InsiderSecurity Report on Asia-Pacific's State of Cloud Security 2025

InsiderSecurity

Introduction

As organisations across the Asia-Pacific (APAC) region accelerate their cloud adoption journey, the need for robust security measures has never been more critical. While cloud computing unlocks new levels of scalability, efficiency, and innovation, it also introduces significant security risks that businesses must navigate to safeguard their digital assets.

The **Asia-Pacific's State of Cloud Security 2025** report provides insights into the evolving cloud security landscape, highlighting the challenges, concerns, and priorities of organisations operating in the region. Drawing from a comprehensive survey of **hundreds of industry professionals,** including **CISOs, CTOs, IT Managers, and Security Analysts,** this report examines the **state of cloud security adoption, common vulnerabilities, and the most effective solutions organisations are implementing.**

Key focus areas of this report include:

- **Cloud Security Readiness:** Evaluating how well organisations are prepared to secure their cloud environments.
- **Common Security Threats:** Identifying top risks such as misconfigurations, account hijacking, and compliance challenges.
- **Adoption of Security Tools:** Analysing the strategies enterprises use to mitigate threats.
- **Best Practices and Recommendations:** Providing actionable insights to strengthen cloud security frameworks.

With **80% of organisations planning to further adopt cloud security measures** in the near future, the insights from this report will help businesses **enhance their cybersecurity strategies, minimize risks, and ensure regulatory compliance** while leveraging cloud technology for growth.

Executive Summary

Cloud security remains a top concern for organisations in the APAC region, with 72% of surveyed companies acknowledging blind spots in their cloud security tools. As cloud adoption grows, so does the complexity of securing multi-cloud environments, enforcing compliance, and managing identity and access controls effectively.

Key findings from this study include:

Cloud Security Readiness:

35% **35%** of organisations experienced a data breach in the past 6 months.

64% **64%** cite hijacking as a primary security challenge, followed by

62% **62%** concerned about shadow cloud IT services.

80% **80%** of organisations struggle with compliance,

76% while **76%** cite solutions that couldn't be extended for business requirements as a key issue

72% **72%** are concerned about hijacked SaaS accounts

53% **53%** report misconfigurations as a top SaaS security issue

9% **9%** of organisations monitor configurations continuously

80% **80% of organisations** plan to increase adoption of cloud security tools.

Despite proactive efforts, organisations continue to face challenges related to human error, misconfigurations, compliance, and the increasing complexity of multi-cloud environments. To address these issues, enterprises must adopt comprehensive security strategies, enhance visibility, automate security processes, and invest in employee training.

Table of Contents

Introduction 2

Executive Summary 3

Cloud Technology Adoption 5

Cloud Security Incidents and Confidence Levels 6

Cloud Security Challenges 7

Misconfiguration 8

Cloud Security Investments and Challenges 9

SaaS Investments and Challenges 11

Conclusion and Recommendations 13

Introducing CSX:
Your Comprehensive Cloud Security Solution 16

Methodology & Demographics 17

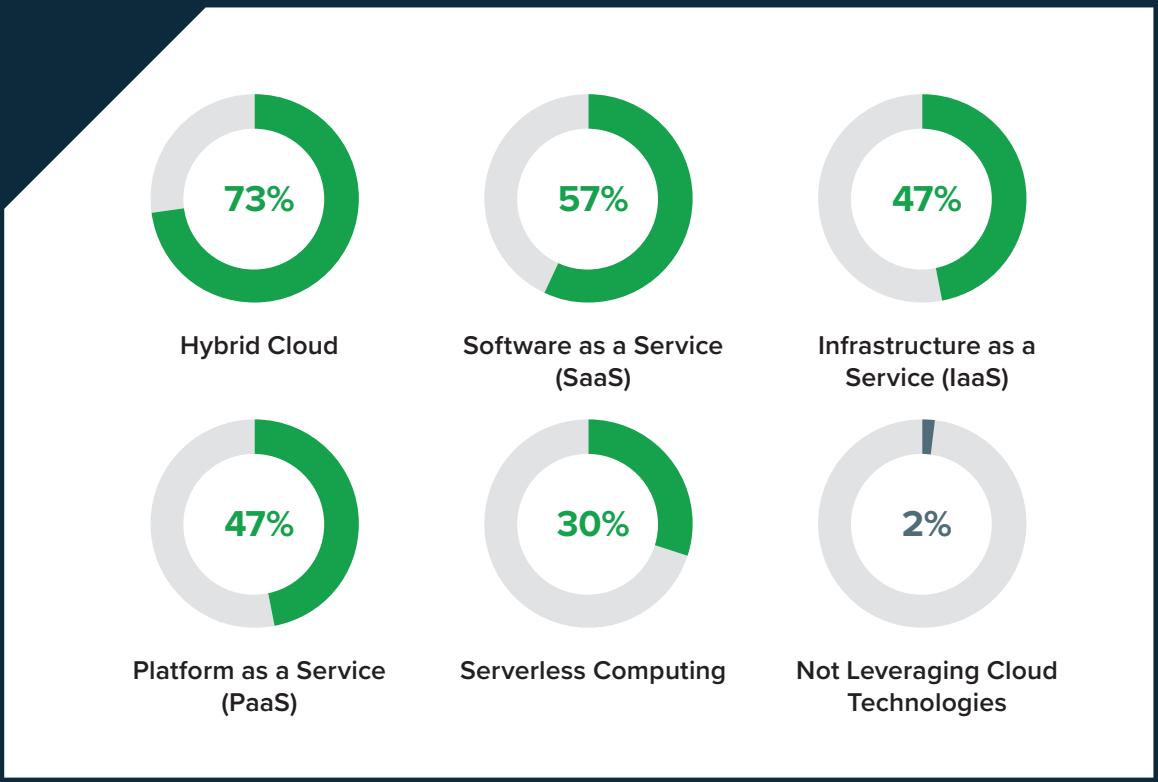
Cloud Technology Adoption

Adoption Rates of Cloud Technologies

Many organisations embrace Hybrid Cloud (73%) to balance control and flexibility by blending private and public cloud infrastructures. This approach is especially beneficial for industries needing secure environments for sensitive data while still aiming to leverage the scalability of public cloud services. The growing use of SaaS (57%) highlights a shift toward subscription-based models that reduce hosting overhead and accelerate deployment times.

