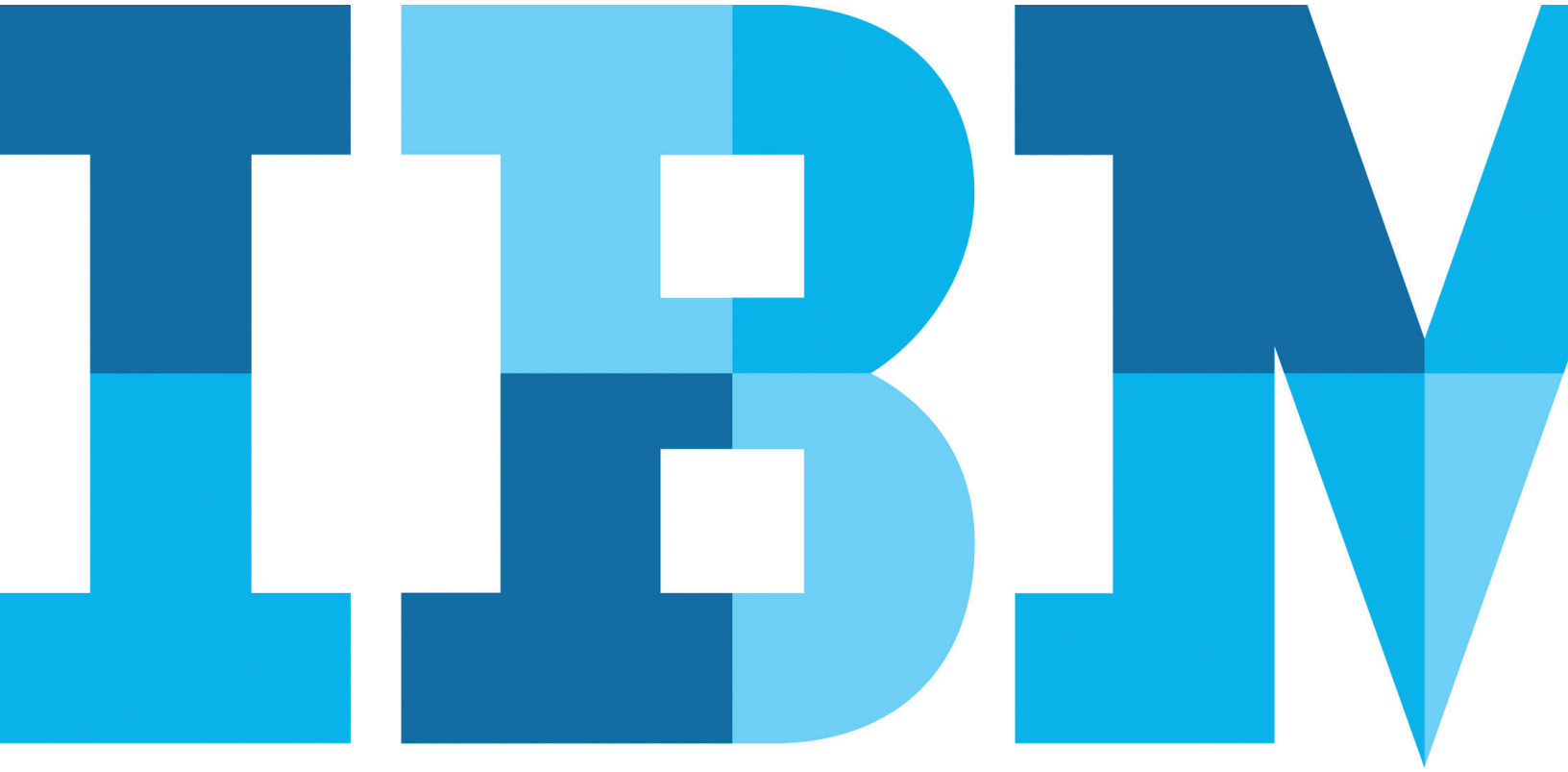
July 2015

Security intelligence for service providers

Expanded capabilities for IBM Security QRadar—including multi-tenancy, unified management and SaaS



IBM

Introduction

The world is full of "get rich quick" schemes, but there are also some solid business opportunities. Case in point: the opportunity to provide Internet cyber-security solutions for midsized organizations. Weekly—almost daily—the headlines are about yet another massive security breach involving large and well-known companies or government agencies. The threat is real and there simply aren't enough skilled individuals to protect smaller businesses and public organizations against sophisticated cybercriminals.

