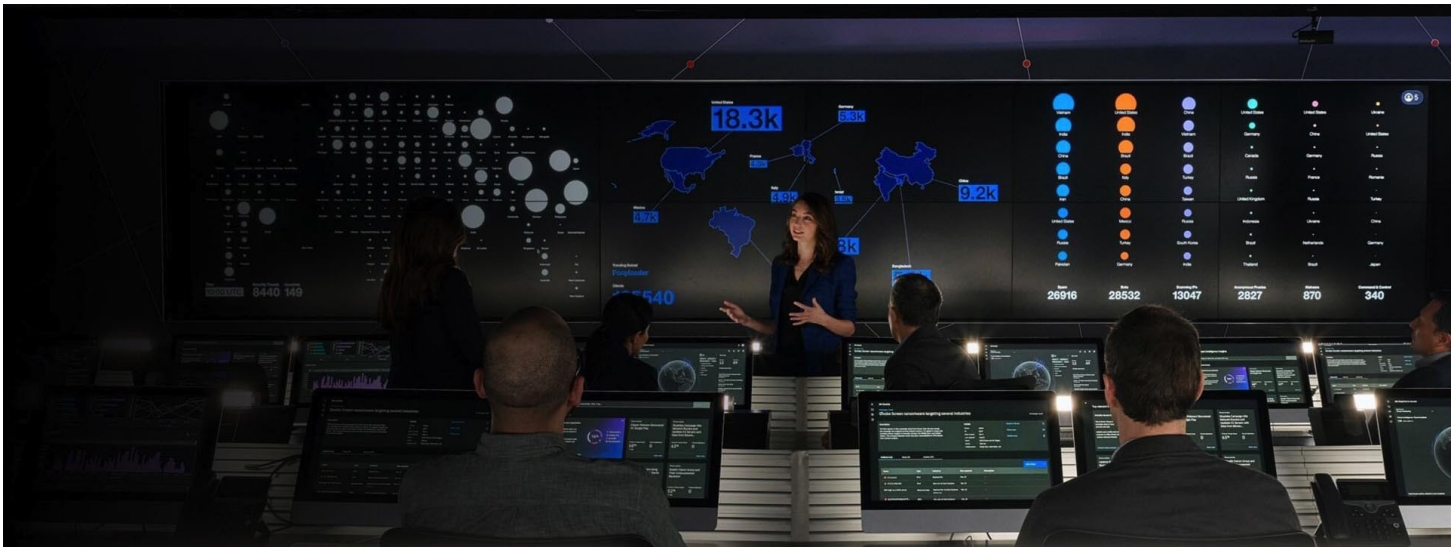
IBM Newsroom

IBM to Expand Security Portfolio with Plans to Acquire ReaQta

Launches IBM QRadar XDR Suite to Simplify Threat Detection, Investigation and Response



ARMONK, N.Y., Nov. 2, 2021 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced an expansion of its cybersecurity threat detection and response capabilities with its plans to acquire ReaQta. ReaQta's endpoint security solutions are designed to leverage AI to automatically identify and manage threats, while remaining undetectable to adversaries. This move will expand IBM's capabilities in the extended detection and response (XDR) market, aligning with IBM's strategy to deliver security with an open approach that extends across disparate tools, data and hybrid cloud environments.

As part of today's announcement, IBM also detailed a new suite of XDR offerings under the QRadar brand. IBM QRadar XDR helps security analysts break down the silos between the proliferation of point products in the industry – providing comprehensive visibility across security tools and data sources, whether in the cloud or on-premises, and equipping security teams with the insights and automation they need to act quickly. Upon closing, ReaQta's offerings will become part of this portfolio, adding expanded native XDR capabilities to IBM's security portfolio aimed at helping clients adopt continuous monitoring and rapid response as part of a zero trust approach.

Companies today are struggling to secure increasingly dispersed IT environments, with the proliferation of devices, users, and technologies spreading across clouds and on-premises infrastructure. As a result, security events are becoming more difficult and costly to detect and contain, with data breaches costing over $4 million per incident and taking an average of 212 days to identify, according to the 2021 Cost of a Data Breach Report from IBM and Ponemon Institute.

"Complexity has created a cloak that attackers are operating under, furthering their ability to circumvent defenders," said Mary O'Brien, General Manager, IBM Security. "The future of security is open, using technologies that can connect the security insights that are buried across disparate tools and advanced AI to identify and automatically respond to threats more quickly across their entire infrastructure, from endpoint to cloud. With our expanded capabilities via QRadar XDR and the planned addition of ReaQta, IBM is helping clients get ahead of attackers with the first XDR solution that reduces vendor lock-in via the use of open

standards."

