CHECK POINT™

in collaboration with

AFRICA – CLOUD SECURITY READINESS REPORT

INTRODUCTION

To better understand the evolving dynamics of cloud security, CXO Priorities, in collaboration with Check Point, conducted an insightful survey in Africa. Our survey engaged 80 security and IT decision-makers from key African markets, including South Africa, Kenya, Nigeria and Morocco. These countries, representing diverse economic landscapes, provided a comprehensive view of the regional cloud security posture.

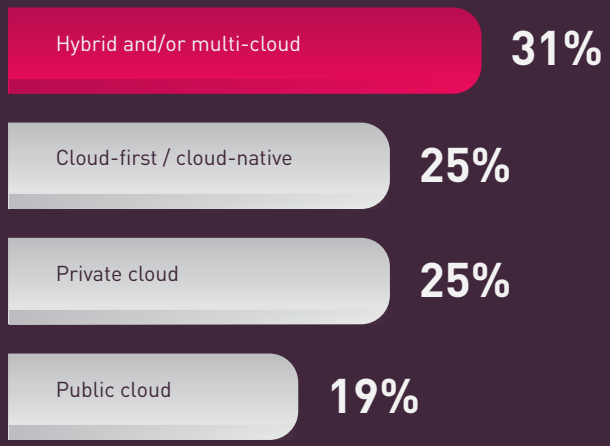
The survey delved into several critical areas: the current state of cloud environments, challenges faced in cloud adoption, strategies for managing cloud security and the division of security responsibilities with service providers. Additionally, it explored the emerging threats in cloud security and the role of Artificial Intelligence in threat detection within cloud infrastructures.

The findings from these respondents offer a nuanced understanding of the complexities and priorities in securing cloud environments across Africa. By examining their insights, we aim to highlight the key trends, challenges and innovative solutions shaping cloud security. This survey not only illuminates the regional context but also provides valuable lessons applicable to the global cybersecurity community. Through these insights, we can better equip organisations to navigate the rapidly changing cloud security landscape and address the sophisticated threats they face.

KEY FINDINGS

- Nearly a third (**31%**) of respondents describe their cloud environment as hybrid and/or multi-cloud
- Cost management and budget constraints (**25%**) is the biggest challenge when considering cloud adoption
- Data loss or leakage (**25%**) and compliance drift (**25%**) are the most critical issues organisations face when managing cloud security
- Continuous monitoring and assessment of cloud security posture (**26%**) was cited as the main cause when addressing the division of cloud security responsibilities with service providers
- Continuous monitoring and analysis of security metrics (**24%**) and incident response simulations (**24%**) were stated as the methodologies used when assessing the robustness of cloud security against emerging threats
- User behaviour analytics and pattern recognition (**33%**) was stated as the main reason AI is contributing to security monitoring and threat detection in cloud infrastructure

1. WHAT WOULD BEST DESCRIBE YOUR CLOUD ENVIRONMENT?

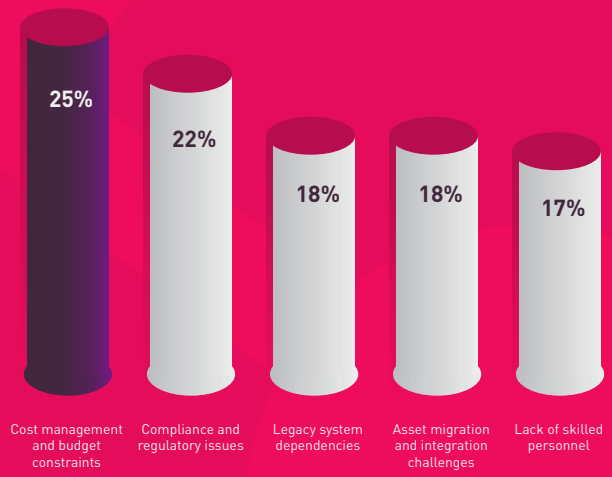


KEY INSIGHTS

The survey results highlight a significant trend toward diverse and flexible cloud strategies. The predominance of hybrid and multi-cloud environments (31%) reflects organisations' need for agility, optimising workloads across various platforms to mitigate risks and enhance resilience. The nearly equal split between cloud-first/cloud-native (25%) and private cloud (25%) indicates a strategic balance between leveraging cutting-edge, scalable solutions and maintaining control over sensitive data. Public cloud adoption (19%), though lower, underscores a cautious approach, likely driven by security concerns and regulatory compliance. These trends illustrate an evolving landscape where businesses prioritise a tailored approach to cloud adoption, balancing innovation with security and control.