The equal adoption rates of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), both at 47%, indicate a balanced approach to cloud adoption. This suggests that organizations are not only migrating existing applications to virtualized cloud instances but are also embracing cloud-native architecture solutions. Despite Serverless Computing being an emerging option with a 30% adoption rate, its growing popularity highlights an increasing interest in cloud-native software development.

The data reveals a significant trend towards integrating cloud-based solutions within the corporate landscape:



Cloud Security Incidents and Confidence Levels

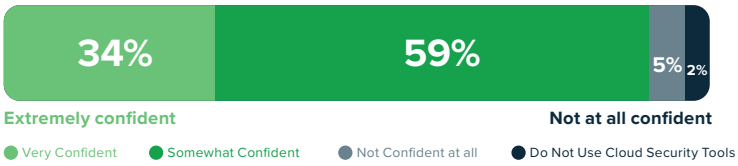
Cloud Security Incidents

A concerning 35% of organisations reported experiencing a data breach within the past six months. This finding suggests that organisations should prioritise enhancing their cloud security measures and improving incident detection and reporting. Continuous monitoring and regular security audits can help organisations better understand their security posture and reduce the risk of cloud-related security incidents and data breaches.

35% of Organisations Experienced a Data Breach in the Past Six Months

With multi-cloud complexity on the rise, it is not surprising that only 34% of cybersecurity professionals are very confident in their organisation's cloud security posture. The survey results emphasise the importance of continuous improvement in cloud security strategies, ongoing training, and the implementation of best practices to increase confidence and ensure a robust security posture in the face of evolving threats.

Confidence in Cloud Security Solutions

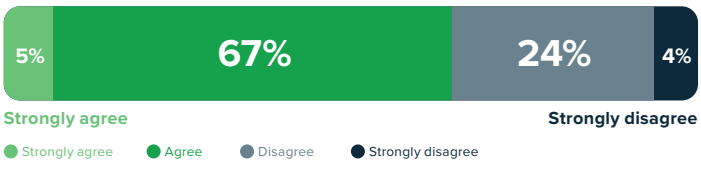


Analysis of Cloud Security Perception

The prevalence of data breaches and the recognition of blind spots illustrate a gap between existing security measures and the actual threats targeting cloud environments.

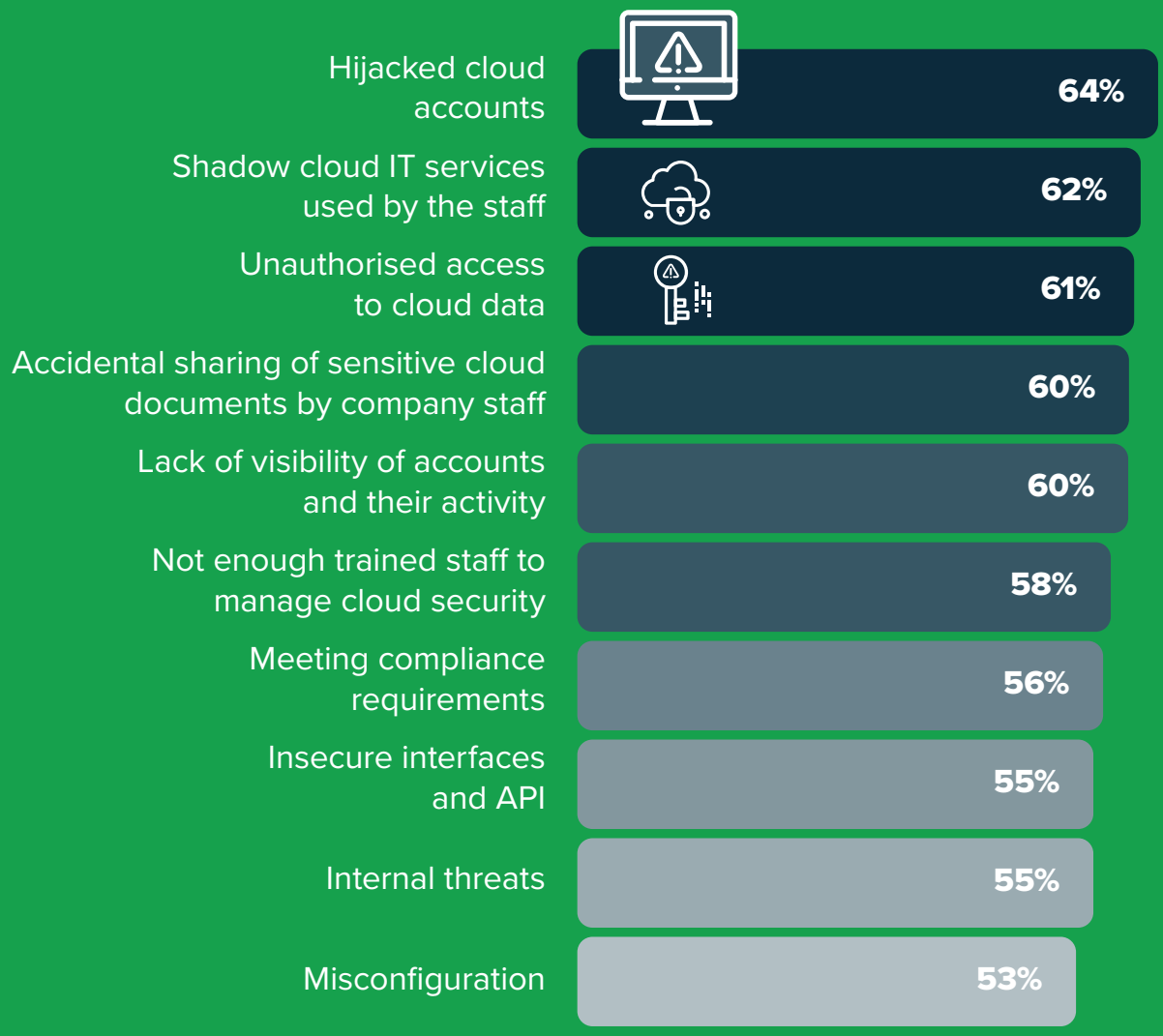
While a subset of organisations feels fairly confident, the majority seek to bolster their capabilities, emphasising the need for more sophisticated solutions and continuous monitoring.

