A Lynchpin Media BRAND

CXO PRIORITIES
REPORTS, EVENTS & WEBINARS

CROWDSTRIKE

Unlocking Cloud Security in the Middle East: Managing Risk and Complexity with AI Solutions

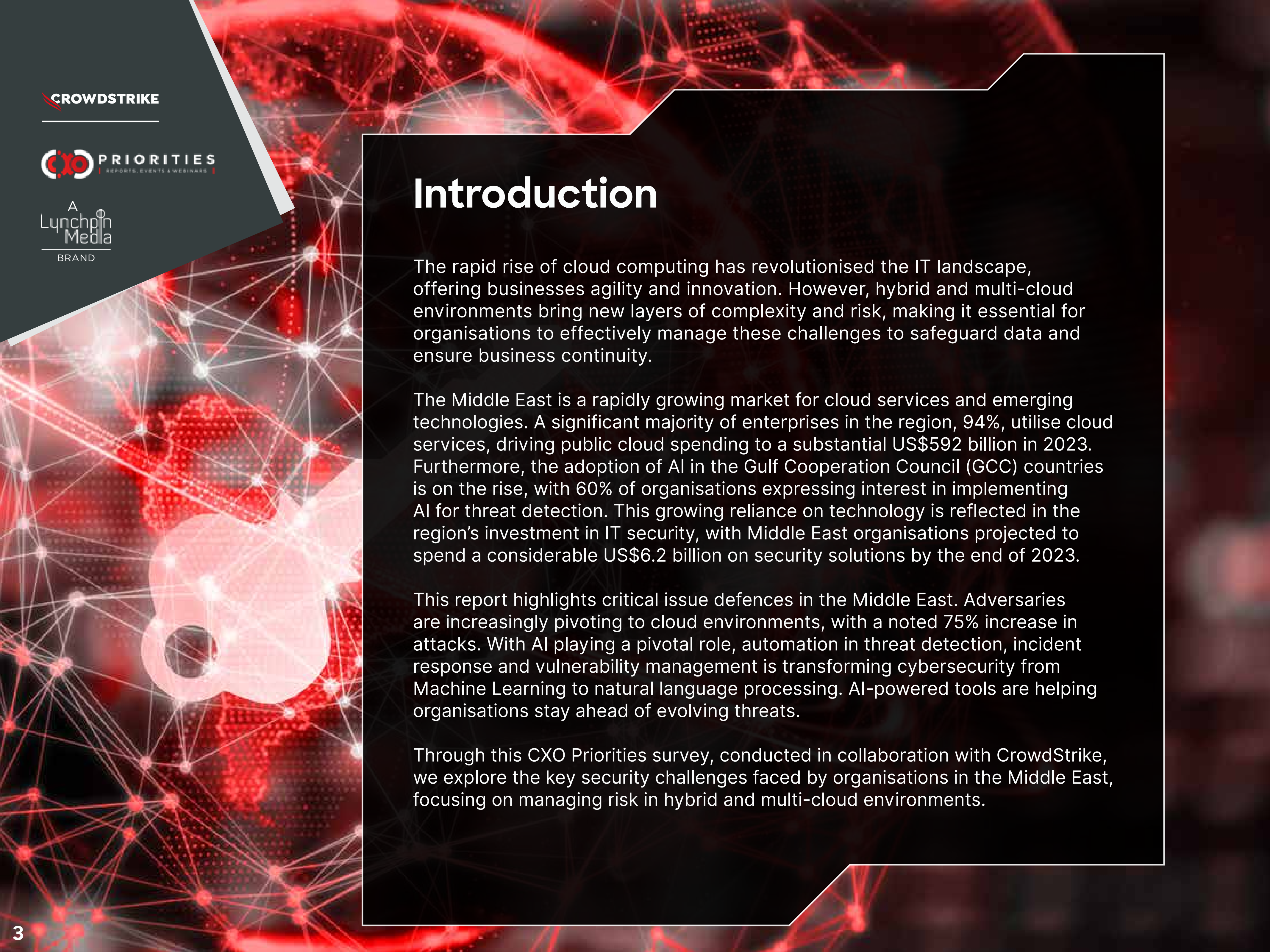
A CXO Priorities survey in collaboration with Crowdstrike

CROWDSTRIKE

CIO PRIORITIES
REPORTS, EVENTS & WEBINARS

A Lynchpin Media BRAND

CONTENTS



Introduction

The rapid rise of cloud computing has revolutionised the IT landscape, offering businesses agility and innovation. However, hybrid and multi-cloud environments bring new layers of complexity and risk, making it essential for organisations to effectively manage these challenges to safeguard data and ensure business continuity.

The Middle East is a rapidly growing market for cloud services and emerging technologies. A significant majority of enterprises in the region, 94%, utilise cloud services, driving public cloud spending to a substantial US$592 billion in 2023. Furthermore, the adoption of AI in the Gulf Cooperation Council (GCC) countries is on the rise, with 60% of organisations expressing interest in implementing AI for threat detection. This growing reliance on technology is reflected in the region's investment in IT security, with Middle East organisations projected to spend a considerable US$6.2 billion on security solutions by the end of 2023.

This report highlights critical issue defences in the Middle East. Adversaries are increasingly pivoting to cloud environments, with a noted 75% increase in attacks. With AI playing a pivotal role, automation in threat detection, incident response and vulnerability management is transforming cybersecurity from Machine Learning to natural language processing. AI-powered tools are helping organisations stay ahead of evolving threats.

Through this CXO Priorities survey, conducted in collaboration with CrowdStrike, we explore the key security challenges faced by organisations in the Middle East, focusing on managing risk in hybrid and multi-cloud environments.

CROWDSTRIKE

CXO PRIORITIES
REPORTS, EVENTS & WEBINARS

A Lynchpin Media BRAND

Survey Overview

To better understand the security challenges and priorities related to hybrid and multi-cloud environments in the Middle East, we surveyed 50 senior technology leaders and decision-makers in July 2024. These findings provide valuable insights into how organisations are navigating security in an increasingly complex digital landscape.

