A Forrester Consulting
Thought Leadership Paper
Commissioned By VMware

May 2020

Tension Between IT And Security Professionals Reinforcing Silos And Security Strain

A Unified IT And Security Strategy Can Lay A Foundation For Future Success

FORRESTER®

Table Of Contents

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.

Executive Summary

In today's modern landscape, 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 learn how executing against a consolidated IT management and security strategy could help break down silos across the two teams to improve security outcomes. We also explored the relationship between IT and security teams, including the relationship between C-level and manager/director level employees within those organizations. Forrester conducted a global online survey with 1,451 manager level and above respondents and interviewed eight CIOs and CISOs to further explore this topic. All respondents had responsibility and decision-making influence over 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 unable to advance as desired.

KEY FINDINGS

- **Collaboration is a top priority for both IT and Security.** Companies ranked collaboration between IT and Security as their top goal for the next year. When security is viewed as a team sport, tasks can move to a shared responsibility model across teams.
- **Despite collaboration efforts, teams remain "frenemies."** Although collaboration is the goal, teams face challenges across the whole portfolio: people, processes, and technology. With an overwhelming majority claiming negative relationships between teams, it's no wonder that collaboration is an ongoing struggle.
- **Consolidated IT and Security strategies lay a foundation for future success.** To combat this tension, companies are implementing a more unified, consolidated IT management and security strategy. While only one-third of organizations have adopted this, more are planning adoption in the next year to improve security and visibility.

Collaboration Is A Top Priority For Both IT And Security

As threats of attacks and breaches grow in sophistication, it is more important than ever for both IT and Security functions to have a unified approach to security. Security team members no longer solely own security responsibilities; it's becoming a collaborative undertaking with IT. By conducting both quantitative and qualitative surveys, we found that:

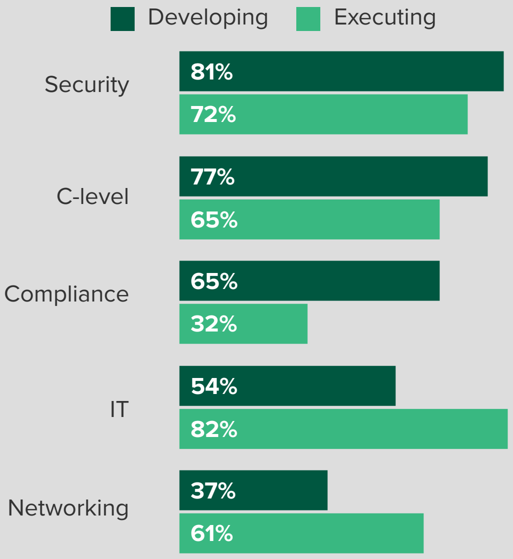
- **Security is moving to a shared responsibility model.** Organizations are aware that security should be a team sport and are moving most security responsibilities to be shared between teams and functions. For example, many different functions are involved in the development and execution of the security strategy beyond just the Security team alone (see Figure 1).

  Respondents also indicated that while many tasks are currently owned by either IT or Security alone, most tasks will be shared responsibilities in three to five years. In the future, more teams will share responsibilities such as IT security architecture (↑39.7%), threat hunting/remediation/incident response (↑33.1%), and cloud security (↑29.9%).

- **Collaboration is the top priority.** There is clear executive buy-in and board attention for security. In fact, when asked what will likely be their IT organization's top priority over the next 12 months, IT and Security teams agreed that the top priority is driving collaboration and alignment between IT and security teams (55%) (See Figure 2).

