

Micro Survey Report

aopg  
Insights

RESEARCH - ANALYSIS - ANSWERS



 **CDNetworks**  
Accelerate. Secure. Control.

# The State of Cloud Security: Are Businesses Addressing Key Vulnerabilities in 2024?

# Table of Content

Introduction	1
Common Cyber Threats Impacting Cloud Security	2
The Preparedness Gap	4
Defence-in-Depth Is the Way to Protect the Cloud	5
The Pressing Need for Secured API Management	8
Intelligence Is Imperative	10
Cybersecurity Is an Ongoing, Never-Ending Battle	11
A Final Word: Ensuring Continuous Vigilance and Protection	14
Notes On Survey Methodology	16

# Introduction

Cloud computing has transformed how businesses operate, offering unparalleled flexibility, scalability, and cost-effectiveness. However, this shift has introduced new security concerns, as sensitive data resides in cloud environments, exposing it to increasingly sophisticated cyber threats.

With cloud security more critical than ever in today's digital age, the pressing question is: Are organisations in Southeast Asia prepared?

To find out, AOPG Insights partnered with [CDNetworks](#), a global leader in Content Delivery Networks (CDN) and conducted a micro-survey to assess cloud security readiness among organisations in the region. The findings were mixed, offering encouraging insights that suggest progress, but also highlighting areas of concern that require immediate attention.

Key takeaways include:

- ❏ **Gaps in Cybersecurity Preparedness:** Many companies acknowledge the importance of cybersecurity but face significant gaps in preparedness and resource allocation, particularly in areas like API security, continuous monitoring, and advanced threat intelligence.
- ❏ **Mixed Results in Cybersecurity Practices:** While there is increased regional awareness and prioritisation of multi-layered cloud security measures, notable deficiencies persist, especially in API management and data-driven security, indicating a need for improved practices and solutions.
- ❏ **Rising Interest in MSSPs:** There is a growing trend towards considering Managed Security Service Providers (MSSPs) to address cloud and security needs, offering a strategic advantage for companies with resource limitations or those looking to enhance their security posture.

We would like to extend our sincere thanks to CDNetworks for their invaluable support in this crucial industry research. We trust that this report will serve as a practical resource for cybersecurity leaders and practitioners, aiding them in navigating the complexities of cloud security and enhancing their strategies to protect their organisations against evolving cyber threats.

# Common Cyber Threats Impacting Cloud Security

The cloud offers immense benefits for businesses, but it also presents a new attack surface for malicious actors. Today's cyber threats are more sophisticated and widespread than ever before, with criminals constantly developing new methods to exploit vulnerabilities, steal data, and disrupt operations.

Here's a glimpse into some of the serious threats organisations face in the cloud environment:

## **Distributed Denial-of-Service (DDoS)**

**Attacks:** These attacks overwhelm a system with traffic, making it unavailable to legitimate users environment.

## **Automated Bot Attacks:**

Malicious bots can be used to automate tasks such as credential stuffing, account takeover attempts, and scraping sensitive data.

## **Ransomware:**

This type of malware encrypts an organisation's data, rendering it inaccessible until a ransom is paid.