More than half (72%) of organisations agree security tools have blind spots.



Cloud Security Challenges

Top Cloud Security Challenges



The survey reveals a critical interplay between human factors and technical vulnerabilities in cloud environments. Hijacked cloud accounts (64%) and unauthorised data access (61%) underscore the risks posed by compromised credentials and insufficient access controls. Meanwhile, shadow IT (62%) and accidental data sharing (60%) highlight the persistent challenge of human error, where employees' use of unapproved services or mishandling of sensitive documents inadvertently exposes organisations to breaches.

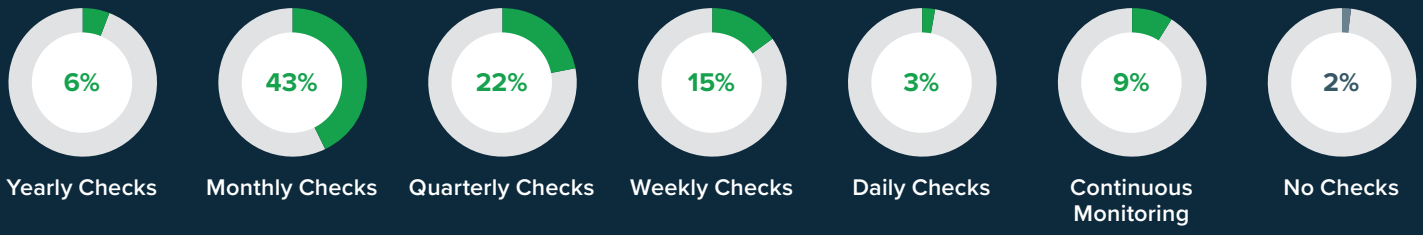
A striking 58% of organisations lack enough trained staff to manage cloud security, exacerbating these risks. This skills gap leaves businesses vulnerable to evolving threats and complicates compliance efforts, with 56% struggling to meet regulatory requirements.

Misconfiguration

The Misconfiguration Paradox

Despite misconfiguration being recognised as a significant risk (53%), the level of checks for misconfiguration is generally inadequate. Only a small minority of organisations (9%) employ continuous monitoring. The vast majority (71%) perform checks monthly or less frequently, creating dangerous windows of vulnerability during which misconfigurations can remain undetected and unresolved.

Frequency of Configuration Checks



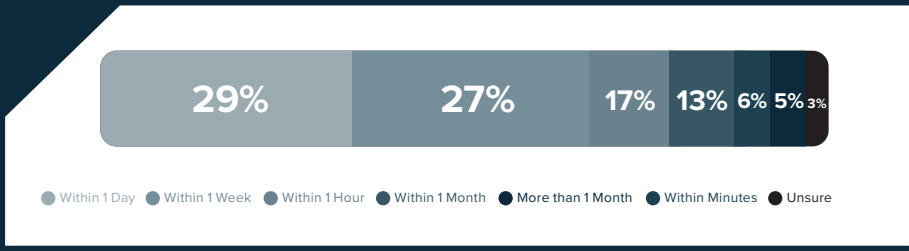
Importance of Regular Configuration Checks

Regular configuration checks play a pivotal role in identifying and correcting misconfigurations before they evolve into larger security incidents. By proactively reviewing configurations, organisations can mitigate risks tied to inadequate or outdated settings, reduce compliance oversights, and ensure that their cloud environments operate efficiently.

Misconfiguration Resolution Timeline Concerns

When asked about the time taken to resolve detected misconfigurations, 29% of organisations can fix issues within one day, and 27% manage to do so within one week. However, 6% admitted that more than one month could pass before a misconfiguration is completely resolved.

