A HURWITZ WHITE PAPER

The Benefits of an Integrated Approach to Security in the Cloud

Judith Hurwitz
President and CEO

Marcia Kaufman
COO and Principal Analyst

Daniel Kirsch
Senior Analyst

HURWITZ & ASSOCIATES
Insight to Action

Sponsored by IBM

Introduction

The advent of cloud computing is beginning to transform the way companies engage with customers, partners, and suppliers to increase flexibility and streamline operations. Cloud computing makes it much easier for the organization to implement new business services and to create new revenue opportunities much faster. At the same time, organizations are grappling with how to use cloud services while protecting the security of valuable assets. Security concerns have forced many companies to delay their use of cloud services.

As cloud computing gains more traction, more businesses are beginning to align their security strategy to better manage the privacy and compliance challenges of this new deployment model. Indeed, cloud models are being used not only to add compute and storage resources, they are also becoming an imperative for data analytics and mobility. The impact of the widening use of cloud computing means that more people are accessing applications, systems, networks, and data. For this strategy to be operational, IT needs to satisfy the business while maintaining compliance and security for critical intellectual property and customer data.

In this paper, we will look at how the growing adoption of cloud computing is changing the way organizations are implementing security. Hurwitz & Associates interviewed customers in a variety of industries to assess how they are approaching security for their cloud deployments leveraging IBM's Security Intelligence Platform.

One of the biggest risks for companies is that cloud services implementations have opened their intellectual property to large numbers of external participants.

Security Challenges Across Public, Private, and Hybrid Cloud

There isn't a single model for adopting cloud computing in organizations. The majority of companies are adopting a hybrid cloud model that combines public cloud services (a multi-tenant approach where the service provider controls security and access) and private clouds (an internally managed service where the company controls security and access). Typically, companies are choosing between public and private cloud services based on the level of security required. For example, a company might use a public cloud service to manage sales prospects or to test new applications. Alternatively, the same company may implement a private cloud for more sensitive applications that incorporate unique intellectual property and leverage customer data. The hybrid cloud model allows the organization to control perimeter security, access, data integrity, and malware in its data center and private cloud.

One of the biggest risks for companies is that cloud services implementations have opened their intellectual property to large numbers of external participants. This may mean that the security organization has less control over who is allowed to access specific resources. As businesses begin to understand that their data and applications can be leveraged as cloud services, it is critical that IT creates a cloud security model that consistently protects the company through the use of automated security controls.

Security levels across different public clouds can vary tremendously and you need to understand the security risks involved if your own on-premises infrastructure is connected to a public cloud. Many public cloud vendors have restrictive Service Level Agreements (SLAs) that absolve them of nearly any security requirements. To make these new services successful, service providers need to use a consistent methodology combined with a technology roadmap that delivers a highly flexible and well-executed level of security to protect customers.

Addressing Security Challenges in the Cloud

While there are many areas of cloud security that require attention including identity, applications, networks, and data, successful organizations are discovering that they can take an incremental, migratory approach to protecting their assets. Once the business focuses on connecting partners and customers outside the firewall, it is critical to implement sophisticated approaches to security. For example, organizations are automating access credential authorization in near real time. Companies also are discovering that they need to provide security for the various applications that are widely used by their various constituents – especially as these applications are delivered as services in the cloud. Customers we interviewed agreed that adding automated security processes such as identity or application scanning is a prerequisite to protecting the organization from intrusion and risk.

Customer Interviews: Entry Points for Cloud Security

The IBM customers we interviewed were at different stages of their cloud implementation, ranging from using public cloud services for test and development to building comprehensive hybrid cloud environments to support their customers and partners. While these companies have a wide range of security issues to manage, all were looking for entry points to implementing cloud security that would deliver results to the business quickly. Each of the customers expressed a need to dramatically rethink their approach to security as a result of the increasing number of cloud implementations. These businesses wanted customers to have seamless access to services without creating new security vulnerabilities.

Each of the customers expressed a need to dramatically rethink their approach to security as a result of the increasing number of cloud implementations. These businesses wanted customers to have seamless access to services without creating new security vulnerabilities.