Figure 1: Security Strategy Development And Execution

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



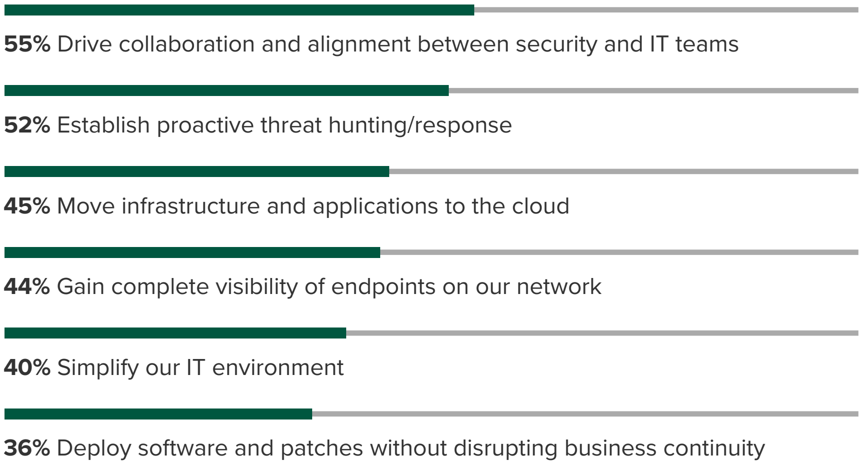
Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

Many different business functions are involved in the development and execution of the security strategy beyond just the Security team alone.

The complete list of priorities, however, comprehensively addresses the entire business portfolio: people, processes, and technology. It is clear to senior leaders that IT and Security need to consist of positive relationships and collaboration, backed by the technology and processes to enable them.

Figure 2: Top IT Organization Priorities

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



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

› **Outage prevention and incident resolution are the focus of teams.** When examining the top priorities of each team, there is general overlap when it comes to the goals of efficiency and preventing data breaches. However, some competing priorities come into play as IT is focused on preventing outages while Security is focused on incident resolution.

Figure 3: Top Team Priorities

"Rank the top three priorities for your team."

Top Three IT Priorities	Top Three Security Priorities
1 Efficiency (51%)	**1 Incident resolution (49%)**
2 Preventing data breaches (47%)	**2 Preventing data breaches (49%)**
3 Outage prevention (47%)	**3 Efficiency (47%)**

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

According to the chief information security officer (CISO) of a technology organization in the US, there is sometimes friction between teams. "We often have conflicting objectives. IT is hammered for uptime and availability and some of the things that Security might want to do impacts that." While the IT organization is concerned about keeping things constantly available and preventing any outages, the Security organization doesn't hesitate to bring something down to resolve an incident or investigate a threat.

