ASIA-PACIFIC CLOUD SECURITY STUDY

paloalto NETWORKS®

SEVENTY PERCENT ASIA-PACIFIC ENTERPRISES HAVE MISPLACED CONFIDENCE THAT CLOUD PROVIDERS' SECURITY IS SUFFICIENT

Overview

Ovum research, commissioned by Palo Alto Networks, shows that large organisations in the Asia-Pacific region, those with over 200 employees, have misplaced confidence that cloud providers' security is sufficient.

While 80 percent of large organisations view security and privacy as key challenges to cloud adoption, they still do not adequately protect themselves once cloud migration has occurred. This can be explained, to some extent, by confidence in the cybersecurity services provided by cloud providers, for their discrete cloud services. In a recent survey, 70 percent of large organisations in Asia-Pacific said they believe that security bundled with cloud services by cloud providers prepares them well or very well against cybersecurity threats.

Although security provided by cloud providers protects data when it resides within their clouds, it cannot protect data as it moves between clouds or on-premises assets.

Furthermore, individual clouds can be vulnerable to identity fraud and Application Programming Interface (API) abuses. Asia-Pacific organisations should reconsider depending entirely on security from cloud providers for protection. The study shows that few large organisations have a unified, holistic view of their cloud assets and the data that resides therein. Instead, they tend to have multiple cybersecurity products operating in silos.

In general, the research indicates that IT security decision makers in Asia-Pacific have misplaced confidence in their ability to protect themselves from cloud cybersecurity threats and are unprepared for potential attacks.

Key findings from the survey include:

- 80 percent of large organisations cite security and privacy issues as their biggest challenges to cloud computing adoption.
- Insecure interfaces and APIs, data breaches, and lack of a unified view of assets pose the greatest threats to cloud environments.
- Business decision makers in Asia-Pacific have misplaced confidence in their cybersecurity posture.
- 70 percent of decision makers believe that security provided by cloud providers, is sufficient to protect them from cloud-related threats.
- Most of the cybersecurity decision makers (64%) within large organisations do not have a unified view of the threats they face across all of their clouds.
- The need for automation is underscored by the study, which revealed that large organisations do not have enough time and resources to dedicate to cloud security audits and training.

80 percent of large organisations cite security and privacy as the biggest challenges to cloud adoption