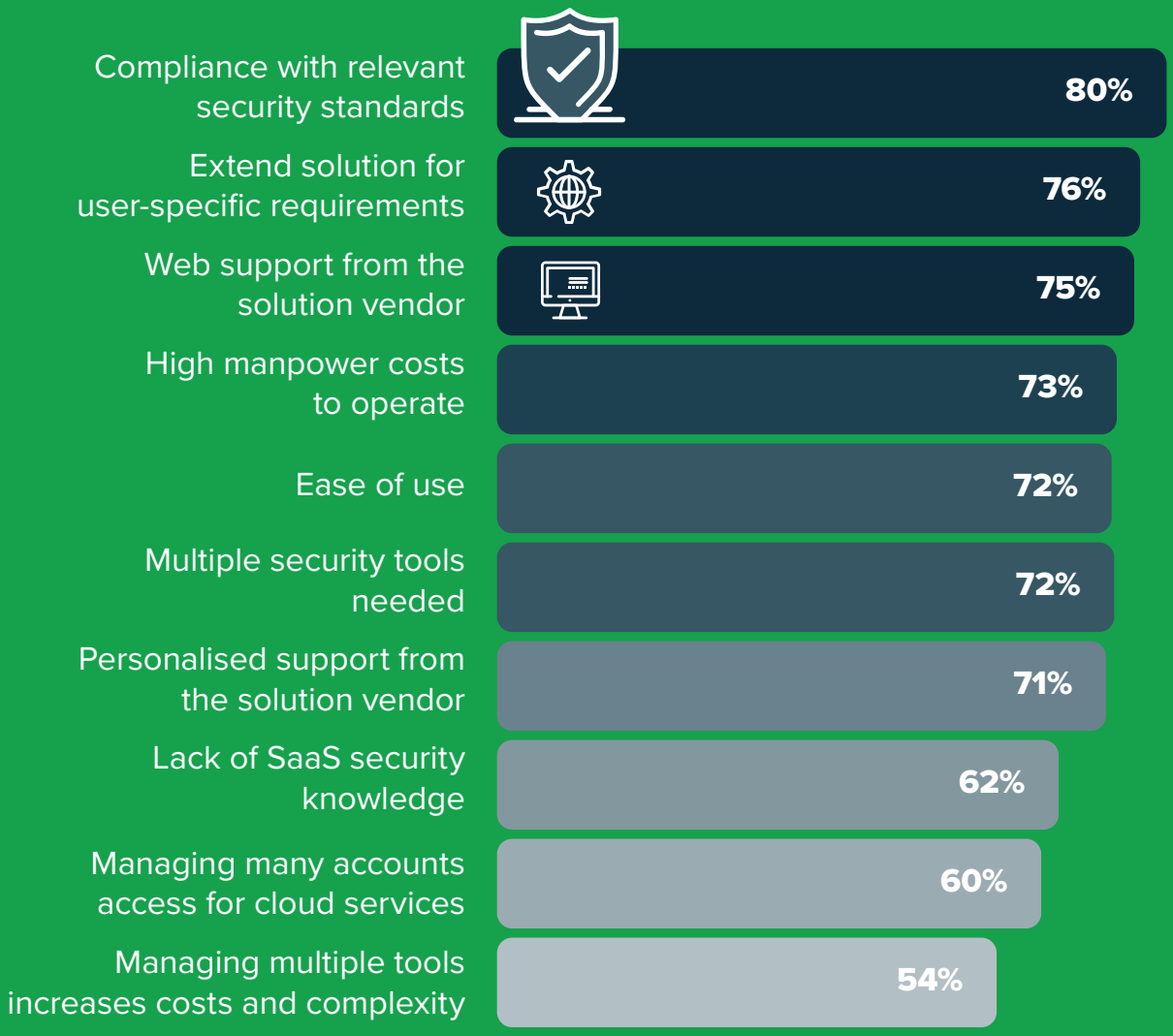
When these resolution timelines are viewed alongside the infrequent checking schedules, the security exposure becomes clear: an organisation performing monthly checks that take a week to resolve issues could be exposed to known vulnerabilities for up to 37 days - more than enough time for malicious actors to exploit these weaknesses.



Delays in identifying and fixing misconfigurations substantially increase the likelihood of unauthorised access or data breaches. Quick resolution, preferably automated, is crucial for maintaining a stable security posture and preventing spiralling costs or reputational damage.

Cloud Security Investments and Challenges

Top challenges that users have with current cloud security tools



Analysis of Reported Challenges

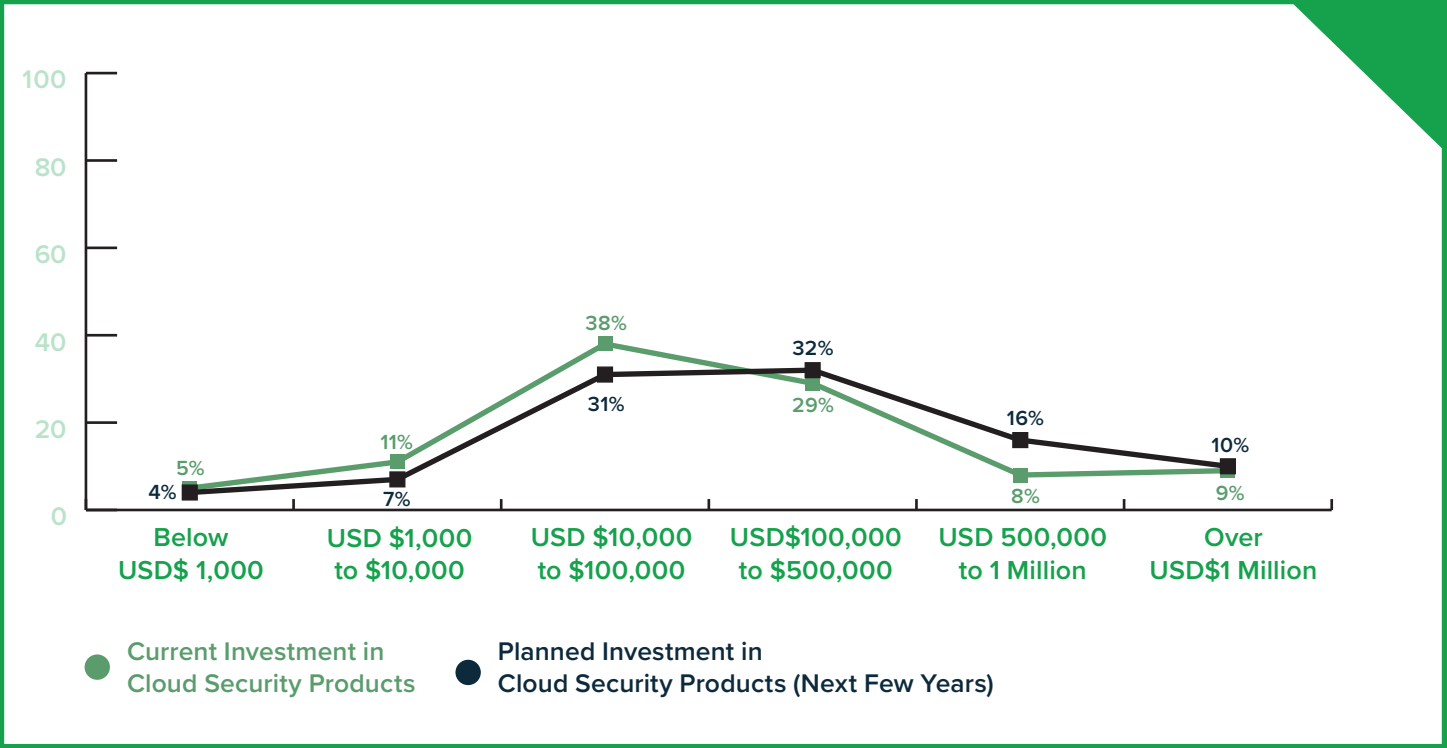
The survey findings reveal that compliance with security standards remains the most pressing challenge, with 80% of respondents struggling to meet regulatory requirements, underscoring the complexity of cloud governance. Additionally, 76% of organisations require solutions that can be tailored to their specific needs, indicating that many existing security tools lack the flexibility needed for diverse business environments. Vendor support is also a critical issue, with 75% emphasising the importance of reliable web support, and 71% seeking more personalised support, highlighting the need for better guidance in deploying and managing cloud security solutions.

