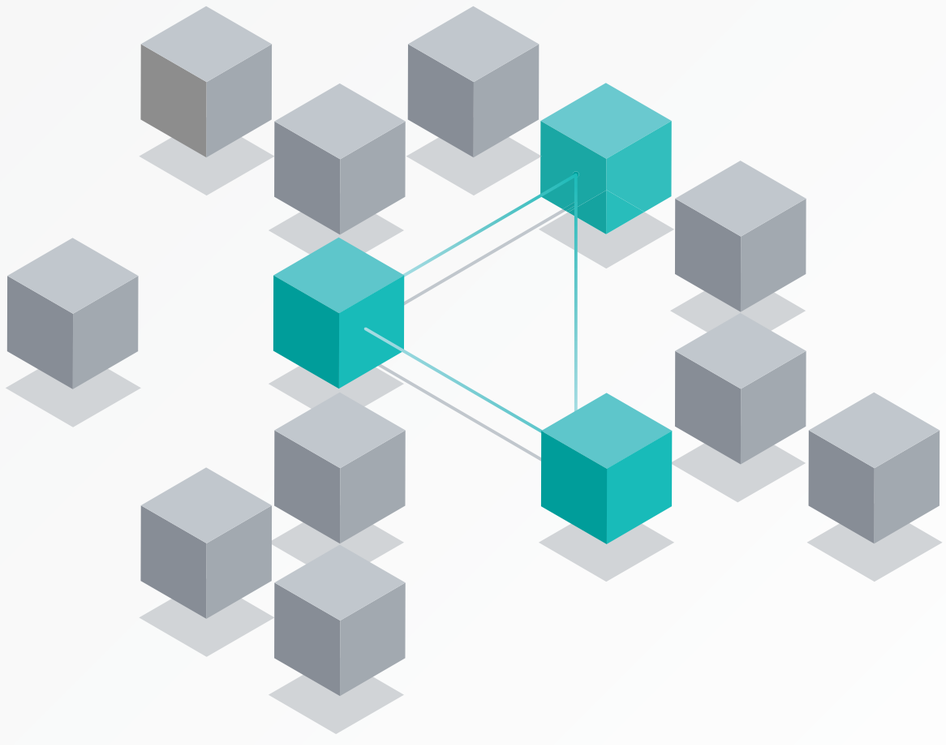
REAQTA
an IBM Company

IBM

IBM Security ReaQta

AI-powered, automated endpoint security



IBM Security ReaQta offers a unique, forward-thinking approach to endpoint security.

The solution uses exceptional levels of intelligent automation, taking advantage of AI and machine learning, to help detect and remediate sophisticated known and unknown threats in near real-time. With deep visibility across endpoints, the solution combines expected features, such as MITRE ATT&CK mapping and attack visualizations, with dual-engine AI and automation to propel endpoint security into a zero trust world.

Why ReaQta?

1

Continuously learns as AI detects and responds autonomously in near real-time to new and unknown threats

2

Helps secure isolated, air-gapped infrastructures, as well as on-premises and cloud environments

3

Maps threats against the MITRE ATT&CK framework and uses a behavioral tree for easy analysis and visualizations

4

Offers a bidirectional API that integrates with many popular security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools

5

Provides heuristic, signature and behavioral techniques in its multilayered defense

6

Allows users to build custom detection strategies to address compliance or company-specific requirements without the need to reboot the endpoint

7

Simplifies and speeds response through guided or autonomous remediation

8

Offers automated, AI-powered threat detection and threat hunting including telemetry from indicators that can be customized for proprietary detection and granular search

9

Makes remediation available with automated or single-click remote kill

10

Provides deep visibility with NanoOS, a unique hypervisor-based approach that works outside the operating system and is designed to be invisible to attackers and malware