IBM Software
Thought Leadership White Paper

October 2013

Security intelligence is the smart way to keep the cloud safe

Integrated, comprehensive IBM solutions provide the visibility necessary for protecting the cloud

Contents

Introduction

Many of the same characteristics that make cloud computing attractive—scalability, flexibility and accessibility, rapid application deployment, user self-service, enhanced collaboration, and location independence—can also make it challenging to secure. When a cloud is up and running today and gone tomorrow, or when the number of users quickly changes from 50 people in one city to 50,000 across the globe—how do you keep it secure?

The answer lies beyond conventional security solutions, which by themselves provide neither the visibility nor the analytic capabilities necessary to proactively protect cloud environments. What today's organizations need for their clouds are integrated, comprehensive solutions that can deliver security intelligence. Advanced security intelligence solutions can close security gaps by using labor-saving automation to analyze millions of events occurring within the cloud, and discover system vulnerabilities through the normalization and correlation of these events. These tools can then remove false positives, add context and reduce vulnerabilities to a smaller, more manageable number for security teams to act upon.

This white paper will examine the intelligence capabilities necessary for gaining visibility into, and control over, cloud security. It will demonstrate how the integrated IBM® Security QRadar® suite of end-to-end security intelligence solutions can help meet cloud security needs.

Cloud computing heightens security concerns

Cloud computing can test the limits of security operations. Externally facing web applications often run the risk of unauthorized access and breaches. Multi-tenancy can threaten data privacy. Quick provisioning—and de-provisioning—can challenge regulatory compliance. Registrations and logins for thousands or even millions of users must be managed. Meanwhile, security measures must be both cost-effective and nondisruptive to business operations.

As security threats increase not only in number but also in variety and sophistication, IT departments are naturally concerned that reduced control of their clouds—especially in public clouds, where security is under the control of a third party, the cloud service provider—will lead to increased vulnerability. They worry about new and unexpected threats to the infrastructure as well as the risk of noncompliance with regulatory standards.

These fears can be well-founded, as host-based tools alone do not secure a cloud. A user can copy an entire virtual machine (storage and all) to access at home, and the host would not know. Users can read and write files without any specific host logging the activity. They can add and use new storage, or even remove logical storage, without the host ever knowing. And while user access can be terminated on the servers, it can be left on in the cloud.

Clouds can be hard to control

Cloud deployments include increased use of virtualization, shifts and changes in workloads, access from different locations and devices, the necessity for bring-your-own-device policies, and more.

The many facets of cloud operations belie a basic premise of cloud design—that the cloud hides complexity from users. But for the cloud management teams in IT, complexity is very real. Traditional tools do not give the IT security team the complete picture they need, making it difficult to understand what cloud resources the organization is using, who is using them, and what data is passing into, across, and out of the cloud.

Security teams must be able to discover and manage weaknesses in resources that span across traditional networks and into the cloud, including internal and external users, applications, databases, servers, and the network—or weaknesses in processes such as managing identities and patching applications. Vulnerability in one area can weaken the entire cloud defense. The cloud is a gateway into the enterprise and requires strong protection—so comprehensive cloud visibility, integrated across domains, is essential.

Visibility is key to overcoming vulnerabilities

For effective cloud security, the IT security team requires full visibility into cloud activities, a thorough understanding of what those activities mean, and comprehensive solutions for managing risk.