Through this survey we aimed to discover:

- **The challenges of managing Cloud Security risks** – including the emergence of new attack vectors, compliance with regulations, incidence response and recovery, ensuring data protection and managing access controls.
- **Investment trends in Cloud Security** – such as the adoption of emerging security technologies and the prioritisation of different security threats.
- **The obstacles in managing endpoint security** – in an increasingly remote work environment, such as resource limitations, visibility monitoring and user compliance.
- **The use of AI tools and technologies for cybersecurity** – for faster cloud detection, reducing false positives and improving policy consistency across cloud environments.

KEY FINDINGS:

To find out more about the current security challenges and priorities around hybrid and multi-cloud facing organisations in the Middle East, we surveyed 50 senior technology leaders and decision-makers about the factors that are driving cloud and endpoint security in the face of evolving technologies. This report aims to present an overview of the current challenges and explore the complexities of managing security risks.

Key Findings

1 2 3 4 5 6 7 8 9 10 11 12

Private Cloud (33%) and **hybrid cloud (31%)** are organisations' most utilised cloud deployments

continued ...

CROWDSTRIKE

PRIORITIES

REPORTS, EVENTS & WEBINARS

A Lynchpin Media BRAND

Key Findings

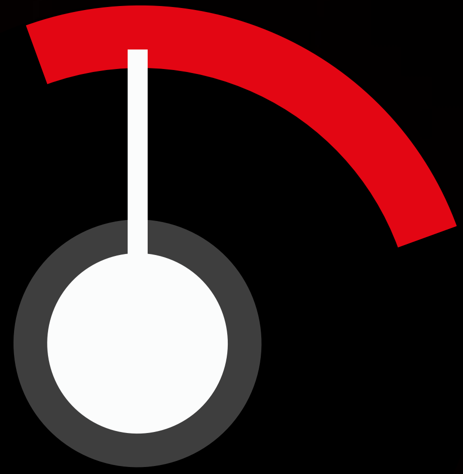
1 2 3 4 5 6 7 8 9 10 11 12

Google Cloud Platform (26%) and **Microsoft Azure (25%)** are the leading cloud service providers for organisations

continued ...

Key Findings

1 2 3 4 5 6 7 8 9 10 11 12



Access control management (25%) is the biggest challenge to organisations when managing Cloud Security risks

continued ...

Key Findings

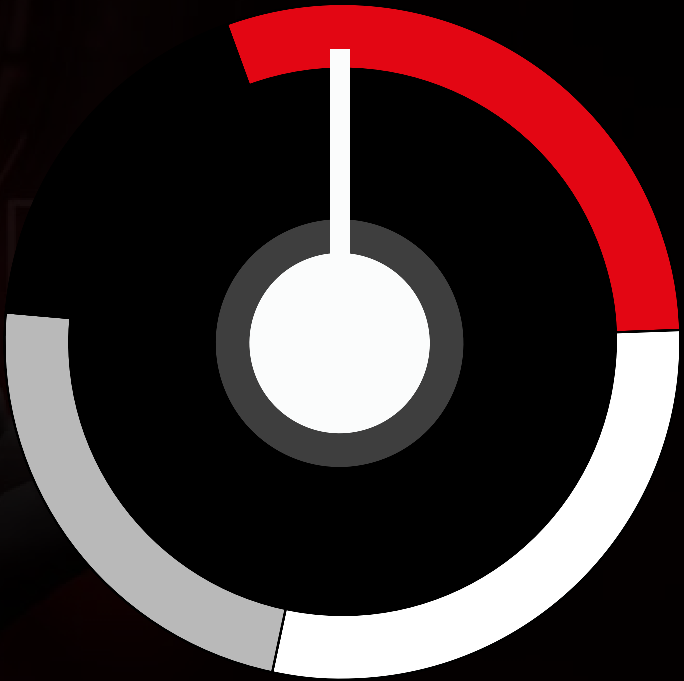
1 2 3 4 5 6 7 8 9 10 11 12

Regarding emerging trends in Cloud Security, technology leaders identified **zero-day vulnerabilities (29%)** and **AI and Machine Learning threats (27%)** as their top concerns

continued ...

Key Findings

1 2 3 4 5 6 7 8 9 10 11 12



Over the next 12 months, organisations will focus on enhancing Cloud Security by **prioritising compliance and governance (30%)**, **investing in new security technologies (29%)** and **strengthening data protection measures (23%)**

continued ...

Key Findings

1 2 3 4 5 6 7 8 9 10 11 12

More than 80% of organisations **plan to invest in cloud solutions within the next 12 months**, with the majority **(31%) aiming to do so within 3–6 months**.

continued ...

Key Findings

The top three challenges in managing endpoint security are **resource limitations (15%)**, **visibility and monitoring (15%)** and **user compliance (14%)**

continued ...

Key Findings

1 2 3 4 5 6 7 8 9 10 11 12

More than 40% of respondents feel **neutral** or **not very confident** in their organisation's ability to detect and respond to security breaches before they escalate

continued ...

Key Findings

1 2 3 4 5 6 7 8 9 10 11 12

Nearly 60% of respondents stated that their organisation typically spends **daily** and **hourly** on manual tasks related to security and IT collaboration, such as asset visibility, querying and patching

continued ...

Key Findings

1 2 3 4 5 6 7 8 9 10 11 12

$

Financial losses

and

regulatory compliance issues

emerge as key concerns

continued ...

Key Findings

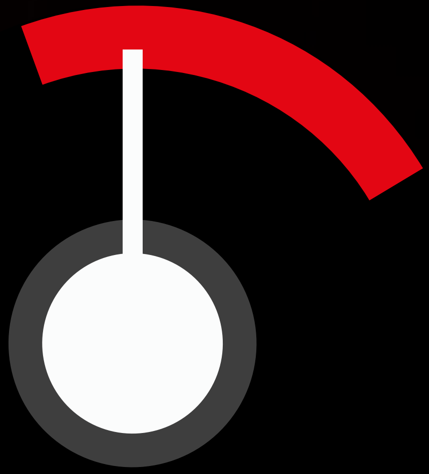
1 2 3 4 5 6 7 8 9 10 11 12

The results highlight an emerging reliance on AI tools for security, with **predictive analytics (30%)** and **automated response (25%)** as the most widely adopted

continued ...

