A Lynchpin Media BRAND

CXO PRIORITIES
REPORTS, EVENTS & WEBINARS

CROWDSTRIKE

Securing the Digital Frontier: Key Insights on Cloud and Endpoint Security in the Middle East

A CXO Priorities survey in collaboration with CrowdStrike

CROWDSTRIKE

CIO PRIORITIES
REPORTS, EVENTS & WEBINARS

A Lynchpin Media BRAND

CONTENTS

Introduction

The rapid adoption of cloud computing has transformed the IT landscape, providing businesses with agility and innovation. However, hybrid and multi-cloud environments also bring increased complexity and risk, making robust security strategies essential.

This is especially true in the Middle East, where cloud adoption is accelerating. According to **Technology Magazine** (February 2023), **94% of enterprises in the region** use cloud services, contributing to global public cloud spending of **US$592 billion** in 2023. Additionally, **McKinsey & Company** (June 2023) reports that **60% of Gulf Cooperation Council (GCC) organisations** are adopting AI, particularly for threat detection. Yet, this reliance on advanced technologies also exposes businesses to greater risks.

Meanwhile, the ***CrowdStrike 2024 Threat Hunting Report*** reveals a **75% increase in attacks targeting cloud environments**, underscoring the need for proactive defences. AI-driven tools are emerging as a critical component of cybersecurity, automating threat detection, incident response, and vulnerability management. These advancements help organisations stay ahead of increasingly sophisticated threats.

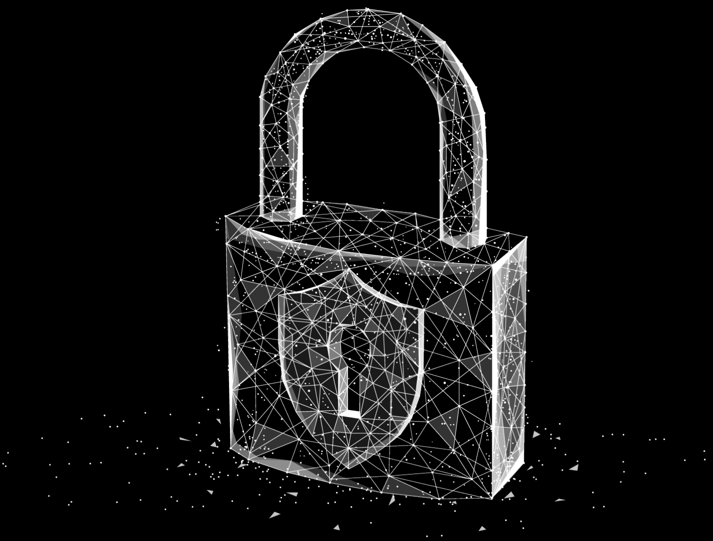
This **CXO Priorities survey**, conducted with CrowdStrike, explores these pressing challenges and provides insights into securing hybrid and multi-cloud environments in the Middle East.

SURVEY OVERVIEW

In July 2024, we surveyed 50 senior technology leaders and decision-makers across the Middle East to uncover the security challenges and priorities associated with hybrid and multi-cloud environments. These findings reveal how organisations are addressing the complexities of securing cloud and endpoint environments in the face of evolving technologies.

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.



