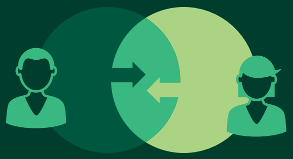
A Forrester Consulting
Thought Leadership Paper
Commissioned By VMware

August 2020

IT And Security Silos: A Spotlight On The APAC Region

Results From Asia Pacific For The May 2020 Thought Leadership Paper "Tension Between IT And Security Professionals Reinforcing Silos And Security Strain"



Introduction

Each day, IT and Security teams face major risks and concerns globally; unfortunately, teams are often working against each other by not presenting a unified front with a consolidated security strategy.

In February 2020, VMware commissioned Forrester Consulting to evaluate the relationship between IT and Security teams, including the relationship between C-level and manager/director-level employees within those organizations. We also explored the challenges and benefits that come from having a unified and consolidated IT management and security strategy. Forrester conducted a global online survey with 1,451 manager-level and above respondents and interviewed eight CIOs and CISOs to explore this topic further. Of those 1,451 respondents, 276 were from the Asia Pacific (APAC) region, including Australia, China, India, Japan, New Zealand, Singapore, and South Korea. This Spotlight concentrates on the survey results from APAC. All respondents had responsibility and decision-making influence over their organization's security strategy. We found that although companies are focused on attempting to reconcile the divide between IT and Security, tensions persist. Without a unified IT and Security strategy powered by technology-enabled collaboration through shared tools, companies are finding it hard to make progress in cybersecurity.

KEY FINDINGS

- **Collaboration is a top priority for Security and IT in APAC, despite challenges.** Companies are focused on collaboration and alignment between IT and Security over the next year and are moving key tasks to a shared model between teams.
- **Negative relationships and technology challenges plague teams.** APAC teams are struggling with major roadblocks across the whole portfolio: people, processes, and technology. Unsurprisingly, collaboration is a challenge, given the overwhelming number of tools and the negative relationships that persist across teams.
- **Consolidated strategies help APAC organizations meet key objectives.** To combat their relationship and technology woes, organizations in APAC are actively implementing a unified and consolidated IT and security strategy. Although only one in three3 APAC organizations have adopted this, more are planning adoption in the next year with the objective of improving security and visibility.

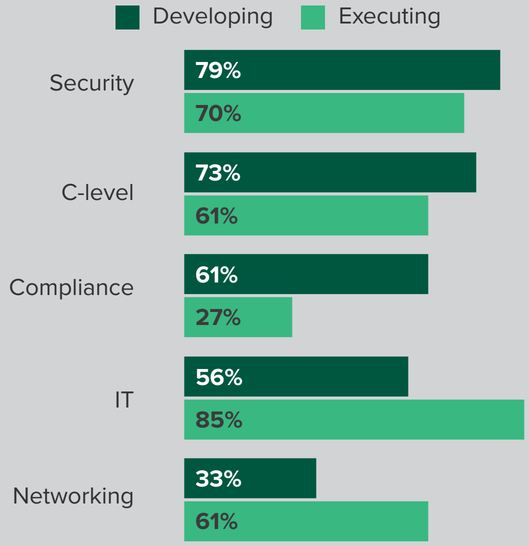
Collaboration Is A Top Priority For Security And IT In APAC, Despite Challenges

As IT and Security teams become even more critical to an organization's success during uncertain times, it is more critical than ever to have a unified approach to security. Despite past tactics for companies when Security essentially lived in its own silo separate from IT, Security team members no longer solely own security responsibilities. Now, security and IT tasks are moving toward a shared model between teams. By conducting a quantitative survey in APAC with both IT and Security professionals, we found that:

› **Security tasks are now shared across IT and Security teams.** Business leaders understand the benefits of having collaboration and shared tasks across teams and are actively moving most security responsibilities to a shared model. For example, many different functions are involved in the development and execution of the security strategy beyond just Security alone (see Figure 1). Although only 56% of APAC respondents note that IT teams are involved in the development of a security strategy (it is typically managed by Security and C-level teams), 85% report that IT is responsible for its execution — significantly higher than even the Security team. However, C-level involvement varies at the country level. Japan (81%), China (78%), and Singapore (76%) respondents report involvement from the C-suite in security strategy development, while this falls to 66% in Australia and 67% in South Korea. Regardless of the split, it is evident that the Security team alone is no longer solely responsible for the development and execution of the security strategy.

