IBM Security

Thought Leadership White Paper

April 2015

The case for security intelligence services, hosted from the cloud

Close the security skills gap and lower capital expenditures with IBM Security Intelligence on Cloud

Introduction

Around the world, organizations are overcoming their security concerns and are taking the leap to cloud computing in order to realize capital expenditure cost savings and leverage a pool of specially trained security monitoring resources. In fact, according to a recent IBM survey of chief information security officers (CISOs), 86 percent of security leaders have adopted or plan to adopt cloud initiatives. The survey found that 60 percent are currently using software as a service (SaaS), 59 percent are using infrastructure as a service (IaaS) and 30 percent are using platform as a service (PaaS).[1]

So where does security intelligence fall in this migration to the cloud? Many organizations want to shift security operations to the cloud to overcome internal skills shortages, or replace their disjointed collection of point products with an integrated solution more capable of delivering an end-to-end security view, without starting over and removing the basic security they have so far achieved. Shifting to the cloud also offers the promise of updating the way they secure their business operations to meet today's changing needs. After all, cloud resources offer fast setup, low infrastructure costs, high availability and rapid scalability. But buyer beware, not all cloud vendors are created equal. Enterprise-grade security is typically outside the scope of most providers, and organizations must carefully review the capabilities inherent in any outsourced monitoring service. When adopting cloud-based security, they should settle for nothing short of the best solution for detecting irregular network activities and anomalistic user behaviors.

This white paper explores the advantages of using a robust security intelligence solution, delivered from the IBM cloud and monitored by IBM service professionals. It will look at how IBM® Security Intelligence on Cloud, a security-as-a-service offering, enables organizations to stay ahead of the latest threats with industry-leading technology and trusted IBM expertise—resulting in greater flexibility, cost effectiveness and peace of mind.

More than a trend, cloud-hosted security makes business sense

Organizations worldwide are choosing to invest in public, private and hybrid cloud services because the cloud is more responsive, efficient and cost-effective than traditional on-premises infrastructure. In fact, the cloud has shifted the economics of technology delivery and consumption—creating an entirely new business model.[2] Now, organizations can consume only the technology resources they need without the overhead of acquiring and managing their own infrastructure. They can significantly lower capital expenses (because there is no need for large, one-time purchases of technology). Plus, they can rapidly adapt to changing business needs at almost infinite scale.

However, as cloud adoption increases, organizations are also more focused than ever on ensuring that strong security controls are in place. In a recent IBM survey, 75 percent of security leaders expected their cloud security budget to increase or increase dramatically over the next three to five years.[1] By taking a phased approach to cloud-based security, organizations can be fiscally responsible about shifting their budgets, and take their time in evaluating vendors.

Naturally, the security industry has responded with a wide range of offerings to help organizations reap all the rewards of the cloud—and reduce security risks. In fact, IDC found that in 2013, security software for public clouds had a 13.7 percent share of the security software market. The worldwide cloud software market is expected to grow to USD102.9 billion in 2018, with a compound annual growth rate (CAGR) of 21.3 percent.[3]

The right cloud vendor will enable organizations to make the most of their on-premises investments, delivering the experienced people and best practices to meet specific security needs. As a first step to cloud-hosted security, the vendor should empower in-house security teams with the advanced correlation and analysis capabilities of security information and event management (SIEM). This way, IT staff can understand the context of threats, prioritize risks and vulnerabilities, and take the right steps for forensic investigations, remediation and mitigation. Then, after building trust with the vendor, they can move to a fully outsourced solution—integrating IaaS, SaaS, data analysis and other managed security services.