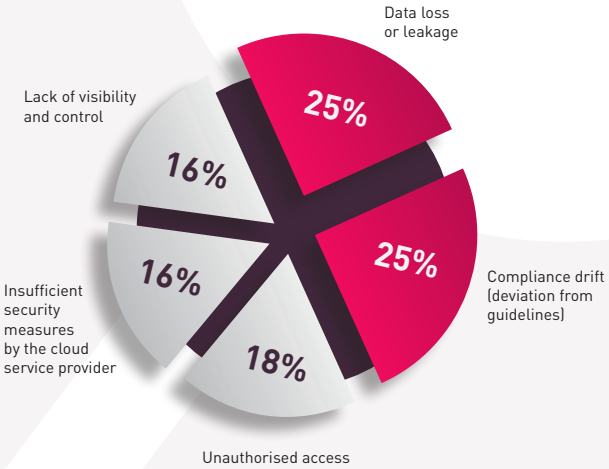
KEY INSIGHTS

Cost management and budget constraints (25%) indicate a growing concern over the financial sustainability of cloud solutions amidst increasing complexity. Compliance and regulatory issues (22%) underscore the pressing need for robust governance frameworks, especially as data protection laws tighten globally. Legacy system dependencies (18%) and asset migration and integration challenges (18%) reflect the significant technical debt organisations face, hindering seamless transitions to cloud environments. The lack of skilled personnel (17%) points to a talent shortage, stressing the urgency for enhanced cybersecurity education and training. These issues underscore the multifaceted hurdles in achieving secure and efficient cloud integration.



2. CONSIDERING YOUR CURRENT CLOUD ADOPTION, WHAT CHALLENGES DOES YOUR ORGANISATION FIND MOST DAUNTING?

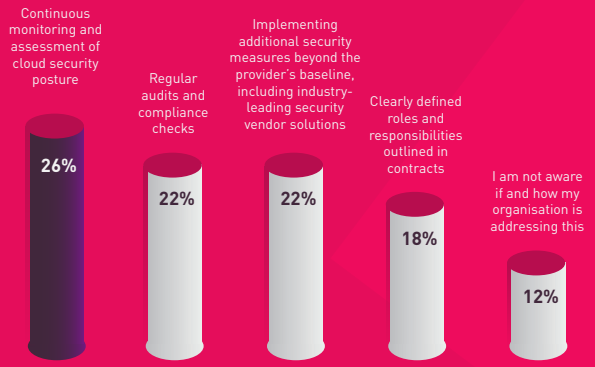
3. WHAT ARE THE CRITICAL ISSUES YOU FACE IN MANAGING CLOUD SECURITY WITHIN YOUR ORGANISATION?



KEY INSIGHTS

Data loss or leakage (25%) and compliance drift (25%) are paramount, indicating an acute need for robust data protection strategies and stringent adherence to evolving regulatory standards. Unauthorised access (18%) highlights the persistent threat of breaches, necessitating stronger identity and access management protocols. Concerns over insufficient security measures by cloud service providers (16%) reveal gaps in trust and collaboration, prompting a call for enhanced provider-client security frameworks. Finally, lack of visibility and control (16%) underscores the complexity of managing dispersed cloud environments, emphasising the demand for comprehensive monitoring and governance solutions. These issues collectively underscore the critical need for a holistic, proactive approach to cloud security.

4. CAN YOU DESCRIBE HOW YOUR ORGANISATION ADDRESSES THE DIVISION OF CLOUD SECURITY RESPONSIBILITIES WITH SERVICE PROVIDERS?



