SECURANCE CONSULTING
Advantage of Insight AI

Insight in the Cloud

Realize Benefits and Reduce Risk with Cloud Security Assessments

www.securanceconsulting.com

INTRODUCTION

Cloud services offer businesses more agility, flexibility, and efficiency, but they do not eliminate risk or guarantee compliance. Ultimately, the responsibility for compliance and security rests with the business, even when the cloud service provider (CSP) offers protection. To safeguard data and reputations, organizations must continue to assess risk, compliance, and liability exposure as they expand into the cloud.

Cloud-based solutions are not inherently less secure than traditional solutions, but the complexity of service agreements and the relationship between internal and external systems can make assessing compliance and security in the cloud challenging. Despite the hurdles, businesses should reap the benefits of cloud services, including cost efficiency, reduced operating complexity, and new ways for employees to collaborate. These benefits are especially important to small and medium-sized businesses (SMBs), for which economies of scale are more difficult to achieve than for large, global enterprises.

This paper provides an overview of cloud services, discusses cloud-specific vulnerabilities, and offers insight on how businesses can assess and mitigate risk in the cloud.

OVERVIEW

As of 2019, 94 percent of businesses were operating in the cloud, whether public, private, or hybrid.[1] In 2020, cloud usage evolved, with 92 percent of enterprises using a multi-cloud strategy and 82 percent a hybrid cloud strategy.[2] Despite this enthusiasm to adopt cloud technologies, many businesses lack a mature cloud strategy or clear understanding of cloud vulnerabilities. Before discussing the unique security threats associated with cloud environments, it's necessary to differentiate between cloud deployment models and the services they offer.

Both the deployment model— public, private, hybrid, or community— and the type of services being delivered— Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as Service (SaaS)— will impact testing and analysis during a cloud security assessment. For instance, some CSPs limit intrusive testing, while others require customers to take full responsibility for security and testing.

Decision makers need to consider how risks and vulnerabilities are typically managed in each deployment model and what level of security providers offer. Even if a CSP takes responsibility for a portion of IT security, those guarantees must be verified before they are trusted. If the provider is attacked, and sensitive information is stolen, customers and regulatory agencies will hold the business, not the CSP, accountable.

> **61%** of businesses plan to optimize existing use of cloud services (i.e., cost savings)[2]

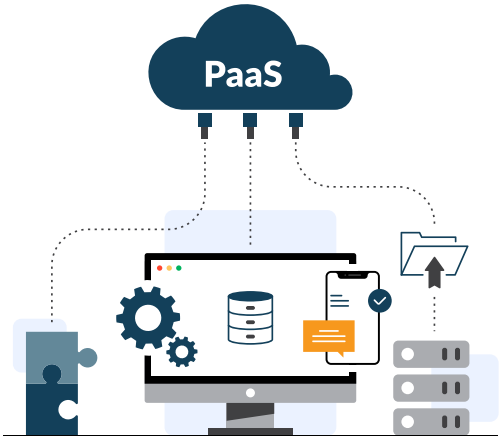
CLOUD SERVICES

Infrastructure as a Service (IaaS)

» Basic computing infrastructure, storage, and networking capabilities built on virtual machines
» Reduces IT administrative effort and hardware and maintenance costs
» Business controls operating systems, middleware, and applications
» CSP secures virtualization technology and physical hardware

Platform as a Service (PaaS)

» Environment and platform used by developers to develop and test software
» Reduces staffing and operating costs, allowing developers to focus solely on development, not maintenance
» Business must secure deployed applications and, in some cases, hosting environments
» CSP manages infrastructure



Software as a Service (SaaS)

