

REAQTA  
NGAV+

# REAQTA-EON

## Hardened Against All Threats

### SOLVING THE AV SECURITY GAP

Cyber-attacks have grown both in number and in sophistication over the years. This has made detection and remediation an increasingly complex task for security analysts.

Without next-generation prevention and attack visibility capabilities, traditional security softwares like Anti-Virus are essentially ineffective and unreliable. As we speak, many organizations without the essential next-generation security software are suffering from business disruptions and financial losses.

ReaQta-EON was designed with the latest breakthrough technologies in artificial intelligence and machine learning to provide the key and essential security that every organization needs to fight modern-day threats. Your organization can now effortlessly strengthen your operational resilience and defense from unwanted cyber-disruptions.

# WHY SECURITY TEAMS CHOOSE REAQTA-EON

Simplicity in usage, elegance in delivery. ReaQta's NGAV+ embodies the concept of "round-the-clock" defenses in all scenarios, even when teams are working remotely or offline.

*"Identifying attacks before they gain entry allows ReaQta to administer resilience during a sudden breach."*

**Frost & Sullivan**

*Trusted by analysts globally. An integral part of the "Multisandbox" project.*

**VirusTotal**

*"Brilliant endpoint protection with the convenience of easily isolating and tackling the problem from its comprehensive and easy-to-use interface."*

**Telco Provider**

*"We now have better visibility on our endpoints and are able to detect threats missed by antivirus and raises our organization security posture significantly."*

**Financial Institution**



**UNPARALLED PROTECTION TECHNOLOGY**

ReaQta-EON combines both traditional and modern defense techniques with the latest AI/ML strategies to stop attackers in real-time. This system protects you from both known and unknown threats, thus reducing the need for expensive response and recovery costs and efforts.



**FAST & EASY MANAGEMENT**

With ReaQta-EON's autonomous protective agent and optimised UI/UX, analysts require minimal management and can respond easily to threats. Accessible via any web browser from any location at any given time, the cloud dashboard can be easily managed on-the-fly.



**CLOUD-DELIVERED NGAV +**

EON agents are cloud-delivered and fully operational within seconds. As a user, this means rapid deployment with major cost-savings. Teams are saved from significant infrastructural and maintenance costs, as ReaQta provisions and manages the server and Hive Brain™ software on behalf of the user.

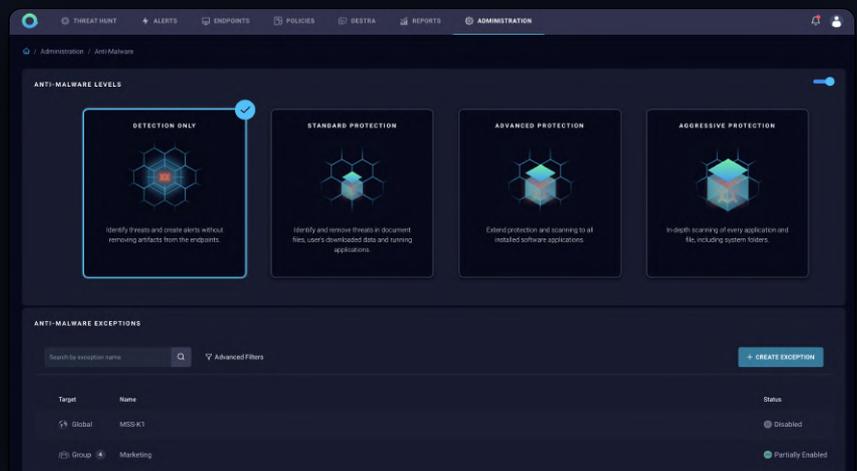
*Note: Installation can be done easily via Group Policy (GPO), System Center Configuration Manager (SCCM) or Manually*