Many customers took a multi-pronged approach that allowed them to implement cloud security across multiple entry points simultaneously. For example, one customer implemented Single Sign On (SSO) for all cloud services and at the same time implemented advanced security analytics to protect against unknown threats in cloud environments. However, one important best practice shared by these customers is that it is not necessary to implement all

HURWITZ
& ASSOCIATES
Insight to Action

elements of your cloud security strategy at once. In fact, it is much more effective to pick a few key places to get started and establish a roadmap for the future. The most common entry points to cloud security fell into the following three categories:

- **Automate routine cloud operations.** As companies share more data and applications with large networks of partners and customers in the cloud, they are beginning to automate routine operations tasks such as identity management. This approach is imperative if companies are to protect against potential data leakage and loss, and application source code loss.
- **Provide Access Controls for Software as a Service.** IT organizations are beginning to automate processes to monitor and track the use of SaaS solutions that have been independently licensed by individual business units. Many of these SaaS applications connect to corporate databases that contained highly secure information and could have created security vulnerabilities if not monitored appropriately.
- **Identify and Protect Against Unexpected Threats.** Chief Information Security Officers (CISOs) are increasingly concerned that existing approaches to security designed for the traditional data-center provide inadequate and hard-to-scale architectures in cloud environments. With so many access points into systems and networks, it is critical to be able to determine when unauthorized groups or individuals are hacking into systems.

A global telecommunications company needed to introduce an automated technique to increase access control and authentication to ensure customers that their data was safe.

Customer Challenges and Solutions: Business Benefits of Implementing the IBM Security Intelligence Platform

In this section we present several customer experiences to represent some of the key themes and entry points we heard from customers. These customers have implemented IBM's Security Intelligence Platform to protect against both known and unknown security threats. The solutions highlighted during our interviews can be integrated to provide a holistic view of security at the enterprise. The solutions include: IBM Security QRadar SIEM (Security Information and Event Management), IBM Security Access Manager (ISAM) Family, IBM Security Federated Identity Manager (TFIM), and IBM Endpoint Manager (IEM) to provide a holistic view of cloud security in their organizations.

Entry Point: Automate Routine Cloud Monitoring

What's the challenge? A global telecommunications company began selling cloud services to its mid-sized customers as a way to establish new sources of revenue. The company began offering a variety of value-added cloud services including email and accounting applications. More and more partners, customers, and employees from across the globe began accessing data and applications that had once only been accessible by a small group of approved users from behind a firewall. The company needed to introduce an automated technique to increase access control and authentication to ensure customers that their data was safe. According to the Chief Information Security

Officer(CISO), one of his greatest challenges was to be able to determine when a breach occurred and what data was affected.

What's the solution? The organization used the advanced security intelligence capabilities of IBM QRadar SIEM to provide visibility into both its traditional and cloud infrastructure. QRadar has enabled the organization to provide a unified approach to detecting and protecting against threats within a highly distributed cloud environment. This was especially important because the company implemented virtualization and needed to be able to efficiently identify which virtual machines presented a security risk.

Entry Point: Identity and Access Management – Gaining control of Software as a Service (SaaS) environments

What's the challenge? A technology company faced a huge security risk in a highly competitive environment as a result of its inability to adequately monitor SaaS services used by employees. For example, the company lost some major customers to a competitor when a member of the sales team left the company and continued to access the company's cloud-based Customer Relationship Management (CRM) system. This ex-employee continued to get inside information on company pricing and other private company information until significant damage was done. Without well-defined identity management automation, it can be difficult to keep private customer information secure.

Without well-defined identity management automation, it can be difficult to keep private customer information secure. A technology company integrated Single Sign-On into their business process, eliminating the need to constantly provision and de-provision users.

What's the solution? The company implemented a suite of IBM products that created a highly automated and consistent set of cloud services to support identity management, web access management, and federated identity and access management. Single Sign-On (SSO) was built into the business process. This approach eliminates the need to constantly provision and de-provision user access rights. Now when new employees join the company, they are immediately given the correct level of access to services they need, and when they leave, they are fully de-provisioned from every service. This has helped the company reduce the number of licensed users they need for SaaS applications, which has driven down costs. At the same time, the IT organization has increased its visibility into who is using each service.

Entry Point: Identify and Protect against Unexpected Threats in Cloud Environments

What's the challenge? The CISO for a large government agency stated that his organization's traditional agent-based approach was not providing the right level of logging detail for virtualized cloud environments. Therefore, the IT organization was concerned that existing tools did not provide visibility into all system traffic. The organization needed a way to move from its traditional approach of monitoring the physical environment to also include monitoring of the virtualized system.