Figure 1: Security Strategy Development And Execution In APAC

"What functions are involved in developing and executing your security strategy?"



Base: 276 IT and Security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

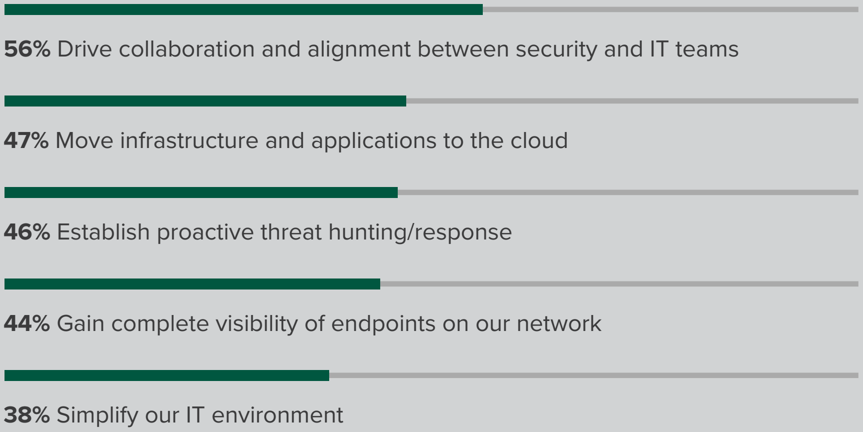
Security no longer lives in a silo, as many functions are involved in both the development and execution of the security strategy in APAC companies.

One example of a key task that is moving to a shared model is threat hunting, remediation, and incident response. Threat hunting allows teams to become more proactive, not reactive, to alerts. However, Security teams struggle to perform since they are often bogged down with tactical activities. In APAC, 57% of decision makers report that this task is currently owned by Security. Only 12% of leaders currently see this as a shared responsibility across IT and Security. However, in three to five years, APAC respondents anticipate that the primary decision-making authority for this task will be a shared responsibility across teams (46%), with only 19% believing Security alone will remain the primary decision maker. This could alleviate the existing bottleneck for Security.

- **Driving collaboration between Security and IT teams is the top priority in APAC.** In looking at top priorities for the next 12 months, IT and Security teams in APAC agree that their No. 1 goal (56%) is to drive collaboration and alignment between themselves (see Figure 2). This goal is not isolated to APAC, as it was the top goal for North America and EMEA decision makers as well. This number jumps even higher in India (69%), while only 48% in China and Singapore see this as a top goal for their organizations for the next 12 months. While this is the top priority for most countries included in the study around the globe, interestingly Singapore respondents rank this as No. 6 on their list, instead naming moving infrastructure and applications to the cloud (67%) as their top priority — a goal that respondents in other nations rank much lower on their list (38% in Australia and 27% in South Korea) as they may have already completed this migration or have not developed their cloud migration plans. The complete list of priorities for APAC comprehensively addresses the entire business portfolio: people, processes, and technology. Senior leaders understand that IT and Security need to have a positive and collaborative relationship to accomplish their key objectives.

Figure 2: Top IT Organization Priorities In APAC

“Which of the following initiatives are likely to be your IT organization’s top priorities over the next 12 months?”



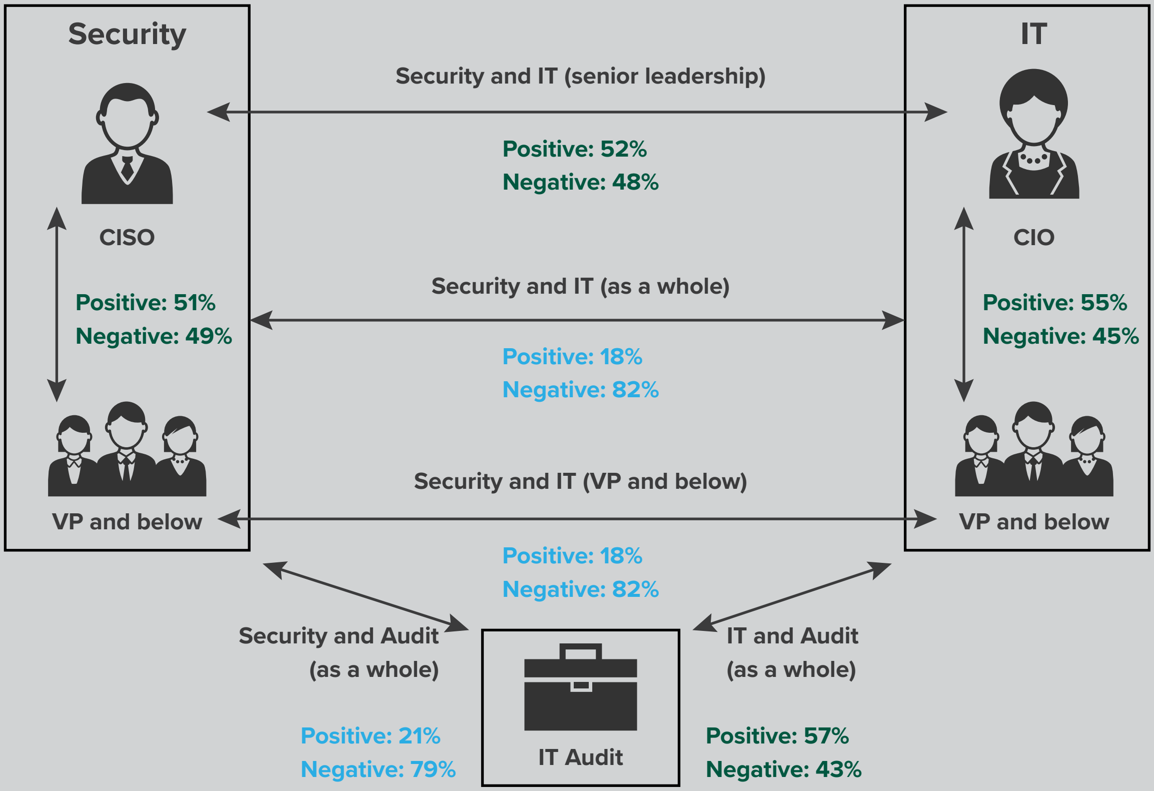
Base: 276 IT and Security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

NEGATIVE RELATIONSHIPS AND TECHNOLOGY CHALLENGES PLAGUE TEAMS

Although collaboration is a top goal, APAC countries face significant barriers to achieving it as strained relationship and technology challenges often stand in their own way. In researching these challenges, we found that:

- **Significant tension often exists between IT and Security teams in APAC despite the goal of collaboration.** In an assessment of these relationships, we found the most negative relationships exist between IT and Security as a whole and IT and Security practitioners (see Figure 3). Security's relationship with Audit is also a strain, but surprisingly, IT has a better relationship with Audit than any other relationship that exists. Audit plays a valuable role allowing organizations to trust, but verify, that what they say is happening, actually is. But oversight bodies aren't often loved by the teams that interact with them. The fact that IT embraces IT Audit above Security teams is concerning considering that Security should be a teammate and Audit should be an overseer.

Figure 3: Nature Of IT And Security Relationships In APAC



Base: 276 IT and Security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

- **Talent shortages for IT and Security abound both globally and regionally.** Although many respondents in APAC report being understaffed, they are not alone. Understaffing is a global issue for both IT (53% in APAC, 53% in EMEA, 52% in North America) and Security teams (65% in APAC, 59% in EMEA, 69% in North America). In reflecting on the global security talent shortage, one CIO noted:

  - "There's a massive shortage. There's no doubt that there's a shortage of resources and expertise in the security domain. I think it's getting better, but very slowly. In the Canadian market, there are now universities that are focusing on dedicated programs around security. In Ontario, they're actually building a dedicated university or college around [cybersecurity], which is fantastic. The US has an improving space, but it's still very challenging to hire the right resources. In Australia, it's almost impossible. I operate there as well. And in the UK, it's very difficult to find. So, there's definitely a global shortage of expertise in the security domain." – *CIO of a tech solutions organization*

  Despite efforts APAC organizations have taken to attract better talent by increasing the salaries and benefits (78%), decision makers note that it is still incredibly challenging to find the right personnel for critical IT and Security roles. In fact, APAC leaders report that it is very or extremely challenging to find the right Security (81%), threat-hunting (75%), or IT (72%) talent. As organizations are moving more threat hunting tasks to a shared model, this challenge will be even more crippling as three in four decision makers find it very or extremely challenging to obtain the right personnel! Leaders in some APAC countries feel the talent shortage worse than others. For example, the percentage of respondents who think finding the right threat-hunting talent is very/extremely challenging is much higher in Australia (81%), Japan (81%), and China (80%) than in Singapore (58%). Meanwhile, an astronomical 96% of leaders in China say finding the right Security talent is very/extremely challenging, perhaps due to their quickly growing economy.

