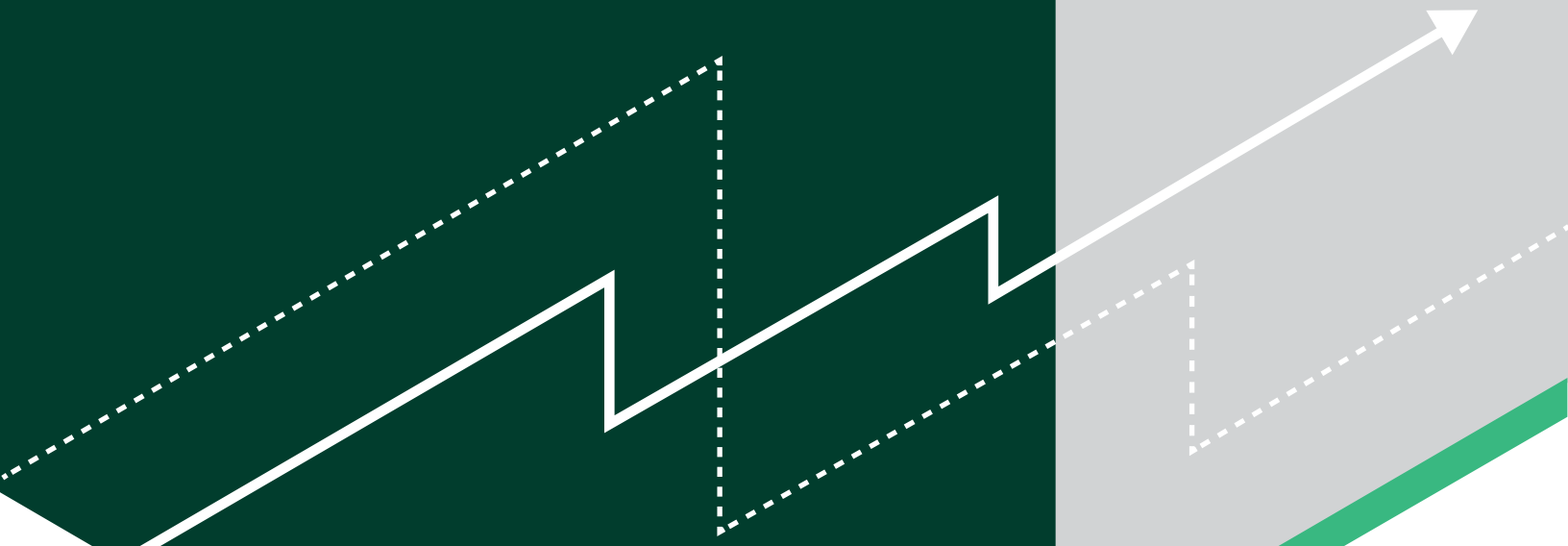
A Forrester Consulting
Thought Leadership Spotlight
Commissioned By VMware

May 2020

Security As A Team Sport: A Spotlight On The Growing Role Of IT In Security Tasks

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

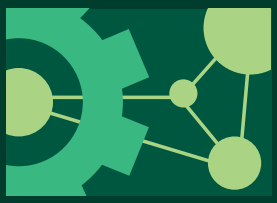


FORRESTER®

Introduction

IT and Security teams shoulder the responsibility of many mission-critical tasks in organizations, yet they often don't work together under a unified 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. This included an understanding of how the responsibilities of critical IT and security tasks are shared. 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 strategies.

We found that security is becoming an even greater shared responsibility with IT. Given this trend, IT and Security teams are transitioning and moving their respective tasks under the umbrella of a unified strategy. Without such a unified IT and Security strategy, companies are increasingly unlikely to advance as desired.



KEY FINDINGS

- **Collaboration between IT and Security teams is a priority for teams.** Fifty-five percent of business leaders cite increased collaboration as their top goal, and most already claim both IT and Security are jointly responsible for the development and execution of their security strategies.
- **Collaboration efforts are met with challenges.** As IT teams look to take on more Security tasks, they are met with an overwhelming number of security products that are not integrated, don't communicate easily with each other, and produce increasingly unsatisfactory results. Compounded by communication and relationship strains, this makes collaboration difficult.
- **Companies are starting to adopt a unified and consolidated IT and security strategy to address key challenges.** While only 30% have already implemented a unified and consolidated IT management and security strategy, 41% are planning to implement one within the next 12 months. Additionally, IT and Security tasks are moving to a shared responsibility model within the next three to five years.