Operational efficiency is another key concern, as 73% of organisations prioritise reducing manpower costs, and 72% emphasise ease of use, suggesting that many cloud security solutions are perceived as resource-intensive or complex. The challenge of multiple security tools (72%) reflects the growing challenge of managing fragmented security tools across multi-cloud environments. Moreover, SaaS security knowledge gaps (62%) and difficulties in managing account access (60%) expose organisations to potential misconfigurations and unauthorised access risks.

These findings highlight the urgent need for security tools that are more adaptable and user-friendly to help businesses navigate compliance, operational efficiency, and security management in increasingly complex cloud environments.

Adoption of Cloud Security Tools

80% of organisations planning to further adopt cloud security measures reinforce the critical importance of proactive threat detection and a well-structured incident response strategy.



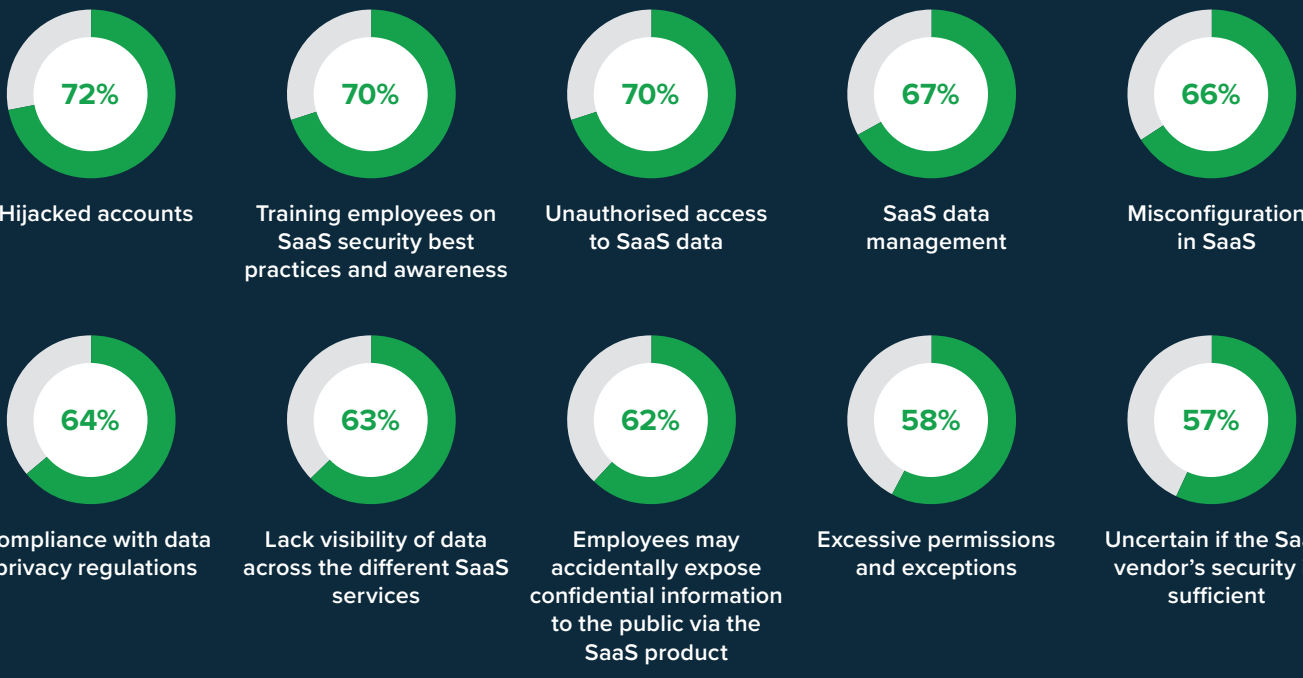
The surge in planned investments indicates that cloud security remains at the forefront of IT and executive priorities. Nevertheless, compliance requirements, multi-cloud strategies, and skills shortages remain pivotal concerns.