## **SQL Injection:**

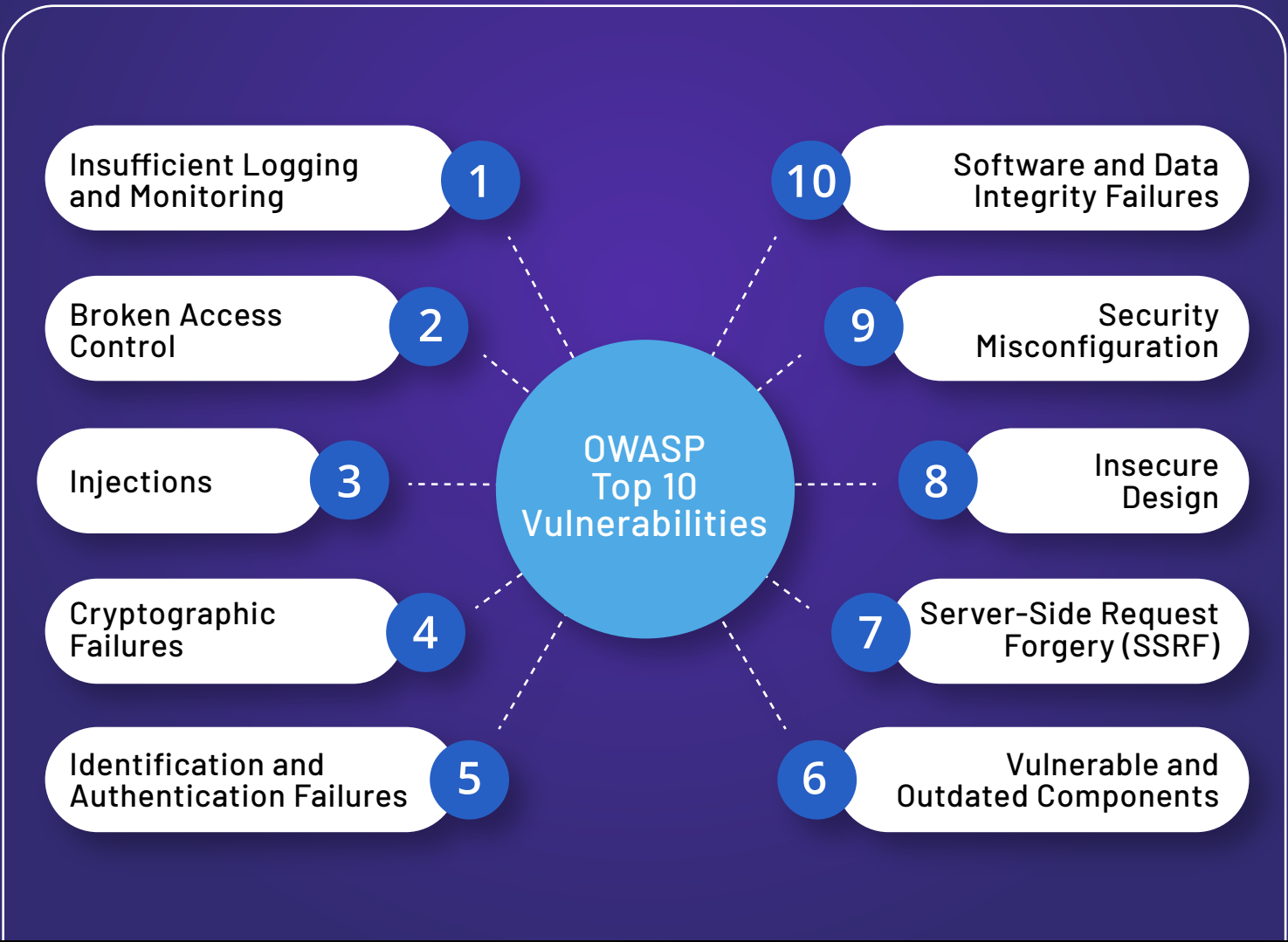
Attackers exploit vulnerabilities in web applications to inject malicious code that can steal sensitive data.

## **Cross-Site Scripting (XSS):**

Hackers inject malicious scripts into websites that can steal user data or redirect them to phishing sites.



These are just a few examples of the evolving threats organisations face in the cloud. For a more comprehensive view of the most critical security vulnerabilities that attackers commonly exploit, we can refer to the [OWASP Top 10](#), a well-respected industry standard.



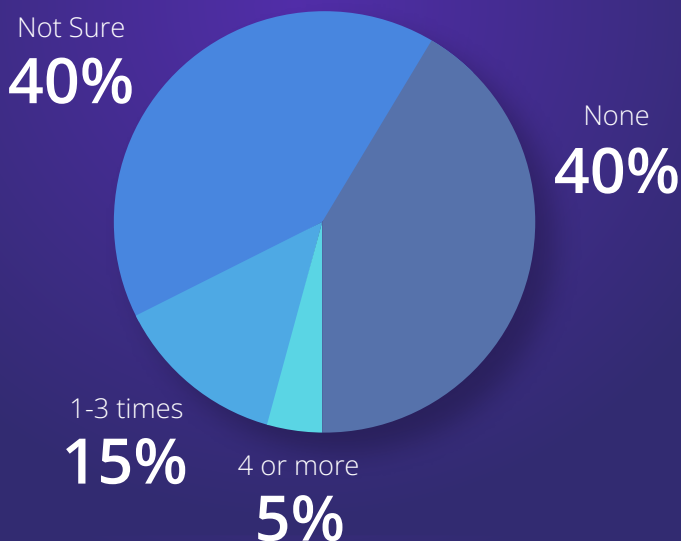
In light of these threats, the key question is: Are organisations ready to address them?



