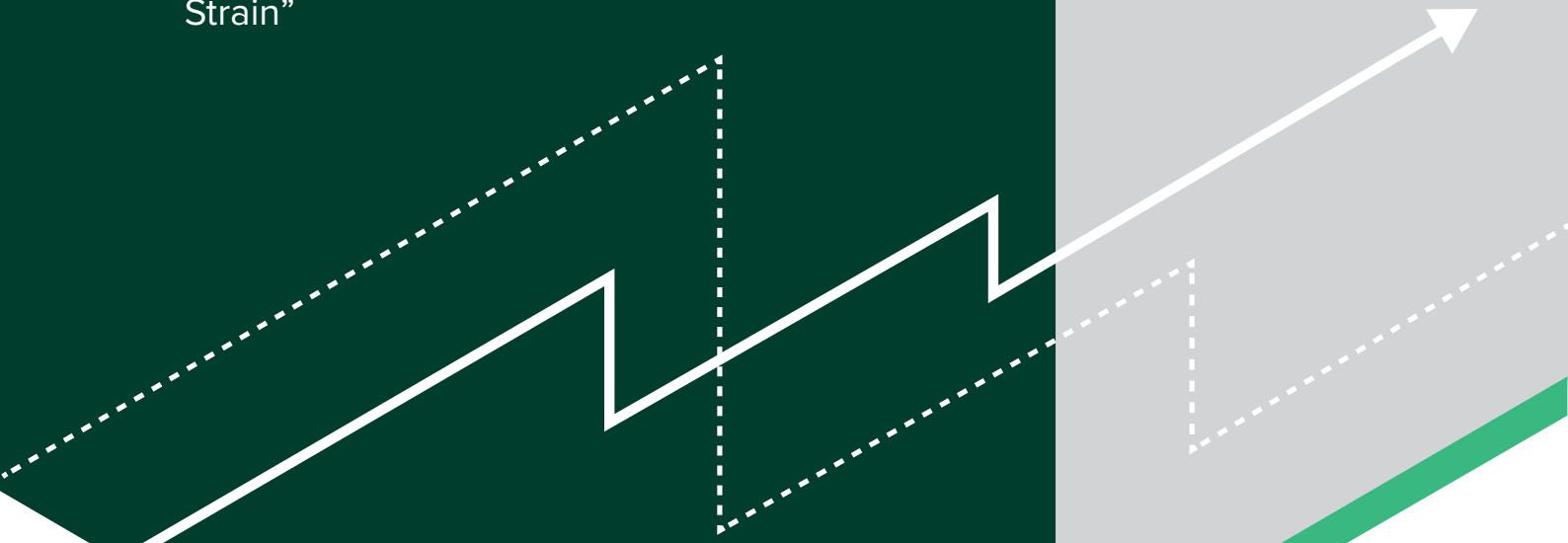
A Forrester Consulting
Thought Leadership Spotlight
Commissioned By VMware

May 2020

IT And Security Silos: A Spotlight On The EMEA Region

Results From Europe, The Middle East, And Africa For The May 2020 Thought Leadership Paper "Tension Between IT And Security Professionals Reinforcing Silos And Security Strain"



FORRESTER®

Introduction

Around the globe, IT and Security teams face major risks and concerns daily. However, in many cases, teams are 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, 665 were from the Europe, Middle East, and Africa (EMEA) region. This Spotlight concentrates on the survey results from EMEA. 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 the area of cybersecurity.

KEY FINDINGS

- **Collaboration is a top priority for both IT and Security in EMEA.** Companies rank collaboration between IT and Security as their top goal for the next year and are moving to a shared tasks model.
- **Despite collaboration goals, negative relationships plague teams.** EMEA teams face challenges across the whole portfolio: people, processes, and technology. With an overwhelming majority claiming negative relationships between teams, it is no wonder that collaboration is an ongoing struggle.
- **Consolidated strategies solve key challenges for teams.** To try to counter this tension, organizations in EMEA are implementing a more unified and consolidated IT management and security strategy. While only a third of organizations have adopted this, more are planning adoption in the next year with the objective of improving security and visibility.