SaaS Investments and Challenges

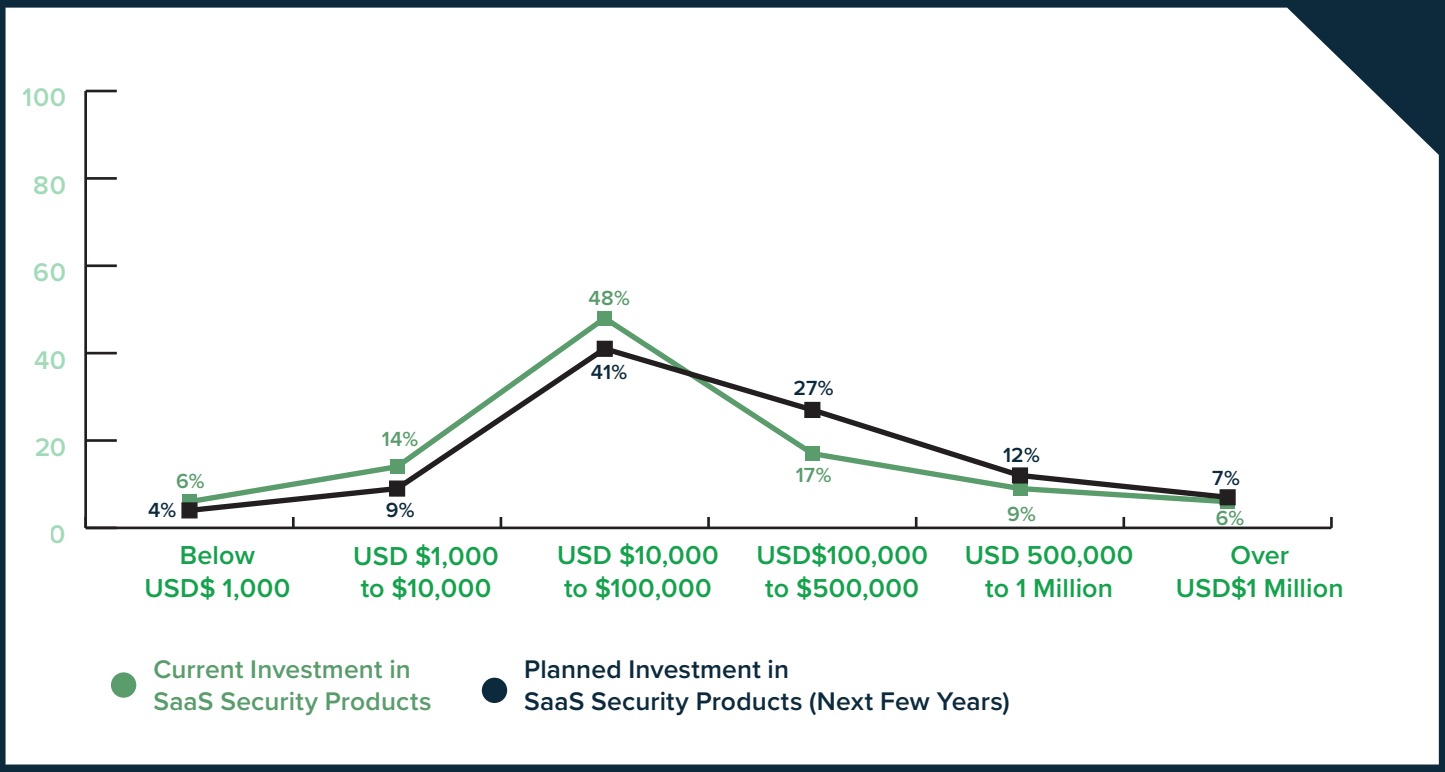
It's important to note that a majority of organisations are also managing multiple cloud SaaS providers within their security landscape. The survey shows that Microsoft 365 leads the market, with 68% of surveyed organisations deploying their cloud services, followed by Google Workspace (47%) and Salesforce (33%).

Top SaaS Solutions in Use

Top SaaS Cybersecurity Challenges



Investment Trends in SaaS Security



Analysis of SaaS Security Outlook

The strong reliance on popular SaaS applications—such as Microsoft 365 and Google Workspace—reflects their crucial role in modern business operations. However, the pervasive threat of account hijacking (90%) underscores the urgent need for robust access controls, continuous monitoring, and ongoing training for end users. The willingness to invest more in SaaS security highlights the importance of safeguarding these often-mission-critical services.

Conclusion and Recommendations

The rapid adoption of cloud technologies in the APAC region has unlocked new levels of scalability, efficiency, and innovation for organisations. However, this surge has also introduced a complex array of security challenges that threaten data integrity and business continuity.

Key Findings:

- Blind Spots in Cloud Security Tools: 72% of organisations believe their current cloud security tools have blind spots, indicating insufficient visibility and protection across their cloud environments.
- Frequent Data Breaches: 35% of organisations experienced a data breach in the past six months, underscoring the urgency for enhanced cloud security measures.
- Primary Security Challenges:
  - Hijacked cloud accounts **64%**
  - Shadow cloud IT services used by the staff **62%**
  - Unauthorised access to cloud data **61%**
  - Accidental sharing of sensitive cloud documents **60%**
  - Lack of visibility of accounts and their activity **60%**
  - Not enough trained staff to manage cloud security **58%**
- Skills Gap: 58% of organisations are concerned about the lack of trained staff to manage cloud security effectively.

Despite these challenges, there is a strong commitment to improving cloud security:

- 80% of organisations plan to increase their adoption of cloud security tools and services in the next three years.
- Significant investments are being planned, with 32% allocating up to USD 500,000 and 10% planning to invest more than USD 1 million in cloud security products.

Recommendations

To navigate the complex landscape of cloud security, organisations should consider the following strategic actions:

1. **Adopt a Phased Cloud Security Strategy Based on Business Risk**
   Cloud environments are complex, and securing every layer—SaaS, IaaS, and PaaS—at once can overwhelm teams and lead to gaps. A phased, risk-based approach helps organisations focus first on what's most critical, then scale security efforts progressively.
   I. Focus first on high-risk, high-usage platforms (e.g. widely adopted SaaS applications like Microsoft 365).
   II. Use tools such as InsiderSecurity to roll out security in stages—starting where incidents are most likely, then expanding coverage.
   III. Align security rollout with operational maturity, ensuring each step delivers measurable value before scaling further.