## The Preparedness Gap

Our survey sheds light on this critical question. We asked respondents about the number of cyber attacks that significantly impacted their operations or security in the past year. The results paint a concerning picture.

How many cyber attacks, which significantly impacted your company's operations or security, has your company experienced in the past 12 month?



40% of companies reported no significant cyber attacks in the past 12 months. While this might seem positive on the surface, it doesn't necessarily mean they weren't targeted. These companies may have been attacked, but the attacks were unsuccessful or caused minimal damage.

Perhaps more troubling is the 40% of respondents who were unsure about cyber attacks. This significant number suggests a potential lack of awareness or inadequate security monitoring within their organisations.

Companies that are unaware of their cybersecurity posture are particularly vulnerable, as they cannot effectively address unseen threats. This lack of visibility can leave them exposed to ongoing attacks that slowly erode their security and potentially lead to a major breach down the line.

These findings highlight a potential preparedness gap. While some companies are actively fortifying their defences, a significant portion may be unknowingly exposed due to a lack of awareness, or insufficient resources dedicated to cybersecurity.



## Defence-in-Depth Is the Way to Protect the Cloud

As mentioned earlier, the cloud has become a big target for cybercriminals, expanding the attack surface exponentially and putting organisations at more risk of cyber attacks. This is why experts like CDNetworks recommend businesses take a **multi-layered approach to cloud security**, where multiple layers of security controls are deployed to protect the organisation's cloud environments from different threats.

This multi-layered approach, also called **defence-in-depth**, ensures that if one layer is compromised, additional layers of defence can still protect the system.



**To what extent does your company prioritise implementing multi-layered security measures in its cloud environment?**

Somewhat important, but not the top priority

**40%**

Critical priority

**51%**

Not a current priority

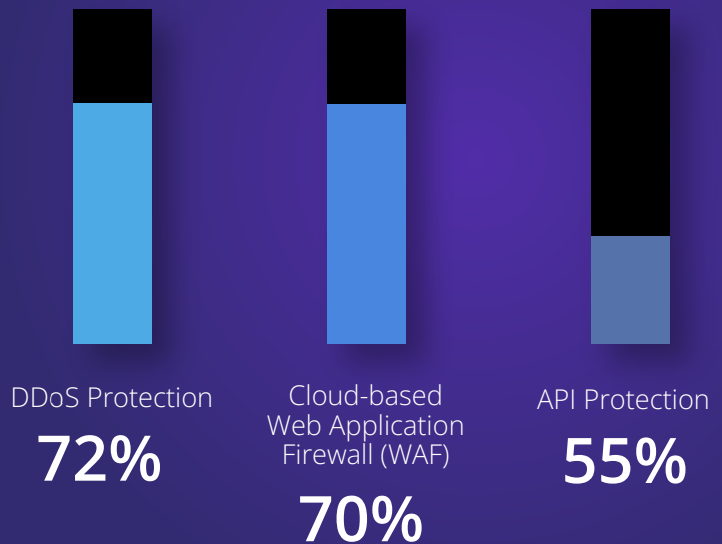
**9%**

It is an encompassing strategy for cloud security, and the survey results indicate a growing recognition of the importance of cloud security, as over half (51%) of the respondents have made it their top priority to implement multi-layered security measures.

However, it's also concerning that a significant portion (40%) view it as somewhat important but not the top priority, and a small number (9%) don't consider it a priority at all. These findings suggest that there is still room for improvement in cloud security awareness and practices.