Key Findings

1 2 3 4 5 6 7 8 9 10 11 12

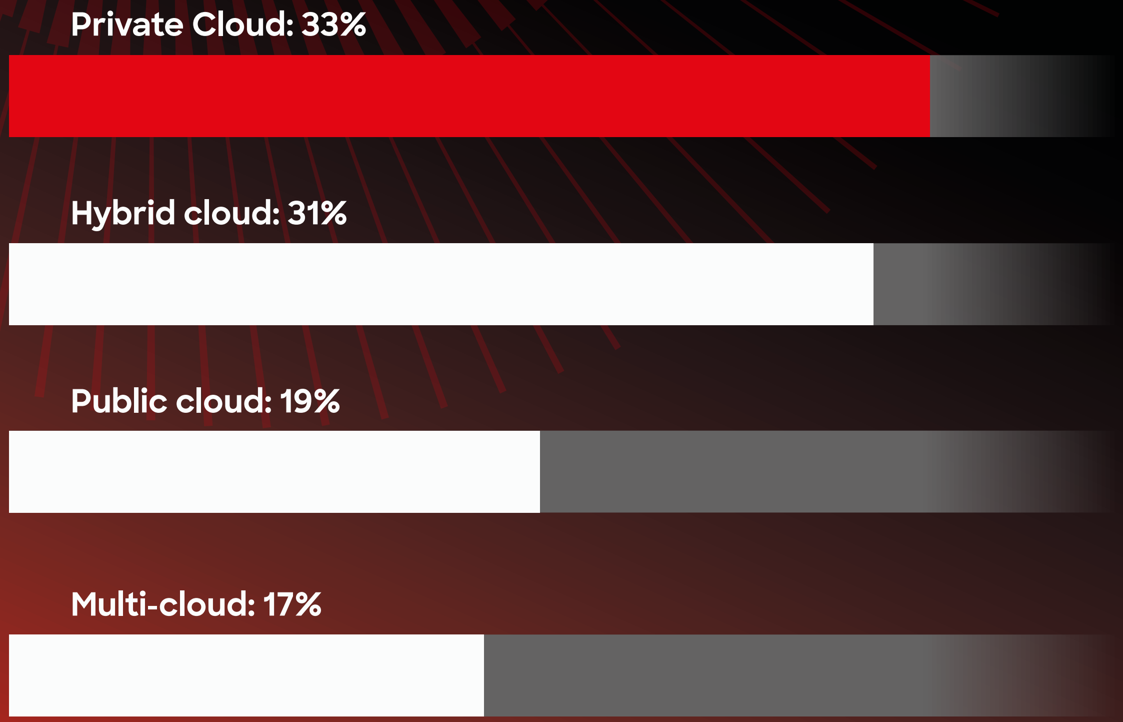


The survey reveals a strong consensus around the areas where automation could most benefit cybersecurity efforts, with **identity and access management (22%)** seen as crucial

PART 1: Cloud Security, priorities and investment

By understanding the security implications of their cloud deployment, organisations in the Middle East can take a proactive approach to protect sensitive data and ensure compliance across their cloud infrastructure. Organisations need strong IAM, enhanced visibility and a unified security platform for comprehensive protection, real-time threat detection and compliance across cloud environments.

What type of cloud deployment does your organisation use?



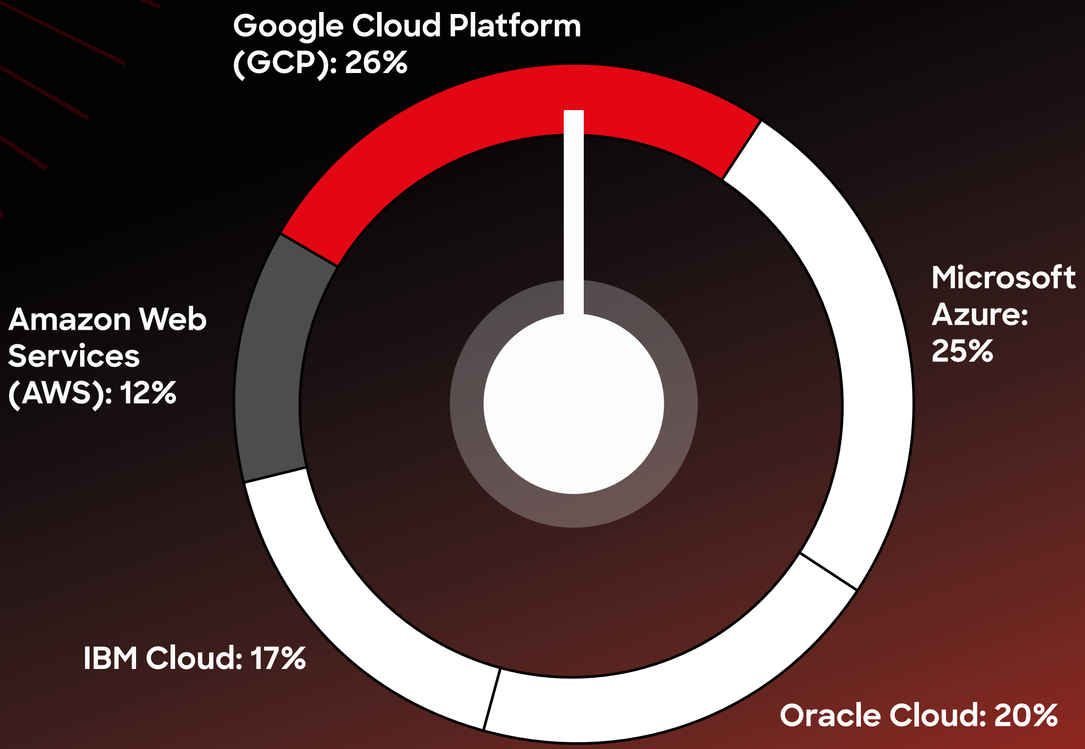
KEY INSIGHT

The survey results show that organisations in the Middle East are heavily utilising private **(33%)** and hybrid **(31%)** cloud deployments, with public **(19%)** and multi-cloud **(17%)** also being significant.