2. **Secure Critical SaaS Platforms Like Microsoft 365**
   Microsoft 365's widespread adoption (68%) introduces unique risks—hijacked accounts, accidental data exposure, and unauthorised third-party apps. InsiderSecurity addresses these SaaS-specific challenges by:
   - Detecting account compromises: AI-driven UEBA identifies suspicious logins (e.g., brute-force attacks, unusual locations).
   - Preventing accidental exposure: Monitors sensitive file activity in OneDrive/SharePoint and alerts on risky sharing.
   - Auditing third-party app permissions: Flags unapproved integrations with excessive access to M365 data.
   - Seamless integration: Unifies security for M365 and other SaaS apps, reducing security tool sprawl

3. **Enhance Visibility and Control**
   Achieve comprehensive visibility over your cloud assets and configurations to identify and mitigate risks promptly.
   - InsiderSecurity automatically discovers your cloud assets and inventories, providing a comprehensive overview and flagging out misconfigurations.

4. **Strengthen Access Management**
   Implement strict identity and access management policies to control permissions and prevent unauthorised access.
   - InsiderSecurity detects suspicious account activities and privilege escalations, and enables immediate remediation.

5. **Automate Misconfiguration Detection and Remediation**
   Utilise tools that identify and correct misconfigurations automatically to reduce the risk of security breaches.
   - InsiderSecurity helps maintain secure configurations with notifications and recommendations aligned with security standards and best practices.

6. **Address Compliance and Regulatory Requirements**
   Ensure your cloud security solutions assist in meeting industry-specific compliance standards and regulatory requirements.
   - Insider Security aids in covering the gaps in the shared responsibility model, ensuring compliance obligations are met and maintained.

7. **Invest in Security Skills and Training**
   Bridge the cybersecurity skills gap by providing training and resources to your IT and security teams.
   - Simplify security management with user-friendly solutions like InsiderSecurity, reducing the complexity and learning curve.

8. **Leverage Artificial Intelligence and Machine Learning**
   Enhance threat detection and response capabilities by adopting AI-driven security solutions.
   - Insider Security leverages UEBA (User and Entity Behaviour Analytics) and machine learning to detect malicious activities, reduce false positives, and decrease investigation times.

9. **Prepare for Incident Response and Recovery**
   Develop and maintain an incident response plan tailored to cloud environments to minimise the impact of security incidents.
   - InsiderSecurity provides actionable remediation and response capabilities directly within the dashboard, enabling swift action when threats are detected.

Introducing CSX: Simplify M365 Data Security

InsiderSecurity's CSX is designed to address key challenges outlined in this report. CSX secures SaaS environments like Microsoft 365 and Google Workspace.

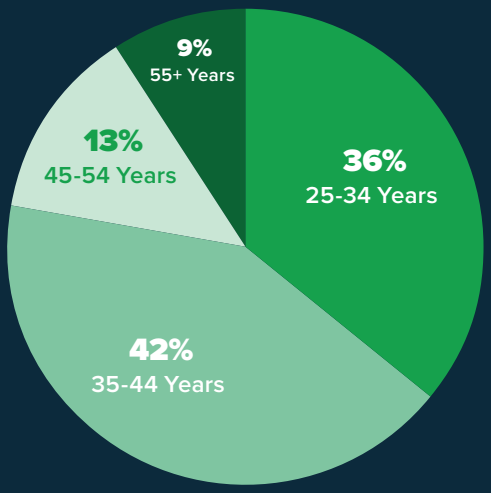
Key Features of CSX:

- **Cover the gaps in the shared responsibility model in cloud security**
  Cloud service providers such as M365 take care of areas of security under the Shared Responsibility Model in cloud security. Significant areas of security remain the user's responsibility. CSX helps to cover these security gaps that are not covered by the service providers.
- **Secure your critical SaaS platforms**
  Designed to monitor and secure SaaS platforms like M365 and Google Workspace, where compromised accounts and misconfigurations are common risks.
- **Simplify SaaS security**
  Using AI, CSX automates and simplifies M365 security monitoring. CSX makes it simple to monitor user behaviour, detect threats, and respond to incidents.
- **Detect malicious and insider activity**
  Identify compromised accounts, suspicious administrator actions, and insider threats such as staff sending sensitive data to personal emails.
- **Security visibility into your SaaS assets**
  Automatically analyse user permissions, third-party app access, and data sharing behaviours to identify cyber risks and support governance.
- **Uncover misconfigurations and accidental data leak**
  Misconfiguration is one of the top causes in cloud data breaches. CSX helps to detect for misconfiguration, including accidental sharing of sensitive files.

For organisations seeking to enhance their cloud security posture and address the challenges identified in this report, **CSX offers a robust, intelligent, and user-friendly solution.**

