

Solution Brief

Simplify Threat Detection and Response with IBM Security ReaQta and Logicalis



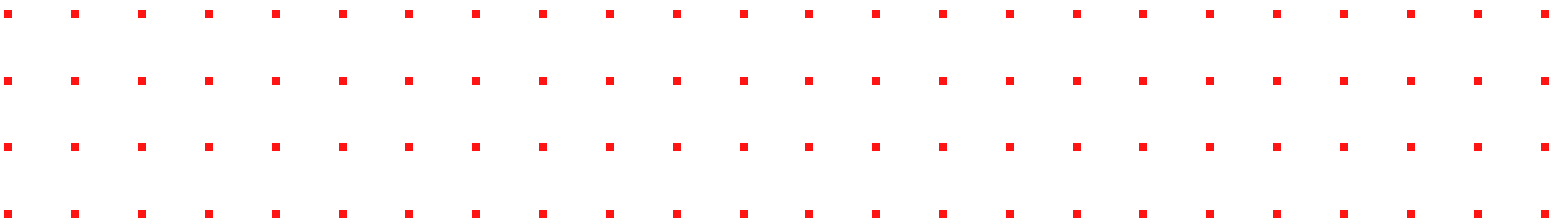


**Protect endpoints, detect
anomalous behavior, and remediate
in near real time.**

The proliferation of data and endpoints, coupled with an increase in cybercrime, has created a substantial threat for businesses of every size. While traditional security methods are effective against known threats, they are vulnerable to sophisticated and unknown attack techniques – nor do they provide visibility into assets, which is a major security impediment.

Endpoint detection and response (EDR) solutions, such as IBM Security ReaQta, provide deep visibility, behavioral analytics, customizable detection strategies, a Cyber Assistant, and other advanced features to detect behavioral anomalies, remediate threats in near real time, and help secure the entire endpoint ecosystem.

With Logicalis' professional and managed services, you can leverage IBM Security ReaQta to simplify threat detection and response, ensure business continuity in the face of potentially disruptive cyber threats, and gain the confidence you need to innovate freely with IT.



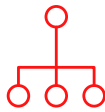
Why IBM Security ReaQta for EDR?

A modern and effective EDR solution comprises four key elements, which are the building blocks of IBM Security ReaQta:



Visibility: One of the main impediments to endpoint security is a lack of visibility. By working at the hypervisor layer instead of within the operating system, ReaQta provides exceptional ability to monitor all process behaviors, while staying invisible to attackers.

- Full endpoint visibility
- Real-time alerts
- Storyline creation
- Frictionless agent
- Unified workflow



Automation: As IT security complexity increases, security teams need a solution that is automated and easy to use. ReaQta uses AI to run autonomously, continuously learn, and automate detection and response, offering a clear, real-time overview of attacks and guided remediations.

- Autonomous detection
- Guided remediation
- Fast response times
- Ease of use



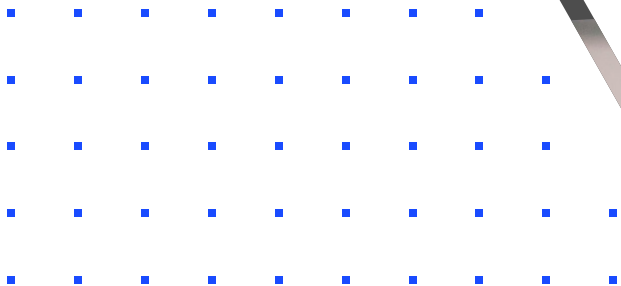
Alert Management: Antivirus solutions need to know about a threat in order to block it. EDR solutions such as ReaQta, on the other hand, use AI to detect behavioral anomalies, manage alerts, and simplify and speed response times.

- High-fidelity alerts
- AI models
- Alert fatigue prevention
- Automated alert management



Threat Hunting: Threat hunting is necessary to maintaining a clean, threat-free environment. ReaQta uses data mining, a large library of prebuilt detection playbooks, easy-to-understand GUI, custom detection strategies, and other features to automate and simplify threat hunting.

- Dormant threat searching
- Automated hunting
- Custom playbook creation
- No scripting required
- Real-time capabilities
- Graphical overview



Simplify Endpoint Security with IBM

Security ReaQta and Logicalis

As an IBM Platinum Partner with a long track record of client successes, Logicalis can help you maximize endpoint security with IBM Security ReaQta.

With our professional and managed services, you can safeguard your endpoint ecosystem, protect against known and unknown threats, and free up IT resources to focus on more valuable activities.

To get started, contact us today and schedule a free executive briefing.

Get in Touch

www.us.logicalis.com

866 456 4422