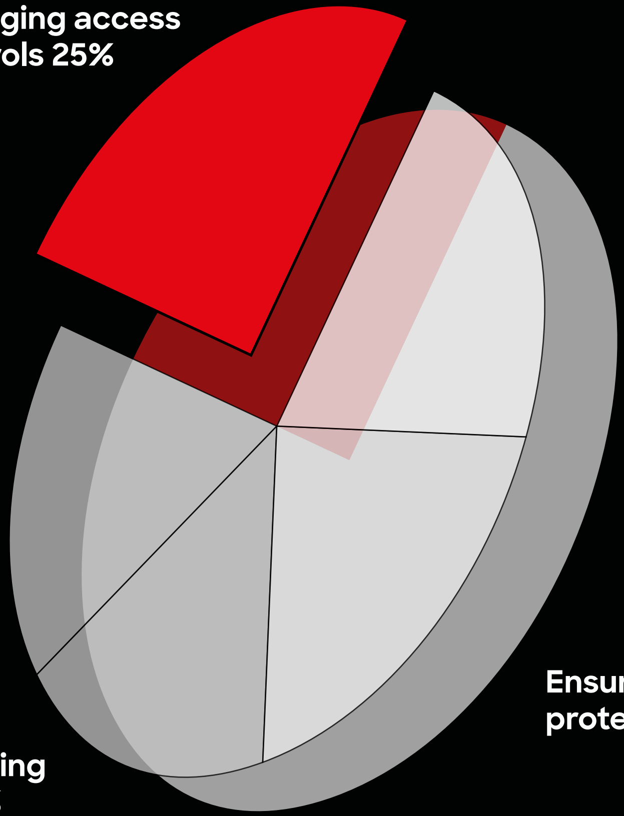
Which cloud service providers are you currently using?

KEY INSIGHT

Google Cloud Platform **(26%)** and Microsoft Azure **(25%)** are the top cloud service providers, followed by Oracle Cloud **(20%)**, IBM Cloud **(17%)** and Amazon Web Services **(12%)**. With organisations spreading their assets across multiple cloud environments, the need for robust, unified Cloud Security solutions has never been more critical. Each platform introduces unique security risks, making it essential to have a comprehensive strategy that safeguards data across all cloud infrastructures.



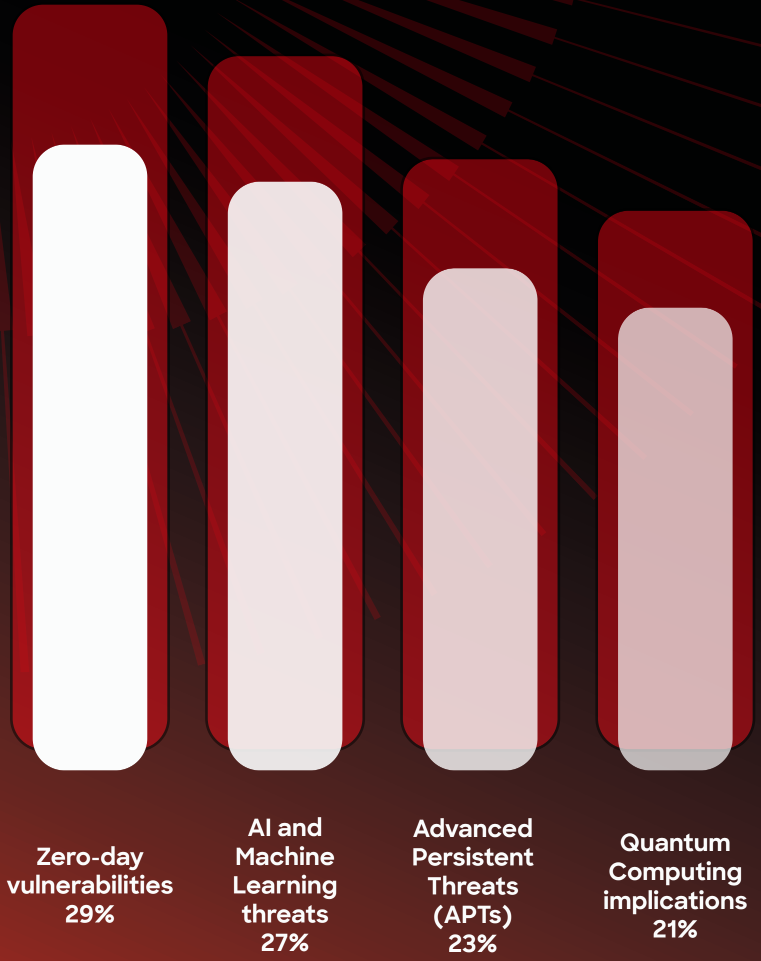
What are your primary challenges in managing Cloud Security risks?



KEY INSIGHT

Our survey revealed that managing **access control** is the top challenge for **25%** of organisations in the Middle East in securing their cloud environments, followed by **compliance with regulations (21%)** and **ensuring data protection (20%)**. These findings highlight the urgent need for advanced security solutions that prioritise robust access control and ensure compliance with evolving regulatory demands Threat actors can pivot between the cloud control plane and cloud-hosted VMs, making cloud environments increasingly vulnerable.

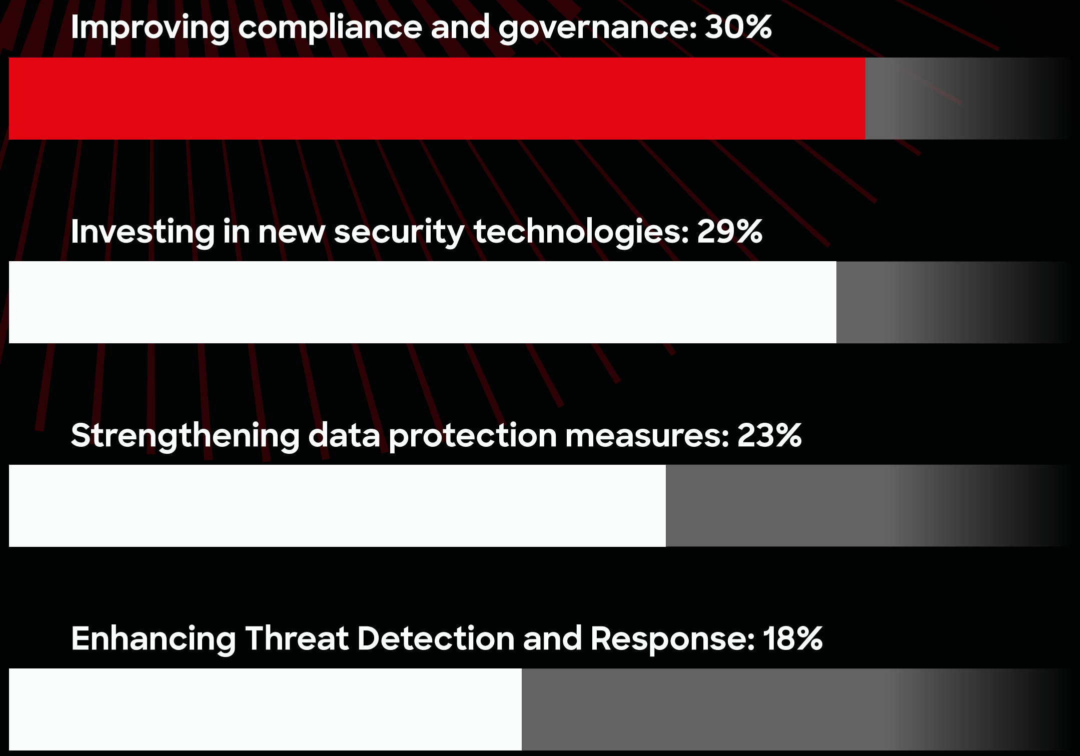
What emerging trends in Cloud Security are you most concerned about?