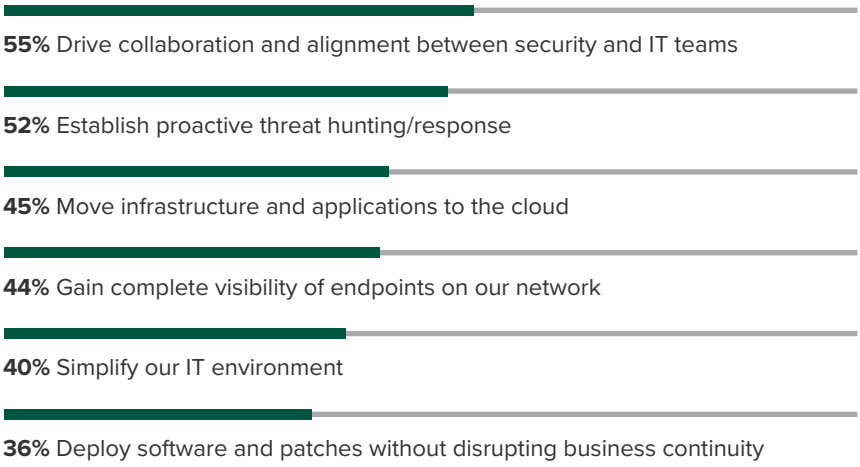
Collaboration Between IT And Security Is A Priority, But Remains Challenging

IT and Security teams are aware of the need for increased collaboration to avoid working against themselves. But is this a realistic goal? As IT teams take on more Security tasks, what challenges do they face? In surveying global IT and Security decision makers, we found that:

- **Companies have a clear goal of greater collaboration between IT and Security.** This collaboration is so critical to the accomplishment of other tasks in the organization that both IT and Security teams rank this as the top priority above other critical tasks such as the establishment of a proactive threat-hunting response, movement into the cloud, and gaining visibility into endpoints (see Figure 1). It is apparent that these teams understand that collaboration must be in place for all the other critical tasks to be successfully implemented within the organization.

Figure 1: Top Priorities Of IT Organizations

"Which of the following initiatives are likely to be your IT organization's top priorities over the next 12 months?" (Top 6 shown.)



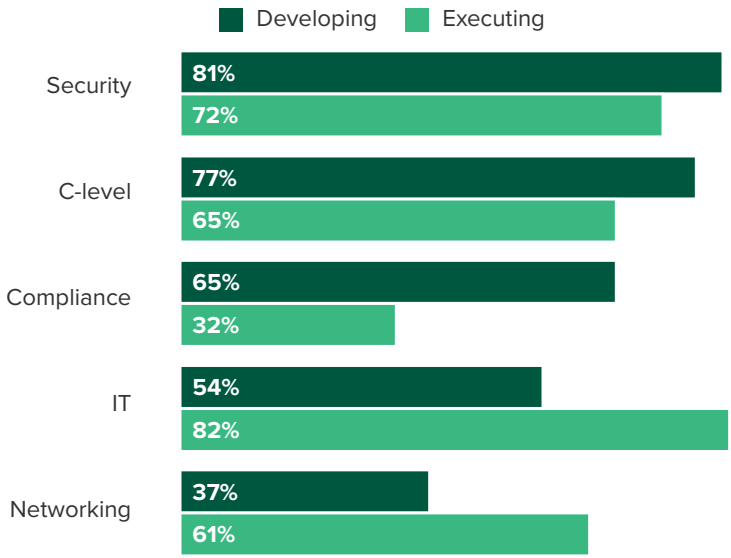
Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

FORRESTER®

› **IT is already involved in the execution and development of security strategy.** While companies are working to increase their collaboration across teams, the development and execution of security strategy is already partially shared between other teams including IT, compliance, and networking (see Figure 2). Although companies are attempting to expand this collaborative activity, IT already plays a large role in the ultimate execution of security strategy. Because they are often held responsible, organizations should make sure that IT is equipped with the tools needed to shoulder their share of responsibility for security.