KEY INSIGHTS

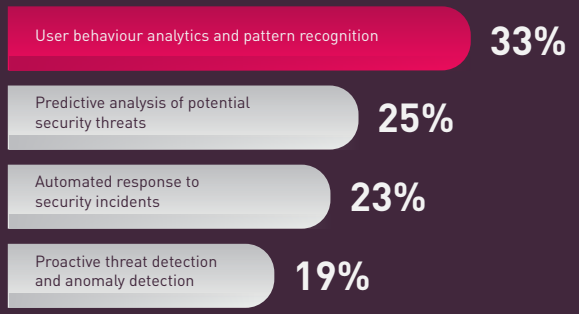
Continuous monitoring and assessment (26%) and regular audits and compliance checks (22%) reflect a proactive approach, crucial for maintaining robust security postures amidst evolving threats. Implementing additional security measures (22%) beyond the provider's baseline indicates a strategic emphasis on layered defences, leveraging advanced security vendor solutions. Clearly defined roles and responsibilities in contracts (18%) underscore the importance of clarity and accountability in mitigating risks. The 12% unaware of organisational practices suggests a critical gap in communication and training, emphasising the need for comprehensive awareness programmes. These insights underline the necessity for a multi-faceted, informed strategy in cloud security governance.

KEY INSIGHTS

Continuous monitoring and analysis of security metrics (24%) and incident response simulations (24%) suggest a dynamic and proactive stance, essential for identifying and mitigating threats in real-time. Regular threat intelligence updates and analysis (21%) underscore the importance of staying ahead of adversaries by integrating the latest threat data into security strategies. Penetration testing and red team exercises (20%) reflect a commitment to rigorously testing defences against sophisticated attack vectors. However, the 11% unaware of their organisation's practices indicates a significant communication gap, stressing the need for enhanced internal transparency and education. These practices collectively underline a comprehensive, adaptive approach to cloud security, vital in an increasingly complex threat landscape.

5. WHAT METHODOLOGIES DOES YOUR ORGANISATION USE TO ASSESS THE ROBUSTNESS OF YOUR CLOUD SECURITY AGAINST NEW AND EMERGING THREATS?

6. HOW DOES ARTIFICIAL INTELLIGENCE CONTRIBUTE TO ENHANCING SECURITY MONITORING AND THREAT DETECTION IN YOUR CLOUD INFRASTRUCTURE?



KEY INSIGHTS

The survey highlights AI's transformative role in cloud security, illustrating a broader trend towards intelligent, adaptive defences. User behaviour analytics and pattern recognition (33%) enable precise identification of anomalous activities, enhancing insider threat detection. Predictive analysis of potential security threats (25%) reflects AI's capability to foresee and mitigate risks before they materialise, shifting from reactive to proactive security postures. Automated response to security incidents (23%) indicates the growing reliance on AI to swiftly neutralise threats, reducing response times and limiting damage. Proactive threat detection and anomaly detection (19%) underscore AI's efficacy in maintaining vigilance over vast cloud environments, ensuring continuous protection. These AI-driven methodologies highlight the critical evolution towards smarter, more resilient security frameworks.

CONCLUSION

Check Point AI-powered cloud security solution has been helping us in securing our critical applications, protecting them from the ever-evolving security threats without having to worry about signatures.

– Dialungana Malungo, Principal Cybersecurity Specialist, Unitel

The cloud security landscape is evolving, with nearly a third of respondents adopting hybrid and multi-cloud environments. This trend underscores the need for agility and resilience in managing diverse cloud infrastructures. Despite this, cost management and budget constraints remain the primary challenge in cloud adoption, highlighting the need for cost-effective yet robust security solutions.

Managing cloud security presents significant issues, with data loss or leakage and compliance drift identified as critical concerns. These challenges necessitate stringent data protection strategies and adherence to regulatory standards to maintain a secure cloud environment. Addressing the division of cloud security responsibilities with service providers, continuous monitoring and assessment of cloud security posture emerged as the main strategy, ensuring that both parties maintain a proactive security stance.

To assess the robustness of cloud security against emerging threats, organisations rely on continuous monitoring and analysis of security metrics and incident response simulations. These methodologies highlight the industry's shift towards proactive security measures, essential for identifying and mitigating threats in real-time. Additionally, user behaviour analytics and pattern recognition were identified as key contributions of AI to security monitoring and threat detection in cloud infrastructure, showcasing the transformative potential of AI in enhancing security.