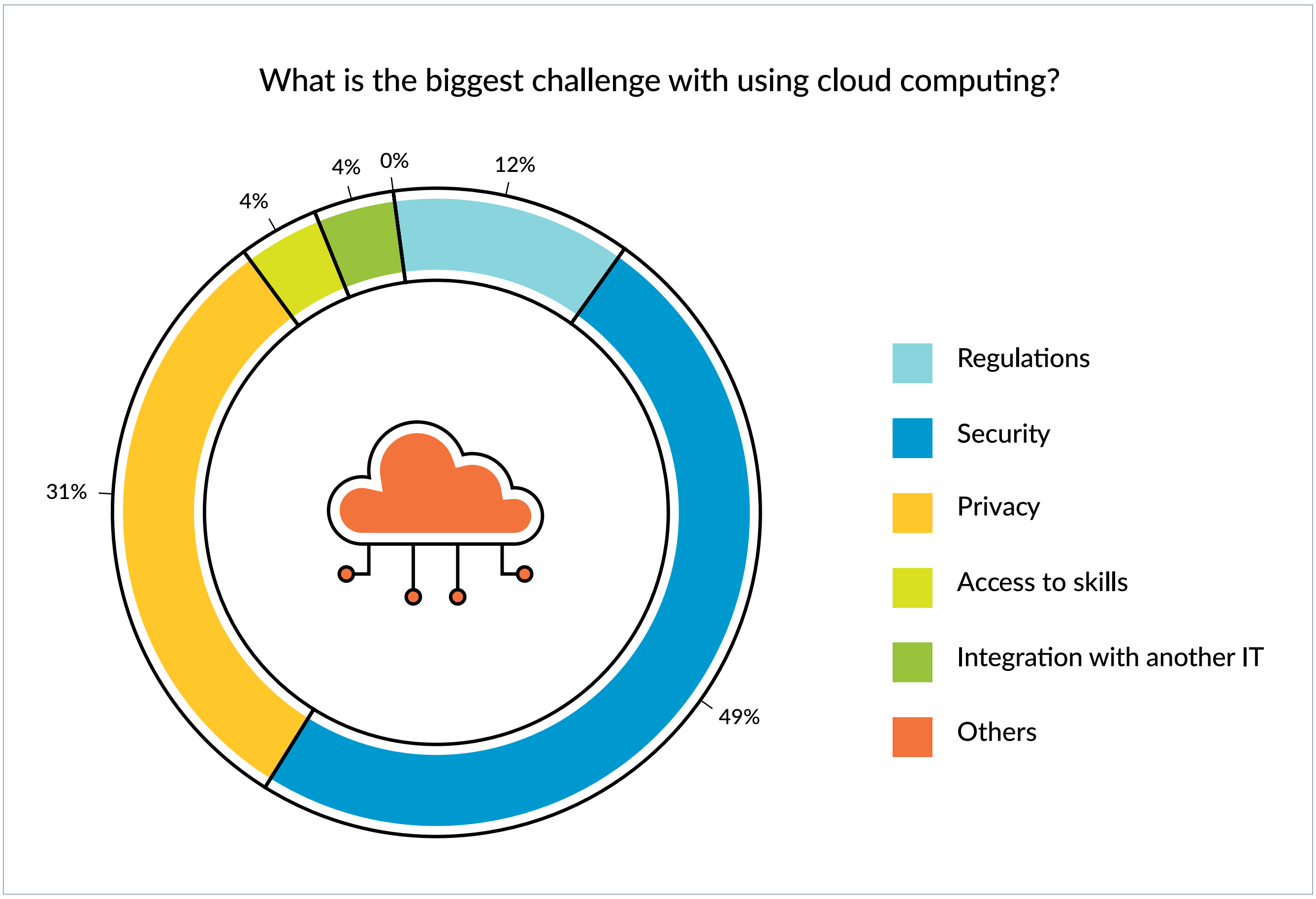


Figure 1: Challenges with cloud computing

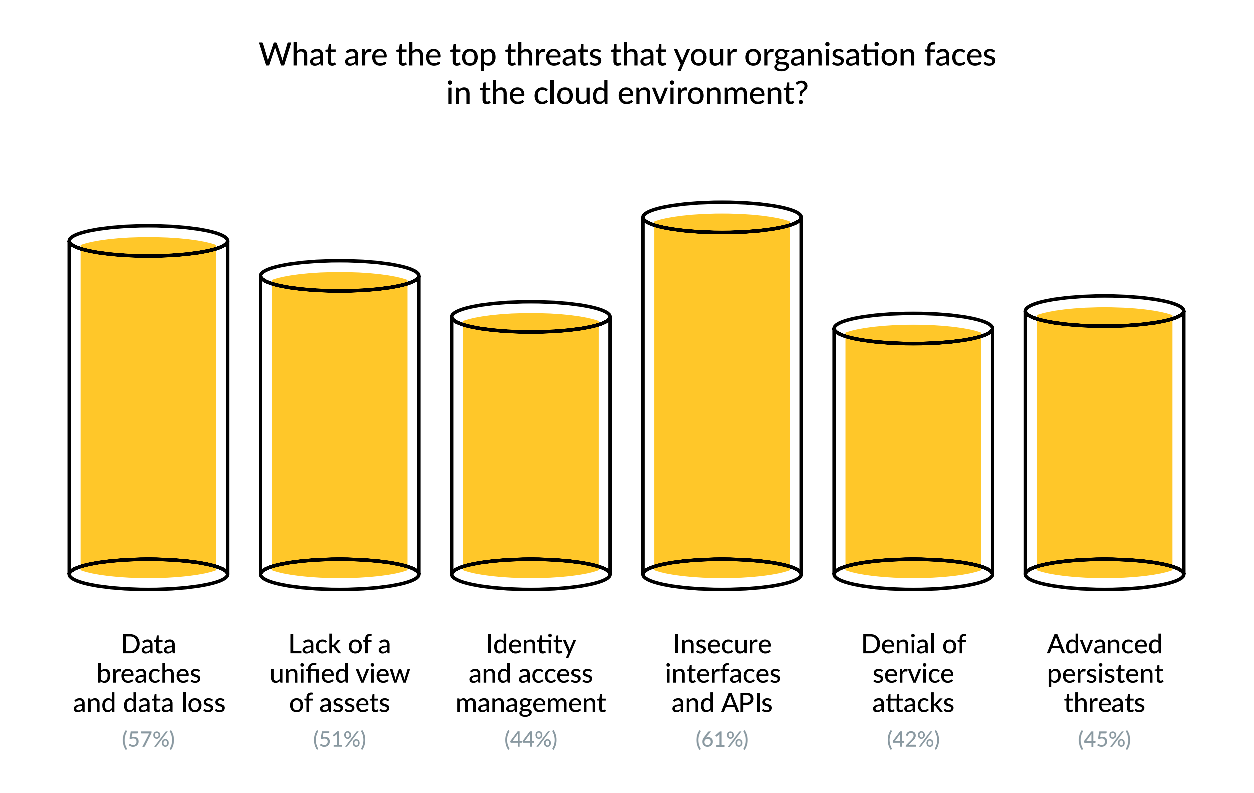
Despite the belief that security and privacy are major challenges, organisations still place their trust in the security provided by cloud service providers. Indeed, the study indicates that cybersecurity protection for the cloud is inadequate for Asia-Pacific organisations. In hybrid, multi-cloud environments, a unified, holistic view of cloud assets and services is critical to securing cloud implementations, rather than multiple point security solutions that are not integrated with one another.

