radware

Stay Ahead of the Curve

9 Ways to Ensure Cloud Security

Whether you've migrated some or all of your infrastructure to the cloud, or are still considering the move, you should be thinking about security. Too often, organizations assume a certain level of protection from a cloud service provider and don't take steps to ensure applications and data are just as safe as those housed in the data center.

The sheer range of cloud technology has generated an array of new security challenges. From reconciling security policies across hybrid environments to keeping a wary eye on cloud cotenants, there is no shortage of concerns. An increasingly complex attack landscape only complicates matters and requires security systems that are vigilant and able to adapt. Here are nine tips to consider before, during, and after a cloud migration to stay ahead of the curve when evaluating security solutions for your cloud service.

1. PLAN FOR HYBRID ENVIRONMENTS

The majority of organizations will have applications housed across hybrid environments, requiring CIOs to coordinate security policies across these environments. It might be tempting to rely on your cloud service provider for security, but that could lead to risky inconsistencies. Identify security services that **overlay a number of different cloud-based apps and provide the same technology and policy management** for on-premise applications.

2. START WITH LOW RISK ASSETS

As you begin migrating to the cloud, start with data and apps that are less sensitive or mission-critical. CRMs, for example, might not be as sensitive to downtime or data loss. Until you've vetted the reliability and security of a cloud service provider, **avoid migrating high-risk assets**.

3. MAINTAIN USER CONFIDENTIALITY

If your cloud provider is defending against encrypted attacks, it might **inadvertently compromise user confidentiality**. After all, detecting encrypted attacks requires some level of decryption of both legitimate and malicious traffic. Check with your cloud provider to see what solutions it uses and whether your sensitive information will stay private.

4. KNOW WHAT YOU HAVE IN THE CLOUD

Your employees are almost certainly using cloud-based applications without the knowledge of IT teams, leaving a trail of vulnerabilities and data leakage. **Unapproved cloud-based apps** can lead to malware, posing a risk to the network. This problem has generated a new category in the security space: the cloud access security broker.

5. DON'T BECOME COLLATERAL DAMAGE

Understand the architecture and security offered by your cloud provider. Sharing computing resources/space can result in outages throughout the network, degraded performance, or denied access for users in certain geographies. If you share space with the target of an attack, **you could become collateral damage**. Can your cloud provider separate attack traffic from clean traffic to prevent attacks on cotenants of a cloud platform?

6. UNDERSTAND COMPLIANCE IMPLICATIONS

If encrypted sessions are being terminated in the cloud, make sure your provider's platform or location fit both internal and industry compliance standards. You may be required to **upgrade or modify security protocols** to ensure the cloud service complies.

7. DETECT WHERE YOU CAN, MITIGATE WHERE YOU SHOULD

Monitoring for attacks at your own data center is relatively easy, but cloud adoption means critical assets aren't as "close" as they use to be. That distance can negatively impact timely detection. **Place detection capabilities in front of your cloud-based assets** just as you would in your data center. It allows you to assess the attack and determine the appropriate response. For example, turning to cloud scrubbing if it's a volumetric attack.

8. UNDERSTAND THE SECURITY CAPABILITIES OF YOUR CLOUD VENDORS

As with any service category, cloud hosting providers have different strengths and weaknesses. Some differentiate based on price, others on speed, and others on security. Be sure to **understand the security capabilities of your provider**.

9. SEPARATE SECURITY REQUIREMENTS FROM HOSTING REQUIREMENTS

Be careful to **not let business units outside IT take ownership of security**. Business units are under a lot of pressure to leverage the cloud to speed time-to-market and reduce costs. Security becomes a secondary consideration. Most of these business teams don't have the skills or knowledge to assess security requirements.

LEARN MORE ABOUT RADWARE'S CLOUD SECURITY SERVICES TO GUARD YOUR CLOUD-BASED ASSETS WITH A SECURITY SOLUTION THAT ADAPTS TO EVOLVING THREATS AND APPLICATIONS.

©2018 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this press release are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.