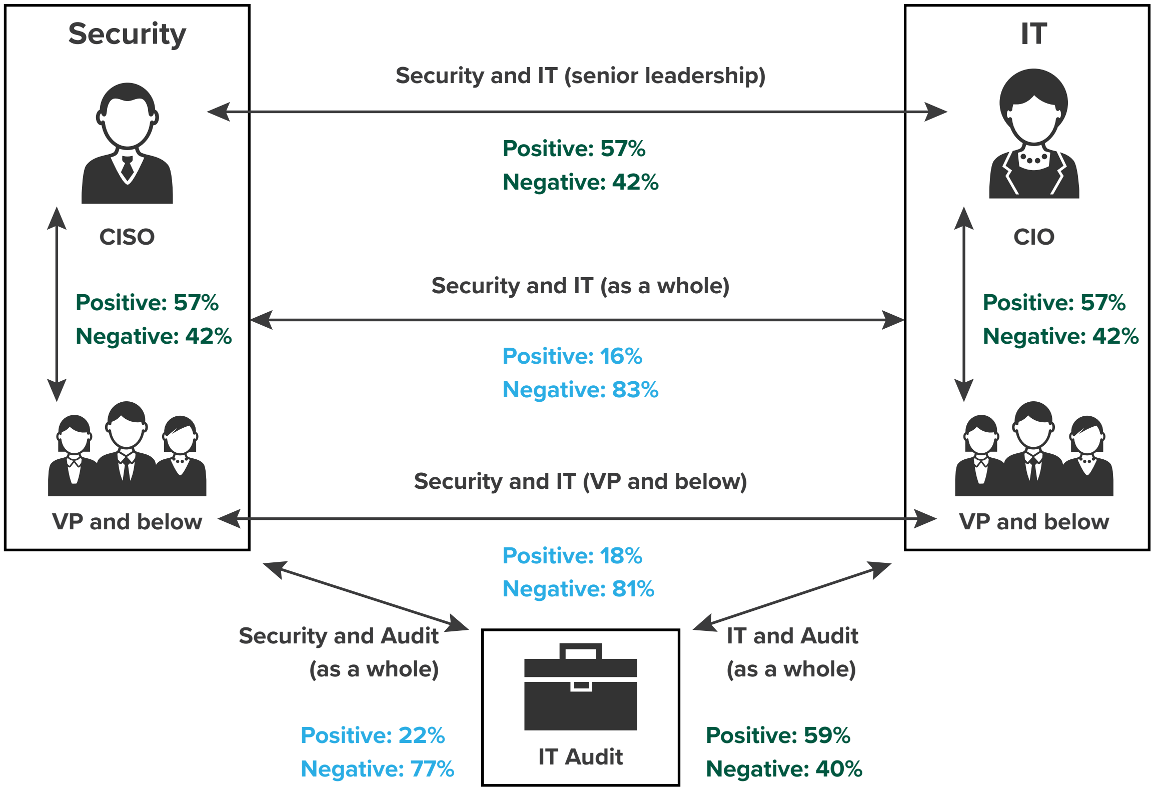
Despite Collaboration Efforts, Teams Remain "Frenemies"

Despite these efforts of collaboration, there are clear hurdles that stand in the way of being successful. In researching these challenges, we discovered:

NEGATIVE RELATIONSHIPS PLAGUE TEAMS

- **Despite the goal of collaboration, IT and Security experience tension.** In assessing these relationships, we found the most negative relationships between IT and security as a whole, but also amongst the IT and security vice president and below (see Figure 4).

Figure 4: Nature Of IT And Security Relationships

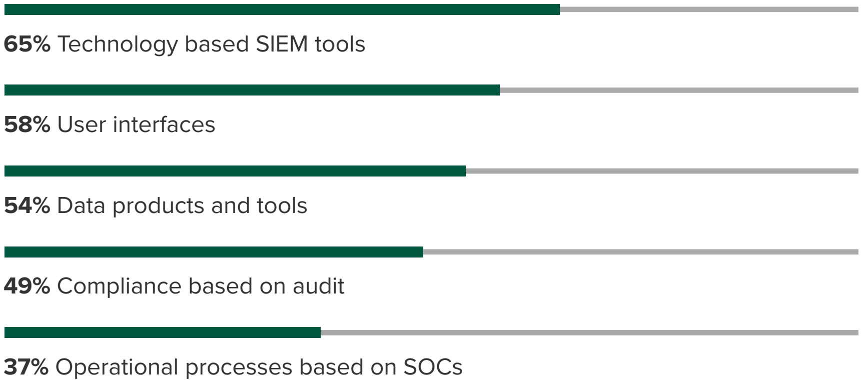


Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

- **Only one-third of 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 actually working at odds with each other. Although collaboration is a top goal for 55% of respondents, only 30% have a unified, consolidated IT management and Security strategy in place today. Although 41% 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 being faced, rather than as a foundation from which both teams should be operating. Even those that claim to have a unified strategy have not consolidated critical items across teams (see Figure 5). Reports of low degrees of consolidation include areas such as operational processes based on security operations centers (SOCs) (37%), compliance based on audit (49%), and data products/tools (54%). Ideally, all of these things would be consolidated (near 100%) across teams to truly signify unification. However, teams are willing to settle for much less than “across the board consolidation” while still considering it a unified strategy. Based on these findings, it appears that integrating just a few of these things makes respondents feel as though they are unified, even though this may only be minimally true.