CROWDSTRIKE

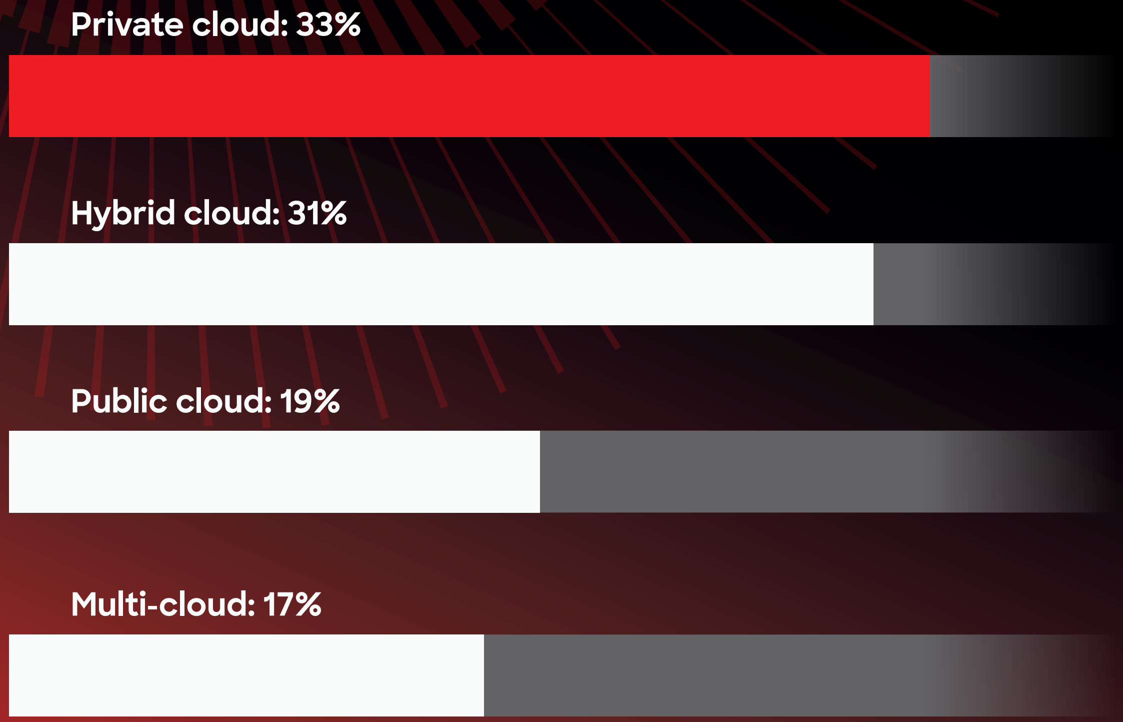
PRIORITIES
REPORTS, EVENTS & WEBINARS

A Lynchpin Media BRAND

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 monitor compliance across their cloud infrastructure. Organisations need strong identity and access management (IAM), enhanced visibility and a unified security platform for comprehensive protection, real-time threat detection and compliance across cloud environments.

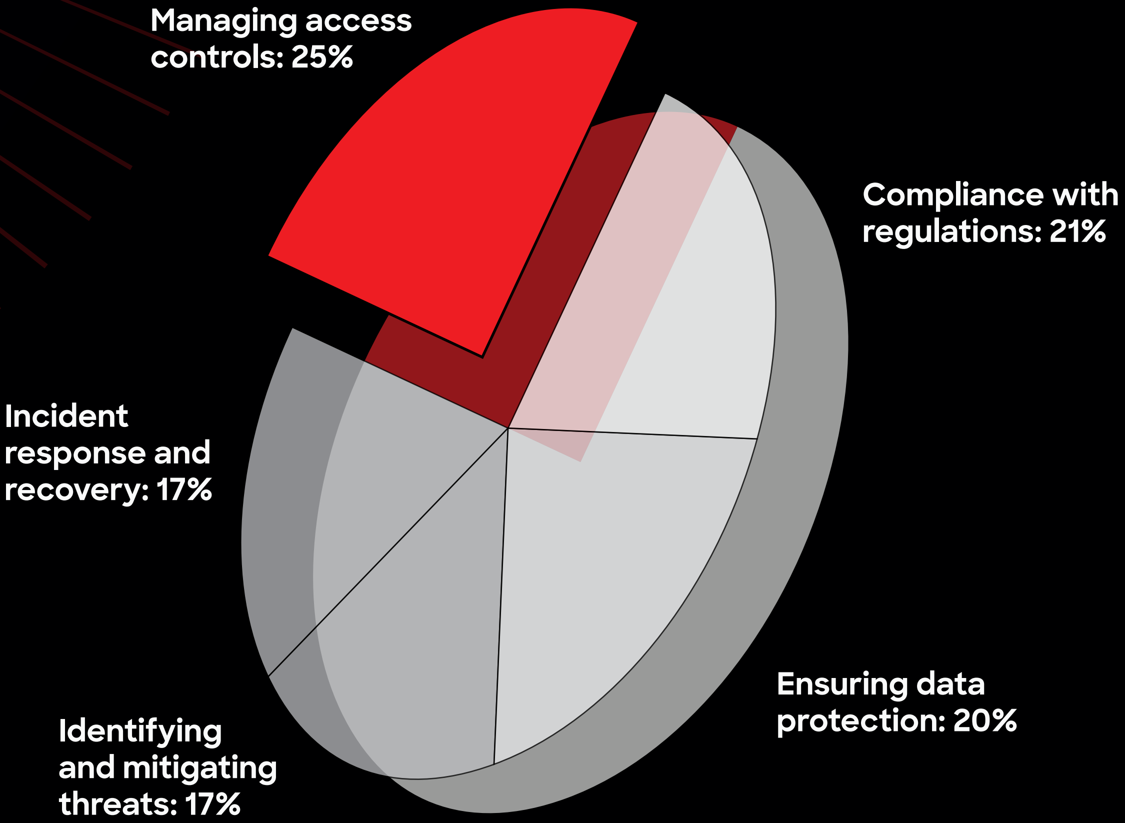
What type of cloud deployment does your organisation use?



KEY INSIGHTS

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.