KEY INSIGHT

When asked about emerging Cloud Security trends, technology leaders in the Middle East highlighted zero-day vulnerabilities **(29%)** and AI and Machine Learning threats **(27%)** as their top concerns, followed closely by Advanced Persistent Threats (APTs) **(23%)** and the rising implications of Quantum Computing **(21%)**. These responses reflect growing urgency around AI-driven threats and the persistent danger of zero-day exploits. The message is clear: organisations in the Middle East must prioritise adaptive security strategies and adopt proactive measures to stay ahead of these evolving risks.

What are your top priorities for improving Cloud Security in the next 12 months?

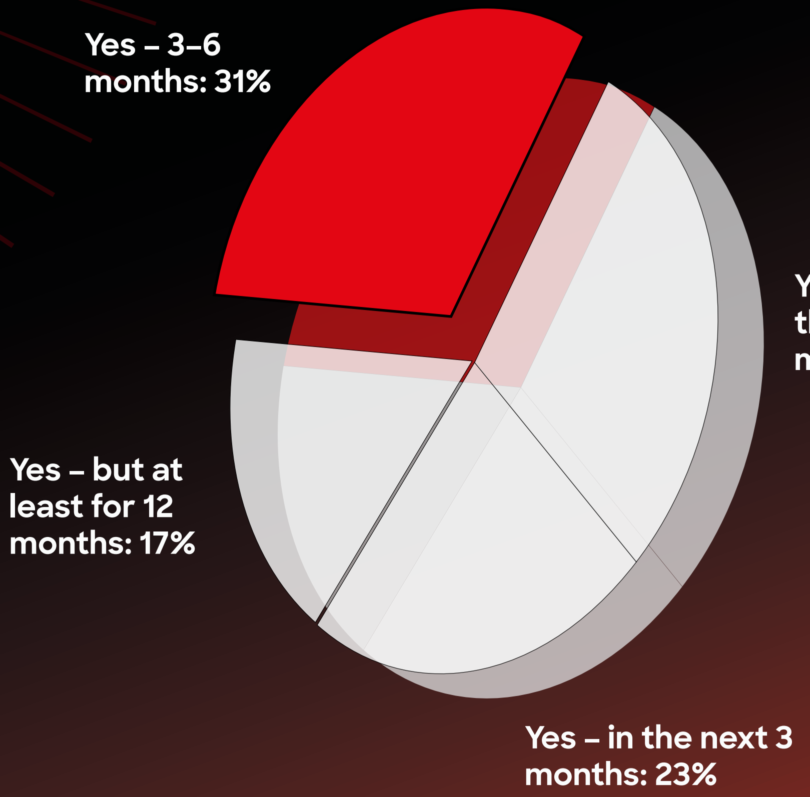


KEY INSIGHT

Over the next 12 months, organisations in the Middle East are set to enhance Cloud Security, with compliance and governance **(30%)** taking top priority. This focus on aligning with evolving regulations highlights the increasing need for businesses to stay ahead of regulatory demands. Close behind, investing in new security technologies **(29%)** signals a proactive approach to combating advanced threats. Additionally, strengthening data protection **(23%)** and enhancing Threat Detection and Response **(18%)** underscore a shift toward a more strategic, layered defence against cyber-risks.

These priorities reflect a growing recognition that comprehensive, forward-looking security strategies are essential to safeguarding cloud environments and staying resilient in the face of emerging threats. Organisations that prioritise these areas will be better equipped to mitigate risks and protect their critical assets. As the Middle East region is expected to grow is important to align investments with regional priorities, focusing on compliance, endpoint security and cloud-specific solutions.

Is your organisation planning an investment in a cloud solution?