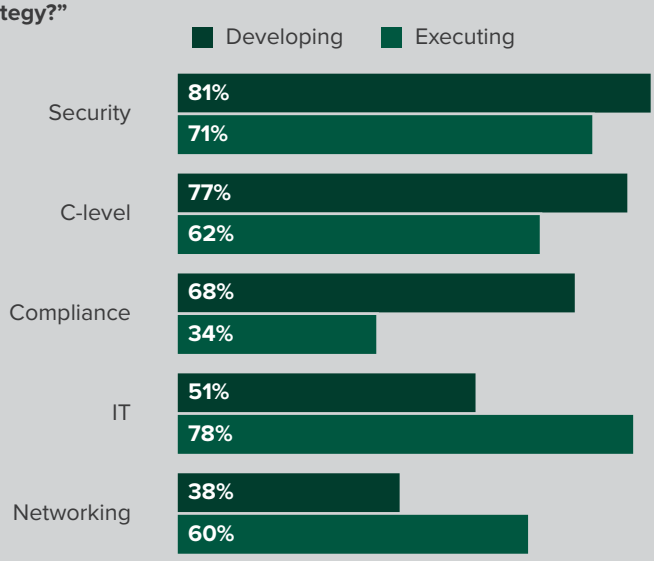
IT And Security Teams Prioritize Collaboration Despite Challenges

IT and Security functions are becoming even more critical to organizations around the globe. Now more than ever, it is becoming vital to have a unified approach to security. Security team members no longer solely own security responsibilities. Instead, it is becoming a collaborative undertaking with IT (including networks). By conducting both quantitative and qualitative surveys in EMEA, we found that:

› **Security is becoming a shared responsibility across teams.** Organizations are aware that security should be a team sport and are moving most security responsibilities to a shared model between teams and functions. 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 51% of EMEA respondents note that IT teams are involved in the development of a security strategy (it is typically managed by Security and C-level teams), 78% report that IT is responsible for its execution. However, C-level involvement varies at the country level. Both Russia (92%) and Spain (90%) report involvement from the C-suite in security strategy development, while this falls to as low as 50% in the UK. Respondents there note that the highest level of both development (83%) and execution (82%) rests in the hands of the IT team. 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 EMEA

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



Base: 665 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

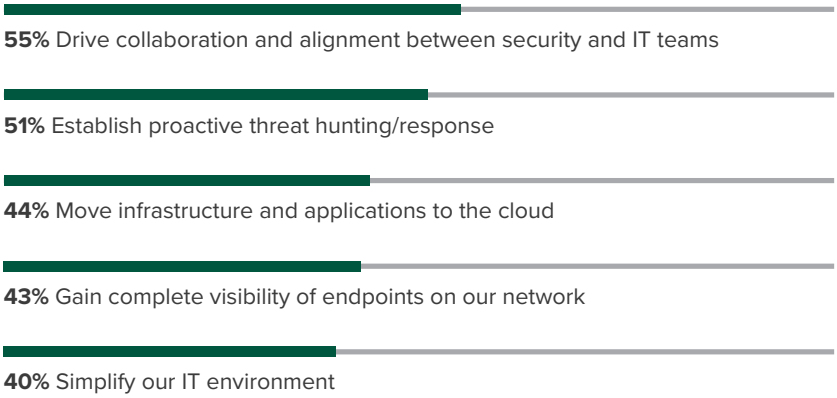
The Security team alone is no longer solely responsible for the development and execution of the security strategy.