In this complex security landscape, solutions providers offering cutting-edge, integrated hardware and software products for IT security will lead the market. Providers must deliver comprehensive solutions encompassing network security, endpoint security and cloud and data security to address the full spectrum of threats. Integrating AI into these products is crucial for enhancing the robustness and responsiveness of security measures.

By understanding and implementing AI for enhanced security monitoring and threat detection, these providers can offer advanced, unified security platforms that protect, anticipate and neutralise emerging threats. Those who excel in providing innovative, AI-driven security solutions will set themselves apart, ensuring their clients are well-equipped to navigate the increasingly complex cybersecurity landscape, ultimately leading the pack in cloud security.

Check Point Software Technologies Ltd. is a leading AI-powered, cloud-delivered cybersecurity platform provider protecting over 100,000 organisations worldwide. Check Point leverages the power of AI everywhere to enhance cybersecurity efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times.

The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network and Check Point Infinity Core Services for collaborative security operations and services.

Comprehensive Cloud Security Across Applications, Workloads and Networks

Check Point CloudGuard (https://www.checkpoint.com/cloudguard/) provides a prevention-first approach to cloud security, enabling you to mitigate threats and prioritize risks throughout your cloud environments. Leveraging the Check Point Infinity platform, CloudGuard delivers robust protection against both known and emerging threats.

- **Prevention-First Cloud Native Application Protection:** Safeguard your multi-cloud environment from both known and unknown risks.
- **Unparalleled AI-Based Web Application Firewall:** Ensure preemptive defense against Zero Day attacks with advanced AI technology.
- **Unmatched Network Security Capabilities:** Gain superior threat prevention, visibility, and intelligence across your cloud networks.

Benefits of CloudGuard

Elevate your cloud security with CloudGuard's innovative capabilities:

- Industry-leading 99.7% block rate, as verified by Miercom.
- 99.8% catch rate, according to CyberRatings Cloud Security Lab.
- 169% return on investment, as reported by Forrester's Total Economic Impact Report.
- 84% reduction in risk.

Ready to enhance your cloud security?

Discover how CloudGuard can transform your security strategy and provide unparalleled protection. Contact us today to schedule a demo or consult with one of our experts.

"With most organisations ultimately adopting a multi-cloud strategy, it is important to invest in security solutions that can accommodate this approach. Check Point's Prevention-First Cloud Security approach provides comprehensive protection for all cloud assets. Whether private, hybrid, or multi-cloud based, it improves security while reducing complexity."

– Hendrik De Bruin, Head of SADC Security Consulting and Security Evangelist with the Office of the CTO, Check Point.

FREE Cloud Security Assessment Here:

Ensure your cloud environment is secure with Check Point's comprehensive assessment. Identify misconfigurations, evaluate compliance, and receive actionable remediation steps. Protect your organization from data breaches and cyber threats. Schedule your Free Cloud Security Posture Assessment via the link or QR code now!

https://www.checkpoint.com/resources/items/how-secure-are-your-cloud-applications-and-workloads-discover-with-check-points-free-cloud-security-posture-assessment?w=c778b

CHECK POINT™

in collaboration with

Lynchpin Media

Lynchpin Media is a global technology media, data and marketing services company. We help to increase awareness, develop and target key accounts and capture vital information on regional trends. Visit **lynchpinmedia.com** for more information.

Contact: Jess Abell, Chief Content Officer:
jess@lynchpinmedia.com

PRIORITIES
REPORTS, EVENTS & WEBINARS

CxO Priorities, a Lynchpin Media Brand

63/66 Hatton Garden
London, EC1N 8LE

Find out more: **www.cxopriorities.com**

Contact Details:

Cloud Security Architect Team:
Saad Nizam **nizams@checkpoint.com** and
Hendrik De Bruin **hendrikd@checkpoint.com**
Follow up discussions:
Maryanne Ndanu **maryannen@checkpoint.com**

Sponsored by

CHECK POINT

www.checkpoint.com