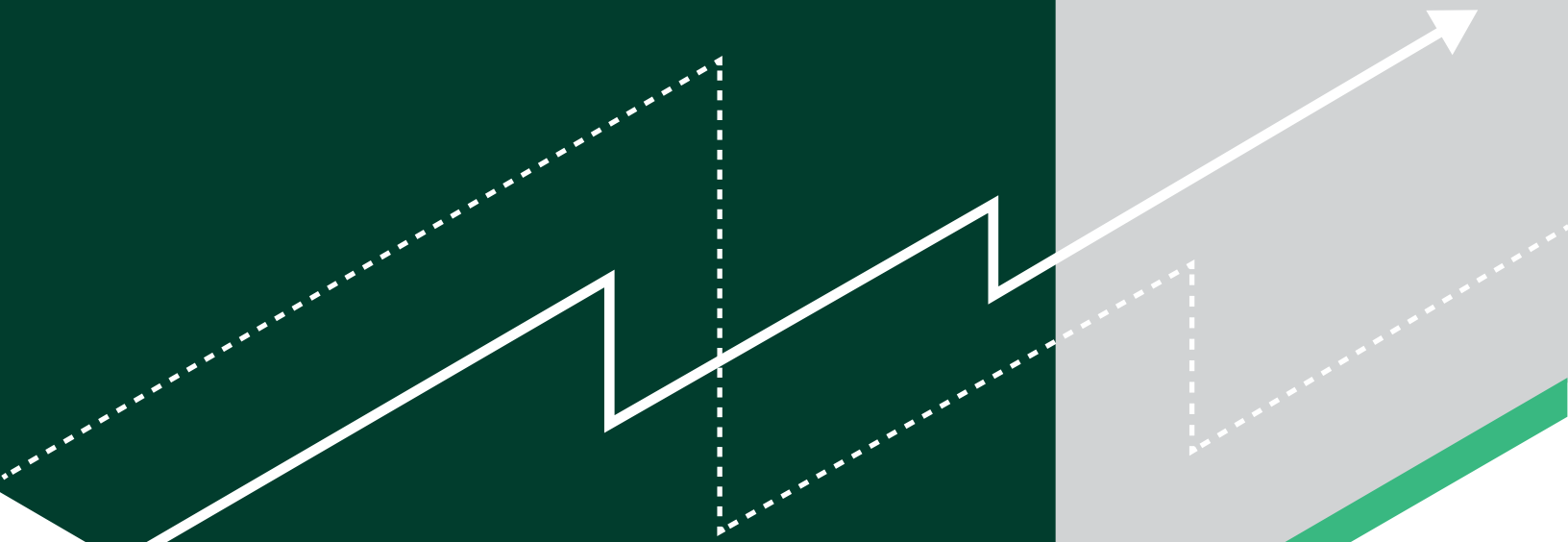
A Forrester Consulting
Thought Leadership Spotlight
Commissioned By VMware

September 2021

Security And Development: A Spotlight On Relationships

Relationship Results From The September 2021 Thought Leadership Paper, "Bridging The Developer And Security Divide"



FORRESTER®

Executive Summary

As security professionals work to create a secure environment for organizations, developers are often left out of the security planning processes but are then tasked with carrying these procedures out. But the relationship between security and development (dev) teams has a major impact on the security of an organization, indicating that security teams need to rethink their processes to further embrace the teams they support. While senior leaders are more focused on improving security and development relationships than before, clear action has not been taken. One in three organizations are not effectively taking strides to improve these strained relationships. However, when companies turn these relationships around into something more positive, they will see an increase in security, agility, and compliance.

VMware commissioned Forrester Consulting to evaluate the relationship between IT, security, and development teams. To explore this topic, Forrester conducted a survey with 1,475 respondents and five interviews with IT, security, and development managers and above (including CIOs and CISOs) with responsibility for development or security strategy decision-making to explore this topic. We found that, despite efforts, teams continue to struggle with negative relationships and a lack of empathy while often failing to include development teams in security strategy and planning.

