NUCLEUS RESEARCH

GUIDEBOOK

IBM QRADAR ON CLOUD

PROGRAM: SECURTY AND INFRASTRUCTURE
DOCUMENT Q170 • AUGUST 2016

ANALYST
Seth Lippincott

Nucleus Research Inc. 100 State Street Boston, MA 02109 **NucleusResearch.com** Phone: +1 617.720.2000

THE BOTTOM LINE

IBM QRadar on Cloud delivers security information and event management services to a hosted cloud environment enabling customers to outsource elements of their security system.

Nucleus found customers could leverage the cloud subscription model and avoid buying expensive infrastructure by selecting IBM QRadar on Cloud. Additionally, customers benefit from the ease of deployment and can quickly extract value by beginning to identify possible compromises in a few days rather than months.

•••

THE SITUATION

Information security and network integrity are becoming a larger focus for IT departments at companies of all sizes. At the same time, companies are more cost-conscious about their technology purchases. Finding the right breach protection and threat prevention technology to meet the needs of the organization is a critical component of keeping spending within budget. For many the answer lies in security solutions that outsource menial tasks and infrastructure to the vendor.

Nucleus found that, although companies are increasing spending on security, those deploying to the cloud spend on average 22 percent less than those on premise (Nucleus Research, *q23 – Buying intentions survey – security*, February 2016). Many firms are reaching the end-of-life for their legacy solutions and have realized they have incurred large costs and achieved mixed results over the course of their deployment. Still, as companies continue to spend money on point security solutions with inconsistent performance and utility, many are looking for more efficient alternatives which keep pace with changes in the threat landscape.

Even as many segments of the business technology sector have shifted to software-as-a-service (SaaS) product delivery, the SaaS deployment model has not been a fixture of security solutions. Previously, customers had no viable alternative to on-premise network security systems which delivered best-in-class technology but could require high capital costs. In addition to the infrastructure, buyers paid for software licenses and annual ongoing support and maintenance fees. Security was achieved by organizations collecting their own data and performing in-house analysis using highly skilled IT personnel. This model was effective in protecting high-value assets but the threat landscape has changed, with attacks targeted more broadly, prompting mid-sized organizations to require a different model.

In order for SaaS security solutions to be adopted in the security solutions sector, it must overcome two hurdles: customer reticence to switching to new security systems and the trust gap in the security of a managed cloud environment. Customers presented with a change in how services are delivered by vendors can either choose to do nothing or adopt a new security capability. Reluctant customers can be more easily persuaded that their limited resources are better spent monitoring the environment than maintaining software. For security vendors, solutions matching the needs of the organization and bringing new value or capabilities will better overcome customer resistance to change. For example, SaaS solutions do not require action by the customer when applying patches or upgrades, simplifying a complex and laborious process for on-premise deployments.

For customers considering an upgrade to their existing log collection solution, both value and capabilities are sometimes not sufficient to overcome a trust gap in the security of a managed cloud infrastructure. Despite the financial benefit of eliminating or avoiding infrastructure capital costs by outsourcing their log collection capabilities, some customers will still perceive that their sensitive business processes and data are more exposed in a cloud environment. However, industry options are rapidly maturing and vendors are beginning to offer cloud-based alternatives with features on par with the on-premise deployments. Furthermore, Nucleus found that cloud security systems are frequently better than the in-house environments, contrary to what customers might believe (Nucleus Research, *Cloud data center security benefits*, November 2015).

Customers have a number of paths forward with regard to their log collection security technology: remain on outdated and expensive on-premise infrastructure that may not fulfill the company's security needs, update their on-premise infrastructure and system to better match their needs, cut overhead by shifting log collection infrastructure to a managed environment, or outsource both infrastructure and personnel to a managed security service provider.

THE SOLUTION

IBM QRADAR ON CLOUD

IBM QRadar on Cloud is a security event management, log and flow collection and reporting system deployed in a managed cloud environment. It caters to organizations that seek to outsource the deployment and maintenance of their network security data collection and analysis solution. By deploying QRadar on Cloud, customers can maintain or expand their internally developed monitoring capabilities while avoiding rudimentary tasks and allowing analysts to spend more time understanding the latest threat intelligence data or applying security to

existing assets. Nucleus expects that further releases and updates to the software will expand its capabilities and deliver additional services to customers to fulfill the variety of their security needs.

Key capabilities:

- Log source data collection
- Netflow collection
- High events per second (EPS) collection maximums
- Automatic software updates
- Customer configuration services
- On-demand scalability to match customer needs
- X-Force Threat Intelligence alert feed on developing situations
- Web browser accessibility
- Highly available service configuration
- Optional additional management services

WHY IBM QRADAR?

