



2024 SINGAPORE A.I. & CLOUD SECURITY READINESS REPORT

Published by:

Spark

In Partnership with:

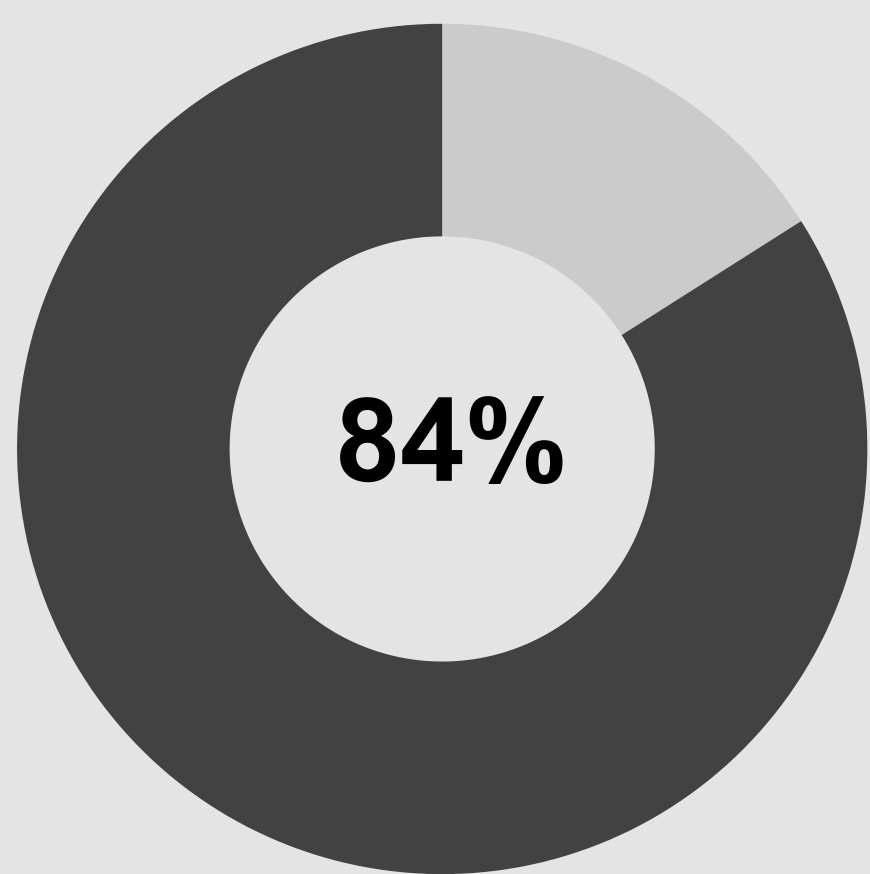
 **paloalto**
NETWORKS

 **TRUVISOR**

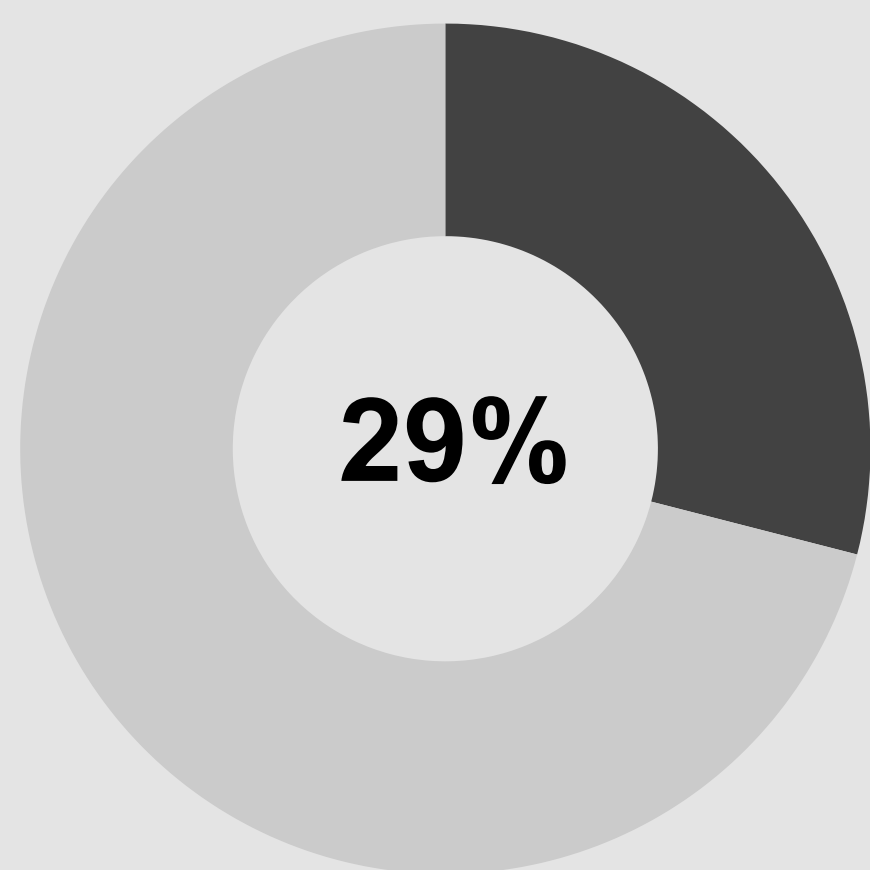
© Copyright 2024 by SPARK (CIO Academy Pte. Ltd.) All Rights Reserved.

www.wahspark.com

OVERVIEW



84%¹ of businesses in Asia plan a full cloud migration by 2024.