KEY RECOMMENDATIONS BASED ON FINDINGS

- **Have strong vision from the top to reduce competing priorities and empower teams with the tools and processes they need.**
- **Embed security advocates into development teams rather than pushing security down from the top.**
- **Speak a common language with developers to ease friction between teams.**

Introduction

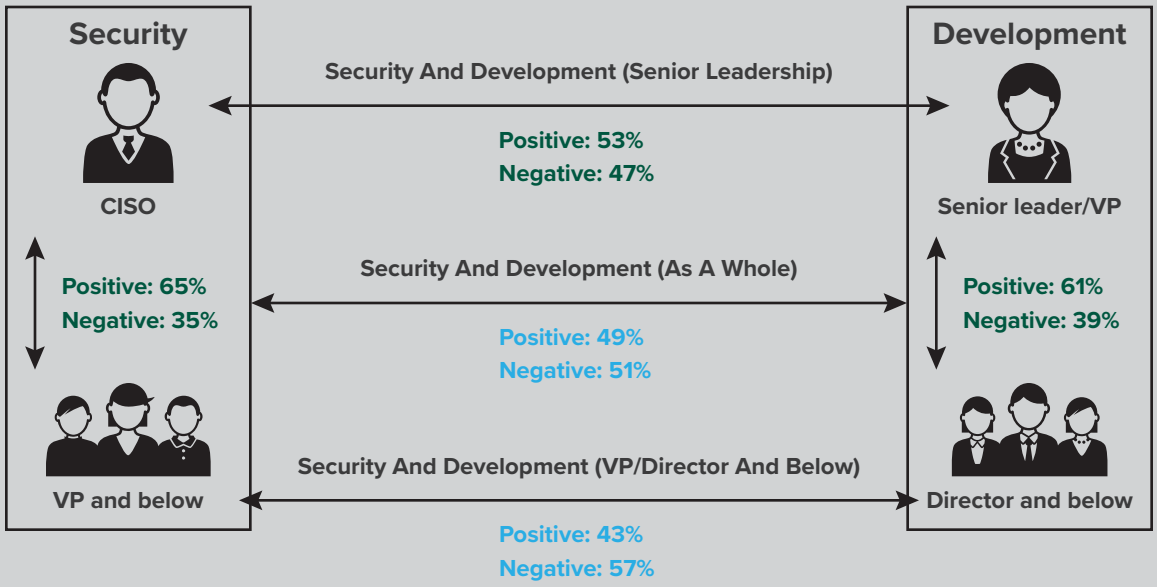
In surveying 1,475 IT, security, and development decision-makers, we found that organizations should:

- **Take specific actions, such as embedding security advocates on teams, to improve relationships across teams.** Leaders are committed to the issue as 72.5% of respondents reported their organizations' senior leadership focuses more on strengthening the relationship between development and security teams than they did two years ago. However, commitment alone to solving the negative relationships between security and other teams across the organization is not enough. Companies must actively take steps to improve the relationships, but one in three (36.5%) decision-makers said their companies are not effectively collaborating or taking strides to strengthen relationships. Consider implementing regular stand-ups with key stakeholders across all teams before implementing new policies and procedures. Additionally, adding a security advocate to development teams embeds security into development processes rather than pushing security procedures down from the top.
- **Focus on repairing disconnected relationships among practitioners.** Despite the attention from leadership, the lack of taking strides to improve relationships has resulted in stagnant or only very slightly improved relationships across teams (see Figure 1).

Despite commitment from leadership, 1 in 3 are not effectively collaborating or taking strides to strengthen relationships.

Figure 1

Security And Development Relationships



Base: 498 IT, 500 security, and 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

FORRESTER®

The practitioners who implement policies and work closely together on initiatives fuel the negative relationships between the teams. Competing priorities, lack of communication, and limited exposure to the other teams fuel the negative relationships.