Security intelligence is vital in today's hybrid-cloud environments

To remain ahead of attackers, security teams need a complete view of their security posture. Organizations need *cloud security intelligence* that is based on network flows and logs from an extensive range of sources from across their organization. The right security intelligence tools can:

- Reduce a large number of security events to a small number of offenses requiring action
- Decrease false positives
- Tell security teams what has been exploited and what kind of activity has taken place as a result (such as data loss, theft or fraud)
- Provide quicker detection and incident response

Security intelligence is about using advanced security analytics, big data and automation to gain deep insights into an organization's security posture. The solutions are designed to collect, normalize, correlate and distill massive amounts of data from network traffic, logs, user behavior, system configurations, vulnerability reports, and numerous other sources to automatically identify unknown or previously undetected threats. Using analytics, security intelligence solutions can help find attackers and predict and prioritize security weaknesses for mitigation or remediation.

While moving their IT infrastructure to the cloud, enterprises face challenges because both the traditional on-premises infrastructure and everything deployed in the cloud need to be monitored and protected. System and network activities from both environments need to be collected and analyzed using a coherent

Closing the gap in security skills

Security risks are increasing—and so is the need for security expertise. How can your organization close the security skills gap?

The skills shortage can lead to security risks.

92%

of security decision makers say that staffing issues contribute to heightened levels of risk.*

Partner with security service providers

Get the help of a trusted expert. Security service providers have the people and the processes to get you ahead of the attackers—and help you stay there.

Security leaders are extremely satisfied with outsourcing.

90% think service provider skill sets are as good as, or better than, internal resources

Business value is up, costs are down.

31% of security leaders were able to reduce the number of staff members

Focus has shifted from operations to innovation.

32% of security leaders reduced budget spent on security operations

* All data contained in this infographic comes from "Surviving the Technical Security Skills Crisis," a commissioned study conducted by Forrester Consulting on behalf of IBM, May 2013.

and integrated approach. With an expectation that on-premises IT and cloud IT will co-exist for the next few years, it is important to deploy a security intelligence solution that is flexible enough to fit into a mixed environment and handle data sources resident on both infrastructures.

With the right vendor, cloud-hosted security can meet specific needs

- **Organizations can rely on security experts to acquire the right infrastructure.**
- **Solutions can be deployed with less time and effort than on-premises technology.**
- **Skilled staff can manage service availability and health monitoring.**
- **Software upgrades and patches are kept up-to-date for effective protection.**
- **Cloud capacity can be upgraded at any time to handle changing business needs.**
- **SIEM capabilities can be customized for different environments, including rule tuning, reporting and dashboards.**

IBM delivers advanced security intelligence, hosted from the cloud

The harsh reality is that today's IT organizations must work within increasingly limited budgets. Rather than deploying another point solution, they need an integrated platform that can provide advanced security intelligence with rapid time to value—while also providing the scalability and functionality needed to quickly and easily meet new requirements.

Integrated, end-to-end visibility

IBM QRadar® Security Intelligence Platform provides a fast, easy, cost-effective way to meet changing needs for security intelligence. IBM Security QRadar solutions offer integrated capabilities for log management, SIEM, data storage, incident forensics, full-packet capture, and risk and vulnerability management. This integration means that information can be correlated and analyzed from across data silos, allowing for automated detection and responses to threats. What's more, the latest information about exploits, vulnerabilities and malware can be accessed by security solutions across domains, providing greater threat protection.

Key capabilities of QRadar Security Intelligence Platform include:

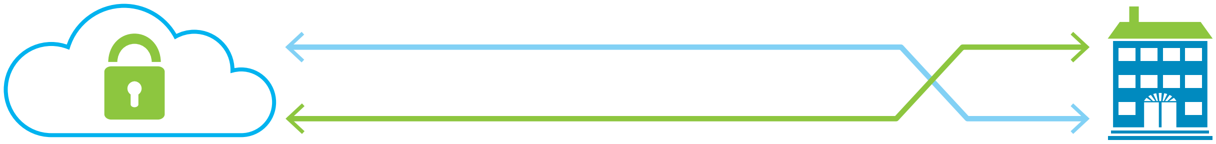
- A single architecture for analyzing log, flow, vulnerability, user and asset data
- Near real-time correlation and behavioral anomaly detection to identify high-risk threats
- High-priority incident detection among billions of data points
- Full visibility into network, application and user activity
- Automated regulatory compliance with collection, correlation and reporting capabilities

And now, IBM Security Intelligence on Cloud delivers the key capabilities of IBM Security QRadar SIEM, configured to customer specifications and deployed within a dedicated private cloud environment. The solutions are hosted by IBM within a secure SoftLayer[4] data center with built-in high availability and failover-supporting infrastructure.

