Cloud Security is a Marathon: Go the Distance With RSA and Ixia

By definition, clouds introduce obscurity, a perennial challenge for those defending the company’s assets. With so many critical workloads moving to public and hybrid clouds, securing data must be considered a marathon—a way of life—not a sprint that ends with migration.

Experts recognize that public clouds create formidable new security challenges, starting with the fact that IT loses some degree of visibility and control. In a 2017 survey of cloud users, more than 90% cited public cloud security among their chief concerns, while 40% felt less than satisfied with the security monitoring done by providers.

Like seasoned marathon runners who compete against their own personal best times as well as the competition, security teams always seek to speed threat detection and response. A step-by-step plan is critical to preparation and endurance, so RSA and Ixia have developed a joint solution and best-practice approach to improving security response times.

Joint solution highlights
• Supplement data logs supplied by cloud providers
• Turn raw data into security intelligence
• Streamline visibility and security across multiple cloud environments
• Improve response times, ROI as deployments scale
• Automate data capture and analysis to make IT’s job easier
THE CLOUD SECURITY LIFECYCLE

Ixia and RSA have identified three critical phases of securing the cloud:

• **Migration: Reestablish visibility.** Steps must be taken to supplement metadata (e.g. logs) supplied by cloud providers to ensure that performance and security monitoring tools receive the same detailed quality of packet data from the cloud as they do from physical networks.

• **Operation: Turn cloud data into security insights.** Intelligence must be applied to analyze the raw data collected in the cloud and speed the process of detecting and mitigating threats.

• **Evolution: Improve response times as you scale.** Continuing to maintain or improve incident response times proves vital to maintaining compliance with industry mandates for secure handling of data, as well delivering a rewarding customer experience and achieving high returns on investments (ROI) in APM, NPM, and security.

**Phase 1: Extending visibility during migration**

Moving services to public or hybrid private/public cloud environments means IT no longer has full visibility into events occurring outside their traditional domain. While we can easily tap and aggregate packet data from physical networks, public cloud providers typically share only log or other metadata that features basic information about each conversation—when it started, how long it lasted, etc.—but does not contain the network-level visibility into valuable data required by tools to help identify threats. For example, actual copies of conversations and email threads that let IT clearly see malicious content or intent.

Without the same granularity of packet-level data, analysis tools cannot deliver the same caliber of security intelligence within cloud networks. Visibility gaps become compounded as a company subscribes to multiple public cloud services.

This is where Ixia's CloudLens visibility solution comes into play, restoring full visibility by capturing packet-level data within the cloud, then sending all (or only) relevant data to RSA NetWitness Platform for analysis. CloudLens sensors deployed within source cloud servers (e.g. Web, applications, databases) capture and deliver copies of the servers packet level data to the RSA NetWitness Network solution.
Phase 2: Operation

Ixia CloudLens continues to improve ROI by intelligently filtering out and eliminating unwanted data at the source within the cloud to reduce the time, effort, and bandwidth required to send tools precisely the right data. Armed with ongoing access to packet-level data, security experts can act fast, and often, act first.

RSA’s NetWitness Platform transforms raw data from the cloud, including detailed packet level data delivered by CloudLens, into actionable security intelligence to speed queries, eliminate blind spots, and refine best practices. RSA NetWitness Network solution allows IT to use rich metadata to reconstruct events to speed investigation, prioritize threat risks, and understand the context and full scope of each attack.

What happened and where did it happen? Are security policies being implemented consistently? Do we have controls in place to prevent users from spinning up workloads that contradict policies?

RSA’s analyst-centric approach equips security experts with full visibility across endpoints, networks, logs, virtual machines (VMs), and cloud environments. The RSA NetWitness Platform applies leading-edge techniques such as modeling and machine learning, along with rich business context, to promote deeper analytics while processing large amounts of threat data.
Phase 3: Evolution

Efficiently scaling any deployment comes down to two things: automation and ease of use. CloudLens streamlines management with easy setup via Ixia’s software-as-a-service (SaaS) portal and drag-and-drop definition of source and tool groups as well as filtering policies. Visibility auto-scales as workloads are created with new instances automatically added to the right source or tool groups based on user-defined criteria. Automation avoids error-prone manual intervention and dangerous time lags.

The RSA NetWitness Platform streamlines workflows by consolidating all the relevant elements needed for investigation into a single pane of glass. The system coordinates processes and orchestrates functionality to allow teams to mitigate threats before they turn into catastrophic breaches. Analysts can easily dig deeper to spot patterns and trends, find clues, and export artifacts for future reference.

CREATE YOUR WINNING GAMEPLAN TODAY

RSA and Ixia work with security teams to meet the unique needs of their business, and to help business leaders understand security and compliance. The RSA NetWitness Platform and CloudLens combine to deliver better data that promotes better security visibility, faster decisions, and responses over time.

To take the next step and see how CloudLens and RSA NetWitness Platform can help your company prepare and go the distance in the cloud security marathon, watch the joint webinar titled, “Cloud Security is a Marathon: How to Get a Running Start.” The session features insights from cloud security and visibility experts as well as a demonstration of the joint solution in action.
ABOUT RSA NETWITNESS

RSA NetWitness® Platform is an evolved SIEM and threat defense solution that empowers security teams to rapidly detect, understand the full scope of a compromise and automatically respond to the threat before damage is done. With a design that aligns business context to security risks, RSA NetWitness Platform closes the gaps of technology-only solutions and ensures that IT security is optimized to support an organization’s strategic goals. RSA NetWitness Platform delivers unsurpassed breadth of visibility and depth of analytics that make security analysts more effective and efficient.

ABOUT RSA

RSA® Business-Driven Security™ solutions uniquely link business context with security incidents to help organizations manage digital risk and protect what matters most. With award-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA solutions protect millions of users around the world and help more than 90 percent of Fortune 500 companies take command of their security posture and thrive in an uncertain, high-risk world. For more information, visit rsa.com.

Learn more at: www.ixiacom.com

For more information on Ixia products, applications, or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info