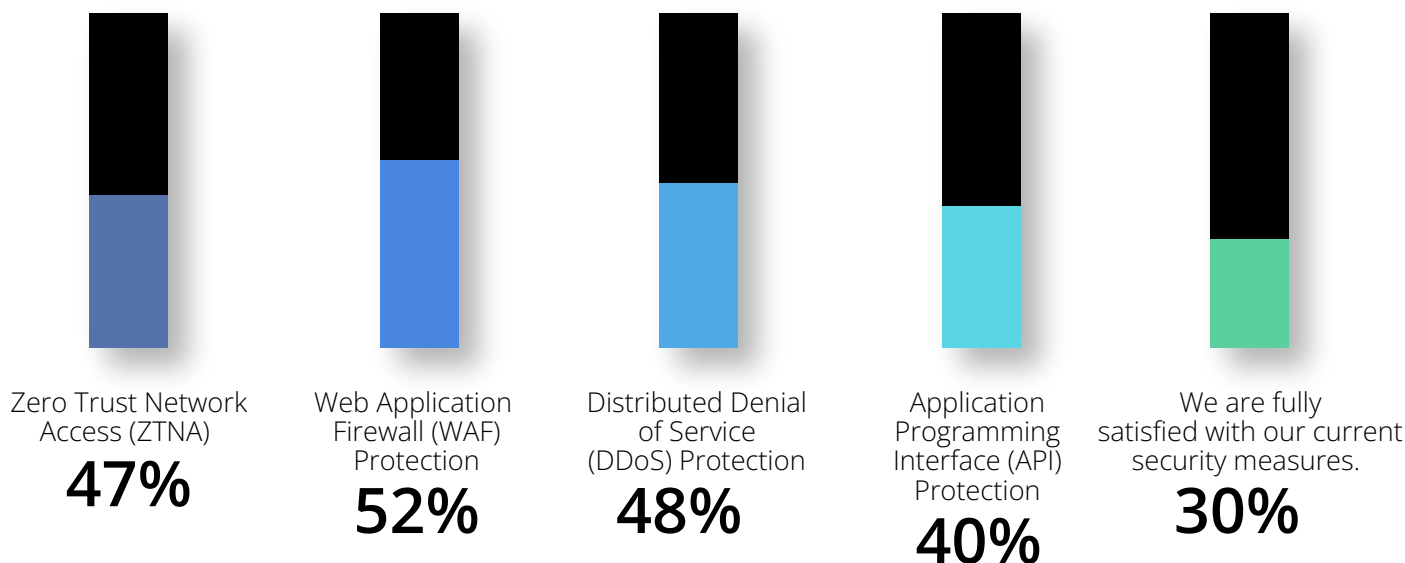
### Which security measures does your organisation use to protect its cloud environment?



Organisations' increasing awareness of the criticality of defence-in-depth likely explains why the survey respondents are primarily using Distributed Denial-of-Service (DDoS) protection (72%), cloud-based WAF (Web Application Firewall) (70%), and API protection (55%) to safeguard their organisations' cloud environment. These choices indicate a high awareness of [common cloud security threats](#), notably DDoS attacks, web application vulnerabilities, and unsecured APIs.



## In 2024, which of the following cybersecurity projects are prioritised for enhancement within your organisation?



These same three measures—DDoS protection, cloud WAF, and API protection—are also prioritised for improvement in 2024. This suggests that while companies are implementing these measures, they see room for optimisation and potentially a need for stronger solutions.

Evolving cybersecurity threats might explain why more organisations have zeroed in on these measures, with an eye towards staying ahead of new attack methods. It is also possible the current implementations might not be comprehensive enough such that they require additional features or functionalities. Companies might also be facing challenges integrating these tools with their existing security infrastructure or managing them effectively.

Zero Trust Network Access (ZTNA) is also getting lots of attention despite not being among the top three implemented security measures. Moving forward, though, 47% of organisations have prioritised ZTNA for improvement, suggesting a growing interest in this technology. Based on the maxim "[never trust, always verify](#)" proposed by John Kindervag, ZTNA can provide granular access control and enhance overall security posture.

The data so far suggests an undeniable focus on preventative measures, like DDoS, WAF, API protection, and ZTNA, rather than detection and response solutions. However, it should be noted that a well-rounded security strategy should also have mitigation protocols in place if an attack does occur.

# The Pressing Need for Secured API Management

While attacks such as malware or DDoS have been around for a long time, companies may benefit from paying more attention to API management in today's API economy era.

API vulnerabilities pose a significant threat because they can provide cybercriminals with direct access to a company's sensitive data and critical services. Since APIs often handle large volumes of requests and facilitate interactions between different systems, they have become attractive targets for attackers

seeking to exploit weaknesses. Cybercriminals are now using various tactics, such as injecting malicious code, exploiting authentication flaws, and launching denial-of-service attacks, to breach these gateways. Once inside, they can steal data, disrupt operations, and cause substantial financial as well as reputational damage.

This is why securing APIs is vital to protecting an organisation's digital infrastructure and maintaining trust with stakeholders.

