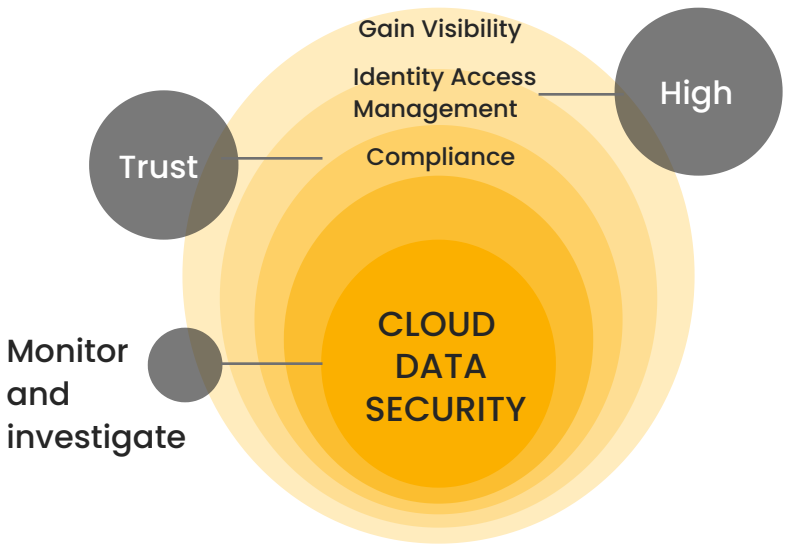
infosec Miners

Skillmine Technology • Consulting • Services

CLOUD SECURITY

INTRODUCTION

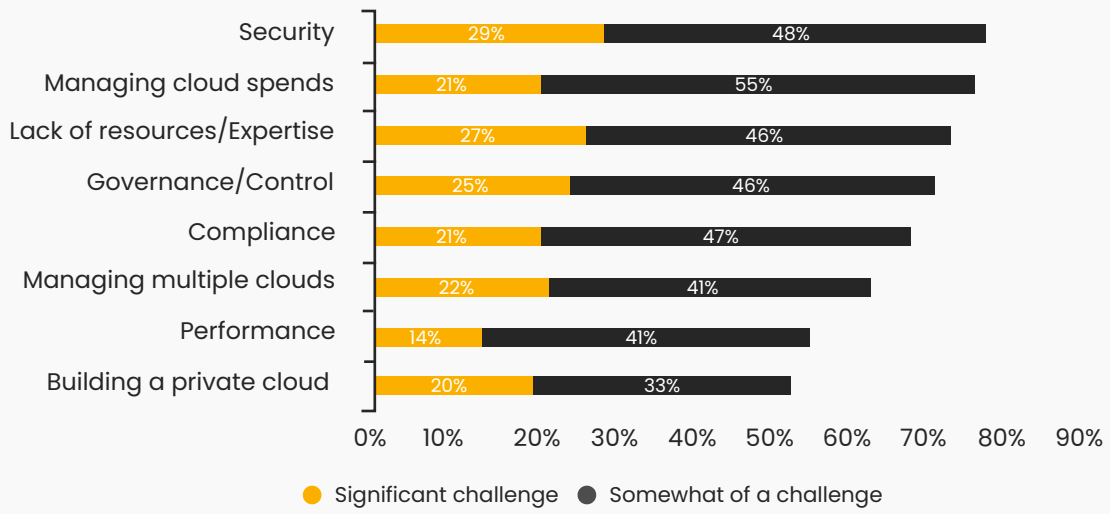
There are a number of cloud-based applications that we use every day, without even thinking about it; the email service, search engines, websites, even our bank application. While some might not categorize the security of their cloud application as important, we beg to differ, since we as users would like to have our personal information secured. For example, imagine an online fitness application that we can log in to in order to view our visits to the gym, our subscription details as well as our personal information like name, last name, and home address.



CLOUD SECURITY FEATURES

- Authentication
- Access Control
- Secondary Approval
- User Behaviour Analytics
- Logging & Reporting
- Data Recovery
- Asset & Data Classification
- Encryption
- Key Management
- Configuration Hardening
- Logical segmentation
- Boundary Enforcement

CLOUD CHALLENGES



Security and spend are the top challenges. Security is a challenge for 77 percent of respondents, while 29 percent see it as a significant challenge. Managing cloud spend is a challenge for 76 percent of respondents, while a smaller 21 percent see it as a significant challenge.

As companies become more experienced with cloud, the top challenge shifts. Security is the largest issue among cloud beginners, while cost becomes a bigger challenge for intermediate and advanced users.

5 MAIN CLOUD SECURITY THREATS

1. Data breach
2. Misconfiguration & inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access & key management
5. Account hijacking

POTENTIAL THREAT- DATA BREACH

What can cause data breaches?

- Targeted attack, Human error, Application vulnerabilities
- Lack of security practices and impact of Cloud
- Large attack surface due to shared resources
- Cloud providers frequent targets due to broad accessibility and a vast amount of data

Considerations and Mitigations

Principle of least privilege

- Cloud visibility to enable logging and monitoring
- Robust and well-tested incident response plan
- Protecting data via encryption
- Establishing policies and procedures for secure data removal and disposal.