Figure 5: Integrated Components Of A Consolidated Strategy

“You indicated that your security solutions are well integrated. Which of the following items are integrated at your organization?”



Base: 480 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

- **Both teams are in high-growth mode, leaving them focused inward rather than on collaboration.** Within the past 12 months, teams have increased their budgets (73% IT, 74% Security), purchased new products (68% IT, 72% Security), and increased their staff (56% IT, 61% Security). With the addition of new staff members, products, and budget, teams are often focused on their own inner workings rather than collaboration with others.
- **IT and Security teams are facing talent shortages.** Fifty-three percent of IT teams and 64% of Security teams reported being understaffed. While the C-level reported taking more measures to increase the salaries and benefits they offer to attract better talent (76%) and find skilled talent to fit evolving needs (70%) than focusing on reskilling current employees (64%), the filling of those roles is a top challenge. Respondents noted that it is very or extremely challenging to find the right security (81%), threat-hunting (70%), or IT (70%) talent. As a result of the shortage, two C-suite professionals reported a larger focus on hiring under-skilled workers to train internally and an increase in task automation in order to reduce the need for more employees.
  - “We’ve hired a lot more entry level folks and then just trained them up, and we’ve hired a lot of people who are not cybersecurity professionals and then added cyber security skills after we brought them over. We still hire experienced cybersecurity people, but a lot less as a proportion of the overall hires than we used to.” — *CISO of a tech solutions organization in the US*

  - "We're just automating everything because we have no choice. We don't have the people." — *CIO of an energy corporation in the US*

- **Communication is not always clear.** IT and Security teams report that communication gaps (80%) and communication silos across teams (74%) have major or extreme impacts on their ability to collaborate. Given the largely negative relationships that abound, it is not surprising that communication is often strained or even nonexistent. When asked what the biggest issue is for IT and Security teams, one CIO said: "It's 100% communication. It's people not communicating, not documenting, not telling somebody what they're doing. That is 100% the problem. You can put meetings together. You can do ticket reviews. It's just so difficult because people fundamentally just don't think about communicating. That's really where it's at." — *CIO of an energy corporation in the US*

- **IT leaders face pressure from the board.** Respondents agreed that senior leadership and boards have a greater focus on Security (89%) and IT (73%) than they did two years ago. CIOs and CISOs also said that the top concerns of the board include:

  - Brand protection (81%).
  - Security threats and risks to the business (78%).
  - Reducing risk and exposure (77%).

  These board priorities mean that CIOs and CISOs face heightened pressures from all sides. The push for collaboration across teams is a focus from the top down, in addition to reducing risk and protecting the company's brand.

ISSUES ARE MAGNIFIED BY TECHNOLOGY AND PROCESS CHALLENGES

- **Security threats are only becoming more advanced.** Senior leaders noted that, beyond internal collaboration and technology issues, security threats pose major challenges to their organizations. Top issues cited by CIOs and CISOs include:

  - **Unknown threats resulting in reputational damage.** "The security threats I'm most concerned about are ones that we don't know. I've got a really good handle on the ones we know about. We've taken a lot of work and a lot of effort to put the security controls and the layers in place to protect against the known. Reputational damage is my biggest fear. And the reputational damage would come from either one of our products being fundamentally insecure or bad guys [overtaking a product]." — *CIO of an energy corporation in the US*
  - **Threats to intellectual property.** "Protecting our intellectual property is always going to be one of the top things that we need to look out for." — *CISO of a tech solutions organization in the US*
  - **Threats from nation states looking to compromise both internal and external contacts.** "Nation states with infinite resources looking for valuable research data or compromising internal employees who have access to sensitive information [is an issue]." — *CIO of an educational institution in the US*