## Do you believe your company as adequate API management measures in place to prevent becoming a victim of API attacks?

We have some API management measures, but there may be gaps that could leave us vulnerable to API attacks.

**34%**

Yes, our company has comprehensive API management measures in place to mitigate the risk of API attacks.

**28%**

Not sure  
**22%**

No, our company lacks clear API management practices.

**16%**

Unfortunately, only 28% of respondents have comprehensive measures to secure their APIs, while 34% admit to potentially having gaps in this regard. Worse, 16% say their company has no protection against API vulnerabilities, indicating either a lack of awareness of the risks posed by unsecured API or a lack of proactive action.

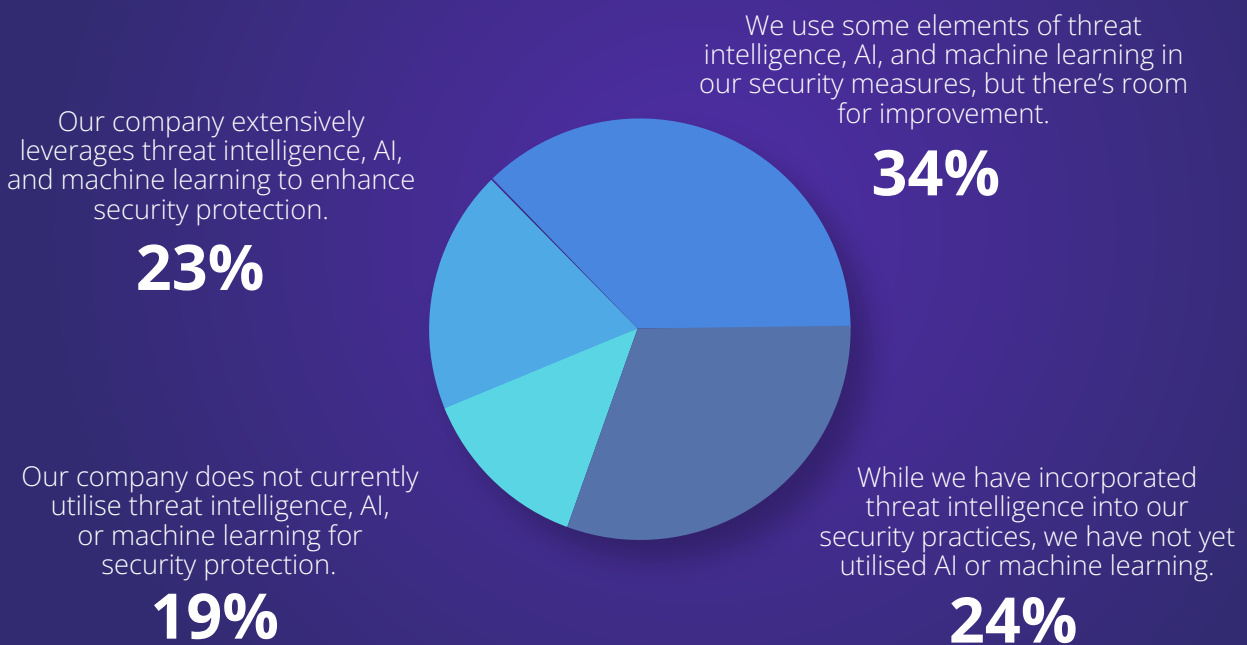
The survey results highlight a critical gap in API security preparedness for many companies—a gap that could pose major problems given the ubiquitous use of APIs. As previously mentioned, today APIs serve as gateways to a company's data and services, rendering them prime targets for cyber threats. Therefore, effective API management is essential to safeguarding these critical access points and protecting organisational assets from potential exploitation.



## Intelligence Is Imperative

Given the points already discussed, the importance of “intelligence” in cybersecurity can no longer be understated. Threat intelligence, including knowledge of current attack methods and attacker behaviours, is crucial for effective security, with Artificial Intelligence (AI) and Machine Learning (ML) automating threat analysis and response to potentially lead to faster and more effective security measures.

### To what extent does your company leverage data-driven approaches such as threat intelligence, AI, and machine learning for its security protection?



However, the survey results show limited adoption of advanced techniques, with only 23% of respondents saying they extensively leverage threat intelligence, AI, and ML for security. A third (34%) uses some of these elements, while 24% utilise only threat intelligence and not AI/ML. This suggests many companies are either not yet fully utilising the potential of these advanced security techniques or are yet to integrate them fully.

