REAQTA HIVE

ReaQta MDR

24x7x365 Security Guaranteed

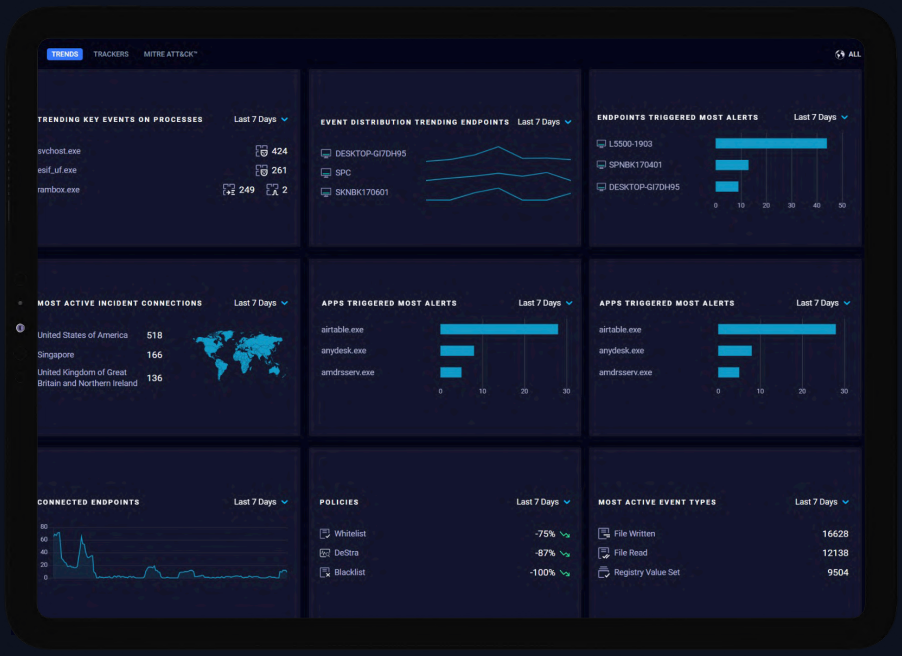
REAQTA

INFO@REAQTA.COM

VISIT REAQTA.COM

SECURE BUSINESS CONTINUITY AND GROWTH

Digitization and journey to the cloud are transforming the way organisations do business but increasing connectivity and scalability also increases cyber risk. Defining a trade-off between security and scaling is often a difficult task where security is on the losing end with long-term consequences that can prove severe for the business. ReaQta MDR services help organisations focus on growth while a team of experts takes care of the essential aspects of their cyber security.



HOW DOES REAQTA-MDR SERVICE SECURE ORGANISATIONS

REAQTA MDR

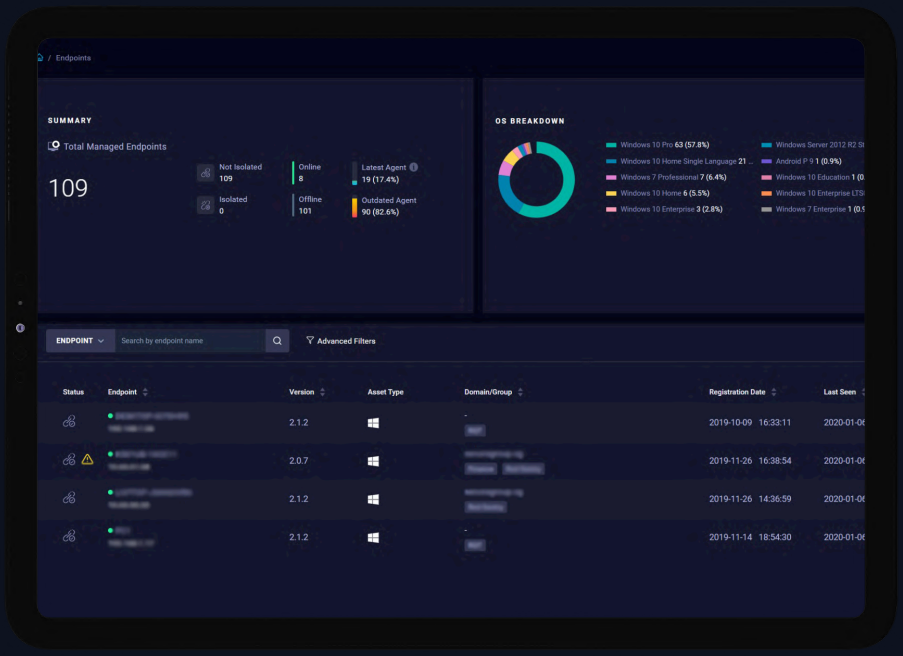
A team of experts with experience in high-profile attacks provides continuous threat monitoring and real-time incident remediation on servers and endpoints (laptops, mobile devices). ReaQta-MDR analysts team works as an extension to organisations with lean IT teams, looking for round-the-clock monitoring and mitigation of cyber threats.

Challenges	How ReaQta-MDR helps
• Limited infrastructural visibility	• Complete visibility over endpoint activites for real-time identification of threats and anomalies.
• Lack of cybersecurity personnel	• ReaQta-MDR security analysts provide 24/7 security monitoring & proactive threat hunting for emerging and active threats.
• Lack of Remediation and Response capability	• Reduction of business interruption damages with fast response, remediation and clean-up by ReaQta Incident Response team.
• Limited reporting and assessment capabilities	• ReaQta-MDR team provides both management and technical level reports within hours from the attack, to help our customers assess and communicate the entity and reasons of a potential breach.

SUPPORTED ARCHITECTURES

REAQTA MDR SERVICES

Ensures business continuity



Attack Resilience

A unique NanoOS enables security analysts to obtain in-depth data from the endpoints while protecting the monitoring platform from attackers trying to disable it. The complete mapping of MITRE ATT&CK events - directly into ReaQta's dashboard - and dual A.I. engines ensure a quick and automated detection and tracking of any malicious activity.

Reduced Cost

The automated and A.I. driven nature of ReaQta-Hive, the platform used by ReaQta-MDR, ensures a real-time detection of threats, reducing the time for attackers to create damages and allowing the analysts to respond immediately to any incident. Remediation activities are carried out directly by the analysts team and without interruption to business continuity.

Easy to use

Our platform ensures full visibility over the organisation's infrastructure, allowing for in-depth searches and threat hunting capabilities on both behavioural indicators and IOCs, to discover and remediate active attackers, dormant threats, lateral movements and supply-chain attacks.

Round the clock defense

ReaQta-MDR analysts provide 24/7/365 cyber security monitoring and coverage against cyber-breaches, analyse the extent of the damage and respond accordingly to each identified threat.

About ReaQta

The company was created by joining former offensive cyber-security experts with intelligence background and threat intelligence professionals. The combined experience of both defenders and attackers helped identify a new path to overcome the limitations of traditional security tools. ReaQta addresses the issue of Endpoint Security in a novel way, by looking at devices as entities with dynamic and evolving behaviors. This approach, combined with the latest advances in Artificial Intelligence, guarantees an unmatched visibility and powerful threat hunting and tracking capabilities for organizations of all sizes.

INFO@REAQTA.COM VISIT REAQTA.COM

REAQTA