Insecure interfaces and APIs pose the greatest threats to cloud environments

Today, cloud computing is critical for organisations. It enables businesses to scale and launch new services rapidly, without a requirement for substantial capital investment. Mission-critical business processes are increasingly underpinned by cloud technology, leading to a need to protect both valuable data that resides in cloud environments and business processes driven by cloud technology.

Migrating to the cloud is proving to be increasingly complex. Organisations typically need to manage a mix of on-premises technology together with multiple clouds, which are often poorly integrated.

These complexities are compounded by the increasing risk from cyberattacks associated with cloud migration and hybrid cloud implementations. In cloud environments, the top cybersecurity risks are insecure interfaces and APIs, data breaches and data loss, and a lack of a unified view of assets as shown in Figure 2.



What are the top threats that your organisation faces in the cloud environment?

Figure 2: Top threats facing cloud environments

Business decision makers have misplaced confidence in their cybersecurity posture

Organisations need an integrated view of all their cloud assets and cloud services. They need solutions that work together with those provided by cloud service providers such as AWS®, Microsoft Azure®, Alibaba Cloud, and Google Cloud.

The research reveals that large organisations are using an average of seven cloud service providers. The security offering for each cloud must be integrated with other security services in order to effectively manage risk.

Figure 4 shows perceptions of security decision makers towards security bundled with cloud services. The research reveals that 70% of organisations view the security offered by cloud service providers for their discrete services to be sufficient. Indeed, the same proportion (70%) depends entirely on cybersecurity services provided by cloud providers for overall protection.

	Responses
One only	26%
1 to 5	47%
6-20	17%
21-50	8%
More than 51	2%
Total	100%

Figure 3: Number of public cloud providers used by Asia-Pacific organisations

To what extent do you believe that the cybersecurity bundled with cloud services by cloud providers prepares you for cybersecurity threats on a scale of 1 to 5 (where 1 is not at all prepared and 5 is very well prepared)?

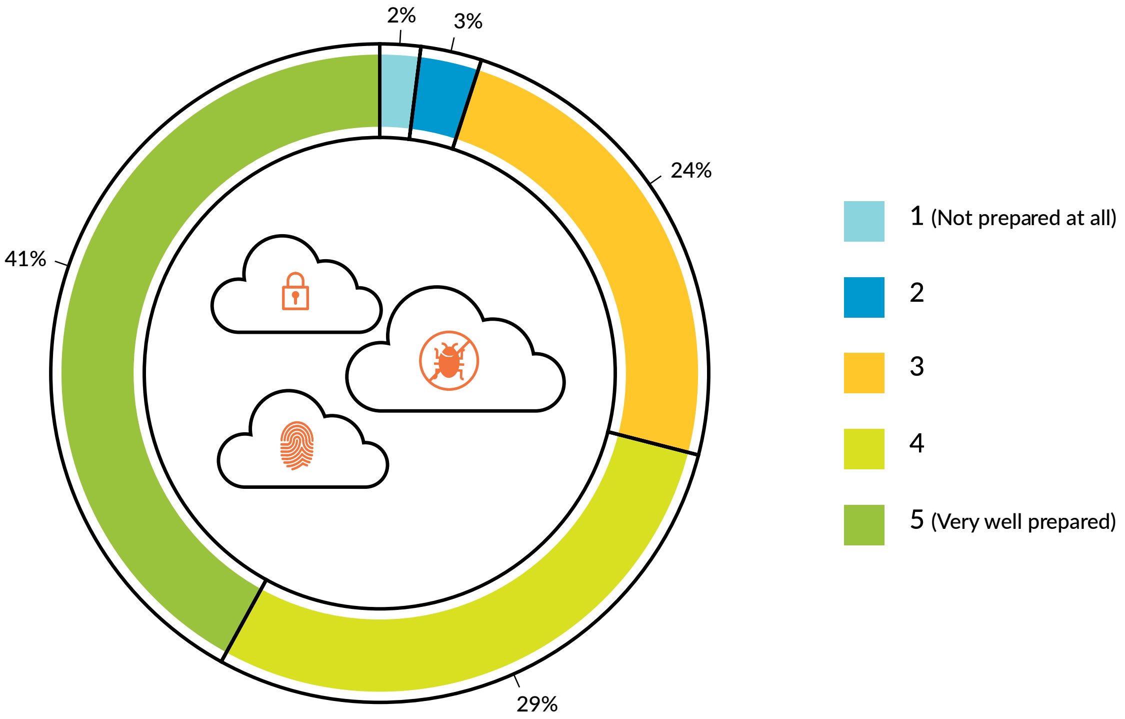


Figure 4: Perceptions of security offered by cloud services providers

Security solutions offered by cloud services providers alone are not sufficient for protecting hybrid, multi-cloud environments. Dependence on these cybersecurity services alone can make organisations vulnerable and does not protect them from the myriad threats they may face.