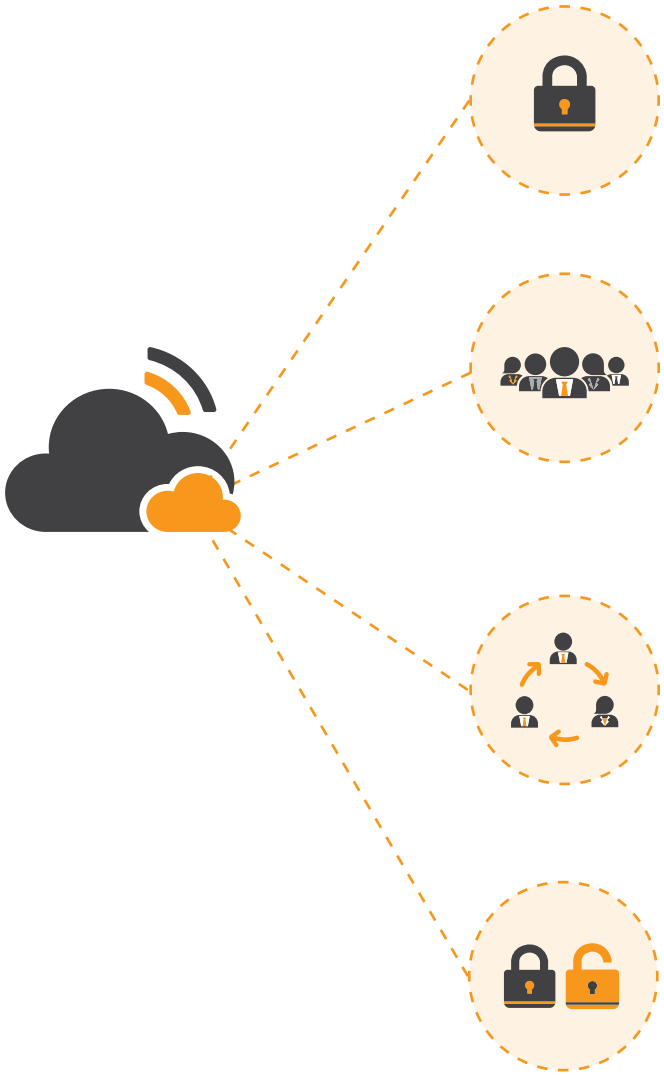
» Applications and software developed and deployed by the CSP and accessed through a thin-client interface
» Reduces complexity while expanding software offerings and availability
» Business has limited ability to control security
» CSP must secure applications and infrastructure

Who holds the responsibility for security in the cloud shifts depending on which services are adopted and which deployment model is used. Security for private clouds is managed internally by the organization. Public clouds and hybrid clouds incorporate extra-organizational components, distributing security responsibilities based on architecture and contractual agreements between the organization and the CSP.

Cloud solutions can increase risk because of variability among solutions and providers and the likelihood that individuals will move data to the cloud without IT approval. However, most SMBs already use cloud solutions and realize the competitive advantages, so delaying cloud adoption unnecessarily prioritizes security concerns over business benefits.

There is no compelling need to approach the cloud timidly or avoid it. Businesses can identify, analyze, and mitigate risks in the cloud to obtain the benefits of increased agility and efficiency, while safeguarding data, systems, and intellectual property.

Cloud Deployment Models



Private

- Internal
- Accessed by one organization
- Major capital and knowledge investment

Public

- External
- Network open for public use
- Cost-efficient
- Easily accessed by non-IT users

Community

- External
- Access is limited to organizations with similar computing needs
- Cost is distributed

Hybrid

- Combination of multiple clouds
- Access is private but bound to public resources
- Cost depends on design

BALANCING RISKS AND ADVANTAGES

New technologies are referred to as "disruptive" for a reason: they alter how people and organizations work, fundamentally transforming behaviors and processes. That degree of change and innovation comes with its own challenges, and many businesses hesitate to advance into the cloud, fearing the costs and consequences won't be worth it. Here we consider four challenges that stakeholders must weigh when they consider deploying cloud services.

Challenge #1: Doing Nothing

Most businesses are already operating in the cloud and realizing the benefits of cloud solutions— cost efficiency, increased collaboration (between employees, business units, and partners), reduced complexity, and enhanced agility. Clinging to traditional models for delivering IT services can feel safe, but it becomes a disadvantage as competitors become more agile. In actuality, pushing further into the cloud is beneficial for many businesses, especially SMBs that can access pay-as-you-go cloud solutions that would be too complex or expensive to deploy and manage on premise.