IBM Announces Intent to Acquire ReaQta

IBM's planned acquisition of ReaQta further differentiates the company's portfolio of connected, open security tools to unify and speed response to security threats. ReaQta, whose primary business office is located in the Netherlands with headquarters in Singapore, will join the IBM Security business unit upon closing. ReaQta was built by an elite group of cybersecurity experts and researchers with AI and machine learning expertise and extensive backgrounds in security operations. Financial terms were not disclosed. The transaction is expected to close later this year, subject to customary closing conditions and required regulatory reviews.

ReaQta's behavioral-based platform helps stop known and unknown threats in real-time and can be deployed in a hybrid model – on premise or in the cloud as well as air gapped environments. Through deep learning done natively on the endpoint the platform constantly improves on defining threat behavior tailored to each business per endpoint, allowing it to block any abnormal behavior. ReaQta's platform also leverages a unique 'Nano OS' that monitors the operating systems from the outside, helping to prevent interference by adversaries.

"Our mission at ReaQta has been to better equip the defenders, who are tirelessly striving to stay ahead of cyber threats, with advanced technology to quickly identify and block new attacks," said Alberto Pelliccione, CEO at ReaQta. "Joining forces with IBM will enable us to enhance and scale our unique AI capabilities across all types of environments via a proven platform for threat detection and response."

QRadar XDR Suite: Open, Connected Approach to XDR

An evolution of the IBM QRadar security intelligence portfolio, IBM QRadar XDR is a suite of security software built on IBM's open, cloud-native security platform, Cloud Pak for Security. IBM QRadar XDR spans the core foundational capabilities of threat detection, investigation, and response to help organizations modernize their existing IT and security infrastructure.

IBM is implementing an open connected approach to XDR, leveraging its commitment to open security and the Open Cybersecurity Alliance, as well as alliances and integrations with 200 plus cloud and security vendors, creating the industry's largest XDR ecosystem. The QRadar XDR suite also includes IBM native security technologies that customers can choose to leverage for Security Information and Event Management (SIEM), Network Detection and Response (NDR), and Security Orchestration Automation and Response (SOAR).

Now with the addition of ReaQta, the QRadar XDR suite will also include an option for Endpoint Detection and Response (EDR), allowing IBM to provide native capabilities for all core XDR functions, while also providing clients the option to leverage existing investments and third-party tools across IBM's broad partner ecosystem. IBM QRadar XDR will also be designed to deliver more accurate alerts while helping reduce manual processes via pre-built detection and response automations.

IBM QRadar XDR is also designed to be deployed by managed security service providers, including IBM and others.

Connecting Existing Investments

Building further on IBM's open approach to XDR, the company also introduced XDR Connect, which helps companies connect and automate threat detection and response across existing toolsets. Part of the QRadar XDR suite, XDR Connect provides a unified streamlined workflow for alert triage, investigation and threat hunting, automated root cause analysis, and response, by connecting to organizations' existing tools or IBM's own XDR technologies.

XDR Connect offers a centralized management of security incidents with pre-defined detection and response rules via more than 30 open source, pre-built integrations, and data connectors. It also provides access to the latest threat intelligence insights and data from IBM and third parties. This unique approach allows companies to better capitalize on existing security investments, modernize with new security tools and data sources, and simplify their overall security operations with unified, AI-driven workflows designed for faster, streamlined response.

For more information on IBM QRadar XDR please visit: http://ibm.com/qradar

About ReaQta

ReaQta is a top-tiered AI Autonomous Detection & Response platform, built by an elite group of cyber security experts and AI/ML researchers. Built with advanced automated threat-hunting features, ReaQta allows organizations to eliminate the most advanced threats in real-time. As experts in AI and behavioral analysis, ReaQta's proprietary dual-AI engines provide organizations across all industries with autonomous, real-time and fully customizable endpoint security, minus the complexity. As a result of automation coupled with intuitive design, ReaQta's customers and partners benefit from performance improvements and are now able to manage and secure more endpoints without the need for highly skilled staff. For more information, visit https://ReaQta.com

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Contact:

Michael Rowinski
IBM Communications
rowinski@us.ibm.com

SOURCE IBM

Additional assets available online:  Documents (

https://newsroom.ibm.com/2021-11-02-IBM-to-Expand-Security-Portfolio-with-Plans-to-Acquire-ReaQta