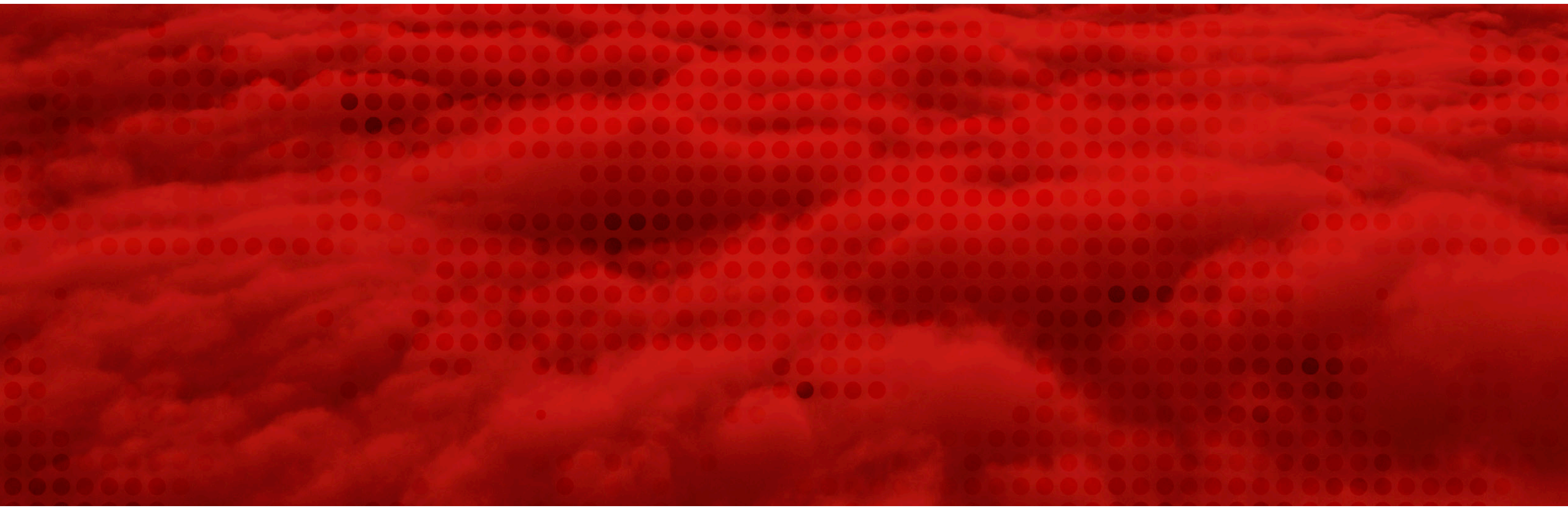
SOLUTION BRIEF

SECURING YOUR CLOUD TRANSFORMATION

MARRYING CLOUD FLEXIBILITY AND SCALABILITY WITH VISIBILITY, SECURITY, COMPLIANCE AND CONTROL



THE IRRESITIBLE APPEAL OF THE CLOUD

Judging by the numbers, organizations appear to have a nearly insatiable appetite for cloud services and infrastructure. According to IDC, total spending on IT infrastructure for public and private cloud environments topped $65 billion in 2018[1], while worldwide spending on public cloud services and infrastructure is forecast to reach $210 billion in 2019[2].

It's no wonder organizations continue to invest so heavily in cloud services: In many cases, cloud platforms and infrastructure represent the backbone of their digital strategies and transformation initiatives. Yet their hearty appetite for cloud services suggests that they must have an equally strong stomach for risk. After all, cloud services and platforms dish up as many risks as they do benefits (see Figure 1).

Figure 1: Cloud Risks and Benefits

RISKS	BENEFITS
Service outages and other availability and reliability issues	Confers agility via fast, easy deployments
Policy and regulatory compliance violations	Scales as workloads expand or contract
Data security, access and privacy issues	Offers budget flexibility (opex vs. capex)
Cloud provider financial viability	User-friendly for external customers and internal employees

Source: RSA

According to the 2018 Cost of Data Breach Study by the Ponemon Institute, factors that increase the cost of a data breach include: third party involvement, **extensive cloud migration,** compliance failure, and the extensive use of mobile platforms.

As organizations' cloud ecosystems grow, they often end up with "multi-cloud" environments (a mix of public, private and hybrid clouds) that require more efficient, risk-based governance than traditional IT governance models can provide. With the right amount of risk-intelligent governance—not so much that it inhibits an organization's speed or so little that it creates exposure—organizations can better position themselves to reap the full benefits of cloud computing.

A CLOSER LOOK AT CLOUD RISKS

Organizations face risks at all stages of their cloud transformations, whether they've adopted a cloud-first strategy, are dealing with shadow IT deployments, or they're being forced to move services formerly hosted in the cloud back on premises due to unexpected long-term costs.

The most challenging aspect of cloud adoption for security teams may be dealing with the complex technical architecture that stems from using a mix of traditional and cloud-based infrastructure. Equally challenging for security teams is the fact that cloud adoption eliminates the traditional network perimeter and increases an organization's attack surface, at the same time that it decreases their visibility into these environments. It also gives identity and security teams more points of access to manage, even as it creates "islands of identity"—multiple user stores containing identities associated with different cloud services that identity and access management teams have little control over. Meanwhile, most SaaS applications, including privileged accounts for SaaS and cloud infrastructure, are still protected only with passwords, making them highly vulnerable to account takeover and other credential-based attacks. Finally, as organizations' cloud adoption increases, security and IT teams have more vendors to vet and manage, and more controls to harmonize.