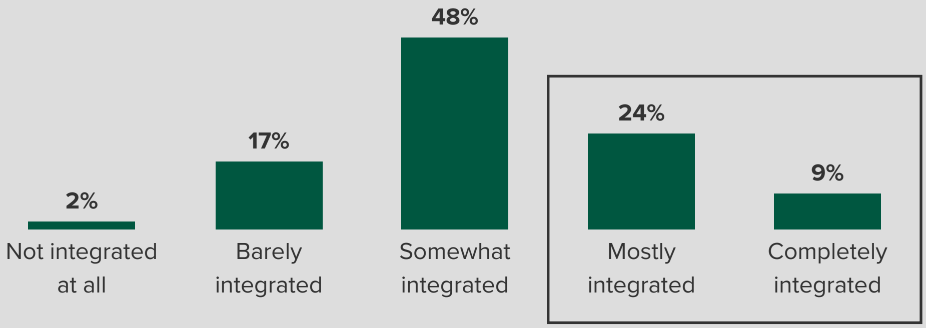
Companies in both the private and public sector must always be prepared for geopolitical risks. In fact, recent Forrester research shows that 72% of global CISOs agreed that they may be affected by geopolitical cyberactivity.[1] Given the advanced nature and exposure to potential threats, companies must be prepared to face these challenges when — not if — they arise.

- **Technology challenges exacerbate this negativity.** Technology challenges exacerbate these collaboration challenges as teams face an overwhelming number of misaligned tools, ineffective security products, and other security challenges. On average, companies have 27.4 security products. However, only one-third said their solutions are mostly or completely integrated (see Figure 6). The overwhelming number of tools combined with the lack of integration leads to high levels of dissatisfaction. Even when looking at enterprise firewalls — some of the most established security tools in the marketplace — only half (52%) said they are satisfied with the firewall products they have. When asked if security solutions were integrated, one CISO with a pharma organization in the US said: "No, I would not say that. As with most firms, the security solutions are built with a bunch of disjointed tools that were purchased because their functions were best in breed — or even currently are best in breed — and then don't necessarily work in harmony with one another."

Teams face an overwhelming number of misaligned tools, ineffective security products, and other security challenges.

Figure 6: Integration Of Security Products

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



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

Consolidated IT And Security Strategies Lay A Foundation For Future Success

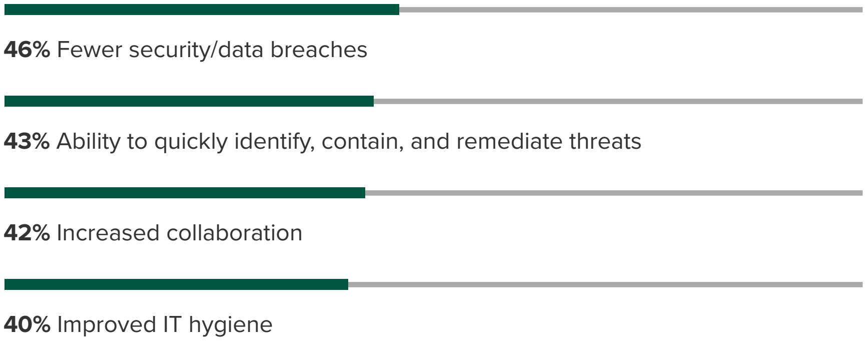
In order to address these critical challenges and create a truly unified security strategy, organizations must address all dimensions of business: people, processes, and technology. In researching the benefits of a unified security strategy, we found:

- **Teams plan to resolve collaboration issues in the near-term.** Despite the barriers, organizations are resolved to address their cross-team challenges and prevent future crises. Fifty-two percent of respondents agreed that IT and Security currently want to be unified, but they face obstacles that prevent unification. However, only 19% believe this will be true 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 resolve key issues.** The key component of resolution for teams is to have a consolidated strategy for the entire portfolio: people, processes, and technology. Alleviating relationship strain and communication issues are key barriers to overcome for the people, but process and technology barriers also inhibit success. Creating a unified, consolidated strategy would put the right tools into the hands of the right people, empowered by the right processes to perform their jobs. This would create tech-enabled collaboration through shared tools and greatly help to reduce the number of security breaches — two things organizations need the most (see Figure 7).
- **Security and technology advancements are top drivers of the adoption of a unified strategy.** Companies that have adopted a unified strategy cited these as their top three drivers of adoption:
  - Increased security (52%)
  - Technological advancement (47%)
  - Better asset visibility (41%)