Figure 2: 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

DESPITE HAVING A COMMON GOAL OF COLLABORATION, TEAMS FACE CHALLENGES

In an attempt to work together to treat security as a team sport, IT and Security teams face key challenges, including:

- **Strained relationships between IT and Security teams.** Relationships between IT and Security teams are strained, with 83% reporting the teams as a whole have a negative relationship (see Figure 3). This is largely fueled by the VP/below teams facing a significant amount of executional pressure from above and from each other. This can leave IT and Security teams working against each other, rather than in unison. Some causes of this friction include:
  - Nonaligned objectives causing teams to work against each other rather than together in a single strategic direction. One CISO noted:

    "A lot of that friction is because we oftentimes have conflicting objectives, right? IT is hammered for uptime and availability, and some of the things that [Security] might want to do impacts that."

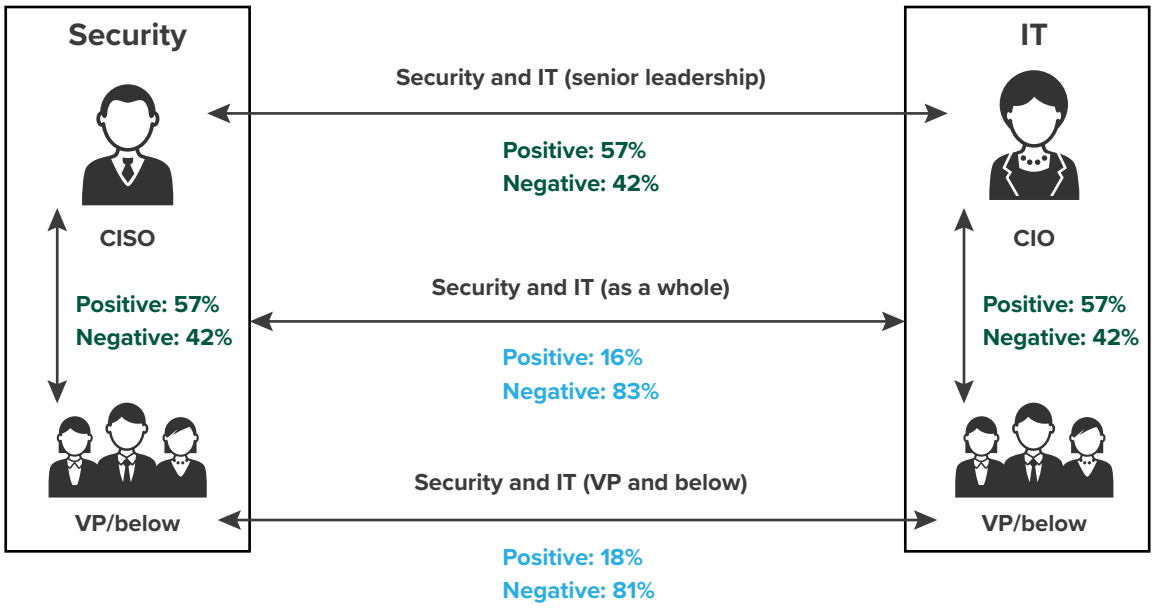
    CISO of a tech solutions organization in the US
  - An inward focus for most organizations. The fact that both teams are in high-growth mode makes them focus inward. In the last 12 months, both IT and Security have seen an increase in staff (IT 56%, Security 61%) and in the purchase of new security products (IT 68%, Security 72%). This means that the two teams are spending a lot of time on their own training and education, rather than on collaboration and outreach to other teams.
  - Communication gaps between IT and Security teams, exacerbating silos and hindering the establishment of a team mentality. According to one CIO: most issues within teams are:

    "[Most issues within teams are] 100% communication. [It's] people not communicating, not documenting, or 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 [the problem is] at."

    CIO of an energy corporation in the US

IT and Security Teams as a whole report negative relationships (83%).

Figure 3: 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

› **The Security team is dealing with an increasingly unmanageable portfolio of nonintegrated and ineffective security tools and point products.** On average, organizations have more than 27 security point products, but only 34% of respondents said that they are working with mostly or completely integrated security solutions. As security tasks move to a model that is shared with IT, IT teams are inheriting archaic systems that inherently don't share data or integrate with custom APIs. The fact that these tools don't meet the complex needs of modern business is causing dissatisfaction in IT and Security to skyrocket. In fact, only 52% of IT and Security professionals report being satisfied with security performance from existing enterprise firewalls — one of the most fundamental and established security solutions in their toolsets. As IT takes on more security tasks, those team members are met with an abundance of unsatisfactory tools to work with. One CIO noted:

"The most challenging part for IT and security is legacy systems. Some are on a sunset path and others are on a modernization path."