"There's definitely a global shortage of expertise in the security domain."

In APAC, it is very or extremely challenging to find the right:

- Security talent (81%).
- Threat-hunting talent (75%).
- IT talent (72%).

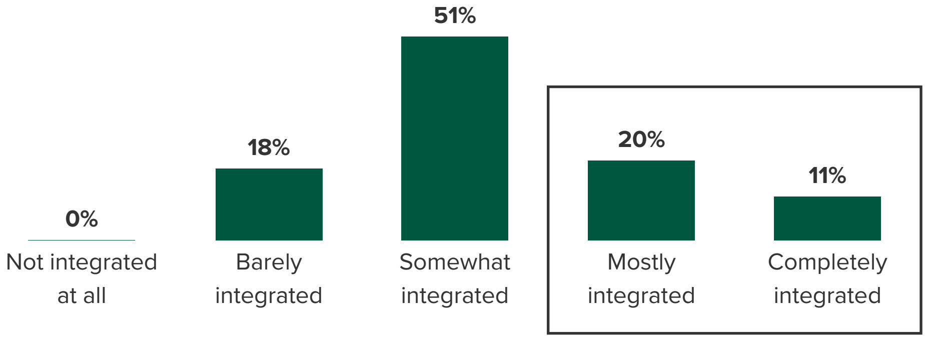
- **Technology challenges compound these problems.** Technology challenges make collaboration shortfalls even worse in practice as teams face an overwhelming number of misaligned tools, ineffective security products, and other security challenges. On average, APAC companies have 27.0 security products. However, only 31% say these solutions are mostly or completely integrated (see Figure 4). When investigating which components need to be integrated for respondents to claim they have well-integrated solutions, we found the bar is set very low. Of those who claim to be well integrated, many critical components are excluded as leaders only report the following integrations:

  - Technology based on security information and event management (SIEM) tools: 67%.
  - User interfaces: 55%.
  - Data products and tools: 53%.
  - Compliance based on audit: 50%.
  - Operational processes based on security operation centers (SOCs): 40%.

The large number of discrete security tools combined with the lack of holistic integration is leading to high levels of dissatisfaction. Even when looking at enterprise firewalls — some of the most established security tools in the marketplace — only half (55%) of APAC respondents say they are satisfied with the firewall solutions they have.

Figure 4: Integration Of Security Solutions In APAC

“How well-integrated are the security solutions in your organization?”



Base: 276 IT and Security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

- **Only one in three APAC respondents has a unified IT and Security strategy.** Collaboration struggles abound as teams are moving to a shared task model but do not share a unified, consolidated strategy. This is true globally and not just in APAC. Even though collaboration is a top goal, only 31% of those in APAC say they have a unified and consolidated IT management and Security strategy in place today (30% in North America, 29% in EMEA). Although 40% in APAC are planning to implement a unified strategy in the next 12 months, these organizations face an uphill battle as their plans to implement a unified strategy are reactive to the challenges they are facing rather than a proactive solution for a shared strategy from which both teams should be operating.

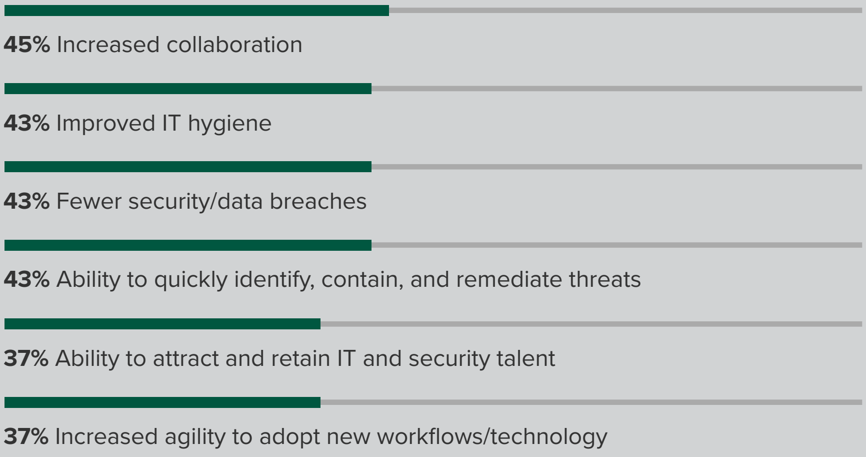
Consolidated Strategies Help APAC Organizations Meet Key Objectives