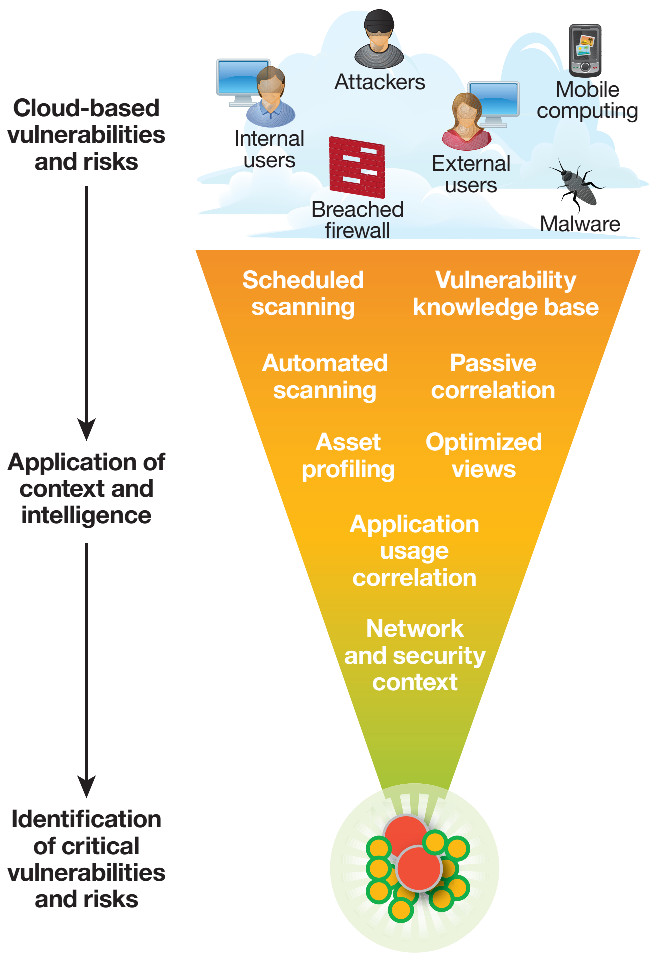
An integrated dashboard for managing cloud security

Private cloud
Public cloud

- Log management
- Security information and event management (SIEM)
- Configuration, risk and vulnerability management
- Network activity and anomaly detection
- Network and application visibility

An integrated dashboard can provide a single, consolidated view of security management capabilities across both public and private clouds. It can also enhance management processes for the security team with benefits such as faster operation, easier transference of management skills, simplified adoption, reduced requirements for staff training, and avoidance of the costs of deploying multiple point products.

By using advanced analytics and correlation—that is, security intelligence—to proactively recognize conditions that are conducive to attacks, or patterns that indicate an attack could be imminent, security teams can take preventive actions before such an attack occurs.


Cloud-based vulnerabilities and risks
Application of context and intelligence
Identification of critical vulnerabilities and risks
Attackers
Internal users
Mobile computing
External users
Breached firewall
Malware
Scheduled scanning
Vulnerability knowledge base
Automated scanning
Passive correlation
Asset profiling
Optimized views
Application usage correlation
Network and security context

Integrated solutions provide intelligence for, and visibility into, a wide range of cloud-based threats, reducing false positives and identifying the most critical vulnerabilities and risks.

Security intelligence can defend the entire cloud

Integrated security intelligence is a critical tool for detecting external and internal threats, predicting business risks, overcoming vulnerabilities, and addressing regulatory mandates. By consolidating and enriching data from across IT silos, and performing near real-time analytics on that data, security intelligence is crucial to providing visibility across the cloud environment.

Effective security intelligence will provide core capabilities across the cloud, such as:

- Providing a consolidated view of the entire cloud to defend against advanced attacks
- Correlating different events from across the infrastructure for actionable insight
- Utilizing a single dashboard to display security events across security domains

A key requirement is the ability to protect and track user activities on the virtual infrastructure, providing effective administrative access control. The security team needs to track suspicious role changes, unauthorized user actions and failed (and potentially harmful) login attempts. It must monitor user activities on physical servers or virtual machines—such as Create, Delete or Move VMs—and create an audit trail.

The team needs the ability to correlate events from virtual machine components, storage, routers, firewalls, switches and more, and to track this data as virtual machines are migrated or moved. They must be able to follow and report on issues such as duplicate IPs and virtual machine connectivity.

For complete visibility, the security team also needs operational intelligence for the virtual infrastructure. It should be able to browse and alert on errors occurring in logs, as well as to track changes to software and hardware resources and configuration changes in the cloud. To complete the team's management function, it will also need information to help investigate application response times and performance, and aid in capacity management.

In delivering visibility, an advanced security intelligence solution should span organizational silos and functions, utilizing centralized controls and capabilities such as granular management of log and flow data, advanced threat visualization and impact analysis, attack path visualization, and device or interface mapping.

Advanced solutions look deep into the flow of data

To identify indicators of attacks before breaches occur, security intelligence integrates information and uses advanced analytics across the security domains of people, data, applications and infrastructure. Advanced security information and event management (SIEM) solutions deliver security intelligence in physical, virtual and cloud deployments by using automation to correlate logs with network flows and a multitude of other data in virtual environments, presenting all relevant information on a single screen.