CIO of a tech solutions organization in the US

- **There are conflicting opinions on how teams should be structured.** As organizations increasingly treat security as a team sport, conflicting opinions are emerging as to whether there should be a single combined team with the CISO reporting to the CIO or if they would function better as two separate entities reporting directly to the CEO. While most CIOs report directly to their CEOs, more than twice as many companies indicated that their CISO reports to the CIO (36%) rather than to the CEO (14%). Despite the current organizational structure, CIOs (44%) and CEOs (44%) generally agree that CISOs should report into the CEO, creating true separation between the teams, but still working towards a unified goal. Generally, the benefits that flow from the organizational structure depend on how security-minded and collaborative the person in each position is. For example, if the CEO is not security-minded, a CIO is likely to be a better boss for a CISO. If a CIO and CISO are at odds, a separate structure is likely to be a better fit.

IT And Security Plan For Greater Collaboration In The Future

As companies make efforts to collaborate in the areas of IT and security, they are typically implementing several key actions to facilitate this. In an examination of these collaborative efforts, we found that:

- **Teams plan for a future of consolidation.** Sixty-five percent of organizations agree that they have taken measures to strengthen the relationship between IT and Security. They also expect to overcome the obstacles that prevent unification now. Today, 52% agree that IT and Security want to be unified but face obstacles that prevent unification, while only 19% believe that will be true in three to five years. Further, only 33% have IT and Security as one unified team today, but 47% believe unification will be the norm in three to five years. Whether rolled up under the same corporate structure or operating as separate teams with a unified strategy, organizations are making plans now and laying the foundation for more Security tasks to be shared with IT in the future.
- **A shift towards shared tasks continues.** Rather than being the responsibility of IT or Security alone, every critical task is moving more towards a shared responsibility model within the next three to five years (see Figure 4). IT and Security teams will no longer just be influencers or beneficiaries of specific tasks. They will actually share the responsibility for the primary decision making associated with those tasks. This change will allow teams to drive their own futures by making sure that everyone involved is working towards a common goal that benefits the entire organization, and not just a single siloed team.

Only 33% have IT and Security as one unified team now, but 47% believe unification will be the norm in three to five years.

Figure 4: Consolidation Of Tasks

"Is IT or Security the primary decision maker for the following categories? Which team do you think will be the primary decision maker for the following categories in three to five years?"

	Now Both teams share responsibility	3 to 5 Years Both teams share responsibility	Delta
IT security architecture	18.2%	57.9%	39.7%
Threat hunting/remediation/incident response	17.8%	50.9%	33.1%
Third-party IT services	22.3%	52.6%	30.3%
Cloud security	21.5%	51.4%	29.9%
Workloads (data center servers) and workload protection (data center security)	28.8%	50.7%	21.9%
Identity and access management (IAM)	43.2%	64.4%	21.2%
Network security (firewalls)	24.6%	41.5%	16.9%
Application modernization	44.5%	58.4%	13.9%
IT tool/technology selection	25.4%	37.4%	11.9%
Cloud infrastructure	30.1%	41.6%	11.5%
Mobile device management	27.0%	37.3%	10.3%
Hardware infrastructure	27.7%	37.8%	10.1%
Endpoint security	25.4%	35.0%	9.6%
Virtualization	29.1%	38.4%	9.3%
Security policies	26.1%	33.4%	7.3%

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

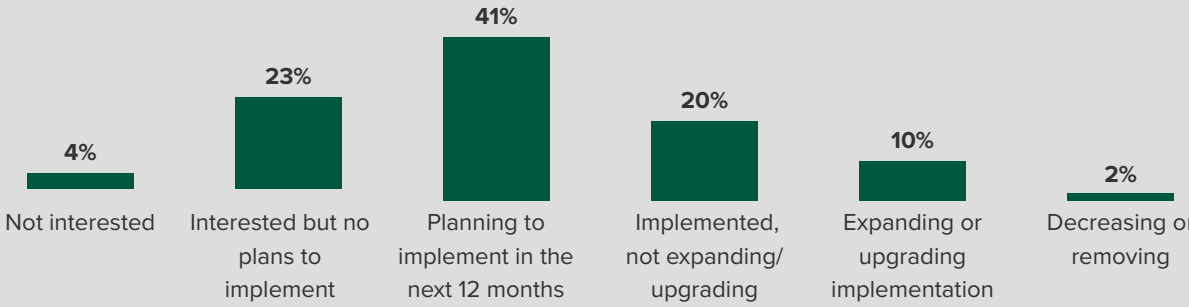
› **Organizations are moving to a unified strategy in order to address critical issues.** While only 30% have already implemented a unified and consolidated IT management and security strategy, 41% are planning to implement within the next 12 months, with another 23% interested in consolidation (see Figure 5). Companies are flocking to this type of strategy for:

- Increased security (52%)
- Technological advancement (47%)
- Better asset visibility (41%)

In fact, both IT and Security teams cite increased security as the top driver for adoption.