5 Business Advantages of Cloud Services

1. **Expanded collaboration between business units**
2. **Reduced operational complexity**
3. **Improved customer service**
4. **Lower operating costs**
5. **Increased flexibility and agility**

Challenge #2: Rogue End-Users and Shadow IT

Cloud services are readily accessible by businesses and individuals. Employees who rely on cloud services for personal use— like email, file sharing, and software solutions— are likely to seek the same level of flexibility and availability in the work environment. Businesses that reject or severely restrict cloud services inadvertently compel employees to find solutions independently, without going through proper IT channels. The use of these unmanaged shadow IT services heightens the risk of breaches and data loss and erodes compliance.

> **80%** of employees use non-approved SaaS applications at work.[3]

Challenge #3: Security Beyond the Perimeter

As discussed earlier, CSPs offer different levels of security, depending on the deployment model and the services provided. Large enterprises can deploy cost-efficient private clouds, but, for SMBs, private clouds may be too expensive, and finding experienced staff too difficult and costly.

SMBs gain more by utilizing public, hybrid, or community clouds, while carefully assessing and managing risk. Unfortunately, relying on self-reported security information from CSPs is inadequate. Organizations must thoroughly test all systems or demand comprehensive reports that adhere to industry standards if intrusive testing of CSP systems is prohibited.

Challenge #4: Compliance

Running afoul of regulatory compliance is a risk whether or not an organization embraces cloud services, but the cloud introduces unique regulatory challenges. In public clouds, resources are shared between many different organizations, and data could be stored anywhere in the world, which could force an organization to adhere to additional regulations in the host country.

These compliance issues do not mean that government agencies, healthcare providers, and financial institutions should avoid the cloud. At this point, the risk of not evolving is too great. Instead, organizations that face considerable regulatory constraints should seek qualified partners to develop and deploy solutions that enhance agility and maintain compliance.

Depending on where the CSP stores data, an organization may be subject to regulatory compliance in one or more foreign countries. Always verify where data will live and how that affects regulatory compliance before signing a contract with a CSP.

THE ADVANTAGE OF INSIGHT

Disruptive technologies transform operations, but the old adage that knowledge is power remains true. Security assessments deliver crucial knowledge about cyber defenses; this insight is essential to risk management and compliance.