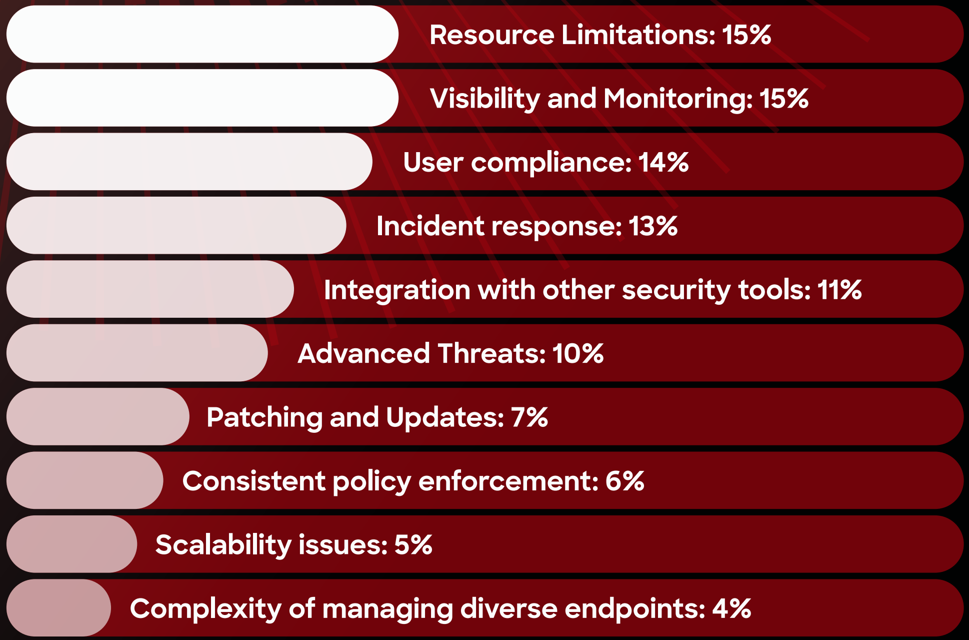
KEY INSIGHT

Our survey shows that **83%** of organisations in the Middle East plan to invest in cloud solutions within the next 12 months, with **31%** aiming for the next 3–6 months. This highlights the urgency of cloud adoption, but as investments accelerate, robust security strategies are crucial to managing increased risks and complexity. Trusted security partners will be essential to ensure comprehensive protection as businesses embrace the cloud. It is recommended that organisations prioritise investments in Cloud Security tools, such as multi-factor authentication and encryption solutions.

PART 2: Endpoint Security

With remote work and sophisticated threats on the rise, securing endpoints like laptops, desktops and mobile devices is critical to protecting sensitive data and preventing breaches. This section explores the key challenges organisations face and the growing role of AI in strengthening endpoint security.

What are the main challenges you face with managing endpoint security in your environment?



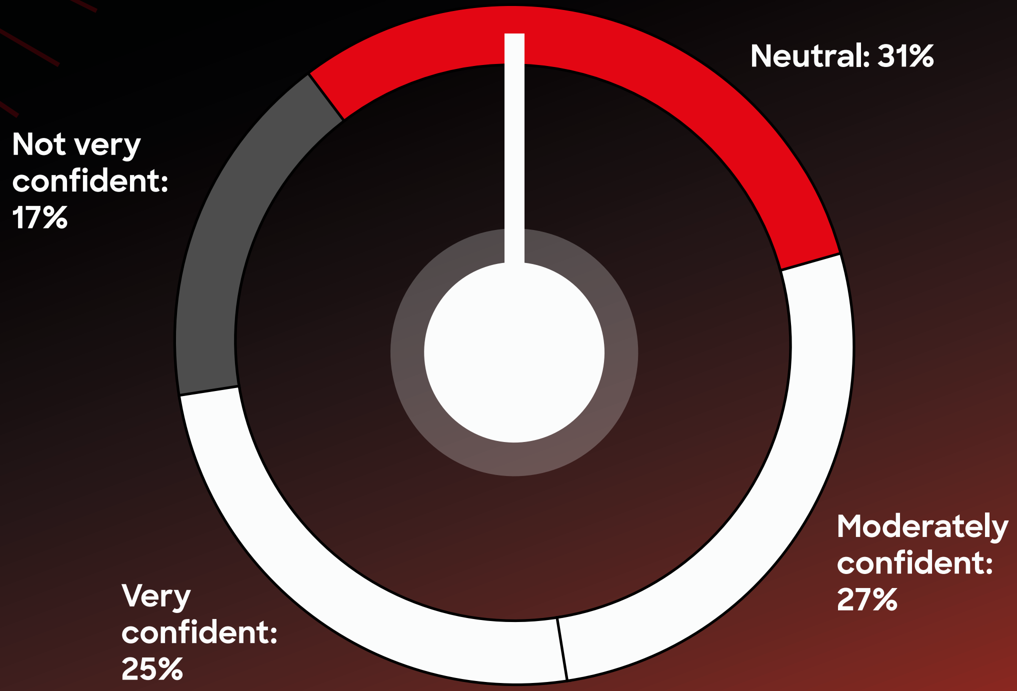
KEY INSIGHT

As organisations in the Middle East region increasingly adopt hybrid cloud infrastructures, the threat landscape becomes more complex. Adversaries are now targeting multiple domains, such as identity, endpoint, and cloud environments. The top three challenges in managing endpoint security are resource limitations **(15%)**, visibility and monitoring **(15%)**, and user compliance **(14%)**. The challenges highlighted reflect wider industry trends in endpoint security management. Resource constraints indicate a growing skills gap, as organisations struggle to maintain adequate cybersecurity staffing. Visibility issues, exacerbated by remote working and IoT devices, hinder real-time threat detection, making advanced threat protection more complex. User compliance reveals the ongoing struggle to secure human behaviour, often undermining security policies. These challenges underscore the urgent need for automation, AI-driven monitoring and unified security frameworks to improve scalability, streamline incident response, and ensure consistent enforcement across diverse endpoint environments.

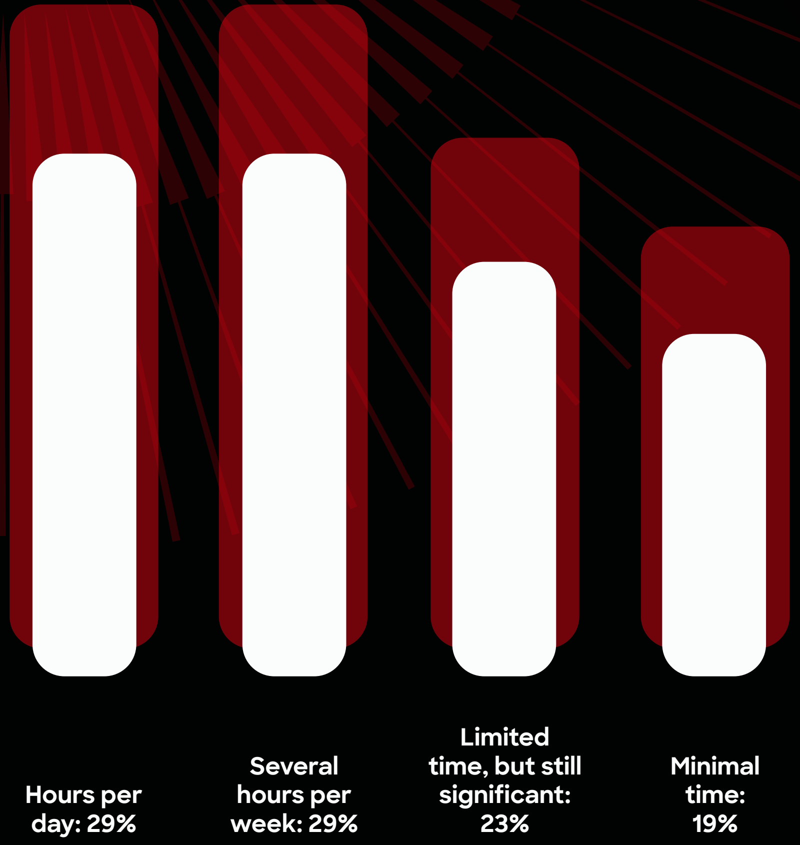
How confident are you in your organisation's ability to detect and respond to security breaches before they escalate?