How it works

IBM Security Intelligence on Cloud enables organizations to obtain the capabilities of an industry-leading security intelligence solution, with less up-front cost and faster setup. Security teams can access the QRadar capabilities from a web browser, just as they would if the product were deployed on-premises. But IBM experts manage the software configuration and implementation, along with its ongoing maintenance, disaster recovery and technical support.

IBM Security Intelligence on Cloud deployment model



Security intelligence as a service

- Market-leading technology is hosted in SoftLayer data center
- Service can be adapted/upgraded at any time
- IBM team manages:
  - Server acquisition, installs and configuration
  - User account administration
  - Service availability and health monitoring
  - Software upgrades and patching
  - Customer issue resolution

Data gateway **Organization**

- Advanced security is provided by the trusted experts at IBM
- Data gateway collects data and forwards it to the cloud
- In-house team handles:
  - Data gateway installation on-premises
  - Log source configuration
  - SIEM customization
  - Security monitoring and incident response

IBM Security Intelligence on Cloud is designed to:

- Collect security events from both on-premises and cloud infrastructure, enabling a faster response to critical threats
- Support a wide variety of workloads with a service upgrade at any time to meet dynamically changing business needs
- Help ensure high availability with expert staff that monitors server health, installs critical patches and upgrades software
- Align with an organization's operational-expense budget model by featuring monthly billing and flexible payment options, as opposed to traditional budgeting based on large, up-front capital expenditures
- Include comprehensive threat intelligence from IBM X-Force® research and development, one of the most respected commercial security research teams

Start your journey to a hosted, cloud-based SIEM solution

To get the full value of security intelligence, a solution needs to have full access to an organization's network data—ranging from documents to website images, as well as the metadata and contents of both structured and unstructured data. This way, the solution can provide security information with context to help reveal threat levels and vulnerabilities. Releasing control of this confidential information to just any cloud vendor, however, could be disastrous for the organization.

But with on-premises deployments, organizations can still have significant challenges, including an increasing shortage of skilled security personnel. Just as security threats become more sophisticated and more widespread, there's a growing lack of skilled people to monitor, analyze, prioritize and respond to threats. In fact, 92 percent of security decision-makers say that staffing issues contribute to heightened levels of risk.[5]

IBM Security Intelligence on Cloud provides organizations with quick access to market-leading SIEM technology, the flexibility to meet changing needs, and the trust of a world-class service team for the right cost. What's more, the IBM offering enables organizations to take a phased approach to cloud-hosted security services. They can start by outsourcing the core infrastructure, SIEM software, and services and support; then, slowly migrate to an even more comprehensive managed services engagement (provided by IBM Security Services).

Expertise

The IBM services team has the people and best practices to help organizations stay ahead of the latest threats. IBM security experts understand how to deliver SIEM as a service that can support the traditional data center and the cloud. By simply installing an on-premises data gateway to collect events and forward them to the cloud via a VPN, organizations can empower their staff to focus on responding to security incidents and potential vulnerabilities.