Log management solutions collect, analyze, report on and archive events across the cloud. SIEM solutions correlate logs with network flows and other data. Flow detection solutions record packet exchanges, or "conversations," between devices in virtualized, cloud environments. Detection and monitoring solutions provide visibility and control for vulnerabilities and risks. And data collectors integrate with SIEM solutions to detect threats, support policy and regulatory compliance, and minimize risks to mission-critical services, applications, data and assets.

The result is a deep look into the cloud's data communications that provides information beyond simply who is participating in an exchange. Security intelligence can discover, for example, when interactions include such recognizable data patterns as social security numbers, credit card numbers or text terms such as *ID* or *password* that indicate protected data.

An integrated dashboard is a valuable tool for minimizing costs and gaining the necessary cross-enterprise view. It can break down conventional siloed views of security data so information can be viewed and used together. Tools such as log management, network flow analytics, and real-time event correlation and analysis of security data can use this information to create the security intelligence necessary for a proactive defense.

A portfolio of security intelligence solutions that is integrated within itself but also with existing processes in each domain of the cloud—for example, identity and access management, network and server infrastructure, or application and data security solutions—is a major component to enabling long-term security assurance.

IBM delivers insightful, integrated solutions

IBM QRadar Security Intelligence Platform integrates log management, SIEM, anomaly detection, flows, configuration and vulnerability management, and risk management to offer a full portfolio of solutions for securing the cloud. The integrated portfolio provides a common user interface, common database and common platform that bring together information from across infrastructure silos to create security intelligence.

IBM Security QRadar Log Manager

Collecting and analyzing data from network and security devices—ranging from servers and endpoints to routers and switches, firewalls, intrusion prevention systems, and anti-virus applications—IBM Security QRadar Log Manager provides near real-time visibility into developing threats and helps meet requirements for continuous compliance monitoring.

Scaling to support hundreds of thousands of events per second across traditional and cloud environments, QRadar Log Manager can process incoming events in real time, assign severity, credibility and relevance attributes, and then trigger an appropriate response via email notification, dashboard posting, or flagging an event for further monitoring. IT staff can run fast, flexible queries on this aggregated log data to quickly identify potential compliance risks and security threats.

QRadar Log Manager also provides rich compliance-reporting capabilities to help meet or exceed many different regulatory requirements.

IBM Security QRadar SIEM

Integrating log, threat and compliance management, IBM Security QRadar SIEM helps protect the cloud infrastructure from a wide range of threats with near real-time visibility that supports threat detection, prioritization and surveillance. Asset profiling and flow analytics enable extensive visibility and actionable insight to control offenses and manage workflows. Automated normalization, context and correlation of raw data can save labor and help distinguish real threats from false positives.

The detailed data, access and user activity reports produced by QRadar SIEM enable more effective threat management. Reduced and prioritized alerts help the organization focus investigations on an actionable list of suspected incidents. Detailed data access and user activity reports help manage compliance.

The resulting insights help organizations detect threats that other solutions might miss, help ensure policy and regulatory compliance, and minimize risks to mission-critical services, applications, data and assets.

IBM network activity collectors

IBM Security QRadar QFlow and IBM Security QRadar VFlow appliances integrate with QRadar SIEM to provide application visibility and flow analysis to help organizations fully understand and respond to activities taking place in the cloud. Unlike many collectors, which typically stop at Layer 4 (transport layer) data, these solutions monitor network traffic destinations and applications using deep packet inspection of Layer 7 (application layer) flow data. This enables advanced threat detection that supports network analytics for identifying dangerous behaviors and anomalies.

QRadar QFlow and VFlow collectors can detect malware and virus/worm activity—including zero-day threats—through behavior profiling and anomaly detection. They can monitor social media, detecting anomalies and alerting security teams about related threats, and correlate security events and network traffic within and between both cloud and traditional environments to accurately prioritize incident data and reduce false positives. They also provide alerts of out-of-policy behavior and traffic to help support regulatory compliance.

IBM Security QRadar Vulnerability Manager

Fully integrated with the QRadar family, IBM Security QRadar Vulnerability Manager scans cloud environments to proactively detect and provide visibility of network device and application security vulnerabilities. It then works with QRadar SIEM to provide context to enrich the results of scans with network asset information, security configurations, flow data, logs and threat intelligence.