Only 29% of respondents cite adequate resilience to protect critical cloud workloads

The **A.I. & Cloud Security Readiness Report** underscores the critical juncture at which organisations find themselves in the evolving landscape of cloud security and AI integration. As organizations continue to migrate and refactor legacy systems to cloud infrastructures, they face a dual challenge: accelerating innovation while managing escalating security risks associated with AI and cloud environments.

Firstly, the report highlights the transformative impact of Generative AI in software development, significantly reducing development times and introducing AI-driven vulnerabilities. Organizations must prioritize the hardening of IT systems against these vulnerabilities as a foundational security practice. The rapid adoption of AI tools in the DevOps pipeline, while beneficial, necessitates a robust framework for AI governance and a collaborative approach between AI and cybersecurity teams to mitigate risks effectively.

Secondly, the data reveals a concerning trend with only a small fraction of organizations having fully migrated to the cloud, indicating a long runway ahead for cloud adoption and security enhancements. This transition period is critical for implementing stringent security measures, particularly around data encryption, continuous monitoring, and the adoption of a unified security operations centre to address threats across diverse cloud environments.

Moreover, the report identifies the top risks associated with AI in cloud environments, including data loss from targeted attacks and misconfigurations due to automated AI deployments. Addressing these risks requires a proactive and comprehensive cloud security strategy that includes regular updates to cloud governance policies and a strong emphasis on incident response capabilities.

In essence, as the battleground for future cyber-warfare increasingly shifts to the cloud, organizations must adopt a forward-thinking approach to cloud security. This involves not only enhancing their defensive capabilities but also continuously adapting to the rapidly changing threat landscape to safeguard their digital assets effectively.

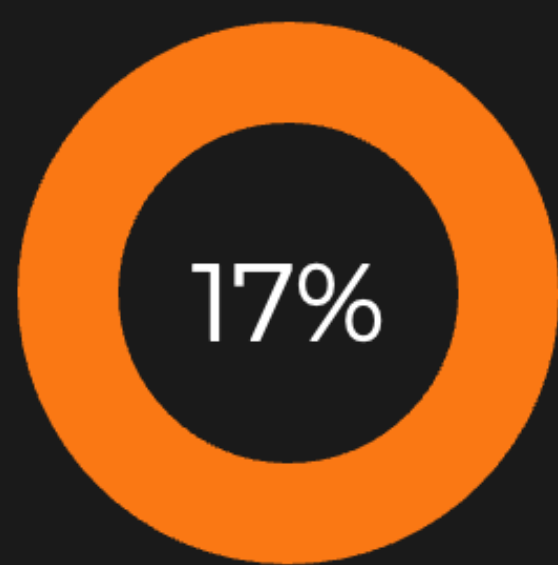
¹ Source: "The Next-Generation Cloud Strategy in Asia", NielsenIQ, 2023



CLOUD IS A A ONE-WAY JOURNEY

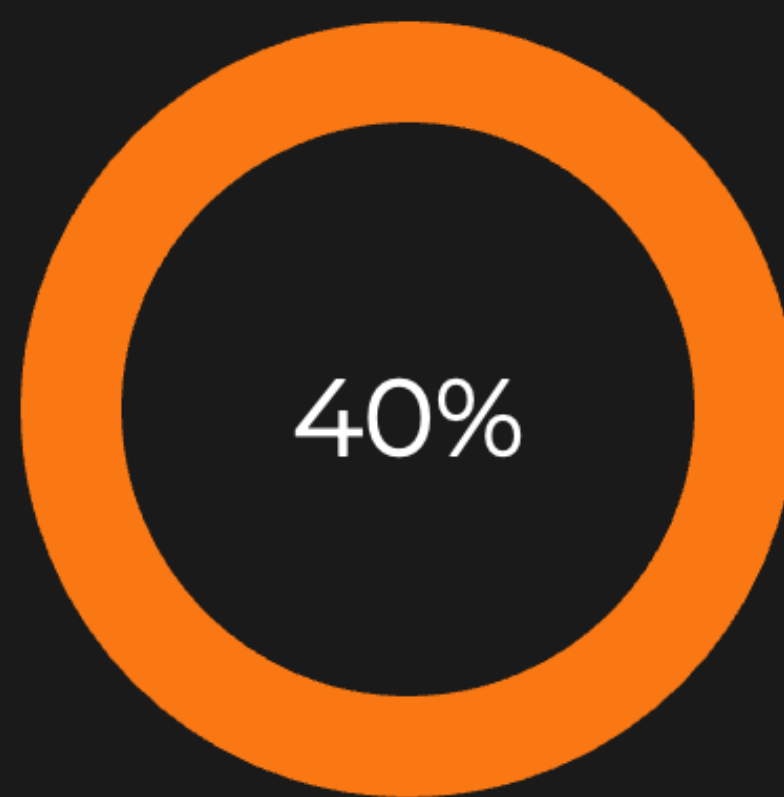
Organisations are migrating legacy IT systems into the Cloud

Survey Question: At which stage is your organisation at, in modernising legacy IT systems into cloud-ready workloads?