APAC organizations must be prepared to address the challenges they face with people, processes, and technology to harness the benefits of a unified security strategy. In researching the benefits of a unified security strategy, we found:

- **Teams plan to resolve collaboration issues in the near-term.** Despite the challenges they face, organizations are determined to address their relationship woes to lay a foundation for future collaboration. Today, 55% of APAC respondents agree that IT and Security want to be unified but face obstacles that prevent unification. Although respondents in Australia (44%) and Singapore (42%) don't claim as many obstacles in their way today, those in China (66%) and Japan (66%) face more difficulties with a significantly higher amount reporting that their unification is hindered. However, APAC respondents expect these hinderances to be greatly reduced in the near future. Only 21% of APAC decision makers (18% in China and 23% in Japan) believe that these obstacles will still hinder unification in three to five years. This significant reduction in obstacles means that companies are hyper-focused on addressing these critical collaboration issues now to create a more solid foundation for the future.
- **Consolidated IT and Security strategies are proven to help resolve critical issues.** For APAC to have such high expecations for overcoming critical IT and Secuirty issues over the next several years, they must have a consolidated strategy across people, processes, and technology. Companies must take a proactive approach to relieving relationship strains and technology barriers that inhibit success. Creating a unified and consolidated strategy will put the right tools into the hands of the right people who are empowered by the right processes to perform their jobs. This creates tech-enabled collaboration through shared tools and will greatly help to reduce the number of security breaches — two things organizations need the most (see Figure 5).

Figure 5: Benefits Of A Consolidated Strategy In APAC

"What are the benefits of a unified, consolidated IT management and security strategy?" (Top 6 shown.)



Base: 276 IT and Security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

- **Increased security and improved asset visibility drive the adoption of a unified strategy for APAC organizations.** In APAC, decision makers whose companies have already adopted a unified strategy cited these as their top three drivers of adoption:

  - Increased security (56%).
  - Better asset visibility (49%).
  - Technological advancement (42%).

  Business leaders around the globe cite increased security as the top driver for both IT and Security teams, indicating that they are aware Security sould be taken out of its silo and viewed as a shared responsibility.

Key Recommendations

APAC companies have a clear desire to unify their IT and Security teams. However, negative relationships and uncoordinated tools have hindered collaboration. Misaligned priorities and a fragmented technology landscape can keep even well-intentioned teams from achieving their collaboration and consolidation goals. Forrester's in-depth survey of security strategy decision makers yielded several important recommendations to help you avoid these pitfalls.

Focus on proactive improvements that can make consolidation efforts more seamless. APAC teams are aware that IT and security tasks should be shared, but they have significant improvements to make for consolidation to be more successful. Security has become a multicompetency discipline that requires expertise and collaboration from different departments. Whether separate teams or units within the same department, both your IT and Security leaders should follow the example of successful peers to turn to a shared responsibility model that incorporates the expertise your teams need to successfully defend technology initiatives, protect users, and avoid costly reputational damage. These collaboration efforts should specifically be of priority for China and Singapore decision makers, who rank collaboration between teams much lower than leaders in other APAC countries. Duplicate what successful teams have implemented, like what exists between IT and IT Audit, as examples of what security and IT should emulate: open lines of communication, complementary (rather than competing) goals, and share consolidated processes/technologies where possible to streamline efforts.

Consolidate your IT and security strategy to have fewer breaches and faster response. By consolidating your strategy, Security and IT can share activities, allowing each to get out of the other's way. This will result in more proactive work like threat hunting. Although finding the right threat-hunting talent is particularly challenging for teams in Australia, Japan, and China, the consolidation of other tasks leaves room to reskill existing personnel for threat-hunting duties. The earlier a breach is caught, the less impact it has overall, freeing up personnel from reactive to proactive tasks. Leaders who feel they have successfully unified their strategies say that it has yielded faster response times and threat remediation — two of the things APAC organizations need the most. They have also experienced collaboration and IT improvements such as improved hygiene. These benefits, combined with fewer security breaches, add great value to IT and Security teams. Consolidating your IT and security strategy might seem daunting, but the wins make it worth it.