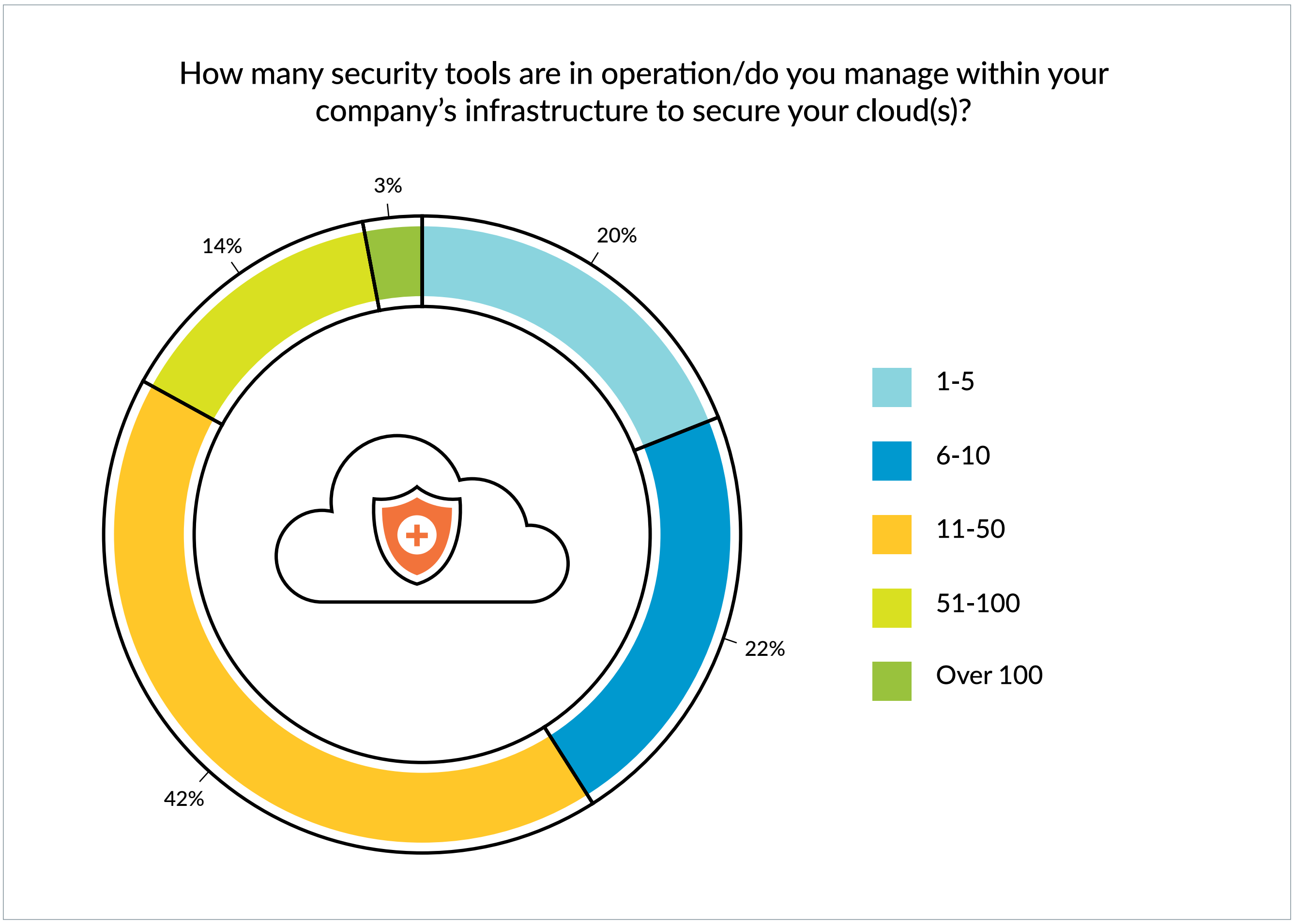
Hybrid, multi-cloud environments require greater focus on securing interfaces and APIs, preventing data loss and breaches, properly managing user access, and mitigating advanced persistent threats and DDoS attacks. Fundamentally, adequate protection must involve a holistic, unified view of all cloud assets and services.