  Interestingly, respondents 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. As noted in a recent Forrester report: “Network security starts and ends with visibility.”[2] By pursuing a unified strategy, companies choose to collaborate across teams and unify their efforts to increase visibility and accomplish big-picture security and technology goals.

Figure 7: Benefits Of A Consolidated Strategy

“What are the benefits of a unified, consolidated IT management and security strategy?”



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

A consolidated strategy would create tech-enabled collaboration and reduce the number of security breaches — two things companies need the most.

Key Recommendations

There's a clear desire for IT and Security teams to work together, but the result of collaborative efforts often leaves both teams unhappy with each other. Misaligned priorities and a fragmented technology landscape give teams a scarcity mindset. Competing for 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:

Security must become a team sport within your organization, not a siloed activity executed by an isolated Security team. Today, this domain has become a multicompetency discipline, requiring expertise from many different departments. Whether separate teams or units within the same department, both your IT and Security leaders should follow the directives 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. The most successful teams have open lines of communication, work under complimentary (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.

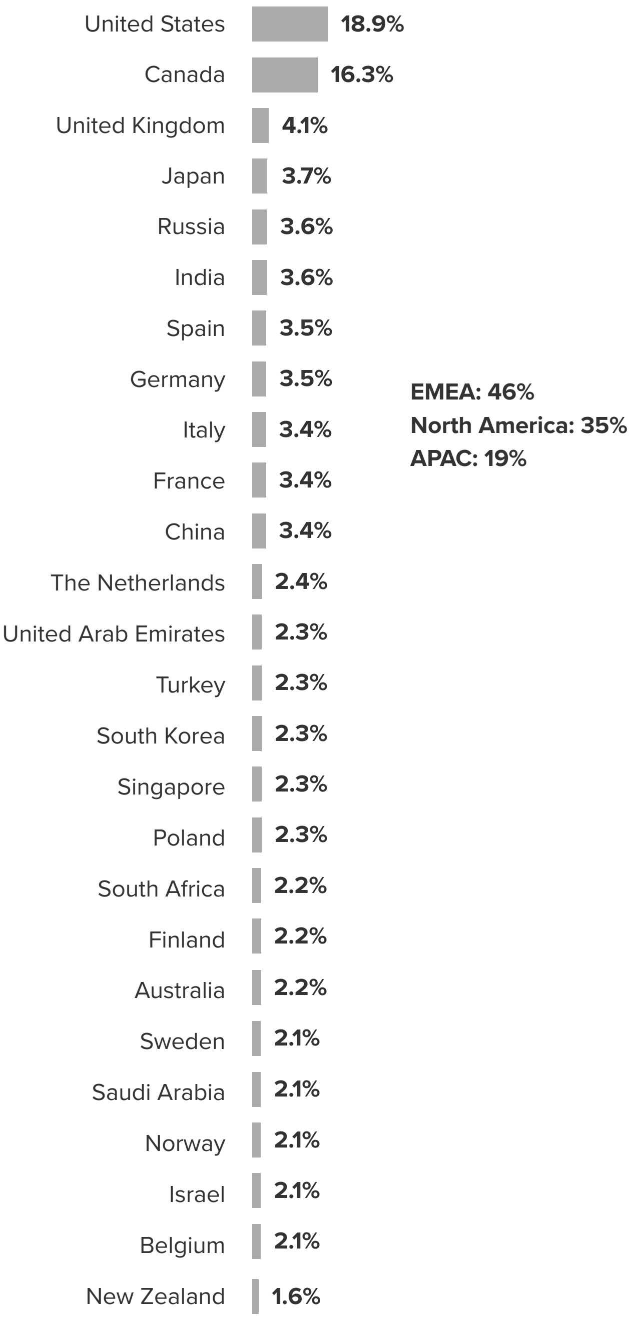
Get the right technology in place to prepare for the team sport approach. Unfortunately, most participants found themselves hobbled by dated approaches from the vendors they worked with. In spite of efforts to unify strategies and become more collaborative, organizations are left unprepared, unintegrated, and unsatisfied with the outcomes produced due to tools and technologies that operate on a legacy basis. To unify your IT and Security teams, you must start looking for technologies that can support the needs of both sets of stakeholders, satisfying both IT and Security teams so that the tension borne from competition over scarce resources can subside. Once the teams come together on agreed upon goals, objectives, and measures of success for projects, they can address their technology stack accordingly. This allows organizations to make more informed and solutions-based purchase decisions resulting in consolidated vendors, reduced operations complexity, and easier day-to-day operations.