All of these issues point to the need to have a clear, cohesive strategy for managing risk and securing multi-cloud environments at all stages of your organization's journey. With more data flowing through cloud services and business processes increasingly relying on cloud platforms, security and risk management are paramount.

> “*Like many companies, we're adopting more and more **cloud-based systems,** and to prevent **cloud-based threats,** we need visibility into that infrastructure.*”
>
> Rich Sheridan
> **RC Willey**
> **Home Furnishings**

MANAGING CLOUD RISKS REQUIRES A UNIFIED APPROACH

Organizations can offload work to the cloud, but clearly, they can't offload all the risk. RSA can help your organization address these risks by providing advanced capabilities to:

- **Establish** a third-party governance program under which your organization can manage all third parties, including cloud service providers, assess the range of risks these providers create, and ensure they meet SLAs for latency, availability, resource optimization and other KPIs.
- **Implement** consistent processes for vetting cloud providers' security, privacy and compliance practices, and for assessing and mitigating the risks associated with bringing cloud-based data and services back in house.
- **Identify** where cloud security is disconnected from existing security capabilities or offers less mature levels of protection.

- **Implement** and manage proper access controls and governance for cloud services to mitigate risks.
- **Leverage** modern, risk-based multi-factor authentication to provide users with convenient, secure access to cloud-based resources.
- **Extend** full visibility into potential security and fraud threats across cloud environments.

Unlike other providers, RSA tackles multiple aspects of cloud security and risk, from authentication and access assurance to threat detection, response and third-party risk, with products you can deploy across cloud or on-premises infrastructures.

RSA NETWITNESS® PLATFORM

Extend threat visibility into any threat anywhere—on devices, on your company network, in the cloud and across virtual infrastructures—with our industry-leading SIEM platform. The RSA NetWitness Platform:

- Leverages a modular structure to conform easily to any cloud deployment requirement.
- Uses pre-built images to choose between running the solution in the cloud or collecting and enriching data in the cloud before transmitting it to an on-premises instance for analytics.
- Integrates with hundreds of security and application solutions, supporting the most diverse IT infrastructures wherever they're deployed.
- Speeds threat detection and investigation by enriching log, network and endpoint data at capture time with threat intelligence and business context, and automates and orchestrates responses with consistent, transparent and documented processes to reduce the risk of a breach.
- Uses a distributed architecture to keep pace with growing cloud traffic.

RSA SECURID® SUITE

Secure access to cloud-based and on-premises systems with modern, user-friendly, risk-based multi-factor authentication and automated identity governance controls. RSA SecurID Suite:

- Gives users timely access to the cloud-based applications they need from any device.
- Offers unified visibility and control across your application and resource landscapes, so the business can holistically manage users and access—thereby reducing blind spots and minimizing risk.
- Empowers employees, partners and contractors to do more without compromising security or convenience by supporting blended cloud and on-premises, bring-your-own-device, and mobile environments.
- Supports an identity assurance strategy that enables users' access to applications quickly and easily, without sacrificing your organization's security posture.
- Deploys "as a service" in the cloud or on-premises.

RSA ARCHER® SUITE

Manage multiple dimensions of cloud risk, including security, data privacy, compliance and resiliency, on a single industry-leading platform for integrated risk management. RSA Archer Suite:

- Allows you to catalog products and services delivered by cloud providers.
- Helps you monitor cloud providers for optimum performance.
- Facilitates the assessment of a broad range of risks related to working with cloud providers.

RSA® RISK & CYBERSECURITY PRACTICE

Assess your organization's ability to mitigate the risks associated with managing multi-cloud environments. As a part of this service offering, RSA will:

- Interview key business stakeholders to gain a nuanced understanding of your organization's strategic goals, objectives, risk appetite and existing risk posture.
- Administer the proprietary RSA Cyber Maturity Quantification tool to baseline risk maturity and readiness for multi-cloud transformation.
- Conduct a gap analysis and develop a customized roadmap designed to help your organization reach its desired level of cyber risk management maturity.

THE MAKING OF A MULTI-CLOUD STRATEGY

As business functions use cloud services and IT departments move toward cloud architectures, a well-defined, multi-cloud security and risk management strategy becomes essential to ensuring your organization can meet its business objectives. At a minimum, you should know which cloud providers are most critical to your business and what data resides on these platforms. You should also ensure you have visibility into these environments, along with risk-based controls for securing access to them.

The security threats to these environments are significant given the extent to which organizations rely on them. RSA can help you gain the flexibility and scalability of the cloud without compromising visibility, security, compliance or control.

DIGITAL RISK IS EVERYONE’S BUSINESS, HELPING YOU MANAGE IT IS OURS

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 protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

1. IDC, “Worldwide Quarterly Cloud IT Infrastructure Tracker,” https://www.idc.com/getdoc.jsp?containerId=prUS44670519 (January 10, 2019)
2. IDC, “Worldwide Semiannual Public Cloud Services Spending Guide” https://www.idc.com/getdoc.jsp?containerId=prUS44891519 (February 28, 2019)

RSA

4/19 Solution Brief H17623 W221628.