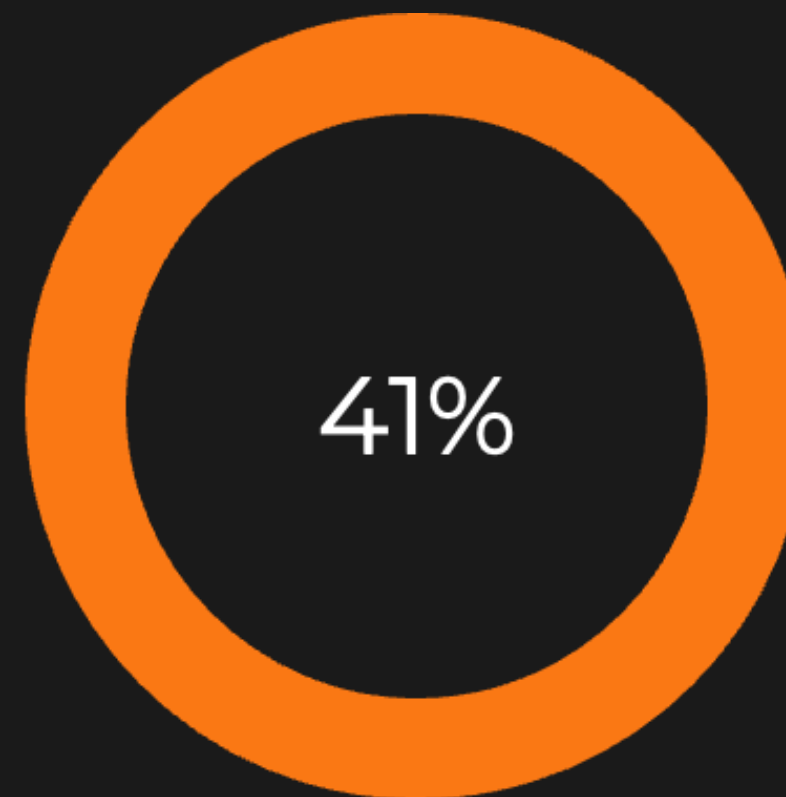
Exploring Options

Early stages of exploring cloud workload integration.



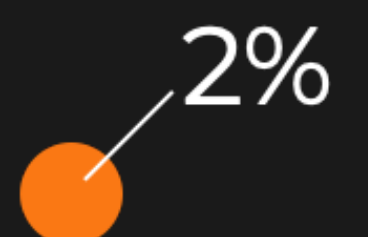
In Transition

Actively transitioning workloads to the cloud.



Advanced Integration

Most workloads are integrated, with ongoing optimisation.



Complete Migration

Moved fully into the Cloud

Organisations have started refactoring legacy applications to be compatible with the cloud and eventually, migrate completely to cloud infrastructure. While a big part of the cloud footprint will be managed as a private cloud, Nielsen predicts 27% of applications and data will be deployed into public cloud, while a good 24% of apps will be supported by a flavour of hybrid-cloud architecture. This transition away from on-premise data centres still has some runway left, considering only 2% of organisations have reported to have migrated fully into the Cloud. The complexities introduced by such heterogeneous environments, add operational and cyber-risks to the mission-critical business applications that run on today's modern IT infrastructure.

CLOUD HAS CREATED

43%

of organisations in Singapore have identified critical workloads to be migrated to Cloud

Yet Only

29%

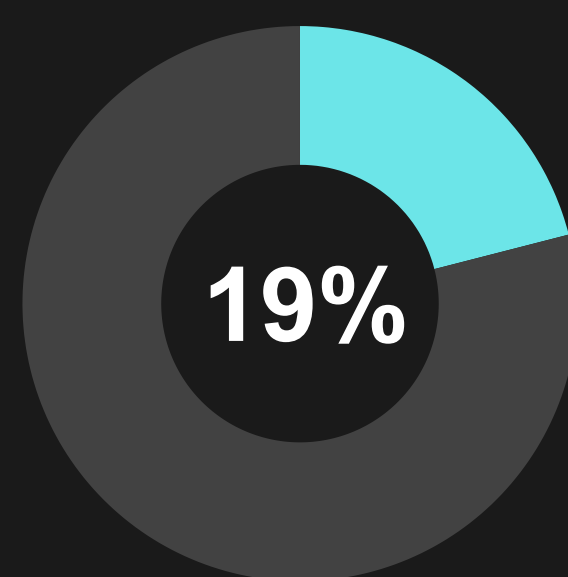
of said organisations have strengthened resilience & put in place reliability processes and toolkits to support critical cloud workloads

A BIG RISK GAP

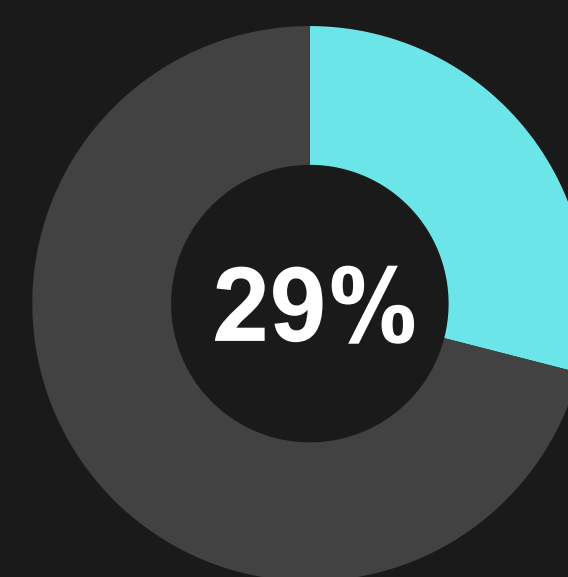
A.I. WIDENS THE CYBER-RISK GAP ON CLOUD

Generative A.I. has changed the game for developing and deploying new apps on the Cloud. From code generation to security testing and code optimisation, Gen A.I. has broken the speed-to-market barrier on an exponential scale, reducing development time by up to 55% per task². The rapid pace of A.I. tools across the DevOps pipeline, also introduces A.I. related vulnerabilities into modern-day software development processes. **Hardening IT systems against new techniques targeting A.I. tools in the software development lifecycle will become a foundational practice.**