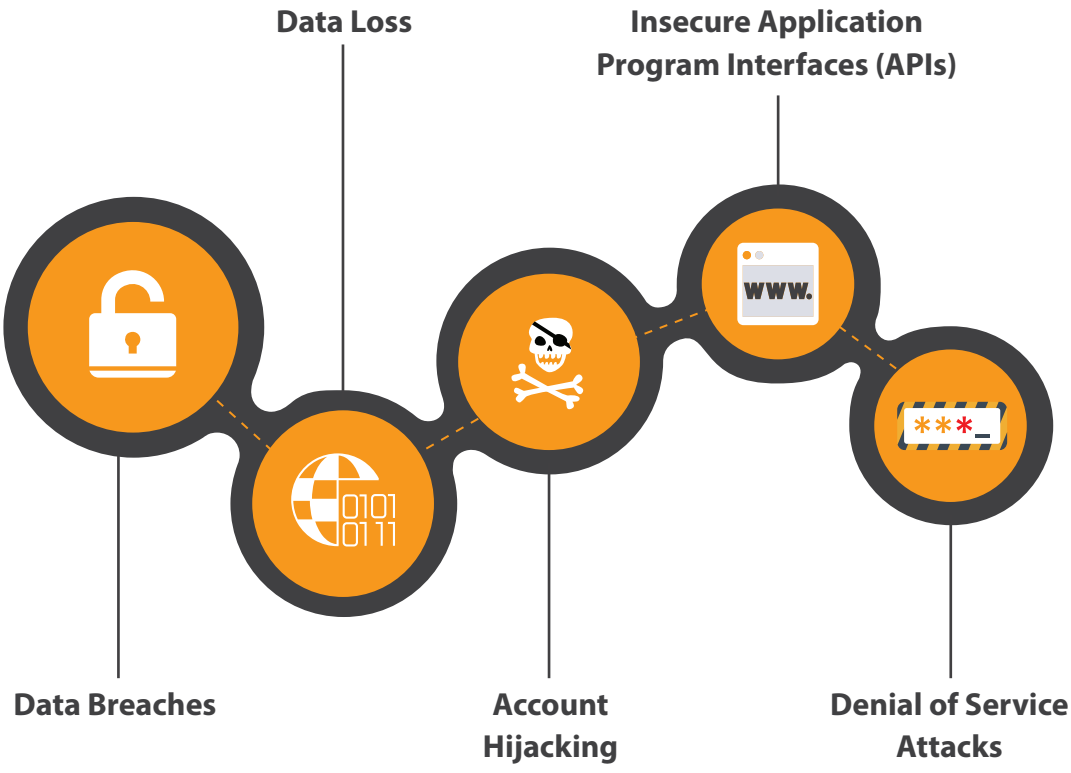
Technology evolves, but risks remain

More than 80 percent of security breaches can be prevented with regular security assessments and practical risk management.[5] Since cloud computing and traditional IT systems have many threats in common, businesses should inventory, classify, and analyze risks in the cloud as they would conventional infrastructure.

> **83%** of SMBs believe that the cloud helps businesses thrive, especially during COVID-19.[4]

In traditional IT environments, testing cyber defenses saves money and reputations by uncovering vulnerabilities before hackers exploit them. Thus far, data breaches have been less frequent in the cloud, creating a false sense of security. Moving forward, the cloud will attract more attention from hackers, who will shift their focus to follow the data. Organizations that proactively extend digital defenses and risk management to the cloud will be less appealing targets.

Top 5 Cloud Security Threats



CLOUD SECURITY METHODOLOGY

There are similarities between traditional IT and cloud security assessments, but the latter require specialized knowledge of vulnerabilities specific to cloud services. Beyond the technical aspects, cloud assessments are complicated by contractual agreements with CSPs. Organizations may be required to take full responsibility for testing and/or face strict limits on testing. Auditors have to analyze the organization's risk management objectives and regulatory requirements alongside restrictions in the provider's service level agreement (SLA).

When intrusive testing is prohibited, organizations should receive reports containing detailed information about the CSP's risk management and compliance controls. Those reports must be evaluated and integrated into risk management and compliance planning within the organization. If the SLA does not provide adequate protection, additional layers of security may be necessary to protect data and ensure business continuity.

> **93%** of organizations are moderately or extremely concerned about cloud security.[6]

Further complicating matters, many CSPs rely on contractual clauses that limit their liability, and an organization's damage claims, to a refund. In such cases, businesses face substantial costs in the wake of breaches, data losses, or service interruptions. Analyzing, and periodically reassessing, business continuity plans, disaster recovery strategies, and incident management should be an integral part of cloud deployments.

Cloud security assessments require experienced auditors and proven methodologies that factor in all of the technical and regulatory complexities of operating in the cloud. Organizations should look for partners that demonstrate an understanding of cloud services, how they integrate with traditional IT infrastructure, how to measure the impact of SLAs, and how CSP controls affect governance, risk, and compliance.

> **50%** of enterprises spend between $1.2 million and $2.4 million per year on cloud technologies.[2]

EXPERIENCED GUIDANCE

Cloud security assessments are complicated by the intricacies of service agreements, competing internal and external interests, geographical complexity, and the need to balance security risks with business benefits. Securance Consulting's cloud security assessment methodology aligns industry best practices, regulatory requirements, and the latest cloud computing standards to deliver customized solutions that support long-term security and risk management.

Contact Securance to discover how our consultants can help your organization evaluate cybersecurity and mitigate risks in the cloud.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf
2. https://info.flexera.com/CM-REPORT-State-of-the-Cloud
3. https://track.g2.com/resources/shadow-it-statistics
4. https://www.xaasjournal.com/the-smb-cloud-adoption-trend-has-a-silver-lining-for-msps/
5. https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/
6. https://www.isc2.org/resource-center/reports/2020-cloud-security-report

Insight in the Cloud
How Cloud Security Assessments Help Businesses Realize Benefits & Reduce Risk
© 2020 Securance LLC. All Rights Reserved.

SECURANCE CONSULTING
Advantage of Insight AI

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com