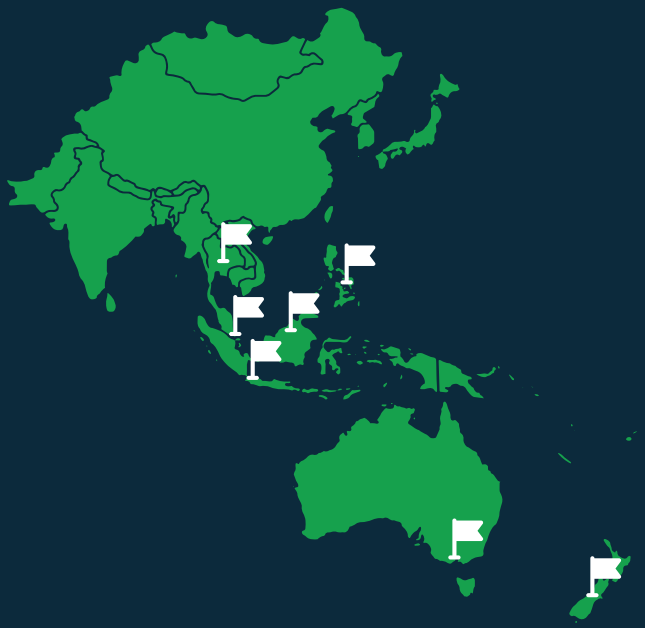
Methodology & Demographics

Age Distribution of Respondents

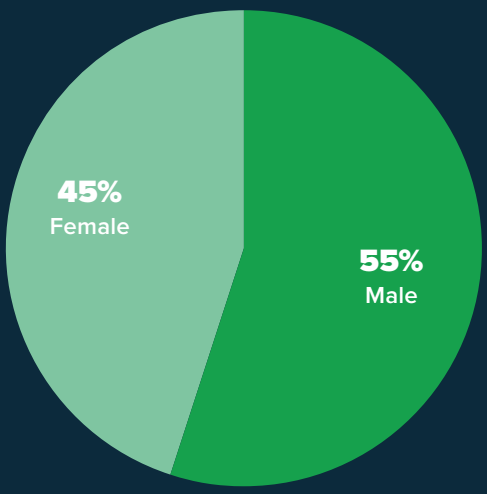


Geographic Representation

- Philippines
- Thailand
- New Zealand
- Australia
- Singapore
- Indonesia
- Malaysia

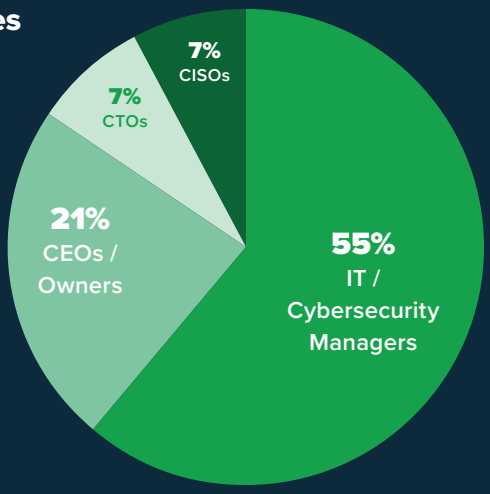


Gender Composition

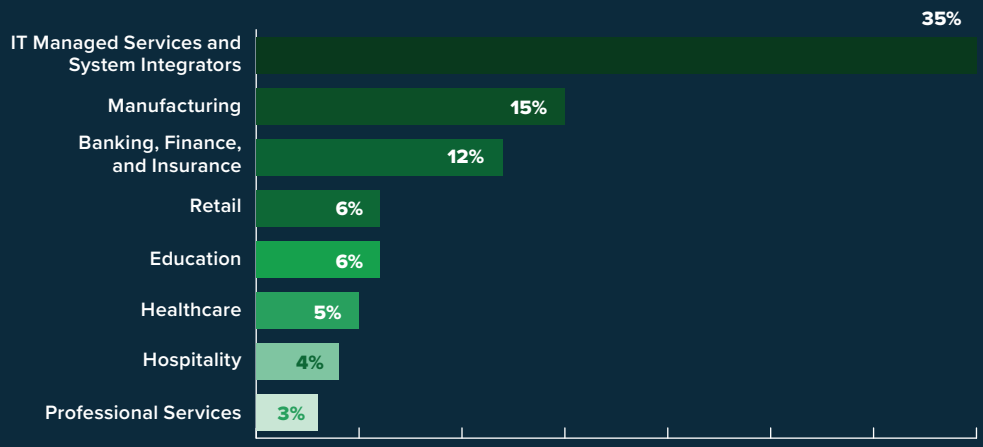


Methodology & Demographics

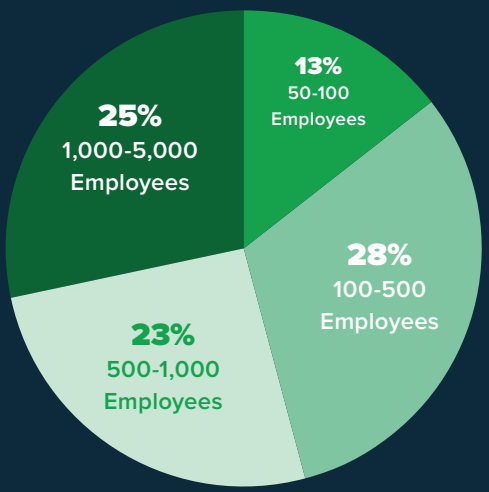
Organisational Roles



Industry Representation



Company Size



Methodology

The survey was conducted by InsiderSecurity, collecting responses across various industries, roles, and countries in the APAC region. The diverse demographics provide comprehensive insights into cloud security adoption and challenges.

About InsiderSecurity

InsiderSecurity is an award-winning cybersecurity software company with cutting-edge solutions developed in Singapore and Malaysia. Our expert engineering team, rooted in the ASEAN region, delivers robust security and unparalleled support to our clients. We are the first cybersecurity software company in ASEAN to achieve CSA STAR Level 2 certification, a globally recognised benchmark in cloud security, and also hold ISO 27001 accreditation.

In addition, InsiderSecurity was the first company accredited by Singapore's IMDA for User and Entity Behaviour Analytics, demonstrating our pioneering capabilities in proactive threat detection. InsiderSecurity has also been recognised by The Straits Times, naming us one of "Singapore's Fastest-Growing Companies 2025" and by the Financial Times as one of the "High-Growth Companies Asia-Pacific 2025."

Trusted by Singapore government agencies, critical information infrastructure (CII) providers, and major enterprises, our solutions offer reliable and comprehensive cybersecurity tailored to the unique challenges of the region.

FT FINANCIAL TIMES
statista
HIGH-GROWTH COMPANIES ASIA-PACIFIC 2025

THE STRAITS TIMES
Distinguished Member of
Singapore's Fastest Growing Companies
2025
statista

STAR LEVEL TWO: THIRD-PARTY AUDIT
STAR LEVEL TWO
SECURITY TRUST ASSURANCE & RISK

Information Security Management System
ISO 27001
Certified

CONTACT DETAILS

+65 6270 4029
hello@insidersecurity.co
2 International Business Park, #06-01, Singapore 609930
www.insidersecurity.co

InsiderSecurity