Thanks to IBM expertise, IBM Security Intelligence on Cloud can save significant time in the planning, acquisition and management, as well the up-front capital cost, of an on-premises SIEM solution. Organizations can rely on IBM teams to:

- Acquire, install and configure hosted QRadar servers
- Monitor the health and availability of services
- Apply critical patches and software upgrades
- Upgrade service levels whenever needed
- Provide one source for customer support

As the first step in a full migration to the cloud, organizations retain the responsibility for monitoring security incidents, investigating events and generating reports, while IBM teams monitor the cloud infrastructure status and health on a 24x7 basis. Clients also have the power of QRadar SIEM on their side for prioritizing threats and remediation or mitigation tasks. Once they are comfortable with the offering, they can move to a more fully outsourced solution with security and threat management services.

Flexibility

IBM Security Intelligence on Cloud is designed to support a wide variety of workloads. The service can be scaled up to meet increased seasonal demand or to support new product launches, and it can be scaled back down as requirements change. Organizations don't have to worry about large up-front capital expenditures, additional setup or IT maintenance expenses; they can simply plan for operating expenses via periodic billing.

At the same time, IBM Security Intelligence on Cloud enables organizations to customize the service to fit their specific needs. IT staff can configure the QRadar log sources to pull in data from across the on-premises environment as well as the cloud. Plus, they can customize the cloud-hosted service with specific SIEM rules, user permissions, groupings, searches, dashboards and reports. Organizations get the flexibility to adapt to their own requirements—with the assurance that the underlying infrastructure is configured according to security best practices.

Trust

The IBM Security team has helped secure some of the most complex cloud networks in the world—monitoring 15 billion security events every day for more than 4,000 clients. Instead of dealing with the high capital cost and complexity of an on-premises infrastructure, companies utilizing IBM Security Intelligence on Cloud have the help of IBM experts, for a predictable cost that aligns with their operations budgets. Plus, the service provides QRadar technology already trusted by leading organizations around the world, including:

- A Fortune Five energy company that reduced 2 billion logs and events per day to 25 high-priority offenses
- A financial information provider that tracked 250 activity baselines and saved 50 to 80 percent on staffing
- A global bank that identified and blocked more than 650 suspicious incidents in the first six months of security operations

Conclusion

Organizations are moving to the cloud at a rapid pace, making cloud security more important than ever. IBM QRadar Security Intelligence Platform enables security teams to collect, correlate and analyze information from across data silos—including the cloud—to automatically detect and respond to threats. And now, IBM Security Intelligence on Cloud gives organizations a way to access QRadar, deployed on the IBM cloud.

IBM Security Intelligence on Cloud provides organizations with a starting point for cloud-delivered security intelligence—but it's a starting point that comes from a trusted vendor, delivering industry-leading SIEM technology, backed by expert services and support. Over time, organizations can continue the migration to a fully outsourced solution. With deep visibility of both cloud and on-premises infrastructure, IBM Security Intelligence on Cloud can help organizations stay a step ahead of the latest threats.

For more information

To learn more about IBM Security Intelligence on Cloud, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/qradar

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle

[1] David Jarvis, “Gaining the Confidence to Fly: Cloud Insights From the 2014 IBM CISO Assessment,” *IBM Security Intelligence blog*, November 5, 2014. http://securityintelligence.com/gaining-the-confidence-to-fly-cloud-insights-from-the-2014-ibm-ciso-assessment

[2] “Monitoring the Hybrid Cloud: Evolving to the CloudSOC,” *Securosis*, January 7, 2015. https://securosis.com/research/publication/monitoring-the-hybrid-cloud-evolving-to-the-cloudsoc

[3] Robert P. Mahowald and Benjamin McGrath, “Worldwide SaaS and Cloud Software 2014–2018 Forecast and 2013 Vendor Shares,” *IDC*, July 2014. http://www.idc.com/getdoc.jsp?containerId=249834

[4] SoftLayer Technologies was acquired by IBM in July of 2013.

[5] Forrester Consulting, “Surviving the Technical Security Skills Crisis: An Assessment Of The Current Security Skills Landscape And How To Overcome It,” Commissioned by IBM Corp., May 2013. http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03030usen/SEW03030USEN.PDF