Three out of five large Asia-Pacific organisations have over 10 security tools operating simultaneously

A typical response by organisation decision-makers to the increasing complexity of their cloud environments—where existing tools can't always detect new and emerging threats—is to deploy brand-new security solutions. Over time, however, this creates an estate of siloed security products, each reporting to its own dashboard. This is a major management challenge, as there is frequently no provision for the centralisation of security alerts, with cybersecurity staff facing the challenge of monitoring multiple consoles and cross-referencing between disparate screens and information formats. Equally, applying security policy changes is a laborious and time-consuming task in a multi-dashboard environment, which represents a security threat in its own right.

The research reveals that 59% of large Asia-Pacific organisations have over 10 security tools operating simultaneously. Three percent have deployed over 100 security tools.

Figure 5 shows the number of security tools operating simultaneously in large Asia-Pacific organisations.



How many security tools are in operation/do you manage within your company's infrastructure to secure your cloud(s)?

Figure 5: Number of security tools used by large Asia-Pacific organisations

From a public cloud perspective, there is a clear tendency for large organisations to perceive the security provided by cloud service providers to be sufficient for the discrete cloud services that they offer.

70 percent of decision makers within large organisations believe that the security provided by cloud providers is sufficient to protect them from cloud-related threats, despite the complexity of today's hybrid, multi-cloud environments.

Nearly two-thirds of organisations do not have a unified view of threats faced across all clouds

When asked the extent to which they have a unified view of cloud threats, 64 percent of large Asia-Pacific organisations indicated that they do not have a unified view of the threats faced across all clouds and hence are unable to adequately manage risk. As shown by the study, nearly 60 percent of organisations are using more than 10 security tools simultaneously, making the creation of a unified, holistic view extremely difficult.

The interconnected nature of hybrid and multi-cloud environments means that a security breach in one area could become an entry point for attacks across multiple clouds.

To address the manifold threats to cloud environments, organisations need to have complete visibility of all their assets and services, cloud, and on-premises, enabling them to address cybersecurity threats across their entire IT environment.

Figure 6 shows the extent to which organisations have a unified view of cloud threats, where "1" is low and "5" is high.