Nucleus analyzed the experience of IBM QRadar on Cloud customers to understand why they chose IBM over other solutions. As one of the few solutions to deliver SaaS security features, IBM benefits from its first-mover advantage and is backed up by expertise developed through monitoring 15 billion security events daily for thousands of clients in its on-premise deployments. Although customers had various motivations for deploying QRadar on Cloud, IBM's existing security service credentials were a contributing factor.

CLOUD SUBSCRIPTION MODEL

IBM QRadar on Cloud expands the market of possible customers by delivering its services as a predictable monthly operating expense. Customers with no prior log source management solution, who were hesitant due to the high initial capital investment and ongoing costs of on-premise solutions, are ideal candidates to take advantage of the cloud-based security system. With infrastructure costs averaging $12,000 per server and $25,000 per server per year for high availability deployments, organizations opting for QRadar on Cloud avoid substantial initial and ongoing expenses.

With infrastructure management left to the IBM support team, small- and medium-sized enterprises are able to implement the solution because they incur only a monthly operational expense based on the subscription model. Additionally, larger companies face the prospect of installing expensive hardware point security

solutions in multiple locations and markets. Integrating and consolidating these log source data adds to the complexity, which large companies are able to avoid by deploying a cloud-based solution.

The subscription model also allows companies the flexibility to adjust based on their security needs. With the speed at which security solutions are changing to keep pace with threats, QRadar on Cloud does not lock-in customers to a certain technology, allowing updates and new services to be easily integrated. Customers said:

- *"The value of the cloud was several folds greater than on-premise options for us."*
- *"We benefit from the cloud with intangibles like upgrade management so our infrastructure is current and the ease of ongoing maintenance."*
- *"No perpetual license was a motivation for us.* [With a cloud solution] *worst case scenario, we are out a year."*
- *"Being able to access it from anywhere is another big benefit for us."*
- *"The space evolves too quickly to be tied down."*

FLEXIBILITY, SCALABILITY, AND SPEED OF DEPLOYMENT

With IBM QRadar on Cloud, customers can collect log source data and network flows with high EPS maximums. Customers reported the flexibility of the cloud allowed them to provision only what they needed and scale their deployment if their needs changed. Customers can scale their log collection without installing additional infrastructure or devoting additional resources to managing the solution. Customers were also impressed with how quickly the solution could be set up and start collecting logs.

Customers also reported that the solution gave them the flexibility to handle over 1,000 sources and more than 5,000 logs per second without establishing an internal management team. Additionally, the solution only required minor infrastructure changes, such as installing an open port in the firewall. The speed of deployment allowed customers to quickly transition to value-adding tasks. The internal due diligence of which log sources are important to collect versus which are noise helps to speed the process of gathering useful information once IBM QRadar on Cloud is deployed. Customers said:

- *"The back and forth internal decision took about a month. Once we decided on IBM, it took about a day to get it stood up and collect the first logs."*
- *"The ease of deployment was definitely one of the biggest benefits for us."*
- *"We had one or two people working on deployment—not even full time—to do the technical setup of the gateway and connect to the cloud."*

- *"We had two guys working for two months to tweak log sources and fine-tune which logs weren't noise."*

IBM SECURITY TEAM

IBM QRadar on Cloud backed by IBM security experts allows customers to put energy into other tasks instead of managing their log source solution. Some customers reported their prior solution had been giving them zero value because the vendor had not supported their deployment sufficiently even though they continued to pay for support. Before moving to IBM QRadar on Cloud, customers had internal discussions about needing proof-of-concept for their security event management tool but realized IBM provided the service they needed and had the expertise to address any issues that might arise.

The IBM security team is able to educate a customer's internal team on what to look for and what is suspicious, bringing years of experience with the IBM QRadar Platform to bear. IBM security experts can help customers understand about their population of log sources and how to sort through what can initially be an overwhelming amount of information. One customer said: *"We didn't have a good sense of what all logs sources were available to us in the environment. We spent the time to hook up the log and consume it only to discover it was noise."*

KEY BENEFITS

When deploying and using IBM QRadar on Cloud, customers benefit in a number of ways. Some benefits are characteristic of any cloud deployment relative to an on-premise counterpart (Nucleus Research, *q65 – Cloud delivers 2.1 times more*, April 2016). Where IBM QRadar on Cloud differentiates is its ability to leverage IBM existing security expertise to help customers quickly start extracting value from the product.