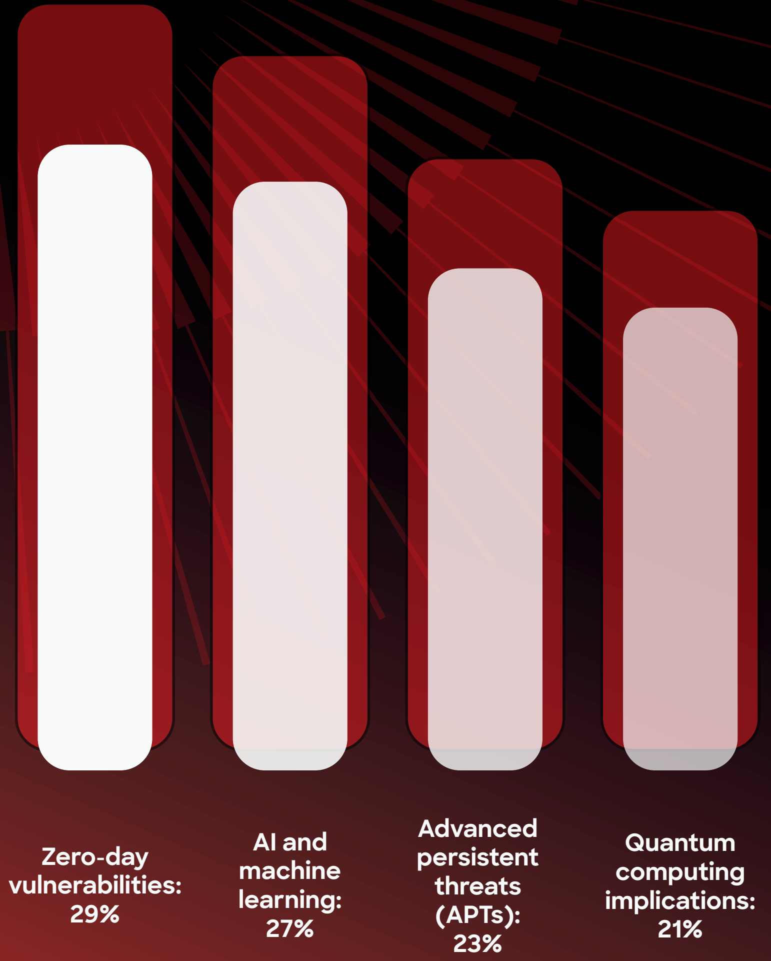
What are your primary challenges in managing cloud security risks?



KEY INSIGHTS

The survey highlights the key challenges organisations face in securing their cloud environments: managing access control **(25%)**, compliance with regulation **(21%)**, and ensuring data protection **(20%)**. ***The CrowdStrike 2024 Threat Hunting Report*** provides additional context, revealing that threat actors can pivot between the cloud control plane and cloud-hosted virtual machines (VMs), further exacerbating vulnerabilities in cloud environments.

What emerging trends in cloud security are you most concerned about?