FORRESTER®

› **Collaboration and alignment are the top priority in EMEA.** In looking at top priorities for the next 12 months, IT and Security teams in EMEA agree that their top priority is to drive collaboration and alignment between themselves (55%) (See Figure 2). This number jumps even higher in countries like Spain (73%) and Russia (60%). However, Russia does rank one priority even higher: the establishment of proactive threat hunting/responses (65%). The complete list of priorities for EMEA comprehensively addresses the entire business portfolio: people, processes, and technology. It is clear to senior leaders that IT and Security need to have a positive and collaborative relationship backed with the technology and processes.

Figure 2: Top IT Organization Priorities In EMEA

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



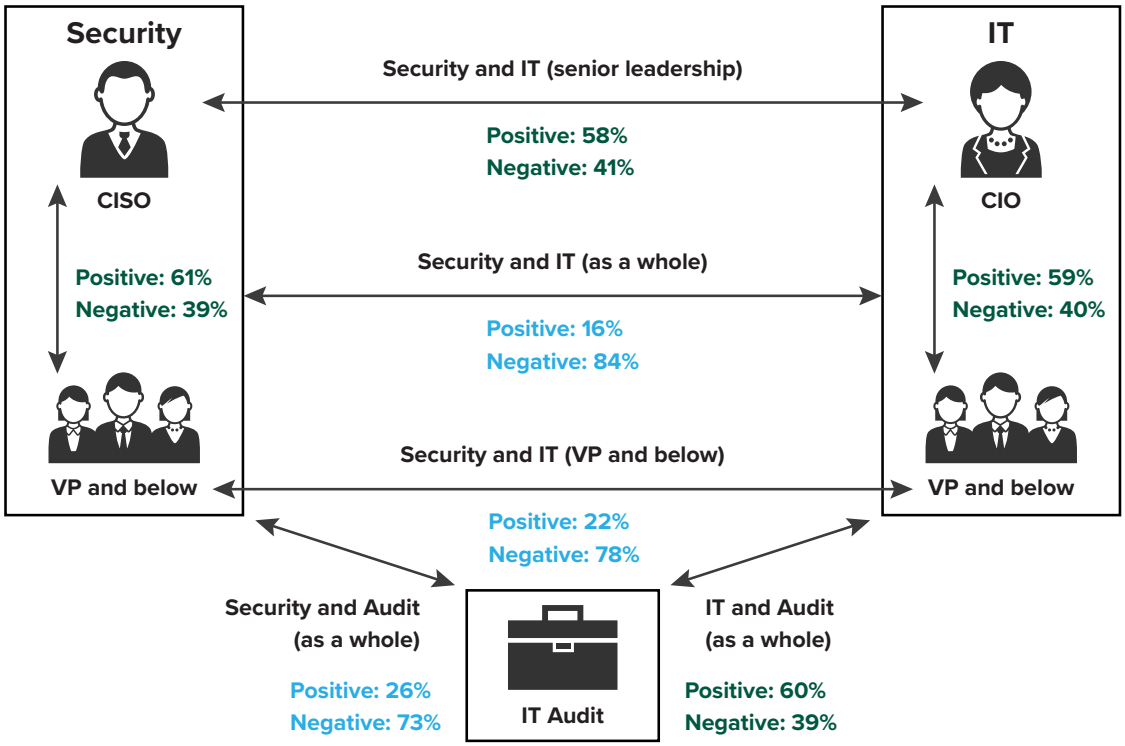
Base: 665 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

DESPITE COLLABORATION GOALS, NEGATIVE RELATIONSHIPS PLAGUE TEAMS

Despite the shared goal of collaboration, there are significant barriers to achieving it as teams often stand in their own way. In researching these challenges, we found that:

› **Despite the goal of collaboration, there is often significant tension in the relationships between IT and Security teams in EMEA.** In an assessment of these relationships, we found the most negative relationships exist between IT and Security as a whole (see Figure 3). This is largely driven by the negative relationships between the IT and Security practitioners (VP/below).