Midsized organizations in particular are rapidly recognizing significant barriers to detecting and responding to attacks, and they commonly suffer from a lack of trained resources that can safeguard their intellectual property or private customer data.

Now, with the availability of cloud-based security solutions, a growing number of organizations are looking to managed service providers (MSPs) as the most effective and cost-efficient path to monitoring, detecting and remediating threats. However, MSPs face several challenges providing cloud-based security intelligence to their customer organizations. This quickly evolving market space requires:

- Flexibility to address a wide variety of customer needs and sizes, from small organizations to large enterprises
- Scalability to grow as needed, with the ability to easily add new customers and infrastructure as required
- Cost-effectiveness to be competitive in a rapidly growing market segment, and to improve margins by constantly increasing productivity

Evaluating security intelligence platforms—what to look for

As an MSP deploying a security intelligence platform for your enterprise customers' data, you want to offer a market-leading technology capable of detecting malicious activities and anomalous behaviors before any data is lost. It also should not require a small army to deploy and maintain it. IBM® QRadar® Security Intelligence Platform was designed from the ground up to address these requirements using automation, intelligence and integration. Plus, it includes multi-tenancy and a master management console to further improve your security and operations management capabilities.

How QRadar Security Intelligence Platform can help

QRadar Security Intelligence Platform delivers security and compliance benefits that are invaluable for businesses that today are collecting, processing, using and storing more information than ever before. This suite of IBM Security QRadar solutions provides a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics and configuration and vulnerability management.

By analyzing more types of data and using more analytics techniques, QRadar technology can provide network visibility that other solutions cannot—often detecting threats that those solutions miss. QRadar uses real-time correlation and behavioral anomaly detection to identify advanced threats, allowing solutions to identify high-priority incidents among billions of data points.

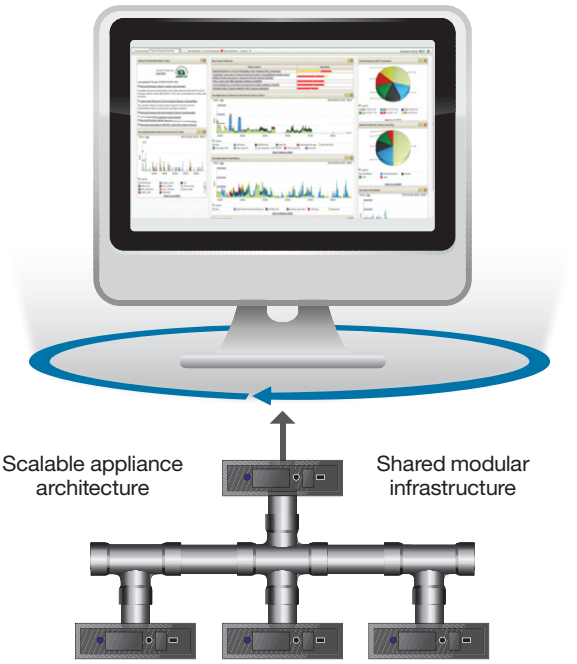
With a common application platform, database and user interface, QRadar technology delivers massive scalability without compromising the real-time intelligence of SIEM and network behavior analytics. It provides a common solution for searching, correlation, anomaly detection and reporting functions. A single, intuitive user interface provides seamless access to all log management, flow analysis, incident management, configuration and vulnerability management, risk management, forensics analysis, dashboard and reporting functions.

MSPs can also take advantage of IBM Security Intelligence on Cloud, which is a security software-as-a-service (SaaS) offering. This enables the MSP to offer a SIEM solution for its clients and outsource the deployment and management infrastructure to IBM. It can scale up to meet dynamically changing business needs, removes the need for additional technical resources to monitor and manage the solution infrastructure, and allows the MSP to pay based on an operating expenditures model rather than making large capital investments. With QRadar, an MSP has the flexibility to manage security for a customer in the cloud, in an environment hosted by IBM, or on-premises at the client's location.

Giving security analysts a management advantage

QRadar solutions are simple to deploy and manage, offering extensive out-of-the-box integration modules and more than 700 pre-defined correlation rules based on known patterns of malicious behaviors to help identify attacks and potential network breaches. Upon implementation, these rules immediately find security issues, enabling service providers to take quick action by banning IP addresses and disreputable URLs, and by closing ports that would permit unauthorized traffic. Rules can also be shared across clients with similar characteristics—for example, those in a particular industry—vastly reducing the need for tuning on a client-by-client basis.