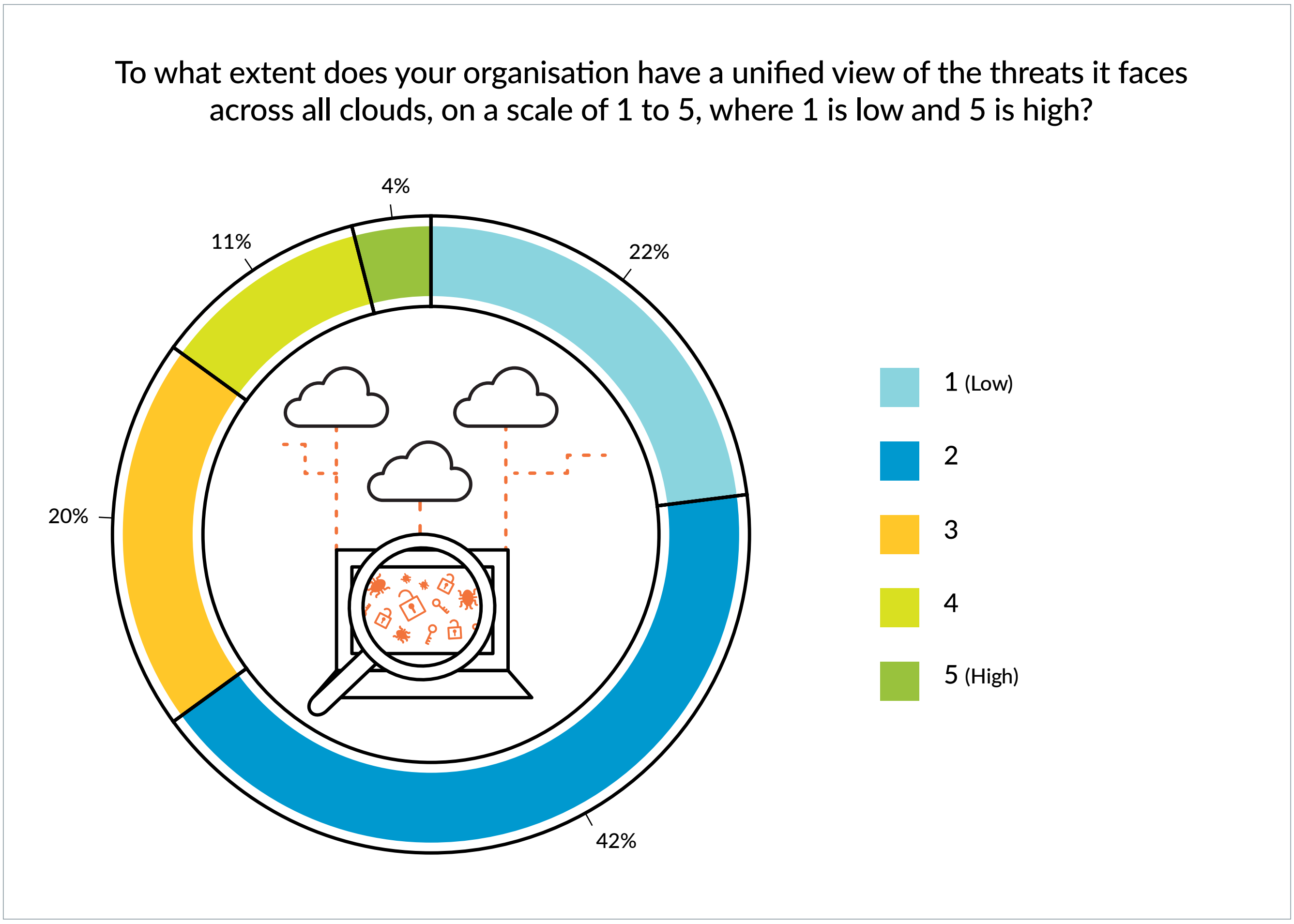


Figure 6: Proportion of organisations with a unified view of cloud threats

The lack of a unified view of cloud assets and services is driven by the large number of disjointed security tools which large organisations have typically deployed. While these deployments are designed to address specific threats, they are often not integrated and report to their own discrete dashboards. This increases complexity and makes it difficult for organisations to have a unified view of their cloud environment, which is necessary to manage risk.

The need for automation is underscored by the lack of adequate cloud security audits and training

It is critical that organisations truly understand the measures needed to protect their vital assets. It is particularly important that they audit their cloud technology, given its rapid adoption and increasing importance. It is only through ongoing audits that organisations can begin to ensure that their security posture addresses contemporary threats. Once an audit has been completed, advisory services are necessary to implement required measures and continually protect vital assets. Few organisations place sufficient emphasis on these measures.

In Asia-Pacific, 76 percent of organisations either never conduct an audit or conduct an audit less than once a year. Figure 7 shows the frequency with which audits are conducted.