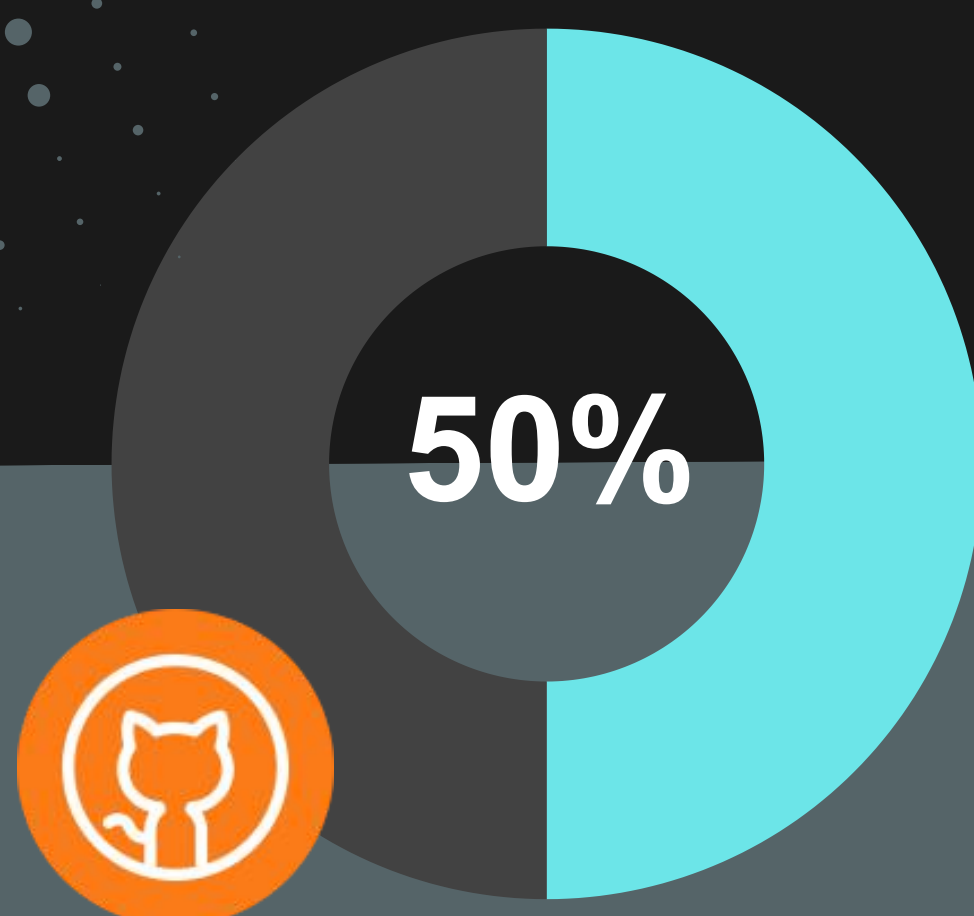
² Source: Github, 2022



**Requirements
Gathering**

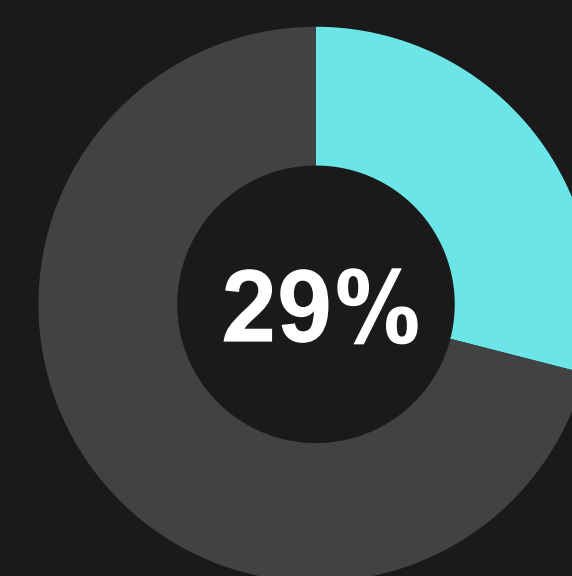


**Design and
Architecture**

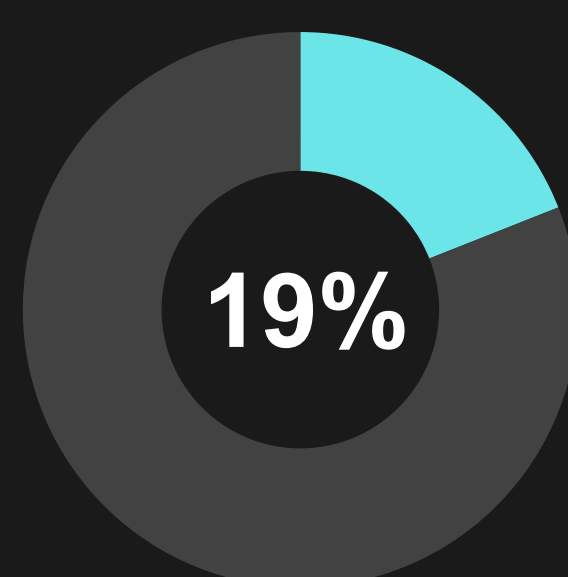


Coding & Implementation see the most A.I. being used in the Software Development & Deployment Cycle