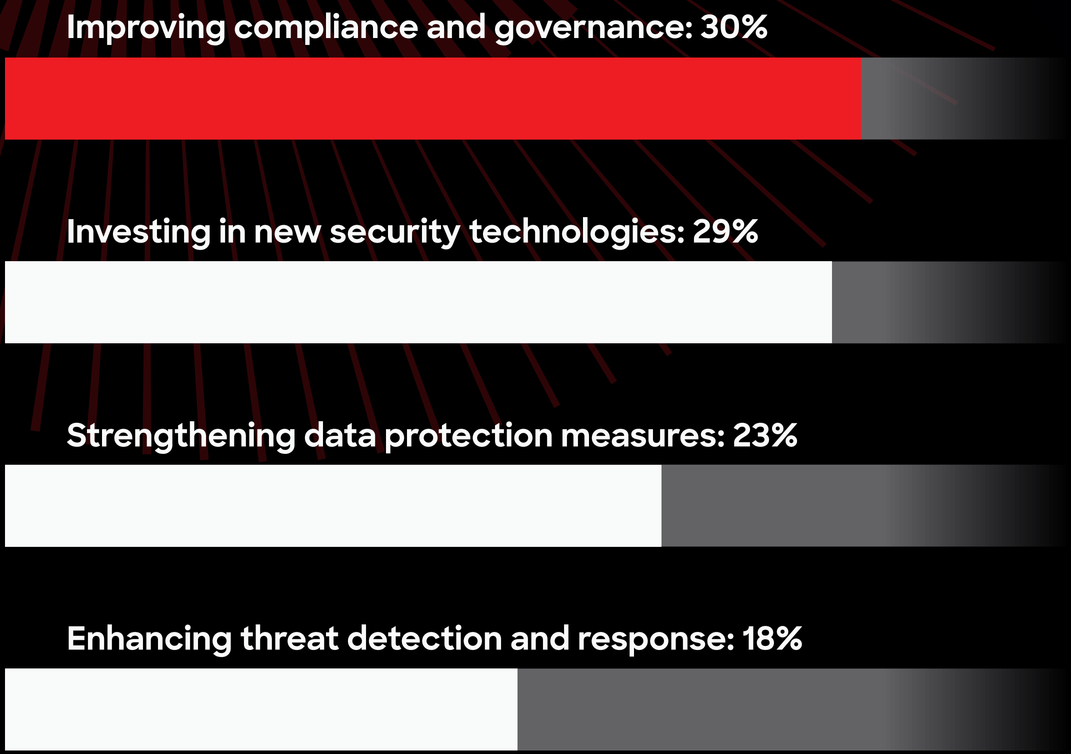


KEY INSIGHTS

Technology leaders in the Middle East identified zero-day vulnerabilities **(29%)** and AI-driven threats **(27%)** as top emerging cloud security concerns, followed by advanced persistent threats **(23%)** and the risks of quantum computing **(21%)**. These findings underscore the urgent need for organisations to adopt adaptive security strategies to stay ahead of rapidly evolving risks.

What are your top priorities for improving cloud security in the next 12 months*?

*From the time of survey, July 2024



Improving compliance and governance: 30%

Investing in new security technologies: 29%

Strengthening data protection measures: 23%

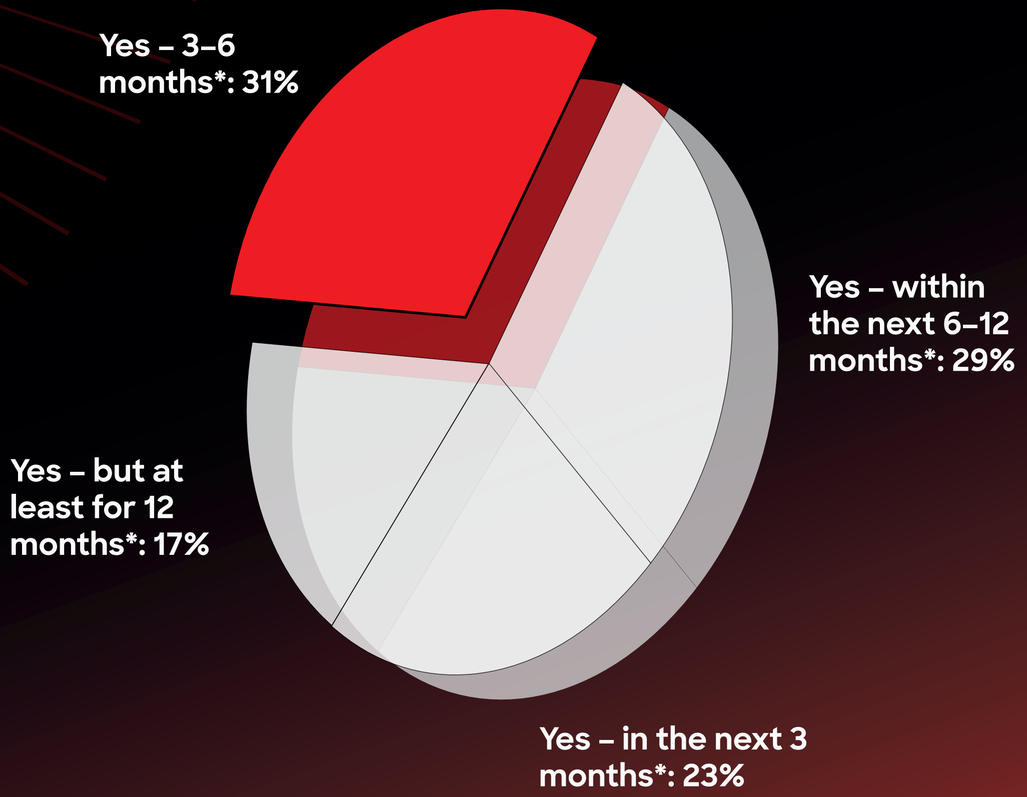
Enhancing threat detection and response: 18%

KEY INSIGHTS

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, it 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 INSIGHTS