The solution helps organizations manage vulnerabilities, prevent security breaches, and achieve compliance with capabilities for discovering and highlighting more than 70,000 known dangerous default settings, misconfigurations, software features and vendor flaws. Consolidated views across vulnerability products and technologies add context to identify key vulnerabilities and reduce false positives. Intelligent scanning provides 360-degree visibility into the cloud, and integration with the security infrastructure leverages all QRadar data, reducing manual effort and risk.

IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager helps reduce risk and increase compliance by monitoring configurations in the cloud infrastructure and security systems, prioritizing vulnerabilities, and simulating network attacks and configuration changes to assess their security impact.

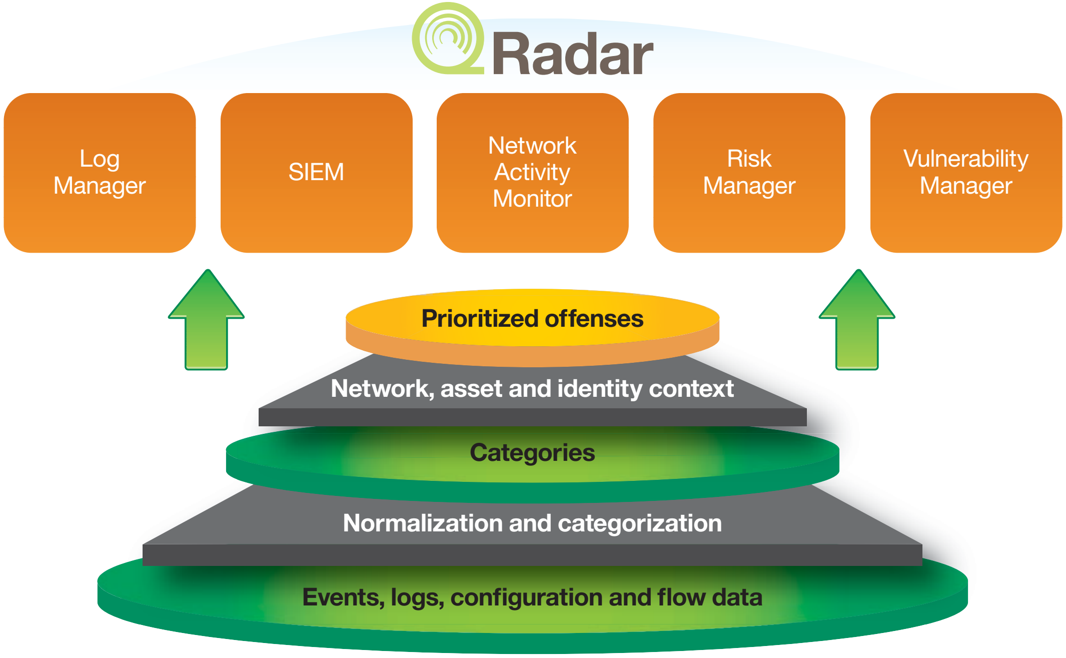
Analysis of firewall configurations helps identify errors and remove ineffective rules. Network topology and connection visualization tools enable data center operations managers and administrators to view current and potential network traffic patterns. And correlation of vulnerabilities, configuration and traffic help identify active attack paths and high-risk assets.

QRadar Security Intelligence Platform provides a single console that is shared by QRadar SIEM, QRadar Vulnerability Manager and QRadar Risk Manager, and is designed to help minimize costs and improve the organization's ability to assess information security risks.

Conclusion

Recognized as an industry leader in security, IBM provides best-of-breed solutions for security intelligence based on innovative solutions such as IBM QRadar Security Intelligence Platform, insights and security alerts for IBM security customers provided by IBM X-Force® research and development, and ongoing investments in developing security technology.

IBM security intelligence solutions deliver integrated, automated and comprehensive capabilities that provide visibility into the entire cloud environment to support regulatory compliance and enable a proactive security posture that helps stop attacks before breaches can occur.


QRadar
Log Manager
SIEM
Network Activity Monitor
Risk Manager
Vulnerability Manager
Prioritized offenses
Network, asset and identity context
Categories
Normalization and categorization
Events, logs, configuration and flow data

IBM QRadar Security Intelligence Platform creates security intelligence and actionable insight from information gathered across the enterprise.

For more information

To learn more about IBM security intelligence solutions, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

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 13 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 Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2013

IBM, the IBM logo, ibm.com, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle