February 2021

MARKET REPORT

Securing your apps in the borderless cloud.

Latest market research shows IT decision makers in APAC express concerns about cloud and app security. »

Barracuda®

Your journey, secured.

Contents

Introduction

Public cloud continues to drive digital and business innovation. Organizations worldwide have enabled employees to work remotely and shifted to cloud and online computing to maintain collaboration and workflows. **This rapid cloud adoption and reshaping of the global workforce has created new challenges and risks.**

Indeed, security is a top public-cloud concern. In a recent Barracuda study, 70% of respondents said security concerns restrict their organization's adoption of public cloud. An overwhelming 96% said they'd increase their adoption of public cloud if barriers were removed.

Network integrations are also an area of concern, including integration of public cloud with legacy technologies, integration with private cloud, and integration with on-premises infrastructures.

This year's pandemic and the resulting reality of work from home have really driven home the importance of applications and the internet. A significant majority of office workers across the world have had to "remote-in" to their digital workplaces over the internet, and this has in turn led to a boom in public cloud adoption. Digital transformation that was already in full swing has received a boost like no other. Workplaces have had to remove their older workflows and rapidly move them to a digital form or perish. These changes have led to many organizations moving to the public cloud, taking advantage of the speed of deployment.

This move to the cloud and the ongoing movement and evolution of applications creates new risks. New strategies and solutions are required to help mitigate these risks, and careful attention must be given to secure the growing application threat vector.

This report takes an in-depth look at public cloud, adoption trends, security concerns, app vulnerabilities, and a variety of related issues contrasting the responses from APAC and the rest of the world.

Methodology

Barracuda commissioned independent market researcher Vanson Bourne to conduct a global survey of **750 IT decision makers** who are responsible for their organizations' cloud infrastructure. Survey participants from the **U.S., EMEA and APAC** represented organizations of all sizes from a broad range of industries. The survey was fielded in February 2020.

Key findings

FINDING #1

Cyberattacks and their associated costs are on the rise.

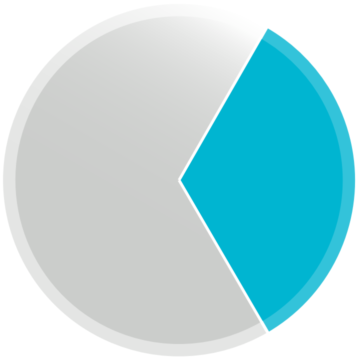
Since 2017, cyberattacks in all global regions have gone up about 20%. Organizations spend between one and two days per week on average preventing and managing cyberattacks—time and money that limits the impact and benefit that IT teams can provide when it comes to business enablement and other proactive initiatives.

Since 2017, cyberattacks in all global regions have continued to rise.

FINDING #2

There's confidence in the cloud, but not all organizations feel fully protected.

A small majority of respondents have already added third-party security solutions to protect their cloud workloads. For organizations that haven't already done so, there are strong intentions in all global regions to implement added cloud security. Overall, about one-third of respondents in APAC believe their applications aren't completely protected in the public cloud right now. There is significant variation by country. In Singapore, it's 52%. In Australia and Hong Kong, it's 36%. In India, it's 25%.



One-third of respondents in APAC believe their applications aren't completely protected in the public cloud.

Key findings

FINDING #3

Concerns about poor app security and related consequences are prevalent.

Most decision makers understand the importance of protecting apps that involve e-commerce or PII, or that can be accessed by external users or via mobile devices. Across APAC, top concerns about a successful cyberattack include loss of data and loss of customers.

Top concerns about a successful cyberattack in APAC.

PERSPECTIVE

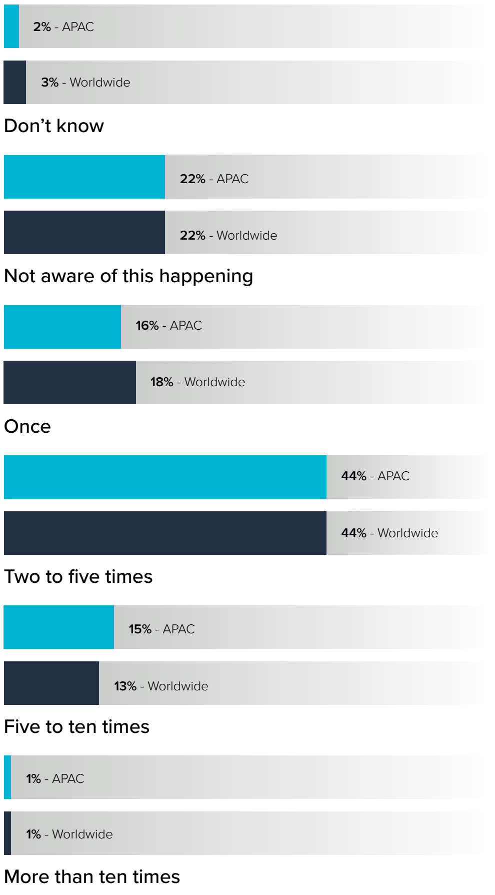
Cyberattacks are increasing in all geographic regions.

More than three-quarters of respondents have already been the target of a cyberattack, highlighting a serious global security challenge. Since 2017, cyberattacks in all geographic regions have gone up by about 20%.

In APAC, 76% of respondents report being targeted by a cyberattack at least once, with 44% saying they've been attacked between two and five times.

Has your organization been targeted by a cyberattack at least once?

Worldwide (n=750), APAC (n=750)



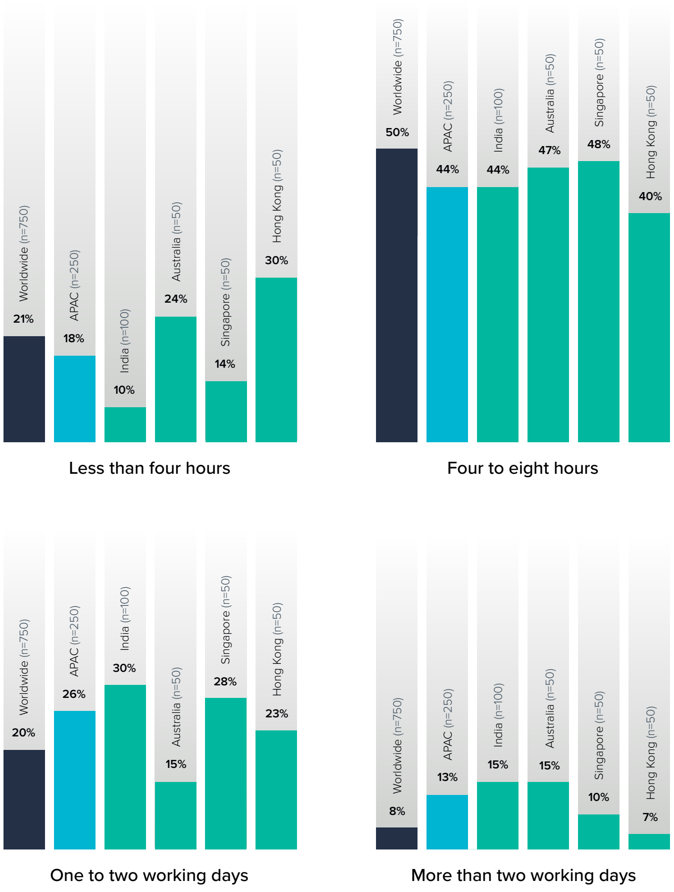
PERSPECTIVE

It’s costing organizations a significant amount of time to prevent and manage cyberattacks.

Approximately 29% of all global respondents average one day or more per week preventing and managing cyberattacks against their organizations. Time spent on this work is highest in APAC (26%); India spends the most, an average of 8 hours.

Investing time in cyberattack prevention limits the impact and benefit that IT teams can provide across the business. Instead, much of this work can be offloaded to advanced security solutions that employ artificial intelligence and machine learning to automate security tasks. This reduces the burden on IT teams and allows them to shift more of their time to business enablement and other proactive initiatives. They would be able to add more value and spend time elsewhere if they were able to better rely on their organization’s security solutions.

How many hours are you spending on preventing and managing cyberattacks?



PERSPECTIVE

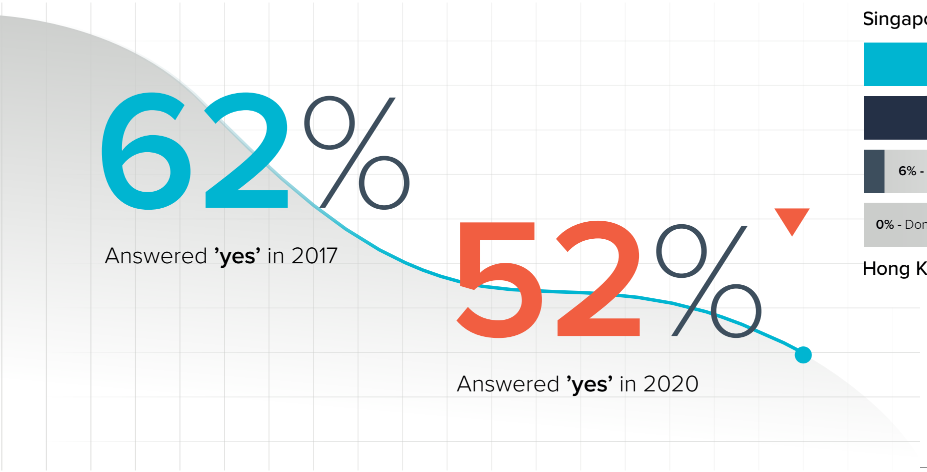
There’s confidence in the cloud, but it’s not universal.

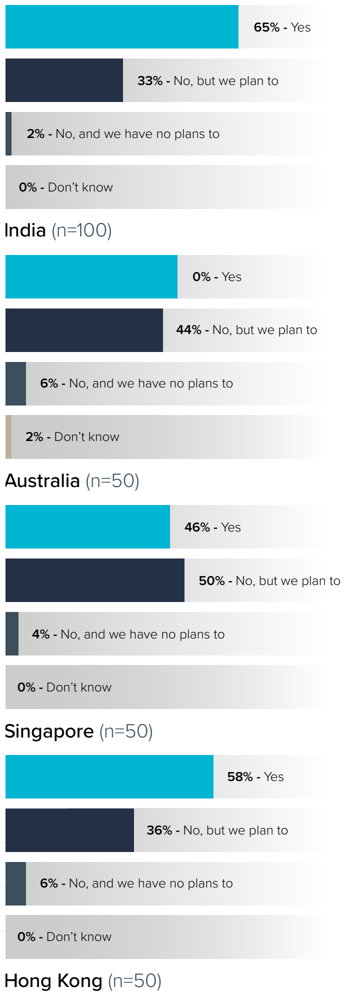
A small majority have added additional security measures to their public cloud deployments, but the adoption of third-party solutions has slowed over the past few years. A full 52% of respondents have added more security to protect their cloud workloads. In 2017, that number was 62%. This may indicate increased confidence for built-in security. APAC respondents, by a small percentage, are more likely to have added these measures to their deployments than respondents in other global regions.

It should be noted that the number of companies that plan to add additional security in the future is nearly equal across all regions. Globally, as well as in APAC, 39% of respondents say they'll add extra security. Singapore and Australia lead the pack in APAC.

Has your organization added any additional security solutions to your public cloud to protect it during access?

(n=750) (2017 n=1,300)



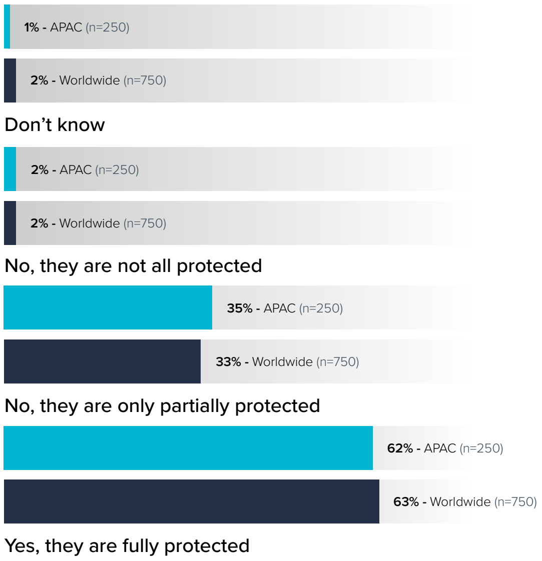


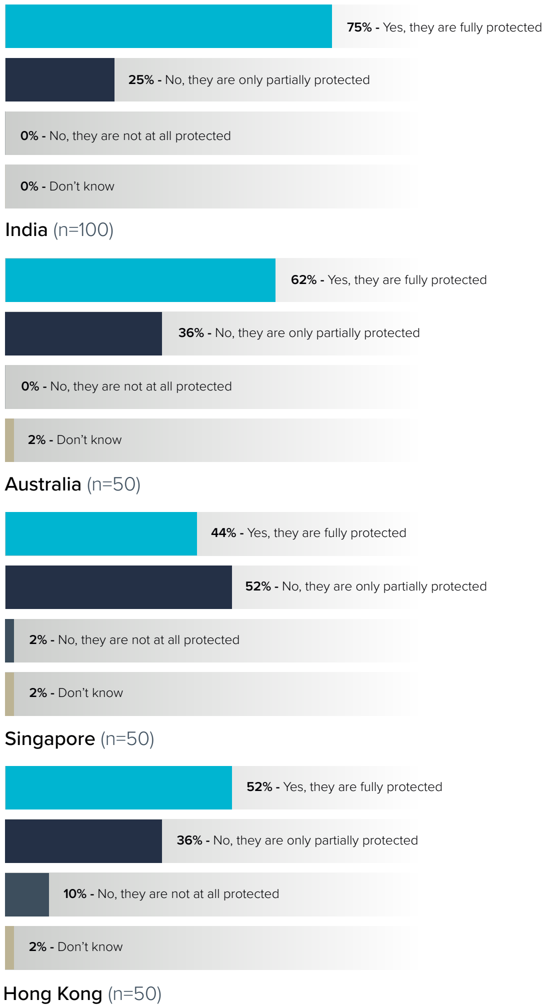
PERSPECTIVE

A third of organizations don’t feel fully protected in the public cloud.

While 63% of organizations believe they are fully protected in the cloud, worldwide and in APAC, there remains a huge gap that will ultimately prompt organizations to seek additional security strategies. Also, the track record for organizations that felt they were protected in the cloud is poor when it comes to reported breaches.

Do you believe your organization’s applications are fully protected in the public cloud?

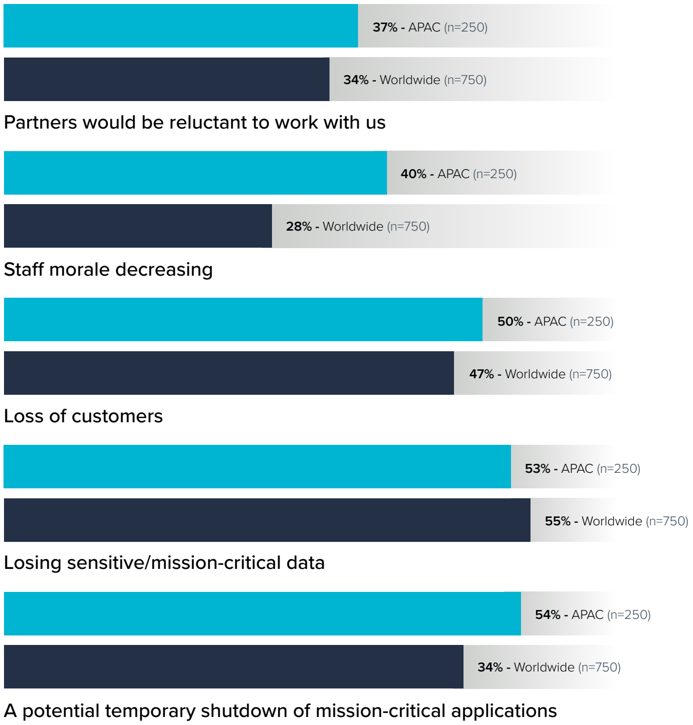




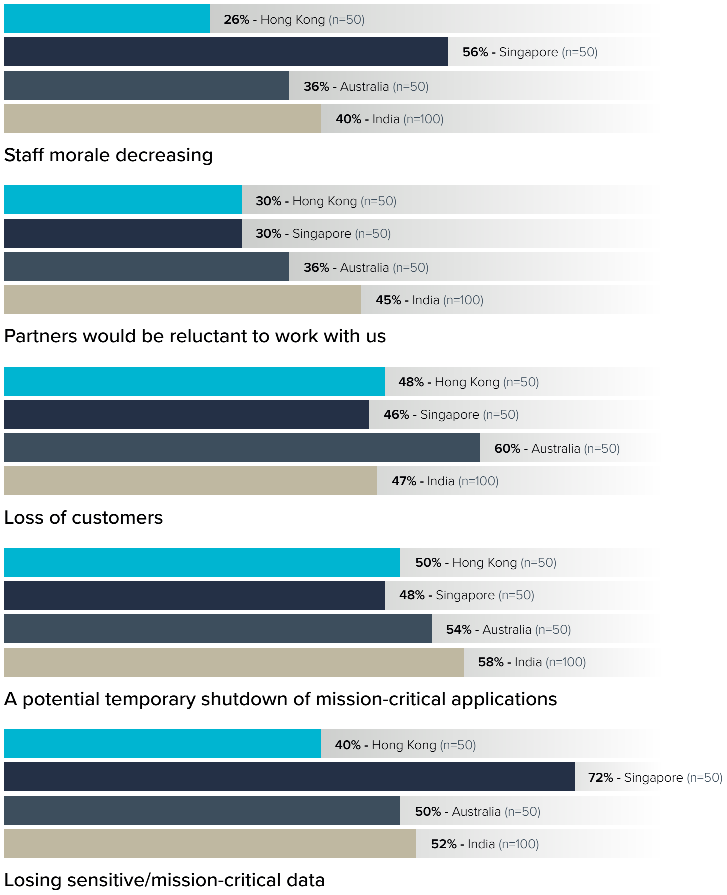
PERSPECTIVE

More than half are worried about losing sensitive, mission-critical data.

In addition to data loss, crippled day-to-day operations, and lost customers, secondary consequences of a successful cyberattack can include lawsuits, regulatory fines, and damage to brand reputation. In addition, 40% of respondents in APAC said cyberattacks have an impact on staff morale. That percentage was the highest in Singapore, at 56%.



What would you expect the consequence to be for organizations with poor application security?