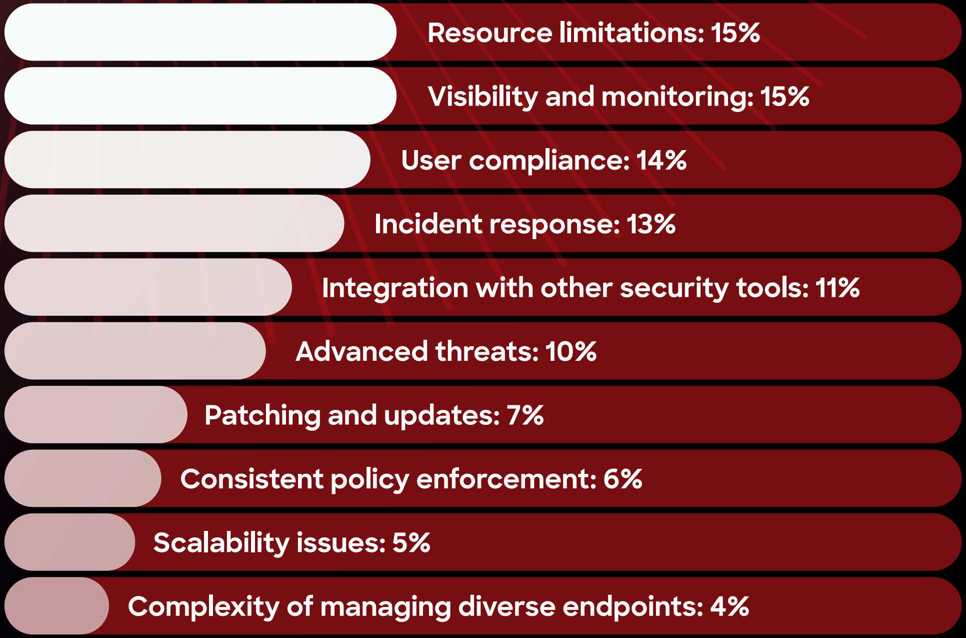
Our survey shows that **83%** of organisations in the Middle East plan to invest in cloud solutions within the next 12 months*, with **31%** aiming for the next 3–6 months*. This highlights the urgency of cloud adoption, but as investments accelerate, robust security strategies are crucial to managing 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.

*From the time of survey, July 2024

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?



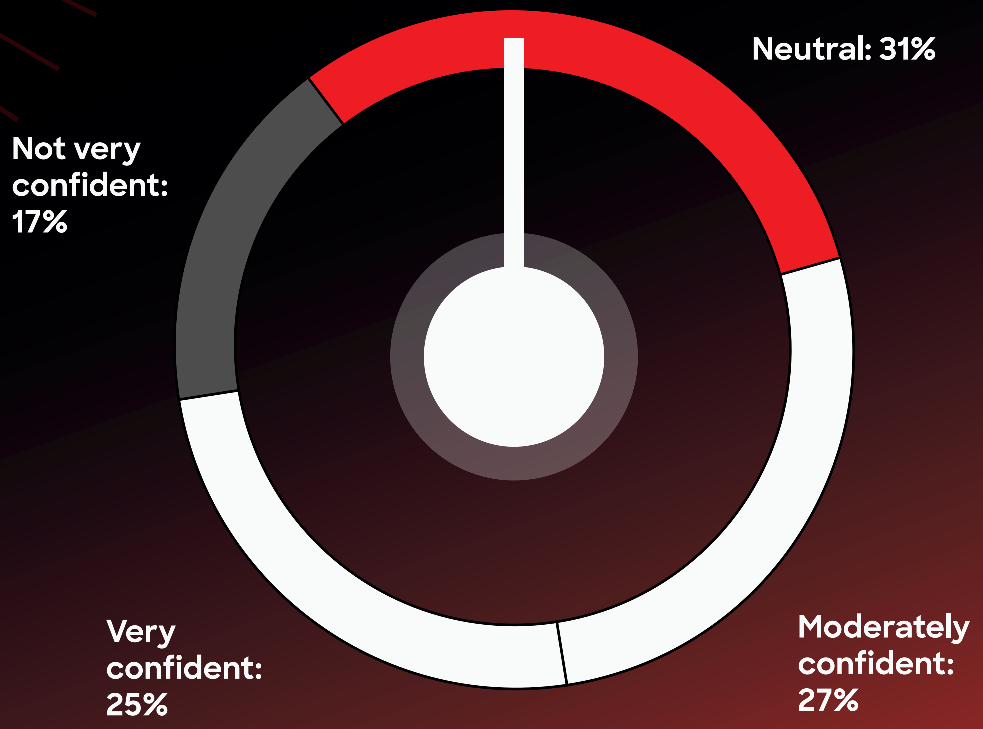
KEY INSIGHTS

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 survey reveals that 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.