POTENTIAL THREAT — MISCONFIGURATION & INADEQUATE CHANGE CONTROL

Impact of Cloud

- Misconfigured cloud servers, including:
- Publicly accessible cloud storage
- Unsecured cloud databases
- Improperly secured ‘rsync’ backups
- Open internet-connected network area storage

Considerations and Mitigations

- Ensuring external partners adhere to the change management, release and testing procedures used by internal developers
- Conducting risk assessments at planned intervals
- Performing security awareness training with contractors, third-party users and employees

POTENTIAL THREAT — LACK OF CLOUD SECURITY ARCHITECTURE AND STRATEGY

Factors contributing to threat

- Secure cloud architecture requires new capabilities and new tools
- Organizations have a learning curve when it comes to adopting cloud

Impact of Cloud

- Need for a new shared security model in a hybrid cloud environment
- Finding the right balance between innovation and control
- Lack of reference architecture and documentation

Considerations and Mitigations

- Ensure security architecture aligns with business goals and objectives
- Develop and implement a security architecture framework
- Ensure the threat model is up to date.
- Deploy continuous monitoring capability.

POTENTIAL THREAT — INSUFFICIENT IDENTITY, CREDENTIAL, ACCESS, & KEY MGMT

What is the threat?

Unauthorized access to sensitive resources due to a lack of protection via IAM. Security incidents occur due to:

- Inadequate protection of credentials
- Lack of regular automated rotation of cryptographic keys, passwords, & certificates
- Lack of scalable identity access management systems
- Failure to use multi-factor authentication and strong passwords

Impact of Cloud

With stolen keys or credentials, attackers can:

- Read, exfiltrate, modify and delete data
- The issue control plane and management functions
- Snoop on data in transit
- Release malicious software that appears to originate from a legitimate source

Considerations and Mitigations

- Cloud access keys (e.g., AWS access keys, Google Cloud keys and Azure keys) must be rotated and centrally managed, while unused credentials or access privileges are removed.
- Don’t embed keys directly into code
- Configure multi-factor authentication for most sensitive operations

POTENTIAL THREAT — ACCOUNT HIJACKING

Factors contributing to threat

Malicious attackers gain access to and abuse accounts that are highly privileged or sensitive.
Leaves systems vulnerable as a lack of:

- Identity and Access Management (IAM)
- Logging, monitoring, and alerting at the account level
- Defence in depth
- Protections against phishing, exploitation, and stolen credentials

Impact of Cloud

- Data and applications reside in cloud services, which reside in a cloud account or subscription
- Impact in cloud environment includes data/asset loss and compromised operations
- Potential elimination of organization assets, data, and capabilities

Considerations and Mitigations

- A robust method of authentication for cloud application users, including single sign-on and multi-factor
- Divide administrative duties between multiple IAM accounts with distinct credentials: E.g., an account that can create backups can't delete backups
- Restrict I.P. addresses allowed to access cloud applications

INSIDER THREAT & ITS PERCENTAGE OF RISKS

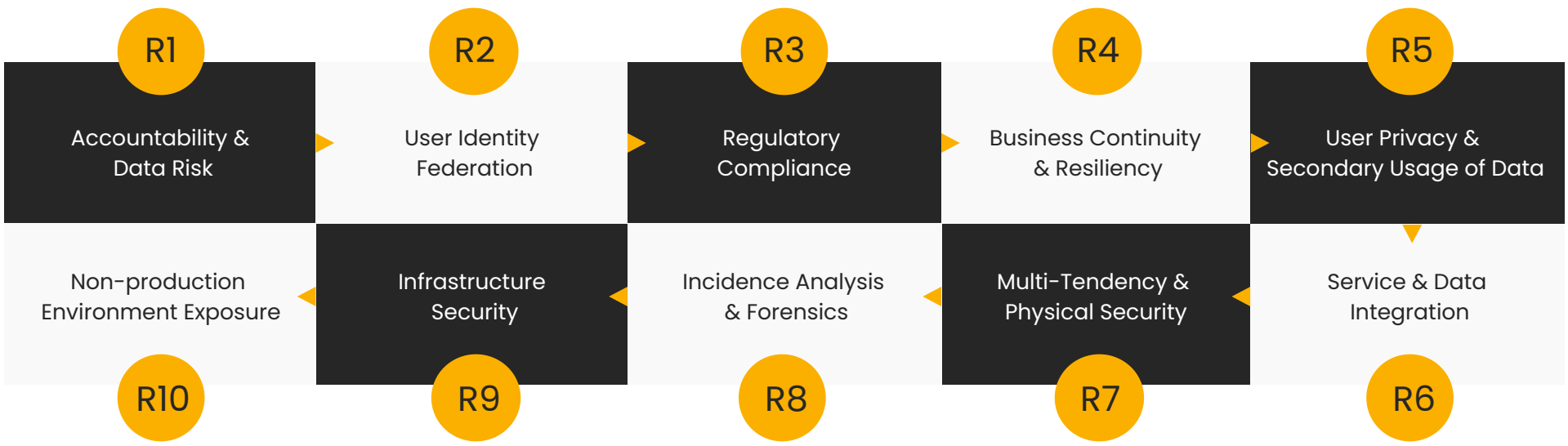
94% Experience at least one insider threat per month

92% Have cloud credential for sale on the dark web

80% Experience at least one compromised account threat

59% Experience at least one privileged user threat

OWASP CLOUD TOP 10 RISKS



> With cloud technologies maturing at rapid seeds, many cloud gurus have concluded that, when properly planned and strategized, the cloud can be more secure than an internal, on-premise data centre.

SKILLMINE CYBER SECURITY TEAM

Skillmine Technology • Consulting • Services
India | KSA | UK | USA

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

Follow us on