IBM Security QRadar: Architected to meet the security needs of service providers



Multi-tenant
enables secure, rapid and cost-effective delivery of security intelligence services

Scalable
scales from smallest to largest customers with centralized management of single and multi-tenanted systems

Automated
drives simplicity and accelerates time-to-value for service providers

By automating many asset discovery, data normalization and tuning functions, while providing rules and reports, QRadar can dramatically reduce the time to value and complexities that can cripple other products. With QRadar automation, administrators can focus on delivering more accurate security monitoring for the entire organization.

Multi-tenancy for flexibility, scalability and economy

A significant challenge to providing cloud-based security intelligence to midsized organizations is that one formula doesn't fit all. With QRadar, however, MSPs gain the flexibility to offer single-tenant deployments for clients that require their own dedicated instances of QRadar solutions, while still offering multi-tenant deployments for others. This gives providers the power to optimize their delivery infrastructure based on their customers' needs.

Another critical issue is data separation. Until recently, single-tenant architectures guaranteed dedicated infrastructure resources and data separation to each supervised environment. Increasingly, MSPs now are rapidly adopting cost-efficient, multi-tenant environments that allow infrastructure to be shared while still separating data—much as virtualization divides a single physical server into multiple isolated virtual environments.

Broadening the market reach with scalability is also a concern. QRadar enables service providers to add multi-tenant customers with ease by using templated configurations—and then to serve them more quickly and effectively with standardized security checks—without having to add infrastructure to accommodate the growing business.

But most importantly, there is the need to overcome the economic squeeze felt by many providers. If they can't amortize infrastructure cost across large numbers of customers, MSPs struggle to control costs. The multi-tenancy capability of QRadar enables them to either lower prices, increase profitability or both. This helps bring cloud-based security services within the reach of more prospective clients—while freeing budgets so providers can deploy best-in-class security solutions.

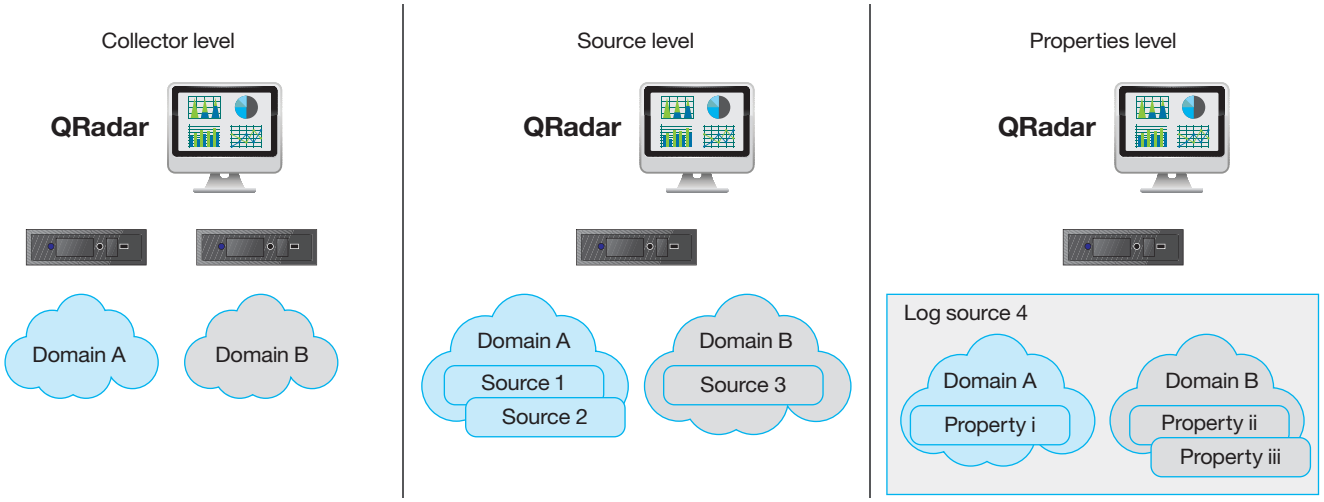
Domain segregation, the enabler of multi-tenant deployments

The muti-tenancy capability in QRadar is based on the use of domains. QRadar employs domains to help recognize which IP addresses are associated with which customers. Domains also allow service providers to support each customer's unique security concerns and risks.