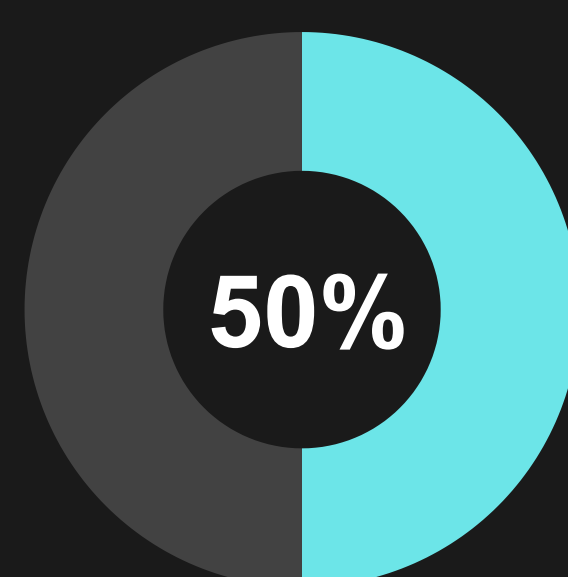
Survey Question: In which areas of software development and deployment has your organisation adopted devops practices in the Cloud?



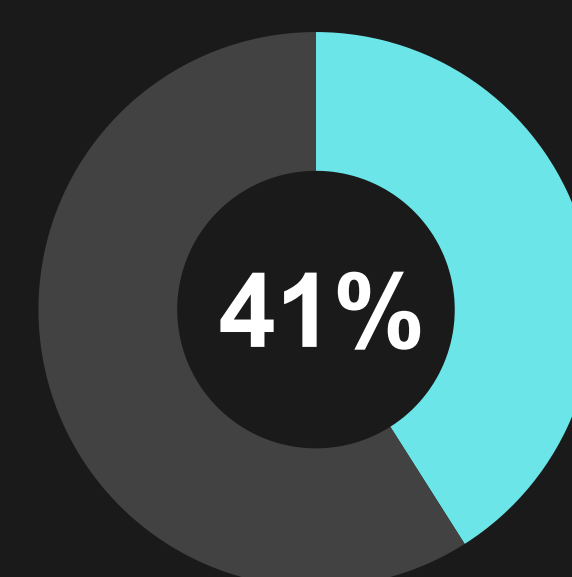
**Testing
& QA**



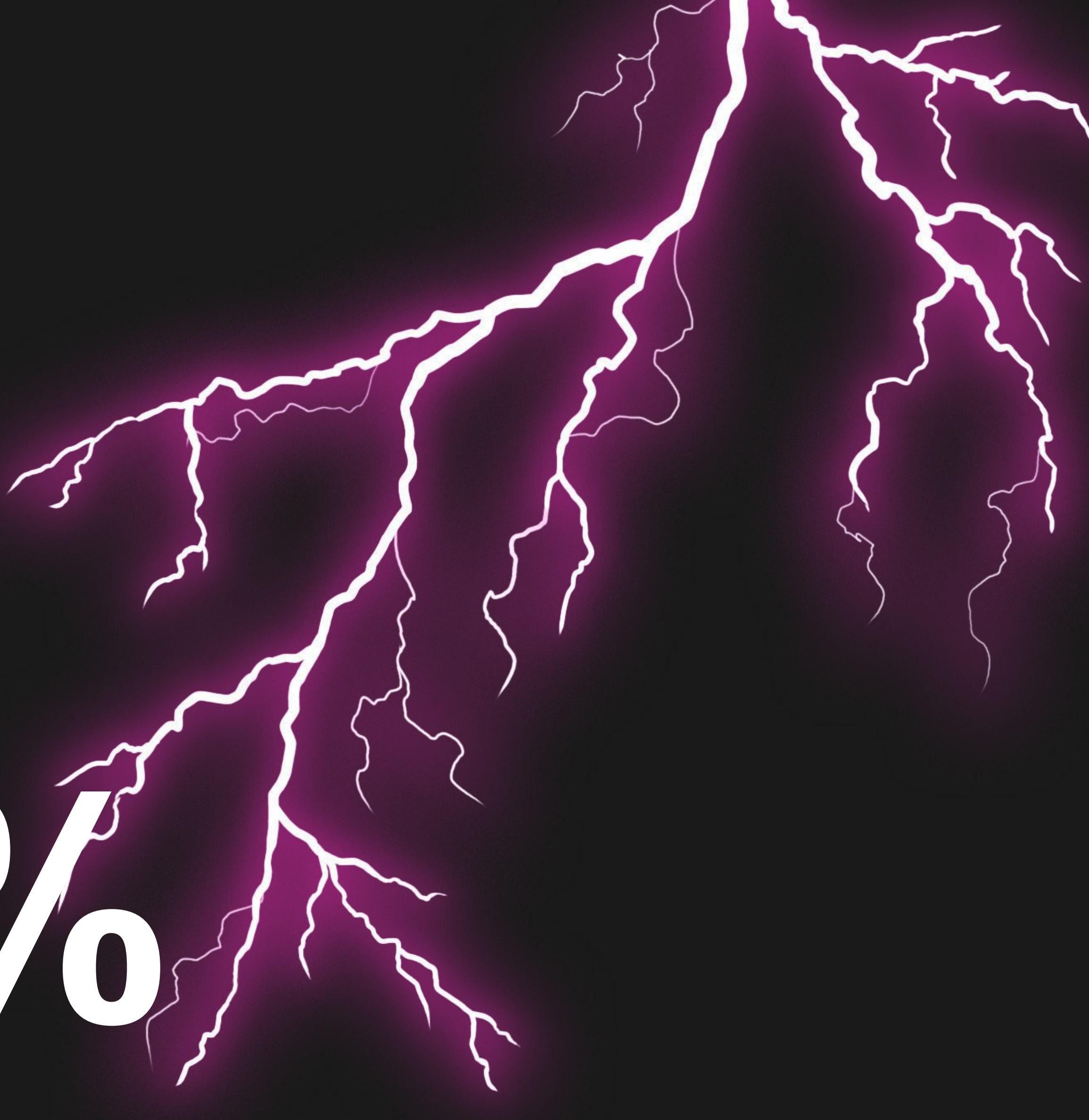
**Site Reliability
Engineering**



**Observability,
Monitoring &
Incident Response**



**CI/CD
Pipeline**

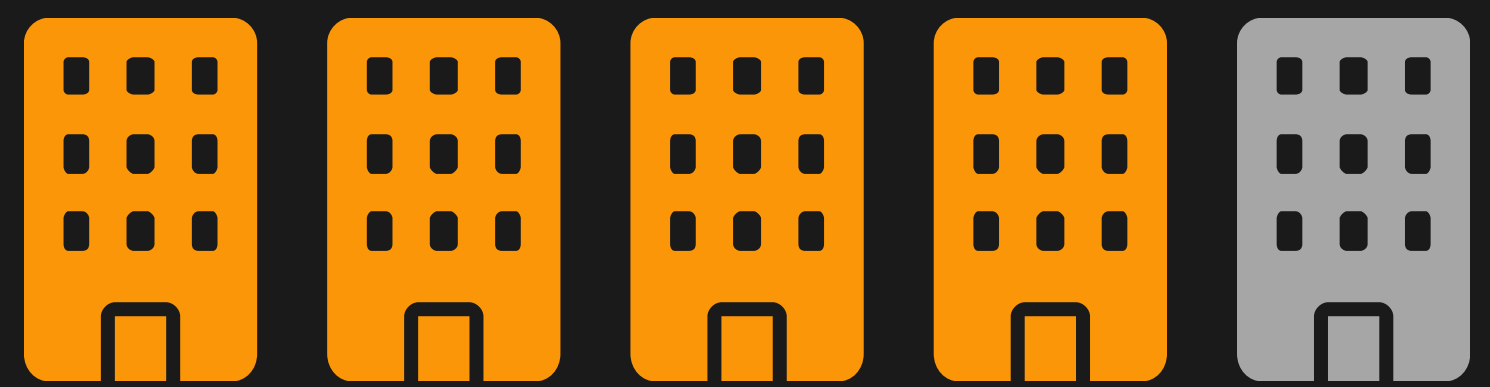


76%

Indicated Enhancing Data Security and Privacy in Production as the Most Urgent IT Priority toward building A.I. Readiness in Software Development.

When asked what is the most urgent IT priority to build readiness for implementing A.I. capabilities into software development and development processes, three-quarters of respondents highlighted data security and privacy in production as their top priority. This is followed by 50% paying attention to implementing an A.I. governance framework, and trailing in third place, 42% emphasised fostering collaboration between A.I. and cybersecurity teams. 40% of respondents were also concerned about improving compliance readiness with new or upcoming regulatory standards.

Increasing cloud capacity for A.I. only saw a modest 21% response, while 28% indicated urgency in implementing automation in their existing DevOps process. Immediately, we observe a stark contrast and urgency for organisations to tighten governance and strengthen data protection capabilities in today's A.I. age.



4 out of 5 surveyed are most concerned about the risk of data loss as a result of the use of AI in software development and in cloud.