KEY INSIGHT

The survey reveals a concerning lack of confidence in organisations' ability to detect and respond to security breaches, highlighting broader themes of preparedness and resilience. With over **40%** of respondents feeling neutral or not very confident, this suggests gaps in incident response capabilities, insufficient threat detection systems and a need for enhanced cybersecurity strategies to mitigate escalating risks.



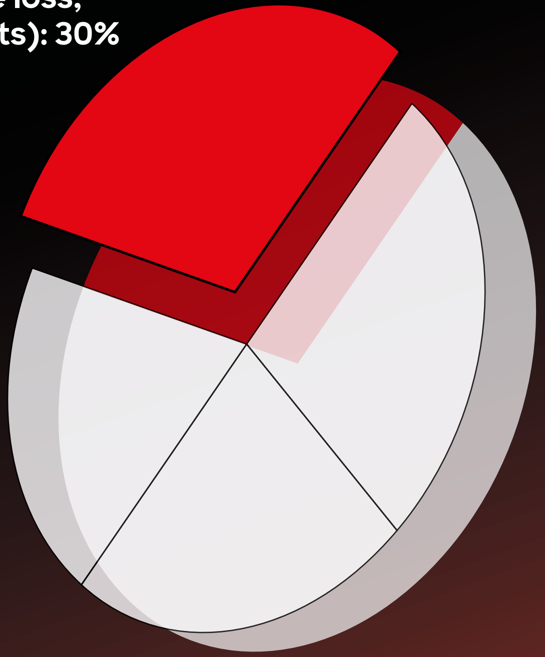
How much time does your organisation typically spend on manual tasks related to security and IT collaboration, such as asset visibility, querying and patching?



KEY INSIGHT

The results suggest that many organisations are still spending considerable time on manual security tasks, highlighting inefficiencies in security and IT collaboration. With nearly **60%** reporting daily or weekly efforts, this reflects broader trends where outdated processes and fragmented tools hinder operational efficiency. This reliance on manual work increases the risk of human error and delays in addressing vulnerabilities, particularly in critical areas like patching and asset visibility. The findings underscore the growing need for automation, integration and AI-driven solutions to streamline tasks, reduce workloads and allow security teams to focus on more strategic, high-priority objectives.

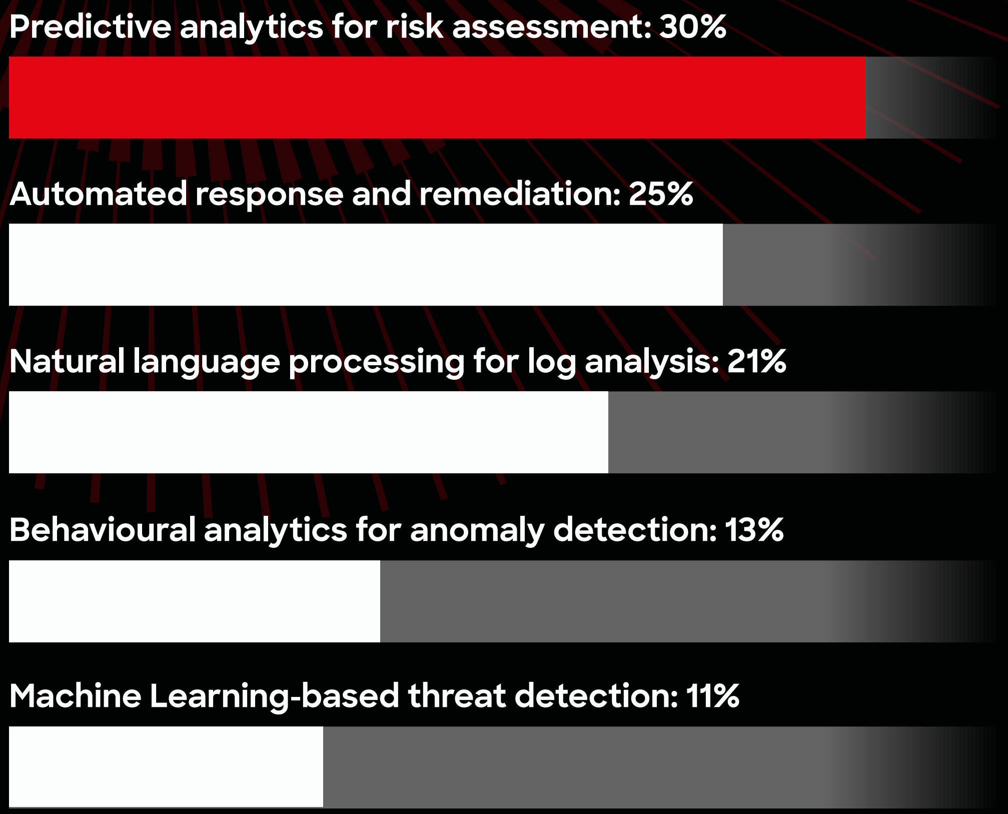
In your opinion, what is the biggest impact of security-related downtime on your organisation?



KEY INSIGHT

The survey reveals that security-related downtime affects organisations on multiple fronts, with financial losses and regulatory compliance issues emerging as key concerns. To mitigate these risks, organisations must prioritise robust security measures, rapid incident response, and strategies that minimise downtime to protect both their bottom line and reputation.

Which AI tools or technologies is your organisation currently using for security purposes?