Domains can be defined at three different levels:

- **Collector level.** A service provider can have a dedicated QRadar event or flow collector assigned to a particular customer, which allows that customer's events to be automatically assigned to a domain.
- **Source level.** A service provider can also assign logs and flows to a client's domain based on data source. For example, if client A and client B are sharing the same QRadar infrastructure, logs and flows originating from Client A can be assigned to a domain dedicated only to Client A. Similarly, Client B would have its own domain. If a log or flow source is detected that has no domain assignment, this data can be assigned to a default domain and later placed in the proper domain by an administrator.
- **Properties level.** For added flexibility, if a service provider has an infrastructure shared by multiple customers, or is aggregating data sources, the MSP can use properties to associate that data with a domain. For example, an MSP may have a single intrusion prevention system (IPS) supporting multiple customers, so there may be a property in the IPS log that denotes which network segment (and customer) an alert applies to.

The building blocks of IBM Security QRadar multi-tenancy

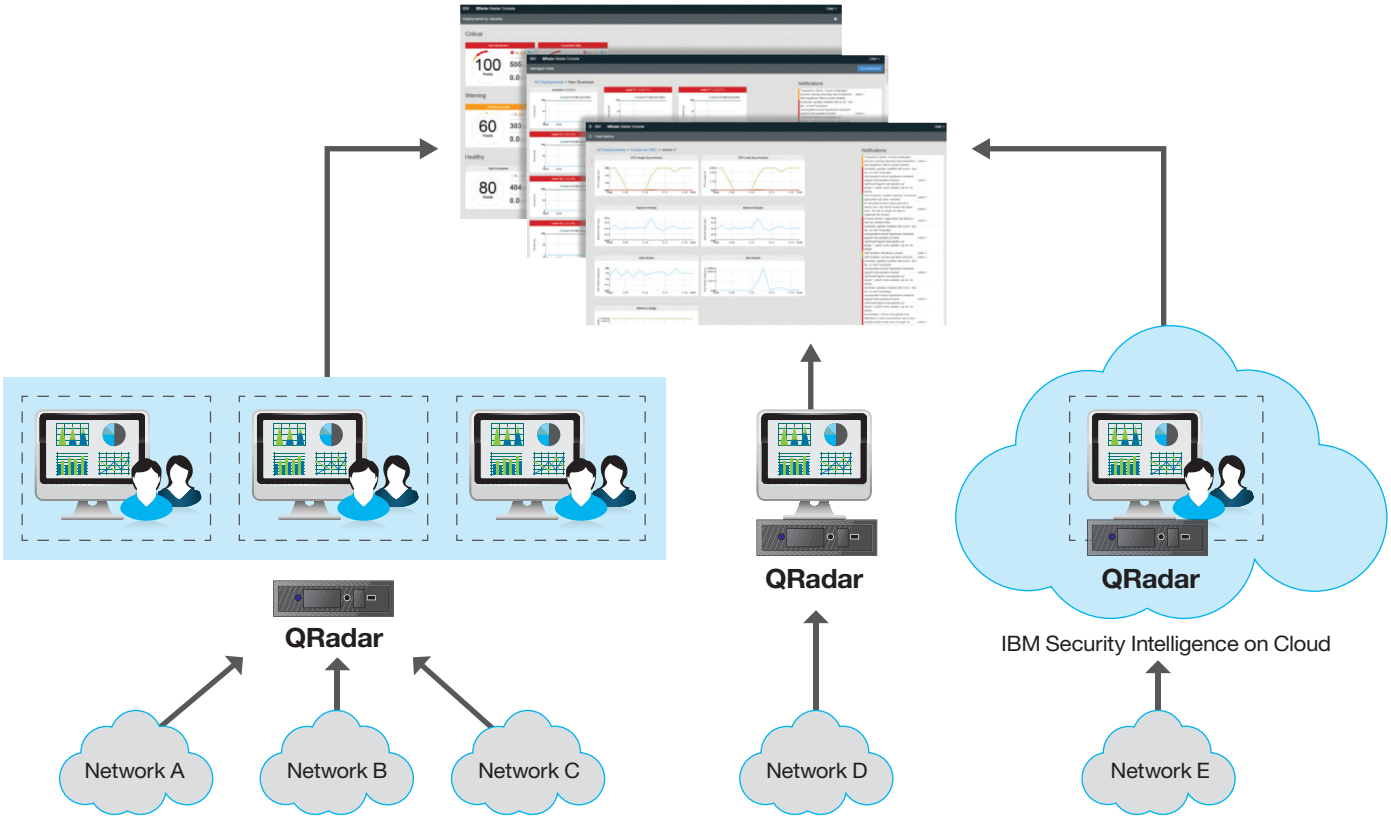


Once domains have been defined and associated with a customer, QRadar enables the service provider to create a security profile for those domains. This allows customers to have individual access to their own domains, and it supports onboarding new users, giving them appropriate access to their data.