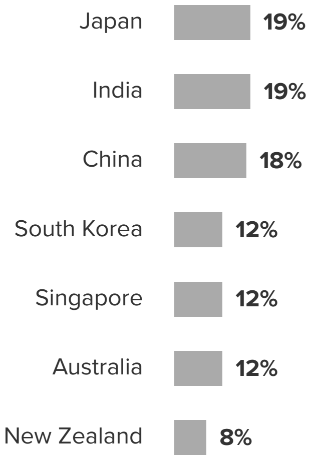
Ensure technology does not stop APAC resources from succeeding together. Unfortunately, most participants are bogged down by dated approaches from vendors. Despite efforts to unify strategies, organizations are left unprepared, unintegrated, and dissatisfied with the outcomes due to legacy technologies. Both China and Japan, whose decision makers report facing significantly more hinderances in their unification plans, should focus their efforts here. To unify your IT and Security teams, look for technologies that can satisfy both IT and Security teams so the tension borne from competition for scarce resources can subside.

Appendix A: Methodology

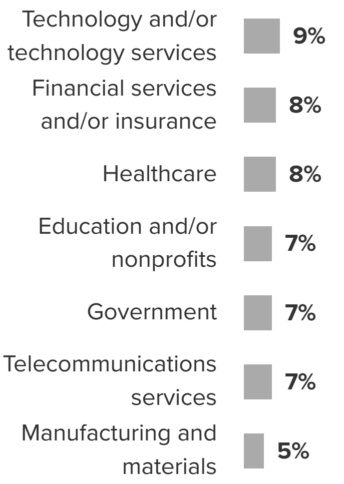
In this study, Forrester conducted an online survey with 1,451 manager-level and above IT and Security respondents at global organizations across industries to evaluate the relationship between IT and Security teams, as well as the challenges and benefits of having a unified, and consolidated IT management and security strategy. Forrester also conducted eight qualitative interviews with CIOs and CISOs about this topic. The study was completed in February 2020.

Appendix B: Demographics/Data

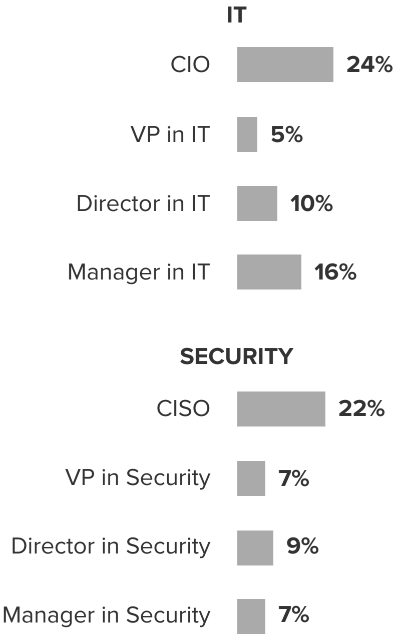
APAC COUNTRIES



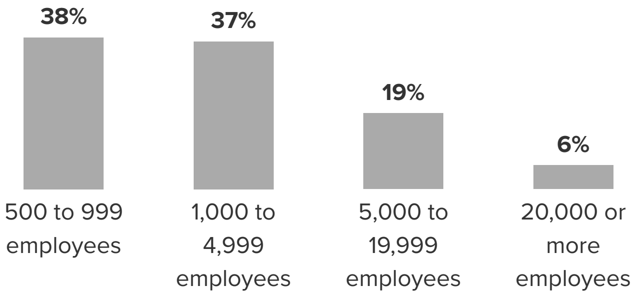
TOP 8 INDUSTRIES



RESPONDENT ROLES



COMPANY SIZE (BY EMPLOYEES)



Base: 276 IT and Security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

To read the full results of this study, please refer to the Thought Leadership Paper commissioned by VMware titled [“Tension Between IT And Security Professionals Reinforcing Silos And Security Strain”]

Project Directors:
Emily Drinkwater,
Market Impact Consultant

Contributing Research:
Forrester’s Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester’s Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.