These results indicate many are lagging in terms of embracing data-driven security, which is concerning because a lack of it renders threat detection ineffective and puts the organisation at greater risk of getting attacked. This means there is an opportunity for security vendors and service providers like CDNetworks to offer solutions and guidance to help companies leverage threat intelligence, AI, and ML to improve their security posture.

# Cybersecurity Is an Ongoing, Never-Ending Battle

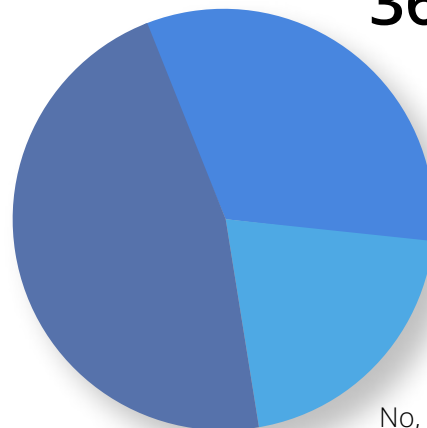
Cybersecurity is a constant battle, requiring vigilance around the clock. So, it is surprising many respondents have limited 24/7 security coverage, with only 47% having dedicated resources and systems for continuous security monitoring and response. This suggests a significant portion of companies may have vulnerabilities in their security posture, especially outside of regular business hours when attacks are often more frequent.



**Does your company have the necessary resources to maintain the security of its environments 24/7?**

We have resources available, but they are stretched thin, resulting in noticeable gaps in our security coverage, especially outside regular hours.

**36%**



Yes, we have dedicated resources and systems in place for continuous security monitoring and response.

**47%**





No, we lack the necessary resources to maintain security vigilance 24/7.

**17%**

Another 36% might not be doing any better as they have resources but are facing limitations, leading to gaps in coverage and highlighting the challenge of balancing security needs with resource constraints. This is especially true for smaller companies. The rest of the respondents—17% in total—admit to completely lacking the resources for 24/7 security, which means they are probably exposed to significant risks as cyber attacks can occur at any time, even outside business hours.



These results highlight the need for companies to reevaluate their approach to 24/7 security, for instance, they should:

-  **Prioritise security resources.** Security needs to be a top priority for companies, and they need to allocate sufficient resources accordingly.
-  **Invest in security automation.** Security automation tools can help streamline tasks, reduce the workload on security teams, and enable more efficient monitoring.
-  **Implement Threat Detection and Response (TDR) solutions.** These tools can help automate the detection and response to security incidents, even outside of regular business hours.
-  **Explore Managed Security Services (MSSPs).** Outsourcing security monitoring and response to an MSSP can help fill resource gaps and provide 24/7 coverage.



Interestingly, the survey results show a relatively even split among companies considering MSSPs, with 27% of respondents already outsourcing their security and 36% open to leveraging an MSSP. The rest—37% of the respondents—prefer internal management, likely because said setup affords organisations internal control. It is also likely that many of these respondents are bigger enterprises that have the resources to operate an in-house team of cybersecurity experts. Nevertheless, 63% do recognise the potential benefits of MSSPs for cloud and security needs.

## Would your company consider engaging a managed service provider for its cloud and security needs?

No, we prefer to handle our cloud and security needs internally without outsourcing to a managed service provider.

37%






We are already using a managed service provider.

27%

Yes, we are open to employing a managed service provider for our cloud and security needs.

36%

Over the years, MSSPs have definitely become a valuable solution for such companies due to reasons such as:

-  **Expertise and resources.** MSSPs offer a pool of security professionals and advanced tools that many companies lack internally.
-  **Cost-effectiveness.** MSSPs can provide a cost-effective way to access security expertise and resources compared to building an internal team.
-  **24/7 monitoring and response.** MSSPs offer continuous monitoring and response capabilities, ensuring security around the clock.

With cyber threats growing more sophisticated and threat actors becoming bolder, more brazen, and more active, it might make sense for an organisation to have experts help out in the constant battle that is cybersecurity.



## A Final Word: Ensuring Continuous Vigilance and Protection

Overall, the survey results show that while many companies recognise the critical importance of cybersecurity, there is a significant gap in preparedness and resource allocation, particularly in areas like API security, continuous monitoring, and the adoption of advanced threat intelligence and automation techniques.