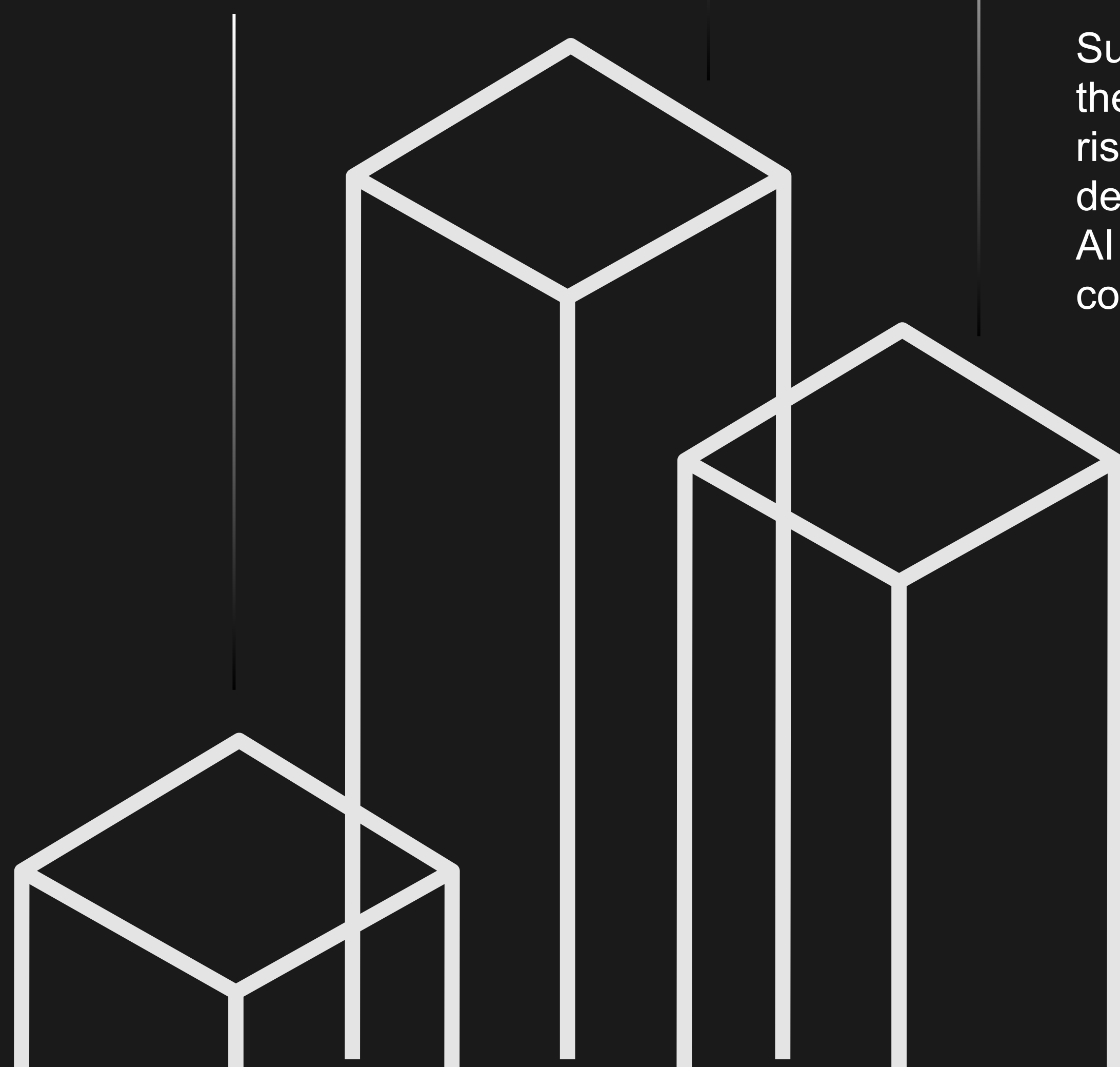
78%
BIGGEST RISK

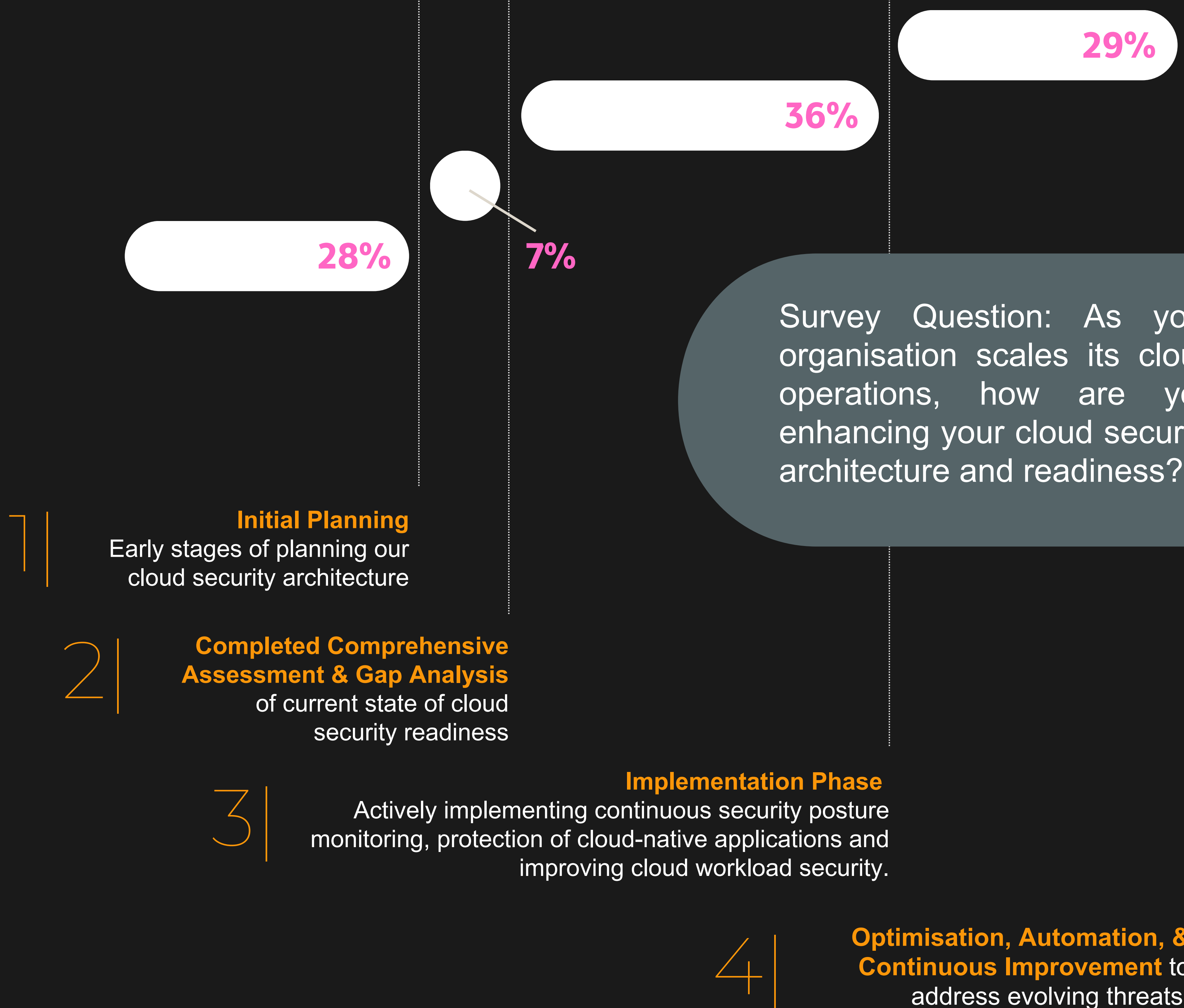
Data loss from targeted attacks on A.I. processes