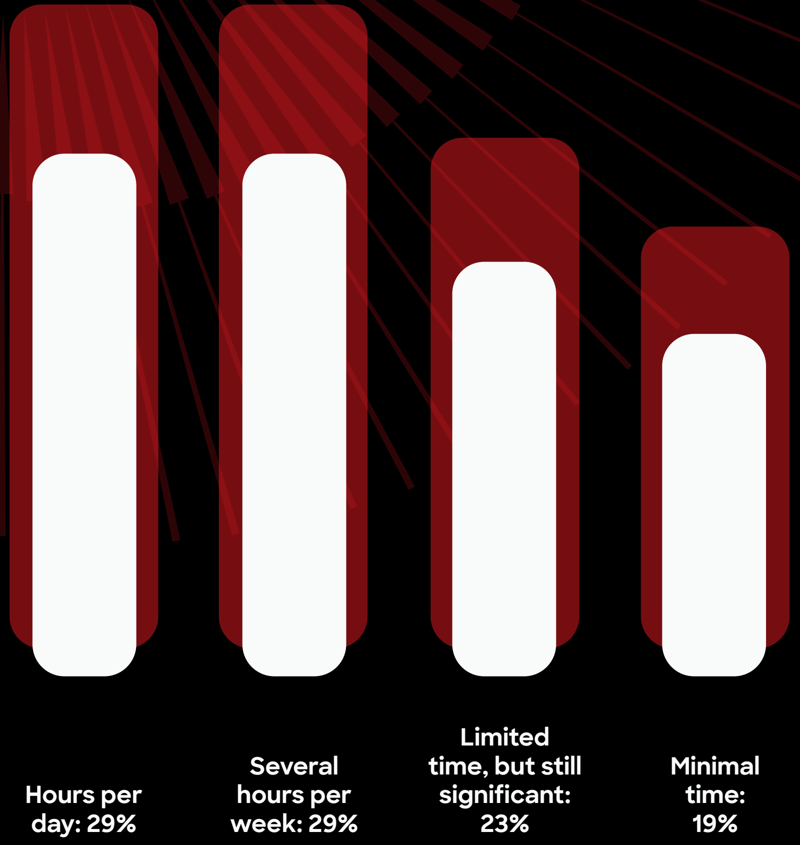
How confident are you in your organisation's ability to detect and respond to security breaches before they escalate?

KEY INSIGHTS

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.



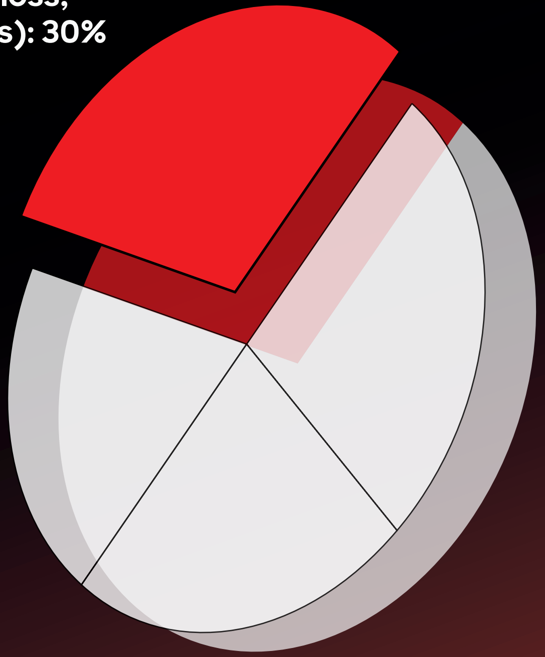
How much time does your organisation typically spend on manual tasks related to security and IT collaboration, such as asset visibility, querying and patching?



KEY INSIGHTS

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.

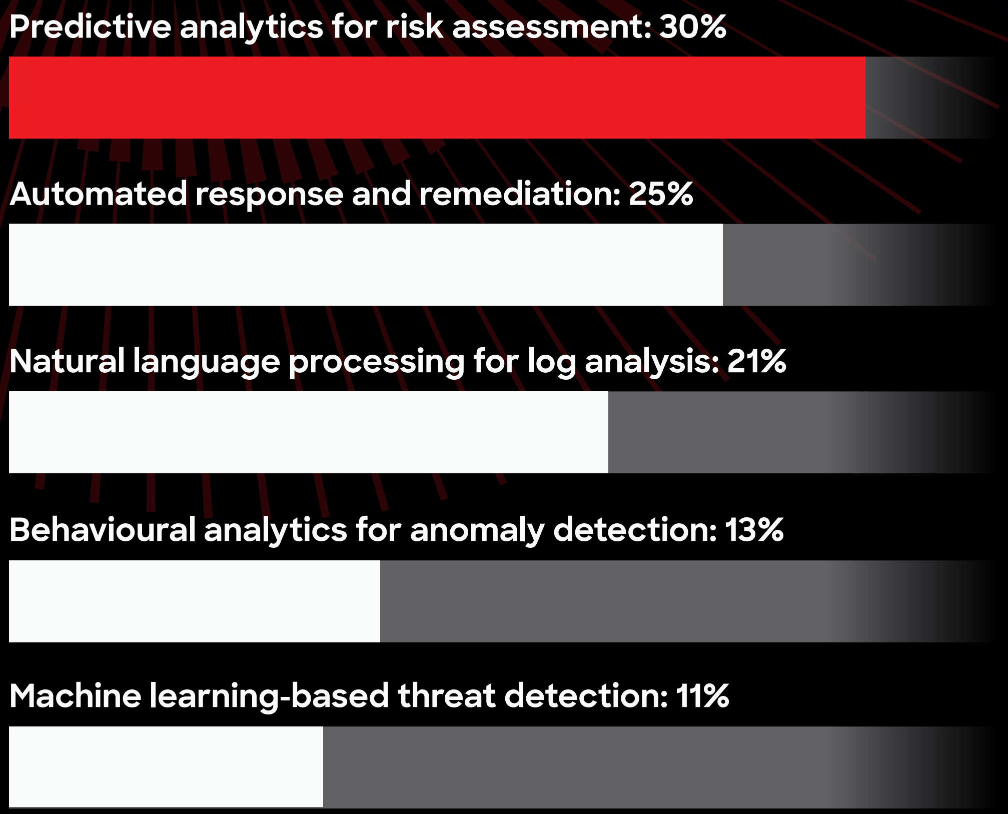
In your opinion, what is the biggest impact of security-related downtime on your organisation?