LOWER DEPLOYMENT AND ONGOING COSTS

As a cloud solution, IBM QRadar on Cloud eliminates or drastically reduces the costs customers incur on an initial and ongoing basis. Traditional on-premise deployments require capital-intensive hardware costs. Frequently, the additional costs associated with the hardware are overlooked, which include scoping, provisioning, and testing time spent by internal personnel or consultants. Once a company puts the hardware in place and purchases the software perpetual license, internal IT personnel, often with a specialized and expensive skillset, must manage the solution, all of which add up to significant costs.

In stark contrast to on-premise deployment costs, IBM QRadar on Cloud avoids the infrastructure costs and tasks IBM security experts with managing the solution. Additionally, since deploying the system can be accomplished in a matter of days instead of months, customers avoid extensive third-party consultant fees and employee time spent on tasks with no value-add. Deploying a managed cloud also eliminates ongoing management applying patches and upgrades by internal personnel. Customers avoid the risk falling behind in the vendor's upgrade cadence and being left with a solution that is no longer supported by the vendor. The ongoing expense of a predictable monthly subscription fee lowers the burden on customers by shifting the deployment from a capital expense, which must be depreciated, to an operating expenditure. One customer noted: *"One pro is that because it is a cloud solution means we don't require a management team. Also, we don't have to patch or apply upgrades to it."*

INCREASED IT PRODUCTIVITY

With solution management outsourced to IBM, customers are able to devote more time to the analysis of possible security issues rather than managing the security solution. Nucleus found that customer IT personnel were able to use QRadar on Cloud more effectively than their prior solution. Customers cited the features IBM has implemented help to streamline the log management process and give users the information they need quickly. As a result, IT personnel are able to identify and address potential problems faster, allowing them to put their time to tasks which bring additional value to the company, such as performing attack path simulations, tuning rules and alerts, and/or tracking and remediating discovered vulnerabilities. Customers said:

- *"Our prior solution wasn't giving the right information, so no one was looking at it. With IBM users are actually looking at it and getting value from it."*
- *"With shared tenancy we can see all the events from all our locations and can aggregate and correlate a much larger dataset, improving our analytics."*

EXTENDED SERVICES

IBM QRadar on Cloud customers have the option of expanding the security management services they purchase from IBM. Customers can address internal skills gaps by outsourcing specialized services and support, such as weekend monitoring and emergency response. Additionally, QRadar on Cloud has built-in multitenancy support. Companies with a presence in multiple regions or service partners managing several clients can effectively isolate views and event processing for only those managed tenants. Nucleus anticipates IBM will continue to expand services with subsequent releases of the product to include data storage options, network forensics using full packet capture technology, and incident response. As a result,

IBM is positioning to fulfill all of a customer's security needs. One customer said: *"The SIEM* [security information and event management] *functionality for on-premise is basically the same as cloud. Since our on-premise infrastructure is several years old, we would like to see parity in the cloud security capabilities."*

BEST PRACTICES

IBM QRadar on Cloud can be the beginning step for many companies in shifting their security solutions to the cloud. As more firms realize that their security system is only as good as their vendor and the personnel managing it, the necessity to keep solutions on-premise will decrease. In a survey of IT security professionals, Nucleus found companies with a cloud strategy spent on average 22 percent less on security technologies relative to those who haven't embraced the cloud (Nucleus Research, *q23 – Buying intentions survey – security*, February 2016). The trend indicates companies will want to expand their cloud deploys and retire expensive legacy systems. As a result, IBM QRadar on Cloud is positioned to deliver additional security services to customers as the product matures.

Already IBM QRadar on Cloud offers configurations for customers who opt to deploy their log collection and network flow capabilities in a hybrid environment. Hand-in-hand with configuration agnosticism, IBM QRadar is agnostic about customer-size. With the cloud, IBM is able to deliver security data collection services to a broader range of companies, particularly small and medium-sized organizations that have been reluctant to deploy an on-premise solution. Large EPS maximums means that even clients with hundreds of locations across the United States and the globe can have their needs met; the technology can satisfy the needs of customers, large and small.

CONCLUSION

Nucleus found IBM QRadar on Cloud brings value to customers by eliminating the need for expensive hardware and IT personnel oversight, deploying quickly resulting in faster time to value, and by offering a growing range of additional security services in the cloud. Existing customers reported transitioning their log source collection capabilities from a capital expense to a monthly operating expense has helped them achieve faster time to value than traditional on-premise solutions. As more companies realize the benefits of moving off their old and possibly defunct infrastructure and into a managed cloud environment, IBM QRadar on Cloud offers a credible path forward from a well-established security technology leader.