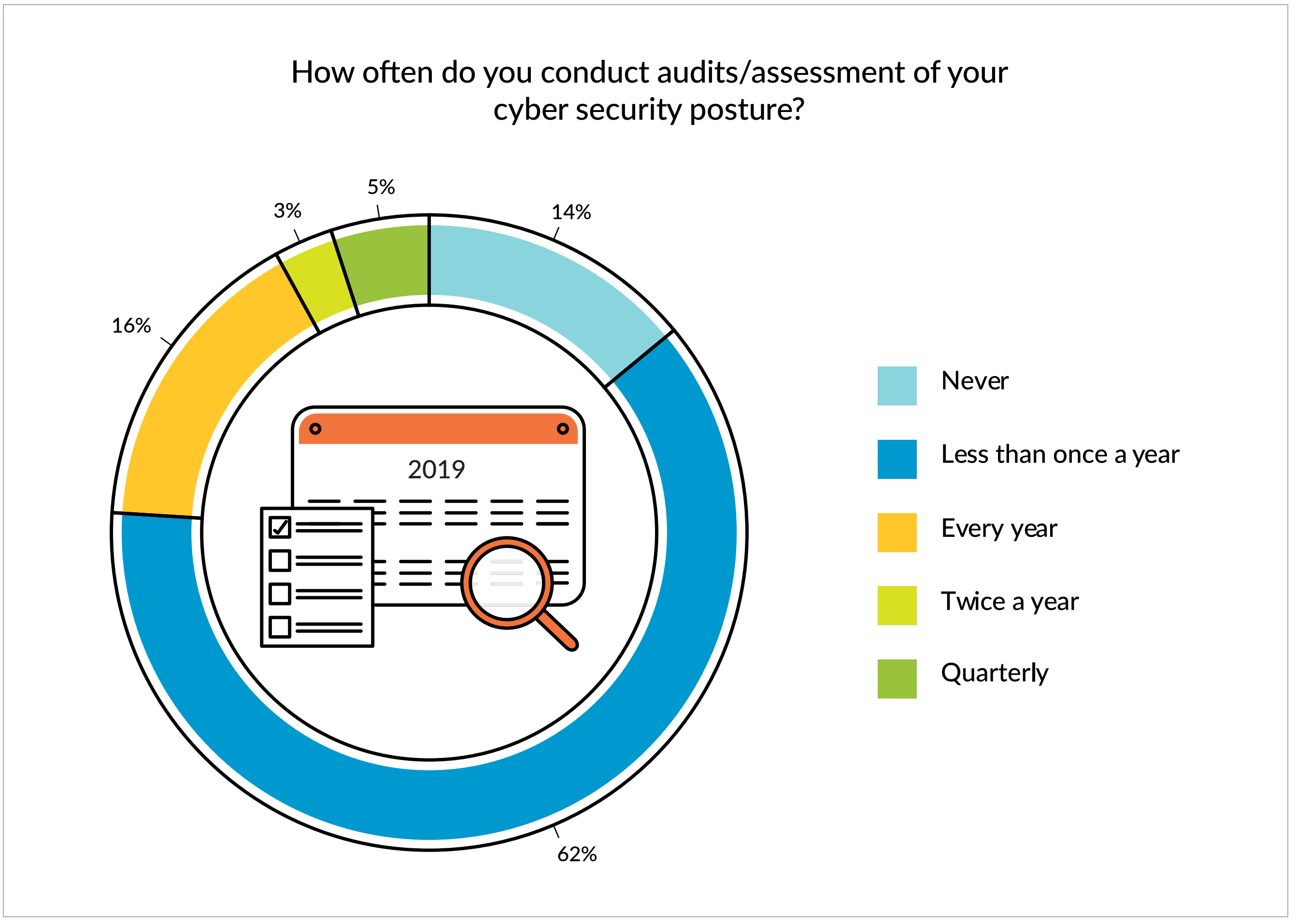


Figure 7: Technology audit frequency

Furthermore, a quarter of audits don't even include cloud assets.

In spite of the cybersecurity skills shortages faced by organisations, 57 percent of the large organisations surveyed do not provide cybersecurity training to IT security employees on a yearly basis as shown in Figure 8. This is not sufficient. The threat landscape is evolving rapidly, and IT teams need to be kept informed of these developments.