HURWITZ
& ASSOCIATES
Insight to Action

What's the solution? To protect the organization from this lack of visibility and to provide a way to look for malicious activity, the organization implemented IBM Security QRadar SIEM. As a result, the agency now has a coordinated and centralized view of their network and application activity. In fact, during the QRadar SIEM proof of concept, seven previously unknown networks were discovered. QRadar SIEM is also being used to integrate the organization's log events and network activity, including network flows. In addition, the agency is using IBM QRadar SIEM to correlate data across seemingly unrelated events to predict, detect and stop malicious activity. The agency also implemented IBM Endpoint Manager to provide compliance and reporting metrics on the status of its systems. After the implementation, the security team has a better understanding of the activity on their systems and is able to better assess their risk exposure.

A large government agency did not have detailed insight into their virtualized cloud environments. By implementing IBM QRadar SIEM the agency now has a centralized view all of their network and application activity.

Putting it all together: Integrating across multiple entry points

What's the challenge? The executive director of IT Security at a global insurance company was tasked with determining an automated way to routinely and safely manage the identities of over 200 external business partners. While the insurance company wants to make it easy for business partners to collaborate, it must retain control over the environment for regulatory and security reasons. One approach to managing the security of this highly collaborative environment is to ensure that IT has a single view of who has access and can quickly add new partners or revoke access when required. In addition to these important business priorities, the executive director is very concerned about protecting the company from unknown security threats that are much harder to identify because of the company's move to the cloud.

What's the solution? The insurance company implemented IBM Tivoli Federated Identity Manager (TFIM) for added visibility in cloud environments and IBM QRadar SIEM to help secure against unknown threats.

The TFIM implementation provides all internal and external users with SSO. Implementing SSO was a key priority for the company and has been a "win-win" between IT and the business. Internal business users and partners who need to access the company's cloud services no longer need to manage different passwords and usernames for each application. SSO has also led to significant cost savings because IT no longer needs to manually interact with customers and employees when passwords are forgotten or lost. In addition, IT can quickly provision a new user without delays. The company now has complete visibility into the systems, data, and applications that each user has access to.

The company took the further step of integrating identity management with access products, including IBM Security Identity Manager (ISIM), IBM Security Access Manager (ISAM) Family, and IBM Tivoli Federated Identity Manager (TFIM), into IBM QRadar SIEM so IT could have a holistic view of their security assets. QRadar SIEM identifies event logs, flows and events, and is also architected to correlate across different cloud services to identify who is using what system, while prioritizing users and assets. As a result, the organization's data is more secure because all access is monitored and correlated to proactively alert the CISO's team when there is inappropriate activity and identify any intrusions. With QRadar, the customer can perform immediate normalization and correlation activities on raw data to help determine if there is a threat. As a result, IT is able to identify connections between events that might have otherwise remained hidden.

. . . as attacks become both more complex and sophisticated, it has become a priority to look across all of these different products in order to identify and respond to threats.

Underlying Principals for a Secure Cloud Environment

Securing a cloud environment requires, and offers a new approach to security: holistic Security Intelligence. Many organizations have dozens of different point products to address security concerns. For example, they may have a firewall from one vendor, identity management from another, and application scanning from a third. This creates a siloed approach to security. However, as attacks become both more complex and sophisticated, it has become a priority to look across all of these different products in order to identify and respond to threats. By reducing the number of point products in an environment and adopting a unified approach, organizations are gaining better insight into unknown threats while also managing continued security risks.

Whether deploying a traditional data center, or a cloud, organizations must protect the infrastructure and applications while monitoring and controlling access to all resources. This security must be accomplished in a way that meets industry regulatory and compliance standards. Organizations must be able to protect against both known and unknown threats across all of these elements of the computing environment.

The following are six key principals for creating a secure cloud.

- **Create a Secure Infrastructure.** Creating a secure infrastructure means that the underlying systems architecture must be protected against traditional vulnerabilities such as network threats and hypervisor vulnerabilities. In addition, virtual machines must be securely isolated from each other and patches must be kept up to date.
- **Build Security into Applications Development.** Developers of web and cloud based applications often lack deep expertise in security and therefore do not appreciate the vulnerabilities that exist with applications. Securing applications requires building application scanning into the development process combined with a patch management plan.
- **Establish an Automated and Unified Approach to Identity Management.** With the introduction of cloud computing, more employees and external users need access to a broad range of systems and services ranging from virtual desktops to public SaaS environments. All of this activity might take place in just a few minutes. A successful identity strategy gives administrators federated identity management and gives users Single Sign On (SSO) capabilities.