Master console, a unified view for efficiency and responsiveness

Until recently, prevailing technology has forced providers to use a one customer/one console/one analyst model. To serve multiple customers, however, this approach requires multiple consoles—and involves higher costs. With the QRadar master console, MSPs gain the advantage of a single view across multiple QRadar deployments, giving them a 360-degree view of all their customers from just one console—regardless of whether a customer is utilizing a single- or multi-tenancy deployment.

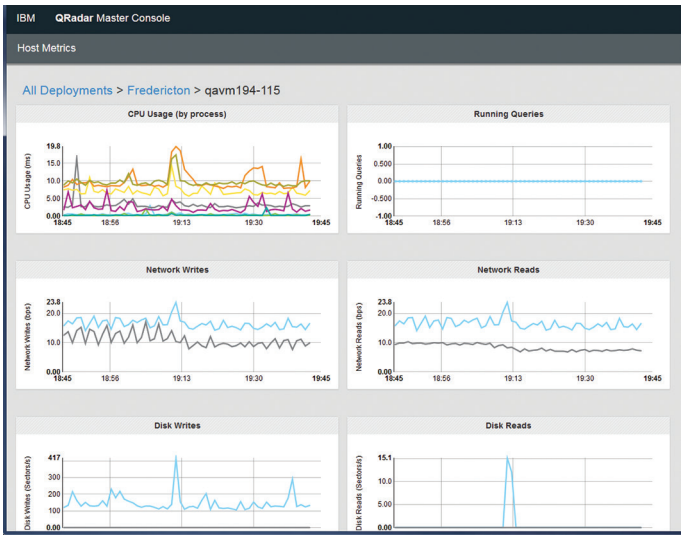
Master console: A single view across IBM Security QRadar deployments



Serving as an aggregation point, the console provides centralized health and system monitoring, as well as a centralized way to view and manage offenses. The single view can help providers understand and standardize on the common threat detection capabilities that may be required to serve their customers. Using an established remediation plan, analysts can then quickly push remediation actions out to multiple customers. This not only speeds response, but also reduces risk—while requiring fewer resources to handle the exploit.

The master console can create dramatic cost efficiencies by reducing the number of skilled analysts required to monitor and manage the customer portfolio. With only one console acting as an aggregation point, a single analyst can manage many clients simultaneously.

Master console: System functions monitored together



Master console: Management capabilities displayed together

- Log management
- Security intelligence
- Network activity monitoring
- Risk management
- Vulnerability management
- Network forensics

Flexible pricing and snap-on horizontal scalability

The need for large capital expenditures adds complexity and can hinder growth. To relieve this pressure, QRadar enables service providers to make fixed monthly payments that make budgeting easier and conserve scarce resources. To scale, providers simply turn on the licensing key to add capabilities. Adding new instances of QRadar is easy as well with true snap-on horizontal scalability.

Conclusion

When selecting a platform for security intelligence services, service providers must consider several critical capabilities. A mixed-tenancy environment that supports both single- and multi-tenant clients can help optimize infrastructure, lower costs, increase profits and provide greater flexibility. In addition, a unified console that allows a single analyst to manage multiple clients can simultaneously reduce costs and make management more efficient. Other critical features include rule-based security, robust reporting, flexible pricing, snap-on horizontal scalability and a wide range of device integration and APIs.

QRadar solutions are ideal for service providers. Easy to deploy and use, QRadar provides a broad set of integrated capabilities, including log management, next-generation SIEM, vulnerability management, advanced network activity monitoring, risk management and forensics analysis. QRadar provides a growth-ready platform that can easily scale to meet the needs of MSPs for the long term.

For more information

To learn more about QRadar, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/category/security-intelligence

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

Please Recycle

WGW03127-USEN-00