45%
3RD BIGGEST RISK
Injection of malicious code into open-source code repositories or private company code repositories

72%
2ND BIGGEST RISK
Misconfiguration of cloud services due to automated AI deployments

Survey Question: What are the biggest data and cyber risks related to AI in software development and the use of AI in cloud environments that concern you the most?





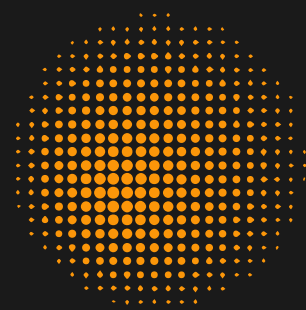
50%

of organisations surveyed have **taken proactive steps** to transition toward a **Cloud-native security architecture**.

For organisations to be fully prepared to secure their cloud estates, our survey segments readiness into 4 stages - planning, gap analysis, implementation and continuous improvement. Our findings point toward a high degree of readiness among organisations in Singapore, with almost a third of organisations continuously improving their cloud security processes and toolkits to deal with the evolving threat landscape.

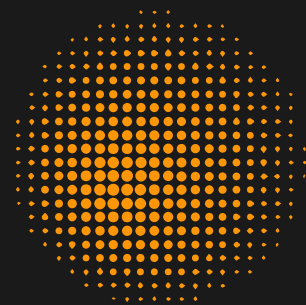
TOP 5 MUST-DOS

FOR A SUCCESSFUL CLOUD SECURITY STRATEGY



52%

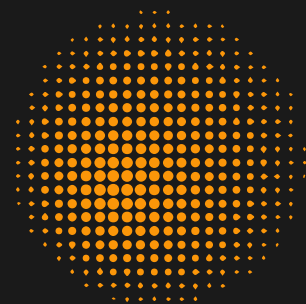
**Build continuous monitoring across
all active cloud estates**



43%

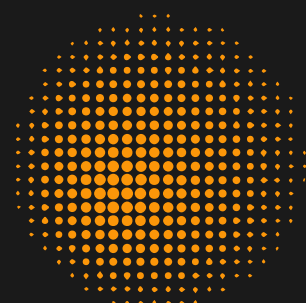
Update policies specific to cloud governance

(e.g. IAM/PAM, network segmentation, audit logging, data
classification, etc.)



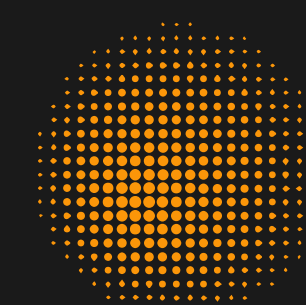
52%

**Improve data encryption and data loss prevention to
safeguard sensitive information on Cloud**



47%

**Adopt a unified, centralised security operations
providing threat detection and remediation across
SaaS/IaaS and multi-cloud operations.**



36%

**Hire cloud-security certified
talent into the security team**





CONCLUSION

In the rapidly evolving digital age, the intersection of A.I. and cloud security is emerging as the new frontier in the battle against cyber threats. As we stand on the brink of 2024, it's becoming increasingly clear that AI is not just an auxiliary tool in cybersecurity; it is transforming into the very battleground upon which the future of digital security will be contested. This pivotal shift heralds a new era where the mastery of AI-driven security strategies becomes critical for organisations to retain their edge against an ever more sophisticated and faceless adversary.

The stakes in this AI-driven battleground are monumental. Traditional security tools, once the stalwarts of digital defence, are finding themselves outpaced by the sheer velocity and complexity of AI-powered threats. The challenge now lies in leveraging AI not merely as a reactive force but as a proactive shield that can predict, detect, and neutralise threats in real-time. This requires a paradigm shift in how we approach cloud security, moving from a posture of defence to one of proactive resilience.

With A.I. evolving at such breakneck speed, meaningful information sharing and joint exercises across industry ecosystems and the development of new standards for AI security will be crucial. As we stand at this crossroads, the path forward is clear: embracing AI as the cornerstone of cloud security strategies will be paramount.

GET IN TOUCH

For General Enquiries
contactus@wahspark.com

Visit us at www.wahspark.com

GOH JING RUI
Research Specialist
SPARK
jingrui@wahspark.com

Gladys Kan
Partnership Manager
SPARK
gladys@wahspark.com

Sara Ramli
Community Manager
SPARK
sara@wahspark.com