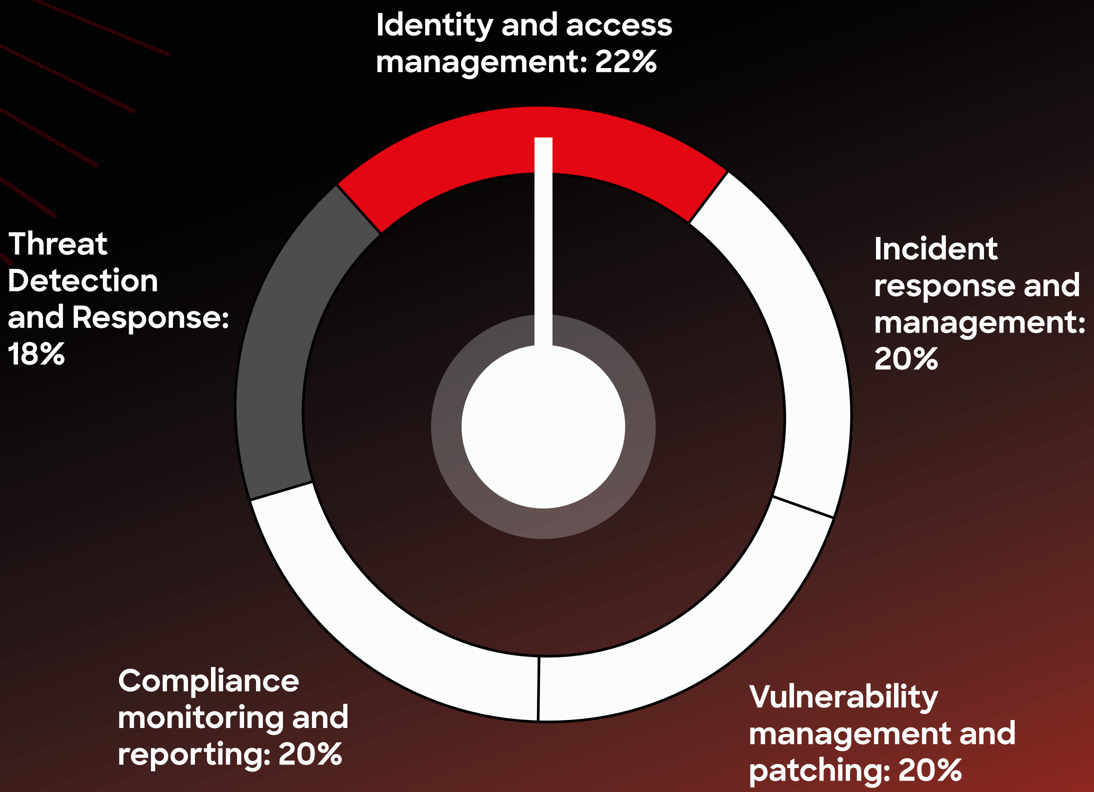
KEY INSIGHT

The survey reveals a growing reliance on AI tools for security, with **predictive analytics (30%)** and **automated response (25%)** being the most widely adopted. This shift reflects the industry's move toward proactive threat mitigation and reducing manual intervention in incident response in the Middle East. Predictive analytics is becoming crucial for assessing risks and prioritising vulnerabilities, allowing organisations to focus on the most critical threats. Automated response tools streamline remediation, addressing the need for faster, more efficient attack mitigation. The use of natural language processing (21%) for log analysis is also gaining traction, improving detection efficiency. However, the underutilisation of **machine learning (11%)** suggests potential growth in AI-driven threat detection, which organisations should explore to further enhance their cybersecurity capabilities. This reinforces that companies should also consider developing a roadmap for integrating AI into cybersecurity strategies to further support this.

In which areas do you believe your organisation would benefit most from automation in cybersecurity?

KEY INSIGHT

The survey reveals a strong consensus around the areas where automation could most benefit cybersecurity efforts, with identity and access management **(22%)** seen as crucial. This reflects the growing need to manage complex access permissions in an increasingly distributed workforce. Incident response, vulnerability management, and compliance (all at **20%**) highlight the pressure organisations face to react swiftly to threats, ensure up-to-date defences and meet regulatory requirements. Threat detection **(18%)** is also crucial, as automation can enhance detection speed and accuracy, reducing human error. These findings point to the necessity for streamlined, automated solutions to bolster cybersecurity resilience across key functions.



Conclusion

The state of cybersecurity in the Middle East is characterised by rapid Digital Transformation, cloud adoption and increasing cyberthreats. The Cloud Security landscape is evolving rapidly, with more organisations adopting cloud solutions to meet their business needs. While private and hybrid clouds remain favoured, concerns around access control, zero-day vulnerabilities and AI-driven attacks are growing. To combat these challenges, businesses are prioritising compliance, governance, technology investments and data protection.

As cloud adoption accelerates, endpoint security remains a critical issue, with resource constraints, visibility and user compliance as key hurdles. Despite these challenges, organisations are proactively seeking solutions that offer faster cloud detection, reduce false positives and improve policy consistency across their cloud environments. Providers that offer robust, AI-powered security services will be well-positioned to meet these demands and lead the market.

To further enhance their Cloud Security posture, Middle Eastern organisations should consider implementing more targeted strategies. Adopting AI for threat detection can provide real-time insights into emerging threats and automate incident response. Improving endpoint security is crucial to protect devices from malware and unauthorised access. Additionally, as organisations increasingly leverage multiple cloud platforms, addressing multi-cloud challenges through effective governance and management practices is essential. To effectively measure cloud security success, organisations should implement key performance indicators (KPIs) and leverage security analytics tools. By prioritising these recommendations, Middle Eastern organisations can strengthen their Cloud Security defences and mitigate potential risks.

CrowdStrike can help organisations streamline their security operations through AI-driven predictive analytics and automated response, enabling businesses to mitigate risks, enhance their security posture and gain a competitive edge in today’s digital landscape.

CROWDSTRIKE

CXO PRIORITIES
REPORTS, EVENTS & WEBINARS

A Lynchpin Media BRAND

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.

CXO PRIORITIES
REPORTS, EVENTS & WEBINARS

CxO Priorities, a Lynchpin Media Brand

63/66 Hatton Garden
London, EC1N 8LE

Find out more: www.cxopriorities.com

Sponsored by

CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical enterprise risks – endpoints, cloud workloads, identity, and data.

Learn more at: www.crowdstrike.com