Figure 5: Consolidated Strategy Adoption Plans

"What are your organization's plans to implement a unified and 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

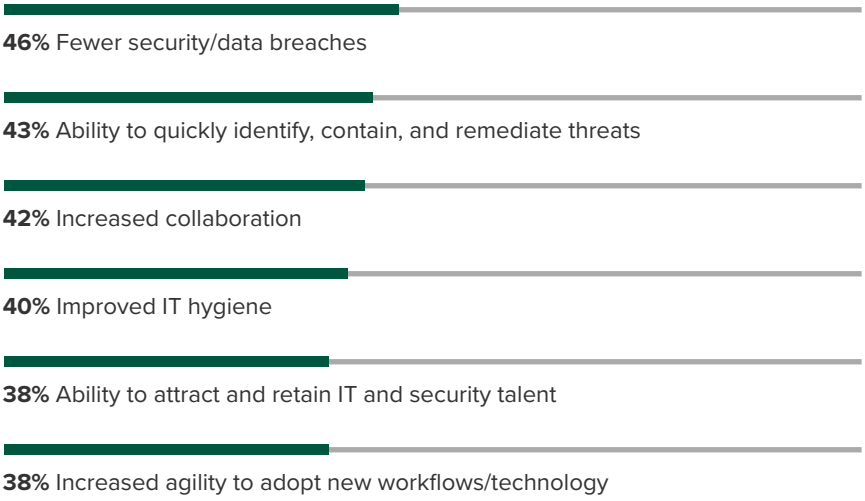
FORRESTER®

› **Consolidated strategies bring key benefits.** Companies are rapidly adopting consolidated strategies due to the wider benefits that consolidation brings (see Figure 6). In addition to reducing data breaches and threats (which are top priorities for Security teams), it also helps increase collaboration, which tends to reduce the inherent internal organizational stresses that come from multiple operational goals coming together (e.g., from IT and Security).

Companies with consolidated strategies see fewer breaches, quicker threat remediation, and increased collaboration.

Figure 6: Benefits Of A Consolidated Strategy

"What are/would be 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

As IT and Security teams increase their collaboration in the future, they are looking for consolidated, unified strategies to help them address key challenges and establish a common goal to work towards.

Key Recommendations

Although the benefits of IT and Security teams working collaboratively are clear, the transition from a culture of functionally isolated teams to a more unified approach can be difficult. Forrester's in-depth survey of IT and Security teams yielded several important recommendations:

Reduce friction between your IT and Security teams to improve mean time-to-detection and overall breach resilience. IT and Security operations staff struggle to prevent, detect, and respond to attacks in a coordinated fashion. To reduce the amount of time required to train new staff and respond to novel threats, it is critical to focus on improving the communication, workflows, and coordination between IT and Security teams. This will reduce the overall friction between the two in areas such as threat identification, policy management, and remediation, leading to an overall stronger posture against future breaches.

Effective collaboration requires simpler and unified tooling. Avoid having too many point tools don't integrate or work effectively together. To help improve the coordination between IT and Security, invest in tools that integrate and share relevant information bi-directionally. For example, certain context gathered from IT asset management tooling can help aid Security professionals looking to identify their critical assets or help with an ongoing security investigation. Tools that share a common platform or information system help unify security and operations workflows while easing the operational tension between the two.