Encouragingly, there's a growing trend towards considering MSSPs for addressing cloud and security needs. Companies facing internal resource limitations or seeking to enhance their security posture can greatly benefit from MSSP expertise and should consider revisiting their current strategies.

The survey results are a mix of optimism and concern. On the positive side, there's a clear regional awareness of cybersecurity issues, with many organisations prioritising multi-layered cloud security measures. Conversely, there are notable deficiencies in cybersecurity practices, particularly in API management and data-driven security.







To address these gaps, organisations should start by conducting a comprehensive security assessment to identify vulnerabilities and areas for improvement. Investing in continuous employee training and awareness programs can also bolster security posture. Additionally, adopting a proactive approach to threat intelligence and integrating automated security tools can enhance defence capabilities.

For those looking for a strategic partner, CDNetworks offers a robust solution. With its industry-leading content delivery network, extensive local infrastructure, and over 20 years of experience, CDNetworks provides comprehensive services such as [Cloud Security, API Shield](#) for enhanced API management, and [Enterprise Secure Access](#) for granular control.

In conclusion, by taking the right steps and partnering with the right experts, businesses can effectively implement a comprehensive "defence-in-depth" strategy that will enable them to better protect themselves from a wide range of cyber threats and maintain continuous, round-the-clock vigilance in today's ever-evolving cybersecurity landscape.



## NOTES ON SURVEY METHODOLOGY

---

**Survey Sample** - We interviewed Asian-based enterprise decision-makers, inclusive of IT managers, system administrators, IT directors, vice presidents, presidents, and C-level executives, all of whom had an element of responsibility for IT and cloud security efforts within their respective organisations.

Respondents were predominantly from Malaysia, Singapore and Indonesia. We received responses from 100 individuals; however, 83 answered most of the questions, while a few others did not complete a significant portion of the survey. Nevertheless, the data obtained from the 83 respondents who provided comprehensive responses still provided valuable insights for our research.

All the surveyed companies were large enterprise corporations from a varied range of industries, including manufacturing, FSI & banking, telco, education, retail, IT services and more.

**Sample Selection** - In conducting this study, we focused on our subscribers and readers, with whom we have convenient access and, where possible, with an identified interest in enterprise technology. For the purposes of a sustainability-related study, this method of sample selection was deemed appropriate as this survey needed to be completed by individuals with an interest in and knowledge of such issues. The insights gained from these highly targeted respondents are expected to be particularly insightful for understanding the challenges and opportunities associated with the impact of technology on ongoing sustainability efforts.

**Modes of Data Collection** - Data collection was conducted entirely online through our digital form. The survey was designed to be user-friendly and accessible, allowing respondents to provide their feedback conveniently through the digital platform.

**Response Formats** - AOPG Insights used a combination of dichotomous and ordinal-polytomous response options for the survey questions. This level of control was implemented to give standardised answers that could be grouped but were still wide-ranging.

**Interviewer Effect** - As the surveys were conducted using an online form, we deem that the chance for interviewers to have affected responses was negligible. However, we do acknowledge that the lack of understanding of some of the terms used in the questions may potentially cause respondents to provide erroneous answers.

**Data Cleansing** - Answers by respondents that were clearly from a non-relevant background were removed from the final selection set. The choice of which respondents to remove was left to individual researcher assessment. We acknowledge that this means it is possible, though unlikely, that a relevant respondent's answers may have been removed. We are confident that the final sample selection was representative of the skill base we needed to tap into.

**Statistical Significance** - Our sample set needed to have a specific skill set, in this case, a strong experience, knowledge and interest in IT and cloud security. As such, the quality of respondents was preferred over quantity. We believe the sample set we have chosen provides a strong feel for the realities of the Asian IT professionals' experience and views on IT and cloud security.



This document format is the copyright of Asia Online Publishing Group Sdn Bhd (AOPG) and cannot be reproduced, reprinted or republished without the written permission of AOPG. The "Micro Survey Report" format is proprietary and is copyrighted to AOPG, it should not be emulated or copied without written agreement.

© Asia Online Publishing Group Sdn Bhd.

AOPG Insights logo is the trademark of Asia Online Publishing Group Sdn Bhd  
CDNetworks logo is the trademark of CDNetworks Inc.