Figure 3: Nature Of IT And Security Relationships In EMEA



Base: 665 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

› **IT and Security teams face global and regional talent shortages.** Although many respondents in EMEA reported being understaffed, they are not alone. Understaffing is a global issue for both IT (53% in EMEA, 52% in North America, 53% in APAC) and Security teams (59% in EMEA, 69% in North America, 65% in APAC). 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 in the US

Although EMEA respondents noted their organizations have taken more measures to increase the salaries and benefits they offer to attract better talent (73%), it is still very difficult to find the right new hires. EMEA respondents noted that it is very or extremely challenging to find the right security (85%), threat-hunting (72%), or IT (69%) talent. Organizations in some countries feel the talent shortage worse than others. For example, the percentage of respondents who think finding the right security talent is very/extremely challenging skyrockets in Germany (90%), Spain (92%), and France (96%).

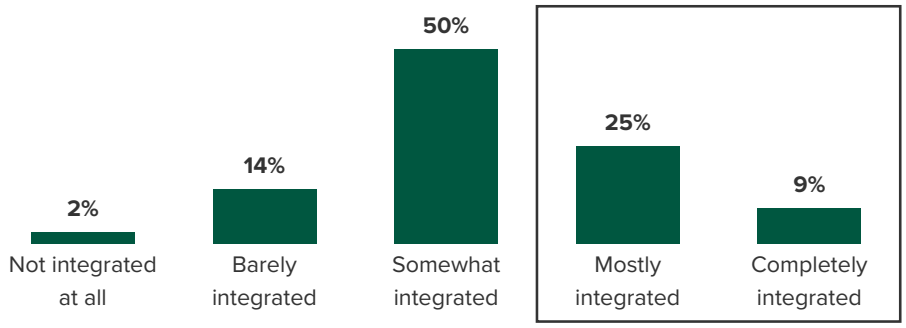
In EMEA, it is very or extremely challenging to find the right:

- Security talent (85%)
- Threat-hunting talent (72%)
- IT talent (69%)

› **Technology challenges exacerbate these problems.** Technology challenges make these collaboration shortfalls even worse in practice as teams face an overwhelming number of misaligned tools, ineffective security products, and other security challenges. On average, EMEA companies have 28.2 security products. However, only 34% say these solutions are mostly or completely integrated (see Figure 4). The large number of discrete security tools combined with the lack of 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 (53%) of EMEA respondents say they are satisfied with the firewall solutions they have.

Figure 4: Integration Of Security Solutions In EMEA

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



Base: 665 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

› **Only a third of EMEA respondents have a unified IT and Security strategy.** To further compound the collaboration struggles, even teams that should be working harmoniously together in the existing model are often at odds with each other. This is true globally and not just in EMEA. Even though collaboration is a top goal for respondents, only 29% of those in EMEA say they have a unified and consolidated IT management and Security strategy in place today (30% in North America, 31% in APAC). Although 40% in EMEA are planning to implement a unified strategy in the next 12 months, organizations are playing catch-up and are consolidating strategies as an afterthought to the challenges they faced, rather than as a foundation from which both teams should be operating.

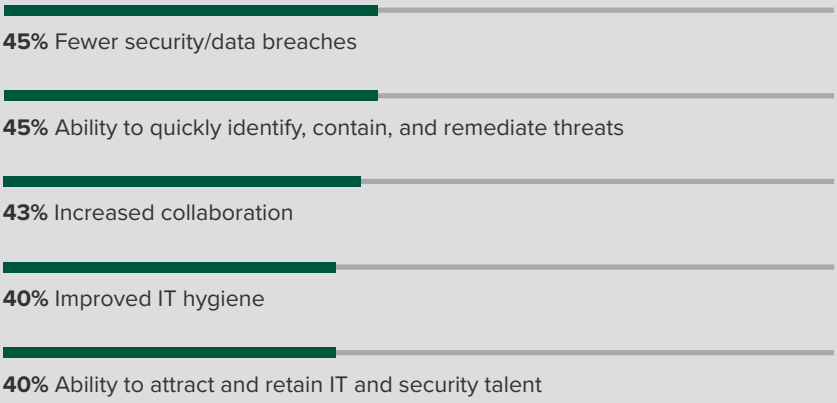
Consolidated Strategies Solve Key Challenges For Teams

