3 TIPS TO SECURE YOUR CLOUD TRANSFORMATION
Digital Transformation Creates New Risks

Adoption of cloud computing is at the heart of most organizations’ digital transformation strategies. Whether they seek to modernize IT infrastructure, connect with customers on digital platforms or automate core business processes, organizations increasingly rely on an expanding array of public, private and hybrid cloud services to meet these objectives.

And why not? The cloud is known for giving organizations more budget flexibility and for conferring them with greater scalability and agility. But without proper governance, cloud applications and services can introduce security, privacy, compliance and resiliency risks.
OFFLOADING WORKLOADS TO THE CLOUD DOESN’T OFFLOAD THE RISK

Increased Access Complexity
As organizations move applications and IT infrastructure to the cloud, the traditional network perimeter, an internally secured boundary, disappears, making it harder for security teams to monitor activity on the network. Cloud adoption also complicates identity and access management by creating multiple identity stores over which security teams have little control.

Decreased Visibility
In addition to the identity and access management challenges, security teams also lack visibility into their organizations’ complex, multi-cloud environments. This limits their ability to proactively detect and respond to cloud-based threats.

Governance Challenges
As organizations continue to shift more data, services and applications to cloud providers, risks multiply, making an effective third-party risk management and governance program essential. However, these programs can be difficult to initiate and operate without leadership and technology support.
TIP 1: IMPLEMENT RISK-BASED ACCESS CONTROLS

Whether your organization uses a single cloud environment or operates across a multi-cloud environment, the first tip to cloud security is implementing access controls that provide the right access to the right users at the right times. The more disparate and varied your cloud environment becomes, the more difficult it can be to monitor access and the more often issues can arise. Thus, it’s important for organizations to implement a solution that allows them to balance availability, reliability and security.

An effective access control system should provide your organization with the following four capabilities:

- **Unified visibility and control** across your application and resource landscape, so you can holistically manage users and access from a single application, reducing blind spots and minimizing risk.

- The ability to manage blended cloud and on-premises, bring-your-own-device and mobile environments, allowing employees, partners and contractors to do more without compromising security or convenience.

- Support for an identity assurance strategy that enables users to access applications quickly and easily without sacrificing security.

- A modern, risk-based, multi-factor authentication engine that doesn’t require step-up authentication unless it identifies risky behavior, thereby allowing a majority of users to gain seamless access to the data, services or applications they need from any device, anywhere.
A well-known axiom for security states that you can’t manage what you can’t see. Following that logic, you need visibility to manage cyber threats in the cloud, but monitoring alone is insufficient. You also need processes and tools to coordinate a swift, cross-functional response in the event of a cloud-based cyber threat. Combining monitoring with response allows you to capture the benefits of the cloud while mitigating many of the security risks.

A fully-visible, properly managed network monitoring solution for multi-cloud environments should:

- **Provide a modular, distributed architecture** that collects data across all capture points (logs, packets, net flow and endpoint) and across all computing platforms (physical, virtual and cloud), and translates that data into actionable insight for security teams.

- **Speed threat detection and investigation** by enriching log, network and endpoint data at capture time with threat intelligence and business context.

- **Automate and orchestrate** security responses with consistent, transparent and documented processes to reduce the risk of breach or fraud loss.
Many businesses are moving critical applications, services and data stores to cloud providers. This level of trust is unprecedented for most companies and should be accompanied by careful planning, assessment and ongoing oversight. Yet keeping track of third-party cloud vendors can be overwhelming. An effective third-party management system should allow you to:

- Manage and monitor cloud services providers through the entire relationship lifecycle, including onboarding, assessment and performance.

- **Catalog** the services provided by each cloud vendor, **track** the relationships and associated contracts, identify the functions or critical business processes each cloud vendor supports, and establish business **owners and processes** for managing each relationship.

- **Identify gaps in security controls** and develop a dynamic roadmap to **measure and manage risks** stemming from each service provider based on the criticality of the applications, services or data stores they support.
RSAs Business-Driven Security™ solutions provide customers with a unified approach to managing the security, privacy, compliance and resiliency risks that stem from using multiple cloud providers. We do this by tackling key aspects of cloud security, including authentication, access management, and threat detection and response, and by helping you establish and mature a robust third-party risk management and governance program.

### HOW WE HELP

<table>
<thead>
<tr>
<th>Assess Third Party Risk Management Capabilities</th>
<th>Secure, Risk-Based Access &amp; Authentication</th>
<th>Third Party Governance</th>
<th>Evolved SIEM/Advanced Threat Detection &amp; Response</th>
<th>Omni-Channel Fraud Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engagement</td>
<td>Risk-Based Authentication</td>
<td>Business Context</td>
<td>Security Platform</td>
<td>Omni-Channel Fraud Detection</td>
</tr>
<tr>
<td>Assessment</td>
<td>Authentication Anomaly Detection</td>
<td>Criticality &amp; Priority</td>
<td>Logs &amp; Packets</td>
<td>Advanced Adaptive Authentication</td>
</tr>
<tr>
<td>Risk Quantification Mode</td>
<td>Identity, Governance &amp; Lifecycle Management</td>
<td>Risk Assessment</td>
<td>Endpoint</td>
<td>Real-Time Risk Assessment</td>
</tr>
<tr>
<td>Benchmark Report</td>
<td>Access Policy</td>
<td>Monitoring</td>
<td>UEBA</td>
<td>Fraud Intelligence</td>
</tr>
<tr>
<td></td>
<td>Violation Detection</td>
<td>Dashboards &amp; Reporting</td>
<td>Orchestration &amp; Automation</td>
<td></td>
</tr>
</tbody>
</table>

RSA Risk & Cyber Security Practice

RSA SecurID® Suite

RSA Archer® Suite

RSA NetWitness® Platform

RSA Fraud & Risk Intelligence Suite

Review other resources that will help you take the next step toward securing your journey to the cloud. RSA – Secure Your Cloud Transformation
ABOUT RSA

RSA Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud prevention and integrated risk management, RSA customers can thrive and continually adapt to transformational change.