**SECURITY THAT SCALES**

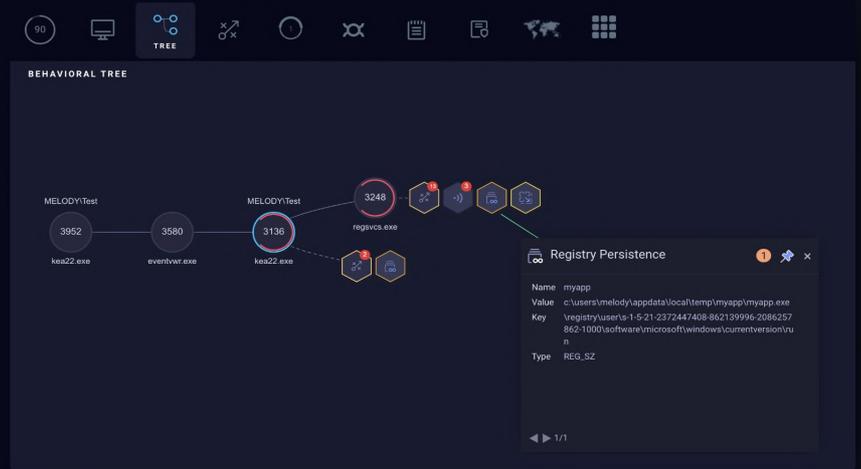
With ReaQta, your protection scales with your business. As security needs grow, you will be able to seamlessly layer-on advance capabilities and analysis such as Threat Hunting, Threat Cloud, Artifact Analysis, Clean-up Automation, Detection Strategies and API Access. Companies looking for continuous monitoring can choose to opt for 24/7 Managed Services by ReaQta's security team with ReaQta-MDR.

*4 Easily Configurable Anti-Malware Modes*



# WHAT MAKES REAQTA-EON SUPERIOR?

ReaQta-EON combines proven techniques with highly advanced detection, pre-execution and prevention technologies to safeguard your organization's key data and information assets.



ReaQta Behavioral Tree provides Full Alert & Attack Visibility

**ALERT DETAILS** 2020-04-20 16:44:47

Summary Trigger

**Anti-Malware Detection/Virus: VB:Trojan.VBA.Agent.BES**

**TRIGGER EVENT**

hr\_covid19\_summary.docx is infected by Trojan.GenericKDZ.66455  
C:\Users\User55001\Desktop\hr\_covid19\_summary.docx

**TOTAL KEY EVENTS (1)**

Anti-Malware Detection

**AFFECTED ENDPOINT**

NABUCODONOSOR Windows 7 Professional  
192.168.71.168 10.0.0(EDR) / 1.0.2 (Anti-Malware)

**STATUS**

2020-04-20 16:44:47 — Notified  
2020-04-20 16:56:14 — Archived by SOC  
2020-04-20 16:56:14 — Marked as **MALICIOUS**

ANALYZE ALERT

Real-time Alert & Prevention Capabilities

START FREE TRIAL

| Key Features                              | How ReaQta-EON Delivers   |
|---|---|
| <b>PRE-EXECUTION PREVENTION</b>           | Employs dynamic emulation and attack sequencing technology to detect malicious code within files in the pre-execution phase. The source code of the file is reviewed numerous times within milliseconds prior to full execution, effectively stopping potential malicious files from running.                           |
| <b>NANO OS™ &amp; DUAL AI ENGINES</b>     | Each endpoint agent is complete with ReaQta's dual AI engines and Nano OS™ technology, which grants extended proprietary detection and autonomous operation capabilities, even when devices are offline. Our AI technology deeply understands and baselines the infrastructure to detect advanced and zero-day threats. |
| <b>FULL ATTACK VISIBILITY</b>             | With ReaQta's AI engines, you can completely detect and correlate complex alert information into an easily comprehensible storyline in real-time, without any manual intervention.  |
| <b>MALWARE QUARANTINE</b>                 | ReaQta-EON quarantines unwanted malware to allow for further investigation and retrieval, unlike traditional protection which automatically deletes such files, including false positives.  |
| <b>ANTI-RANSOMWARE</b>                    | ReaQta-EON utilises behavioral analysis to extend protection capabilities to stop zero-day threats and ransomware attacks. By analysing file behaviours according to the cyber-kill chain, ReaQta-EON understands when an attack is imminent and stops the malicious processes right from the execution.                |
| <b>SIGNATURE &amp; HEURISTIC MATCHING</b> | Designed to continuously stop known attackers in their tracks via proven security techniques of heuristics and signature-based prevention.  |

## ABOUT REAQTA

ReaQta was founded by an elite team of offensive and defensive cybersecurity experts and AI/ML researchers. Combining these backgrounds, the team has designed an AI Endpoint Security Platform that leverages on Artificial Intelligence, data mining and a unique NanoOS to protect endpoints from advanced malware attacks and data exfiltration.

This novel approach applies the latest technologies to automate, optimise and simplify the process of detecting and handling new threats. Organisations can now eliminate the most advanced threats in the fastest way possible with an elegant, powerful and easy-to-use platform - entirely without the need for additional skilled personnel.

Security teams can now do more, with less.



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



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