Appendix A: Methodology

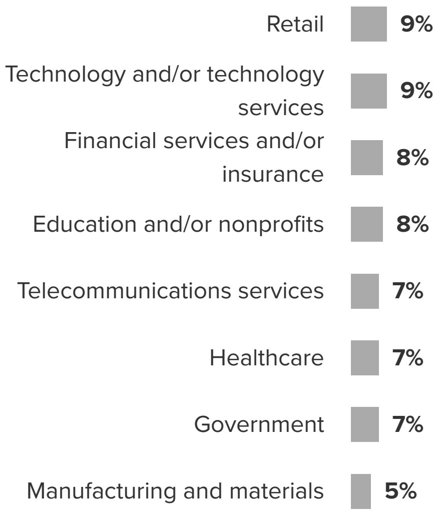
In this study, Forrester conducted an online survey with 1,451 manager level and above IT and Security respondents at global organizations across industries to evaluate the relationship between IT and Security teams as well as the challenges and benefits of having a unified, consolidated IT management 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

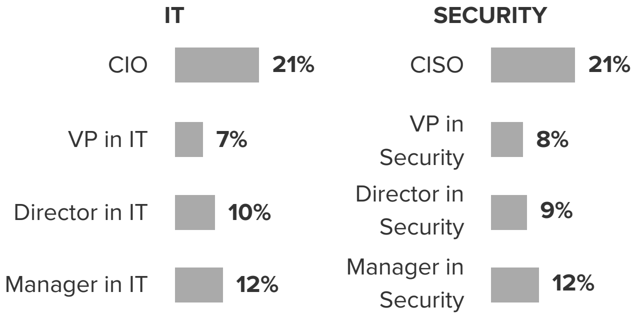
COUNTRY/REGION



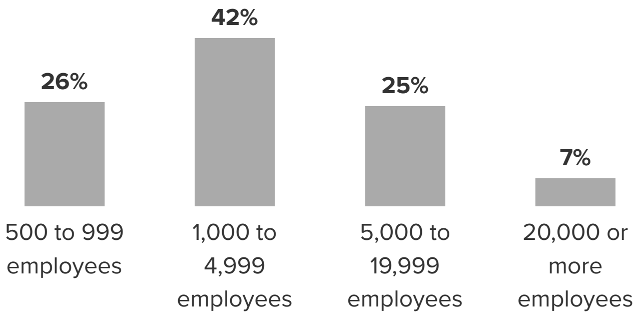
TOP INDUSTRIES



RESPONDENT ROLES



COMPANY SIZE (BY EMPLOYEES)



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

Appendix C: Endnotes

[1] "Ignore Geopolitical Risk At Your Peril," Forrester Research, Inc., January 31, 2020.

[2] "The Eight Business And Security Benefits Of Zero Trust," Forrester Research, Inc., September 25, 2019.