Continued next page

- **Keep Data Secure Regardless of the Deployment Model.** A successful cloud data management strategy allows an organization to know where data is located and who has accessed that data. Often this data is not static, it will change and move based on business transactions. In addition, data must remain secure whether it's being accessed in the office or from a mobile device. All of this data must be backed up in a reliable and secure manner.
- **Ensure Compliance within a Hybrid Computing Model.** Compliance and regulatory requirements are quickly evolving and organizations are struggling to stay current. Many industries require compliance with specific regulations related to protection of customer and corporate data.
- **Prepare for Advanced Persistent Threats (APTs).** APTs are ongoing slow attacks that masquerade as ordinary activity and are typically not identified by traditional security technology. These sophisticated threats are becoming commonplace. Companies need to be able to anticipate these threats so they can be stopped before they cause significant damage.

A successful cloud data management strategy allows an organization to know where data is located and who has accessed that data.

Selected IBM Security Offerings for the Cloud

IBM's security offerings have four main entry points: people, data, applications and infrastructure. The following are key cloud security offerings that Hurwitz & Associates discussed with IBM customers and business partners when researching this white paper.

IBM QRadar SIEM (Security Information and Event Management)
QRadar automation brings together previously disparate data, correlates it, analyzes it, merges it with network flow information and removes false positives. This process provides security teams with actionable and prioritized information on security incidents. For example, QRadar collects logs from thousands of endpoints so that the system can correlate and analyze data in context with log and network data from other enterprise resources. In addition, QRadar can incorporate third-party security feeds, such as IBM Security X-Force Threat Intelligence, which publishes malicious IP addresses with corporate data so that the system can analyze internal events with the most up-to-date emerging threats.

IBM Security Identity Manager (ISIM)
IBM ISIM automates the creation, modification, recertification and termination of user privileges throughout the user lifecycle. Companies use ISIM to create a more unified and policy-based approach to managing users identity, access rights, and passwords. The product is pre-configured to enable customers to manage user access rights and passwords as needed to meet audit and compliance requirements.

IBM Security Access Manager (ISAM) Family
ISAM portfolio helps companies provide users with a Single Sign On (SSO) to access all their applications. This solution simplifies password management,

HURWITZ & ASSOCIATES
Insight to Action

protects information with strong authentication, and helps secure kiosks and shared workstations.

IBM Tivoli Federated Identity Manager (TFIM)
TFIM provides web and federated single sign-on (SSO) to users throughout multiple applications. It uses federated SSO for security-rich information sharing for private, public and hybrid cloud deployments.

IBM Endpoint Manager (Formerly IBM BigFix)
IBM Endpoint Manager is a management and security platform for mobile, desktop and servers endpoints. The platform helps customers address the security concerns and complexities that arise with bring your own device (BYOD) policies. For example, IBM Endpoint Manager delivers a unified platform that spans mobile device platforms including Google, Android, and Apple iOS.

Conclusion

Businesses are increasingly focused on the requirement to provide constituents with easy and effective access to services in a hybrid cloud environment. This ease of access comes at a price. Therefore, organizations are demanding that IT maintain consistent and correct protection for customer data and their own intellectual property. To be successful, the IT security team needs an incremental, holistic, and predictable approach to automate and integrate security. A combination of modular software combined with best practices can lead a company to a customer-centric approach when securing the hybrid cloud based environment.

… organizations are demanding that IT maintain consistent and correct protection for customer data and their own intellectual property.

HURWITZ
& ASSOCIATES
Insight to Action

About Hurwitz & Associates

Hurwitz & Associates is a strategy consulting, market research and analyst firm that focuses on how technology solutions solve real world customer problems. Hurwitz research concentrates on disruptive technologies, such as Big Data and Analytics, Security, Cloud Computing, Service Management, Information Management, Application Development and Deployment, and Collaborative Computing. Their experienced team merges deep technical and business expertise to deliver the actionable, strategic advice clients demand. Additional information on Hurwitz & Associates can be found at www.hurwitz.com.

HURWITZ
& ASSOCIATES
Insight to Action

13A Highland Circle • Needham, MA 02494 • Tel: 617-597-1724
www.hurwitz.com