KEY INSIGHTS

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?



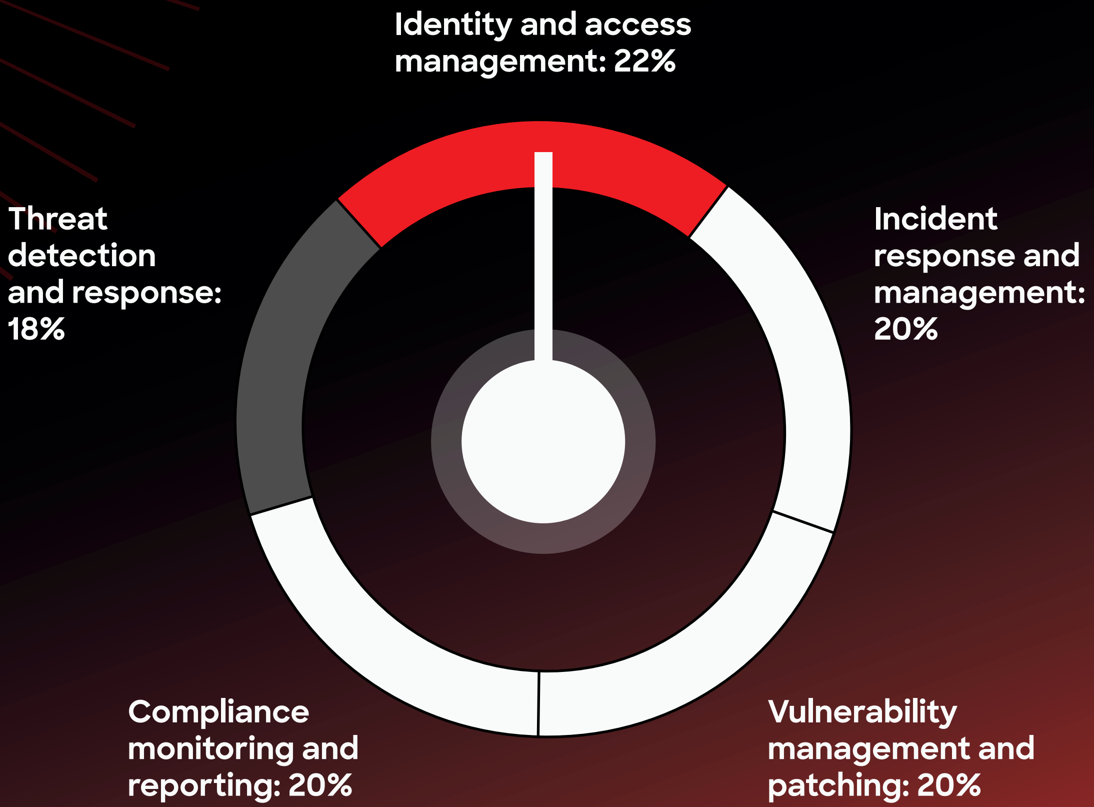
KEY INSIGHTS

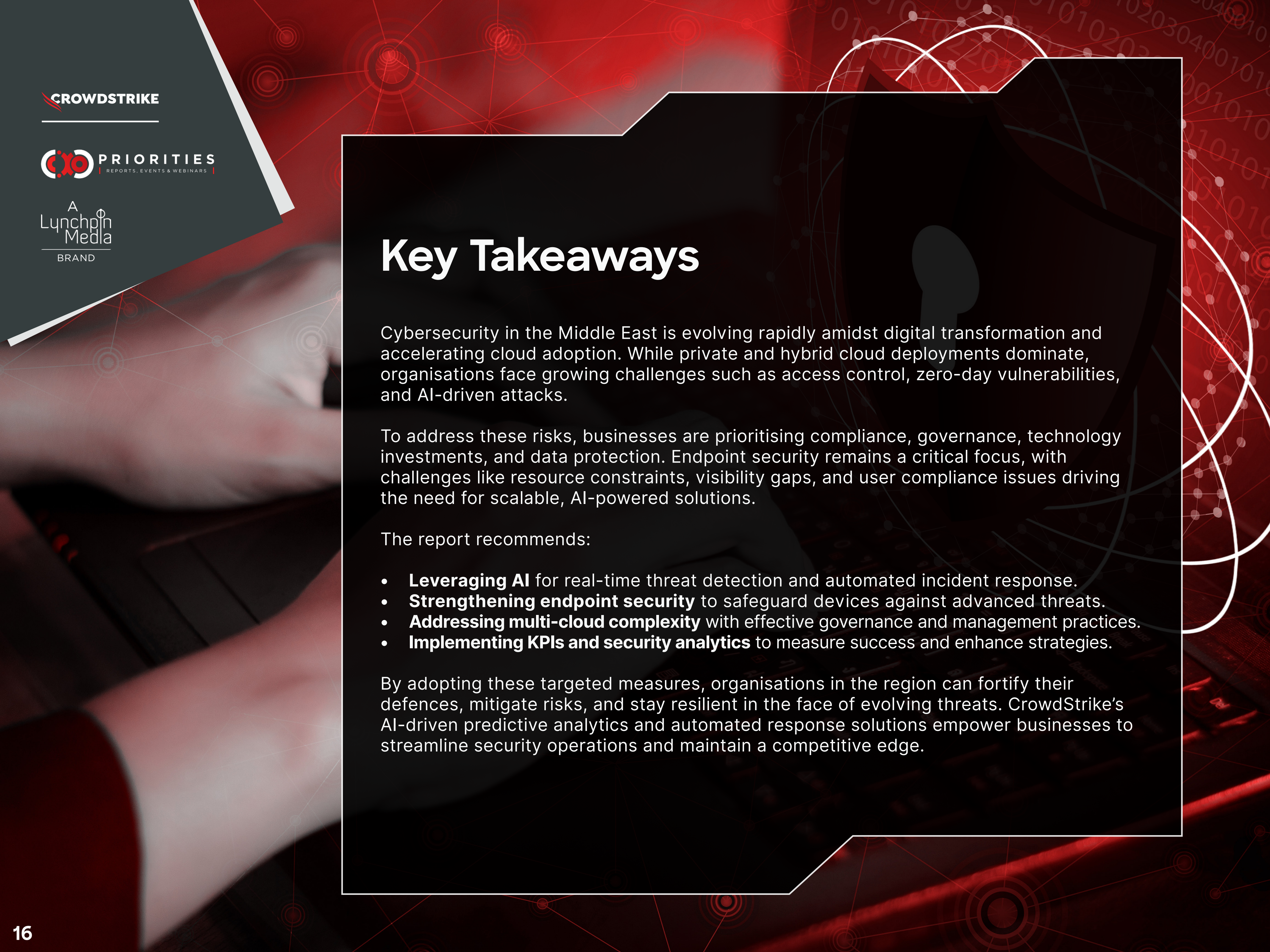
The survey reveals a growing reliance on AI tools for security, with **predictive analytics (30%)** and **automated response (25%)** being the most widely adopted. This shift reflects the industry's move toward proactive threat mitigation and reducing manual intervention in incident response in the Middle 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 INSIGHTS

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.





Key Takeaways

Cybersecurity in the Middle East is evolving rapidly amidst digital transformation and accelerating cloud adoption. While private and hybrid cloud deployments dominate, organisations face growing challenges such as access control, zero-day vulnerabilities, and AI-driven attacks.

To address these risks, businesses are prioritising compliance, governance, technology investments, and data protection. Endpoint security remains a critical focus, with challenges like resource constraints, visibility gaps, and user compliance issues driving the need for scalable, AI-powered solutions.

The report recommends:

- **Leveraging AI** for real-time threat detection and automated incident response.
- **Strengthening endpoint security** to safeguard devices against advanced threats.
- **Addressing multi-cloud complexity** with effective governance and management practices.
- **Implementing KPIs and security analytics** to measure success and enhance strategies.

By adopting these targeted measures, organisations in the region can fortify their defences, mitigate risks, and stay resilient in the face of evolving threats. CrowdStrike's AI-driven predictive analytics and automated response solutions empower businesses to streamline security operations and maintain a competitive edge.

CROWDSTRIKE

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.

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