PERSPECTIVE

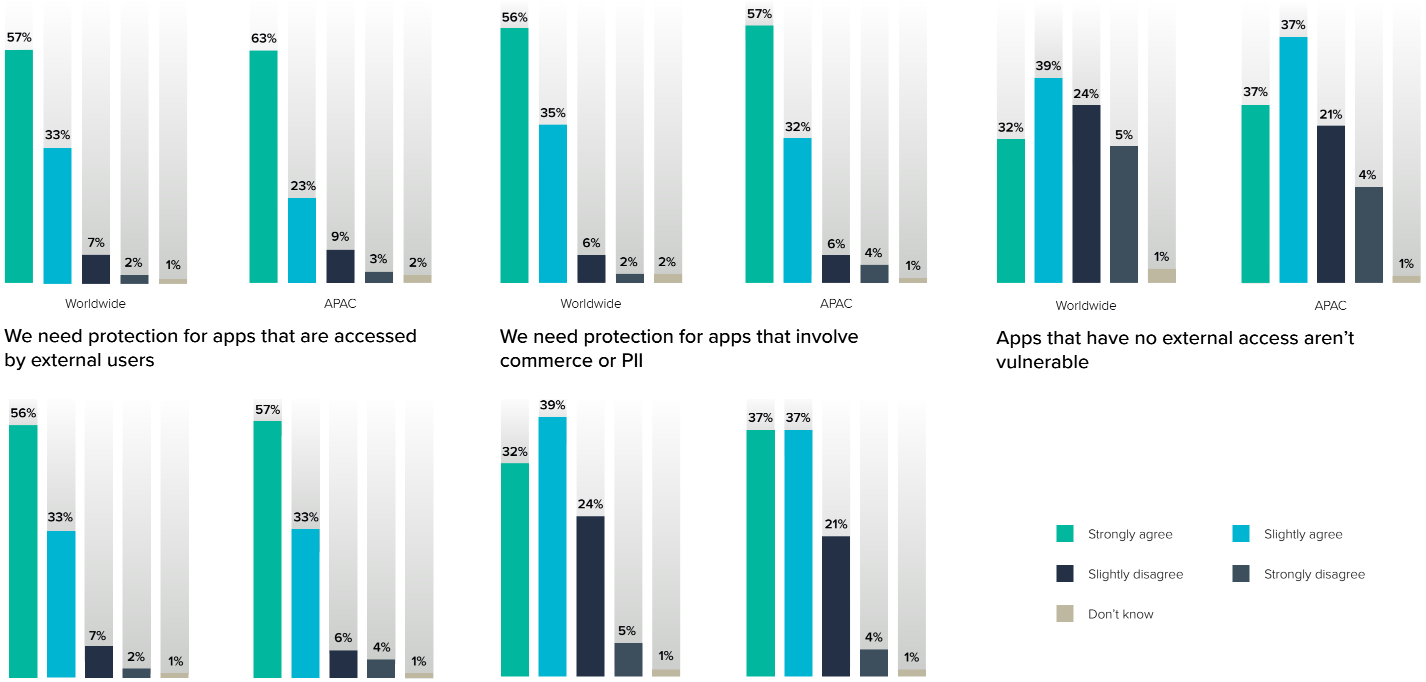
Most are concerned about the need for app protection.

Most respondents understand the need to protect apps that can be accessed by external users, involve e-commerce or PII, or can be accessed via mobile devices. A small majority even feel that applications without external access are still vulnerable, which shows the extent of the concern.

These concerns underscore the importance of providing customers with a strong and secure IT solution that provides reassurance about public cloud security to increase adoption and help them take advantage of all the business benefits inherent in leveraging the cloud.

To what extent do you agree or disagree with the following regarding enhanced protection for web-facing apps?

Worldwide (n=750), APAC (n=750)



We need protection for apps that are accessed by external users

We need protection for apps that involve commerce or PII

Apps that have no external access aren't vulnerable

We need protection for apps that are accessed via mobile devices

App security provided by cloud infrastructure is sufficient

Conclusion

Organizations are showing more trust in the public cloud than in previous years, but significant security concerns remain. The overwhelming majority of respondents said they look to third-party solutions for full protection of their cloud applications. APAC and the United States lead the way in deploying additional security measures to enhance cloud-native security tools. This may contribute to our finding that both regions have higher confidence that their applications are fully protected in the public cloud. EMEA respondents were less likely to believe that their applications were secure.

When it comes to application security, there's no substitute for the benefits and protections of a web application firewall (WAF). WAFs are specifically designed to protect websites and applications from advanced threats. When properly deployed in front of web-facing apps, a WAF ensures protection from web and distributed denial-of-service (DDoS) attacks, protects APIs and mobile apps, blocks malicious bots and automated attacks, secures application delivery, and controls access and authentication. Many Software-as-a-Service (SaaS) solutions also include built-in, WAF-related tools to help discover and remediate vulnerabilities before they lead to attacks.

As apps remain one of the most exploited threat vectors and security remains a top concern, WAFs provide the ability to safeguard data with confidence by eliminating application vulnerabilities and stopping data breaches.

Organizations are showing more trust in the public cloud than in previous years, but significantly security concerns remain.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-enabled, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them—in ways they may not even know they are at risk—so they can focus on taking their business to the next level.

Get more information at barracuda.com.

Barracuda®
Your journey, secured.