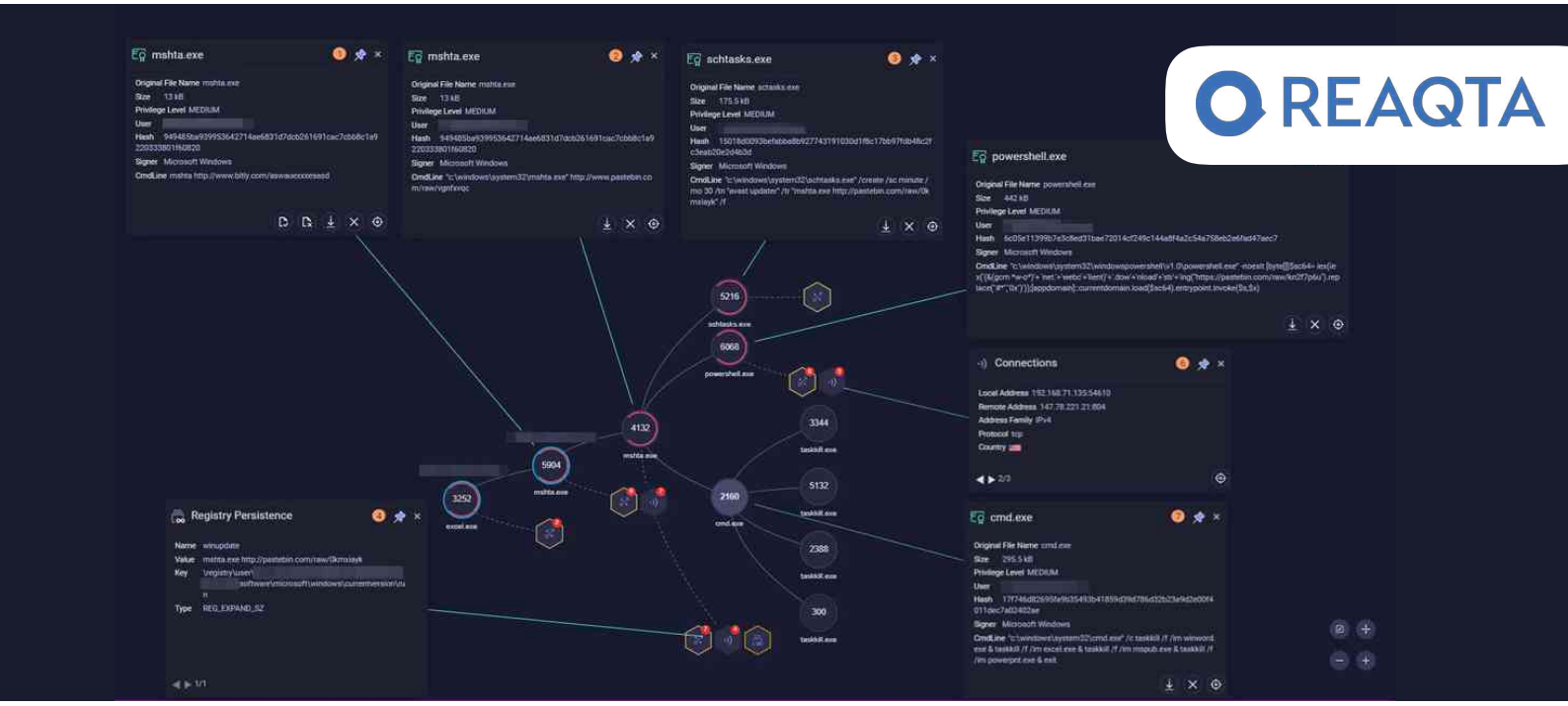
Case Study

SEdesk™

Endpoint threat response through A.I. and Isolation



Background

The shifting of computing to mobile devices like smartphones and tablets, and the increasing adoption of BYOD (bring your own device) policies, have created new areas of exposure and a large attack surface for cybercriminals who need to identify one single vulnerable system to gain a foothold in the enterprise network. An array of attacks is targeted to endpoints being used in the field or taken home from the office, aimed at bypassing the layered defence originally designed to protect the network and the data centres.

Challenge

Even if security teams recognise the importance of securing endpoint from attacks, they find it extremely frustrating as standard products are not able to rise to the challenge. Attackers employ increasingly sophisticated techniques and stealthy tools escaping the radar of traditional signature-based technologies focused on detecting and responding to known threats. While signature detection still plays a vital role in network security, it's no longer sufficient. To thwart security breaches organisations must protect themselves from known and unknown attacks focusing on prevention.

Industry

Cyber Security
Endpoint Threat response

Challenges

- BYOD impacting the traditional security model of protecting the perimeter of the IT organisation
- The sheer amount of software installed on the endpoint creates vulnerabilities
- Lack of IT expertise and resources to effectively administer endpoint security

Goals

- A complete endpoint threat response solution incorporating advanced technologies such as A.I., deep machine learning and application control techniques capable of defending against advanced threats that leverage zero-day attacks

Solution

- SE*desk*™ is a unified workspace providing secure remote access to whitelisted resources and on-device isolation to reduce the surface of attacks.

Solution

Although antivirus solution protect nearly every endpoint and server in the world, security breaches continue to happen at an alarming rate. The widespread use of unknown malware and vulnerability exploits in targeted attacks require advanced technologies.

ReaQta-Hive is an Endpoint Threat Response platform powered by A.I., used both on the endpoints and at the infrastructural level, capable of detecting new and previously unknown threats, ranging from simple ransomware to more sophisticated non-malware attacks like file-less and in-memory. State-of-the-art machine learning, applied to applications' behaviours, automatically alerts about active or emerging threats without need for prior knowledge of the attacks. This signature-less approach, combined with an A.I. driven behavioural analysis, ensures that threats are detected independently of their delivery techniques and payload types.

The integration of ReaQta-Hive in SEdesk™ complements the robustness of the web-platform by adding application authentication through multi-factor mechanisms, application isolation by creating a defined perimeter for whitelisted apps and transport layer protection from the endpoint to the network. Web application vulnerabilities are some of the most common flaws leading to modern data breaches. The need to secure data from the Internet all the way to the endpoint is the key concern today, maintaining compliance and regulations.

SE*desk*™ is the perfect combination of application and network layer protection through isolation. By defining a controlled perimeter, SE*desk*™ provides authenticated service isolation and data protection through delivery and storage. Leveraging SE*desk*™ technology data sharing is anonymised and protected. A multi-layer approach applied at network and endpoint level.

Benefits

- **Complete isolation** of data and applications on endpoint devices
- **Fine-grained access control** to the central network through context-based policies and User-Device-Server multi-factor authentication
- **VPN-free secure connection** between the dashboard at the SoC and the endpoints
- **Strong encryption mechanisms** for data integrity and protection
- **Zero configuration** on endpoint devices for easy deployment

> "Being in the cybersecurity industry, some of our customers were looking for an added secured access to our dashboard. We are glad to integrate SE*desk*™ into our product offering to give better protection for our customers. The solution is easy to use (plug & click) and convenient"
>
> Alberto Pelliccione, CEO ReaQta

REAQTA

ReaQta is founded in 2014 by a team with rich experience in government-led cyber intelligence operations and Threat Intelligence. With a deep understanding of the modern cybersecurity landscape, ReaQta is one of the fastest growing solution providers to craft a highly advanced, Artificial Intelligence (AI) powered endpoint threat response platform and solution service that analyses, detects, hunts and remediates cyberattacks. Headquartered in Amsterdam and Singapore, the company is currently represented in 18 countries.

Blu5 Group
info@blu5group.com
www.blu5group.com