In order to address the challenges outlined earlier and to create a unified security strategy, organizations must address all key internal dimensions of business: people, processes, and technology. In researching the benefits of a unified security strategy, we found:

- **Teams are aware of and plan to resolve collaboration issues in the near-term.** Despite the barriers, organizations are resolved to address their cross-team challenges and to help mitigate future crises. Currently, 54% of EMEA respondents agree that IT and Security want to be unified, but they face obstacles that prevent unification. Although respondents in France don't claim as many obstacles in their way today (only 34%), those in Spain face major difficulties with 69% reporting that their unification is hindered. However, respondents in Spain, along with those in all EMEA countries, expect this to fall in the future. Only 17% of EMEA organizations (18% in Spain) believe that these obstacles will still hinder unification in three to five years. This means that companies are hyper-focused on addressing these critical collaboration issues now to create a more solid foundation for the future.
- **A consolidated IT and Security strategy would help to resolve key issues**. The key component of resolution for EMEA teams is to have a consolidated strategy across people, processes, and technology. Companies must look to alleviate 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 will create tech-enabled collaboration through shared tools and it 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 EMEA

"What are the benefits of a unified, consolidated IT management and security strategy?" (Top 5 shown.)



Base: 665 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

FORRESTER®

› **Security and technology advancements are top drivers of the adoption of a unified strategy.** EMEA organizations that have already adopted a unified strategy cited these as their top three drivers of adoption:

- Increased security (46%)
- Technological advancement (45%)
- Better asset visibility (45%)

Interestingly, organizations around the globe cited increased security as the top driver for both IT and Security teams. They know security should be a team sport, and not just left to Security teams alone.

Key Recommendations

From the research, it is clear that there's a strong desire in EMEA for IT and Security teams to work together, but the result of attempted collaborative efforts often leaves both teams unhappy with each other. Misaligned priorities and a fragmented technology landscape give teams a scarcity mindset. Competing over time, attention, and budgets can cause even the most well-intentioned strategies to fail.

However, Forrester's in-depth survey of security strategy decision makers about unified IT and Security strategies yielded several important recommendations to help you avoid these pitfalls.

EMEA teams already see IT and security becoming a team sport, but they must work to make consolidation efforts seamless. Today, this domain has become a multicompetency discipline that requires expertise from many different departments. Whether they're 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 various types of expertise your teams need to successfully defend enterprise technology initiatives, protect your users, and avoid costly brand and reputational damage. Recognize that the most successful teams have open lines of communication, work under complementary (rather than competing) goals, and share consolidated processes and technologies where possible to streamline efforts.