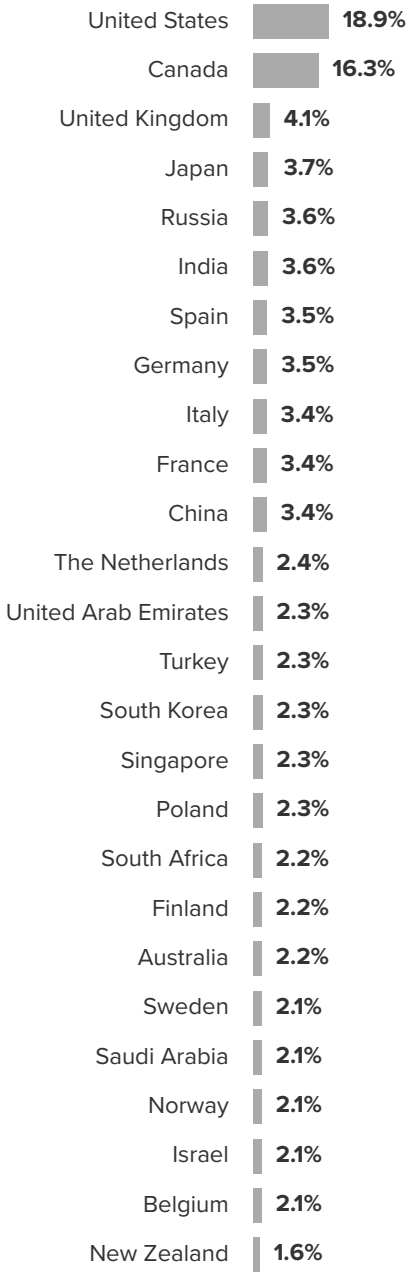
Focus on providing relevant metrics and insights that both teams can leverage. IT and security teams can have diverging goals — at least partially. IT wants to provision access and ensure uptime, while Security is often viewed as being about locking down or limiting access to company resources. In order to reduce this inherent friction between the two teams, it is useful to identify mutually beneficial metrics and analyses only possible through the cooperation of the two from a technology and process perspective. For example, endpoint security software can often provide insight into the typical use, stability, or network resource utilization on corporate devices, identifying issues relevant to IT operations. Likewise, for the Security professional's benefit, there are endpoint configuration metrics that require integration between endpoint configuration management tools and endpoint detection and response (EDR) tools. These tools provide additional security context such as risk analysis and secure configuration enforcement to empower Security teams to make more informed decisions. By agreeing to a common set of metrics and insights, teams can work together from common ground to find solutions that fit the needs of both teams.

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.

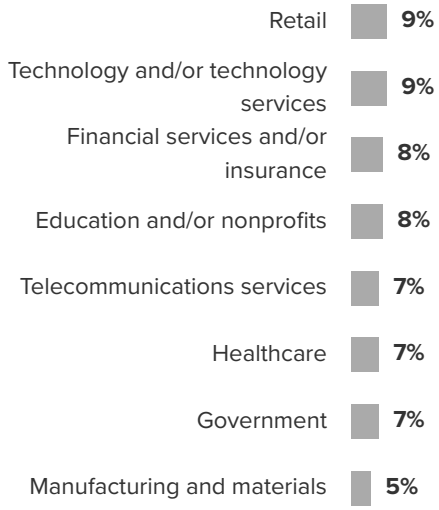
Appendix B: Demographics/Data

COUNTRY/REGION

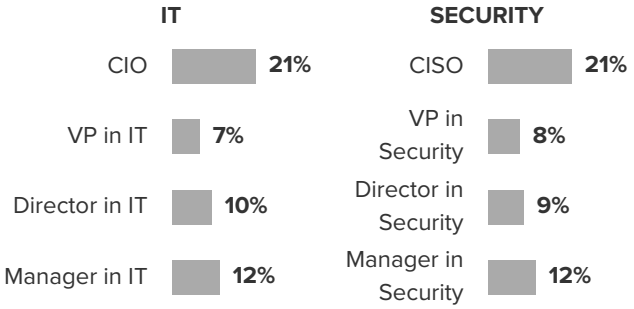


EMEA: 46%
North America: 35%
APAC: 19%

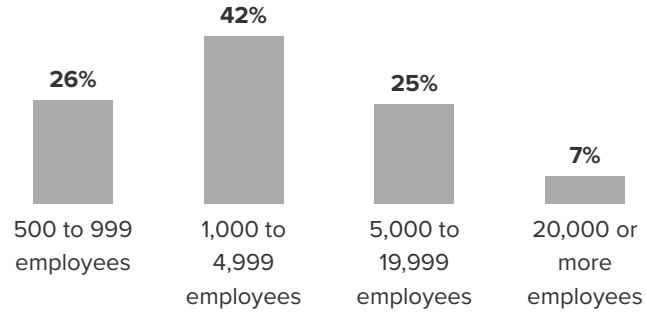
TOP INDUSTRIES



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

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®