supports GPO, SCCM or any other software inventory solution for seamless push installation
- User-friendly dashboard provides a unified workflow towards the resolution of incidents

### Automated Reports

- Reports are automatically generated and management-ready
- Reports provide clear visibility on infrastructure and capture noteworthy activity

### Cloud Scanning

- Metadata relating to any incident is cross-checked against ReaQta's cloud for a severity impact score
- Uncover potential threats before the real attack begins

### Customizable Detection Strategies

Freedom to customize the engine to detect every threat scenario - whatever, whenever!  
Create your own response and remediation playbooks

FOR MORE INFORMATION, VISIT REAQTA.COM

ReaQta was founded by an elite team of offensive and defensive cyber security experts as well as machine learning researchers. Combining these varied expertise, our team has built a powerful Active Defense Intelligence Platform. Our solution provide clients with advanced detection and response capabilities, without requiring additional or highly skilled personnel. This innovative approach applies the latest A.I. algorithms to automate and simplify the process of detecting and handling new threats.

On this single, highly integrated active intelligence platform, our clients gain flexibility and speed in performing complex analyses that were only possible with large and highly specialized teams. It is a dynamic approach that doesn't just protect organisations in the here and now, but also far into the future. With ReaQta, businesses are empowered to pursue growth and ambition fearlessly.



[INFO@REQTA.COM](mailto:INFO@REQTA.COM)



[VISIT REQTA.COM](http://VISIT REQTA.COM)