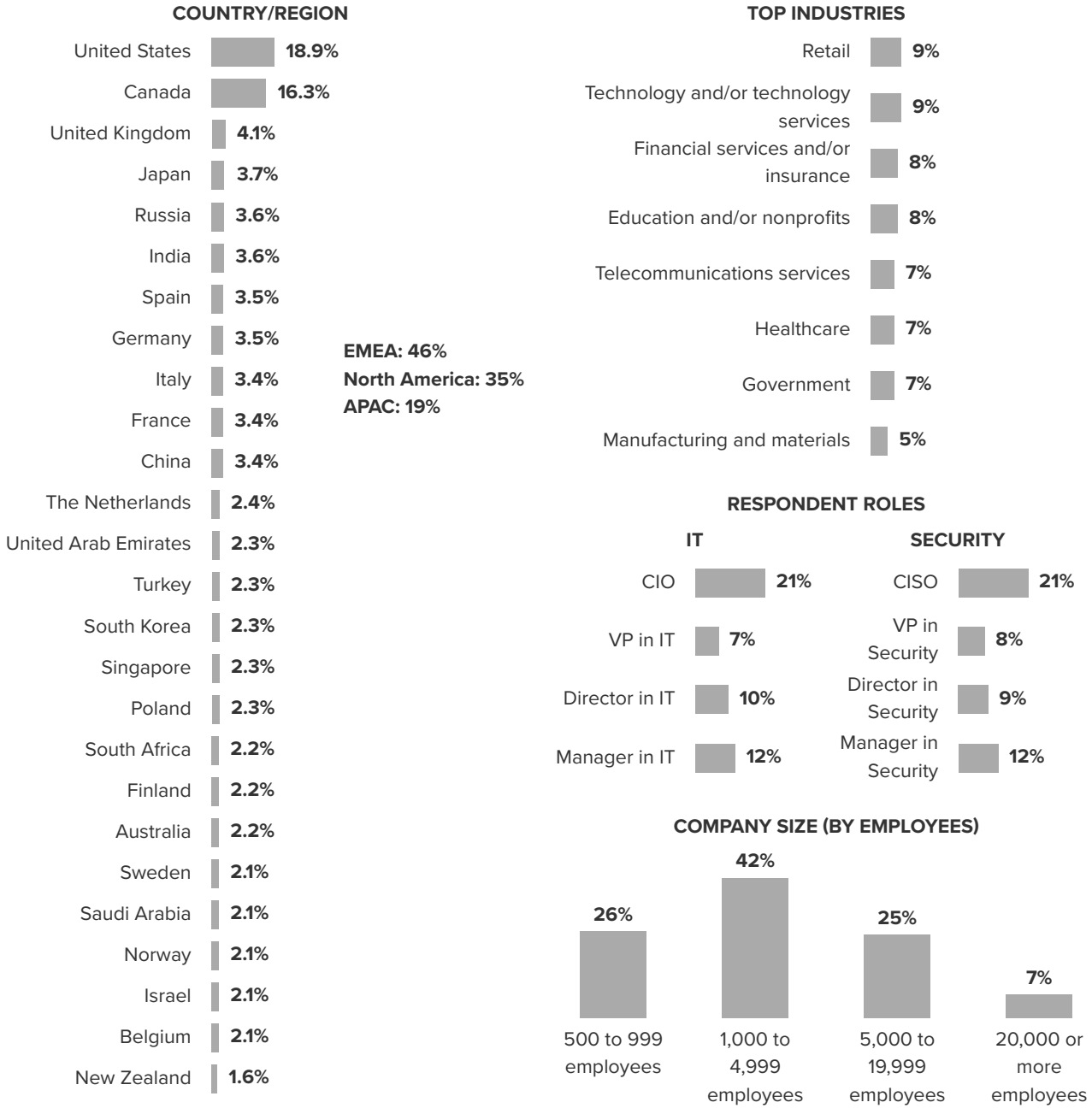
Consolidate your IT and security strategy to have fewer breaches and faster response. Organizations that felt they had successfully unified their strategies showed it paid off for them with reduced friction for the Security team in the form of faster response times and threat remediation. They also experienced collaboration and IT improvements such as improved hygiene. These benefits combined with fewer security breaches add great value to IT and Security teams. While consolidating your IT and security strategy might seem daunting, the wins make it worth it.

Make sure technology does not stop EMEA resources from succeeding together. Unfortunately, most participants found themselves hobbled by dated approaches from the vendors they worked with. In spite of efforts to unify strategies and become more collaborative, organizations are left unprepared, unintegrated, and unsatisfied with the outcomes due to tools and technologies that operate on a legacy basis. To unify your IT and Security teams, you need to start looking for technologies that can support the needs of both sets of stakeholders, satisfying 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



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

FORRESTER®

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 Director:
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.

FORRESTER®