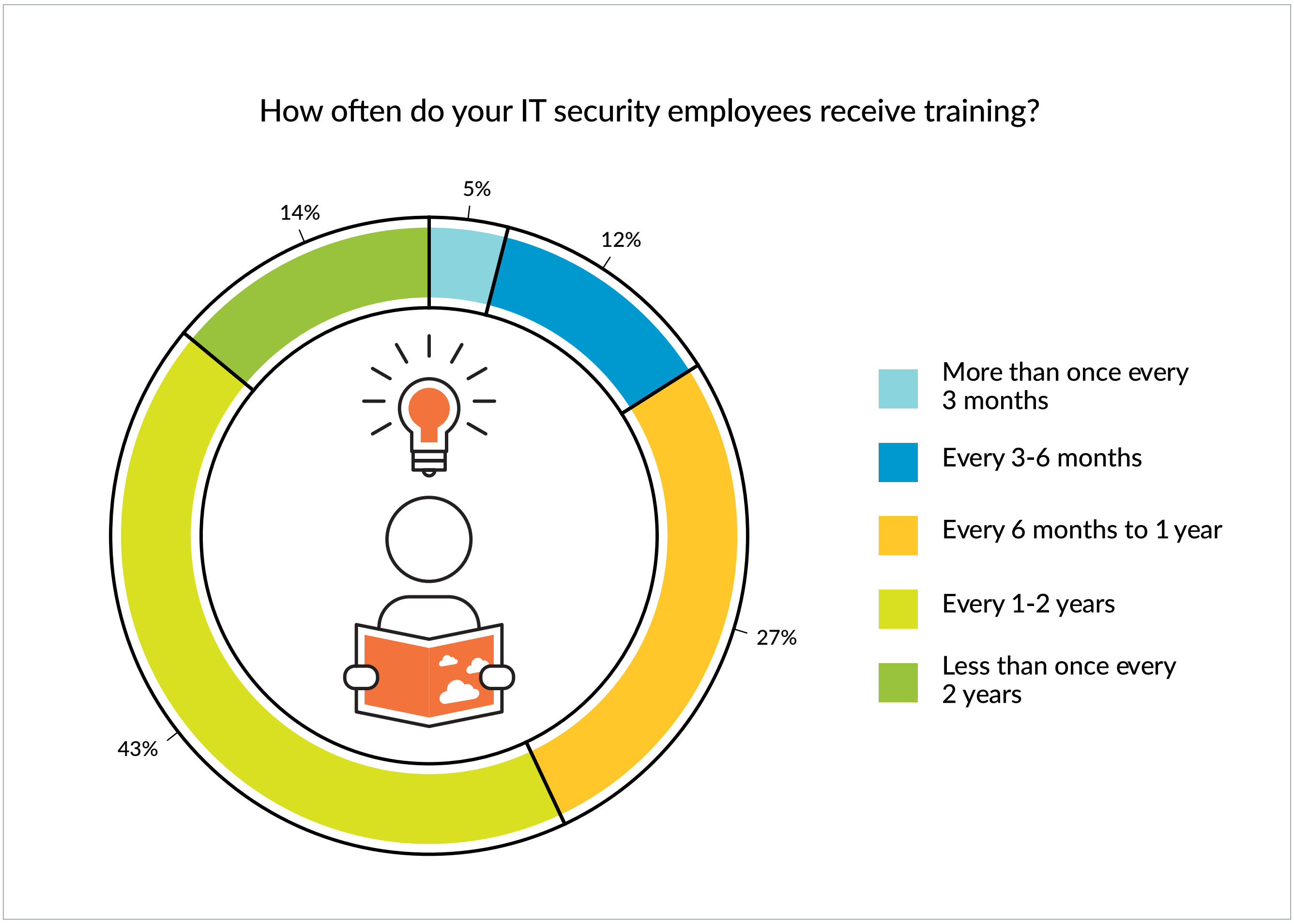


Figure 8: Cybersecurity training frequency for IT security employees

To address these shortages, organisations must either invest to a greater extent in training or consider alternative solutions, such as greater use of AI and automation. Threat intelligence tools are becoming more popular as organisations look for alternative ways of assessing the threat landscape and adjusting their security posture accordingly. Almost half (49%) of Asia-Pacific organisations use threat intelligence and analytics to identify new threats and take necessary action. Some 19 percent of large organisations in Asia-Pacific have also equipped themselves with real-time threat monitoring capabilities.

Businesses, government, and educational institutions will need to work collaboratively to address the cybersecurity skills shortage that exists. The shortage has been a key challenge for many years, but the gap is growing even faster today — particularly for talent with deep cybersecurity expertise, which is typically built up from years of experience.

Recommendations

The research shows that, despite general awareness of cybersecurity challenges, organisations are not prepared for the security threats posed by cloud technology. Organisations should always include cybersecurity planning as part of their cloud adoption and migration processes.

Fundamentally, a unified view of their cloud computing environments is critical as shown in Figure 9.

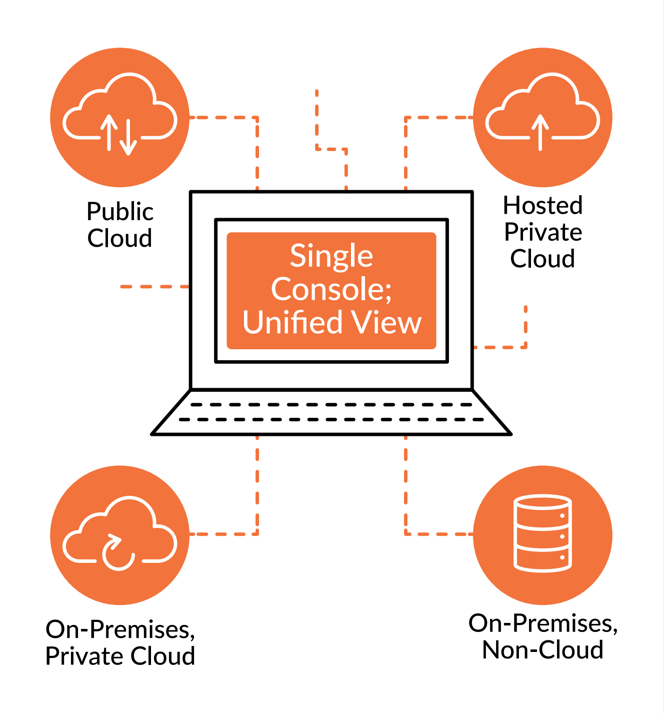


Figure 9: Unified view of the cloud

Organisations must also take the following approaches to securing their cloud assets and the data residing therein:

- Building security into the cloud environment from the get-go; security should be an enabler to accelerate cloud adoption.
- Developing consistent security policies across all types of cloud deployments, which can be implemented properly through the help of tools that provide a unified view of all cloud assets and the threats they face.
- Allowing for frictionless deployment and easy scalability in multi-cloud environments, bridging the gap between highly controlled security teams and highly agile development teams.
- Increasing audits and training for employees, both IT and non-IT.
- Automating threat intelligence with natively integrated, data-driven, analytics-based approaches (leveraging machine learning/artificial intelligence) to avoid human error.

Methodology

Palo Alto Networks commissioned Ovum Research to conduct a survey among 500 respondents from large businesses in Asia-Pacific. All respondents had to be using public cloud at the time of the study.

The respondents to the survey ranged from owners to business directors and C-level executives, all of whom had to be either the final decision maker or influencer when it came to the organisation's cloud strategy.

There were 100 respondents each from five key markets in the region, including Australia, China, Hong Kong, India, and Singapore.

For the purposes of this study, large organisations are defined as businesses with over 200 employees.

Author

Andrew Milroy, Head of Advisory Services, Asia-Pacific
andrew.milroy@ovum.com

Copyright notice and disclaimer

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard - readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

3000 Tannery Way
Santa Clara, CA 95054

Main:	+1.408.753.4000
Sales:	+1.866.320.4788
Support:	+1.866.898.9087

www.paloaltonetworks.com