ReaQta
Artificial Intelligence-Powered Threat Response

Alberto Pelliccione

Amsterdam-headquartered ReaQta is a fast growing cybersecurity company that is founded by a team with rich experience in government-led cyber intelligence operations. Powered using Artificial Intelligence (AI), their solution is constantly evolving to incorporate the latest technological advancement. Their current solution is a game changer in the market when they moved away from traditional "static binary analysis" to "behavioral analysis" to guard enterprises against modern attacks. According to Pelliccione, the CEO of ReaQta, their state-of-the-art cybersecurity solution creates behavioral models of the infrastructure to allow quick identification of new and unknown threats. This method is far better than conventional ones which only analyze binary files, as it now makes it extremely hard for an attacker to breach an endpoint and remain undetected. Recent cases in exponential proliferation of data and endpoints have shown that cyberthreats are constantly evolving, use of legacy cybersecurity systems have failed to tackle attacks and that they often require human intervention for monitoring. Realizing these loopholes, ReaQta brought their AI and security expertise together to create behavioral models that analyze, detect, and eliminate potential threats.

"Our AI-enabled solution not only detects and thwarts potential threats in real time but also calculates the level of risk through an easy-to-use dashboard that gives the IT administrators an integrated view into the entire infrastructure," says Pelliccione. "Cybersecurity analysts can instantly understand which devices are being compromised and which attack vectors the culprits are using to run malicious applications, during an ongoing breach. These insights enable them to act with lightning-fast response, thereby reducing critical dwell time, especially in the case of a successful breach." With a deep understanding of the modern cyberattack techniques, ReaQta is among the few leading cybersecurity solution providers to craft a highly advanced, AI-powered endpoint threat response platform—ReaQta-Hive.

> "Cybersecurity analysts can instantly understand which devices are being compromised and which attack vectors the culprits are using to install malicious files, during an ongoing breach"

Built to detect any emerging or unknown threats and their lateral movements across the endpoints, the platform encompasses tracking and remediation tools coupled with machine learning models that are extremely powerful in detecting nefarious elements lurking in the network. Reinforcing the platform's engine with an additional security measure, the firm has also created the world's first technology—called NanoOS—which monitors operating systems from both inside and outside, while remaining invisible to the malware. This means that the NanoOS cannot be shut down by the attackers and it provides inspection capabilities that cannot be reached in other ways. The tools empower the IT staff with the ability to monitor local as well as global infrastructures effortlessly.

One of ReaQta's customers, a large financial entity, has a distributed IT infrastructure with offices across multiple geographies. As a large financial organization, they had many employees who often traveled for business purpose, carrying along a device that was connected to the customer's infrastructure. The customer discovered that a criminal organization was targeting their VIPs to breach into their accounts. Moreover, the hackers managed to carry on a file-less attack aimed at stealing sensitive information, pushing the organization to look for a more sophisticated solution to shield their external endpoints. Partnering with the customer, ReaQta helped them quickly to address their security issues using its pioneering AI-enabled platform. Leveraging the platform, the customer was not only able to block the attackers but could also collect relevant information to correct abnormalities through real time notifications.

Forging ahead, ReaQta aims to educate the security community about the potential emerging attacks and envisions providing enterprises with a comprehensive solution that monitors their security posture, ranging from workstations to servers and mobile phones. "We plan to move forward in our path of success by expanding our wings internationally, including the APAC region such as the Australian and Japanese markets," concludes Pelliccione. ES