The security team has a history of negative relationships with other teams (see Figure 2). In 2020, we assessed the relationships between security and IT. Given their negative starting point in 2020, significant improvements were needed to even be somewhat positive.[1] Although security and IT relationships have improved slightly over the course of a year, in 2021, these relationships remain disconnected across the organization even though driving collaboration is still a top priority, indicating that there is a lack of action.

Figure 2

A History Of Negative Relationships: Security And IT Relationships In 2020 vs. 2021

	% Positive In 2020*	% Positive In 2021
Security and IT (as a whole)	16%	39%
Security senior leadership and IT senior-most leadership	57%	62%
Security practitioners and IT practitioners	18%	34%
Security practitioners and security senior leadership	57%	65%
Security and IT audit	22%	39%
IT practitioners and IT senior leadership	57%	60%
IT and IT audit	59%	64%

Base: 498 IT, 500 security, and 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021
*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

Focusing on improving these relationships is not a nice-to-have; it's a must-have because increased collaboration yields both increased agility and security. The strain among practitioners is likely the result of not being consulted on security policies, competing goals with other teams, and security controls that stifle innovation. Security can combat this through increased education, embedded team members, speaking the language of developers, and empowering developers with secure tools that do not stifle their productivity.

› **Take action now to avoid the consequences of negative relationships between security and development.** The consequences of these negative relationships can have a big impact on the teams' ability to meet goals, the culture of the organization, and the security and innovation the teams are striving for. A senior director of development operations (DevOps) at a tech services organization elaborated on the far-reaching consequences of the lack of collaboration:

"**Consequences of a lack of collaboration include things like having a database server that is slow, not being able to respond because of certain added security tools, locked down laptops, and the inability to virtualize**. Especially in the new remote working world, a developer not having the password to go into the BIOS [basic input/output system] to do things all by themselves, but needing to go into the IT help desk to turn that on — it has literally taken six months to get that done in the time of COVID.

Those developers have had to work on lower-priority things instead of the higher-priority Kubernetes and containers on their local laptop. The security team put in compliance tools on the actual instances of the clusters that run the containers themselves and the time it takes to do that.

All of that causes dates to slip and goals to pass internally, as well as having customer databases that we need to import, validate, and troubleshoot slowed down by order of magnitude. It used to take maybe two days to do an import and pull that in. Now, with the added security and compliance, it's takes almost four weeks."

Given that security tasks are increasingly given to developers in the future, the time to improve relationships is now. Positive relationships of trust must be in place for increased security responsibility to be effective. Without the relationship of trust and the understanding of risk mitigation and compliance, developers will resist taking on new security tasks and look for workarounds, exposing the organization to risk.

› **Make the case for investing in improved relationships as positive relationships speed up software development life cycle (SDLC) tasks.** When teams effectively communicate and collaborate, they accomplish tasks more efficiently together. As you make the case for your organization to have embedded security advocates on development teams, also make the case that teams with positive development and security relationships complete the SDLC five days faster than those with negative relationships (see Figure 3). In an example scenario, it is clear how quickly these savings can add up over time.

Teams with positive development and security relationships complete the SDLC five days faster than those with negative relationships.

Figure 3

How Positive And Negative Relationships Impact The SDLC:

Time To Complete SDLC

Positive Development And Security Relationships

Average number of business days:

Plan:	24.6
Code:	32.1
Build:	31.3
Test:	11.3
Release:	7.7
Deploy:	14.3

Total: 113.6 business days

Negative Development And Security Relationships

Average number of business days:

Plan:	29.9
Code:	32.2
Build:	31.7
Test:	10.1
Release:	8.7
Deploy:	14.4

Total: 118.3 business days

Example Scenario

If you had 5 dev teams ...

That completed 3 releases per year...

Teams with positive relationships would save:

70.5

business days

Base: 498 IT, 500 security, and 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

Key Recommendations

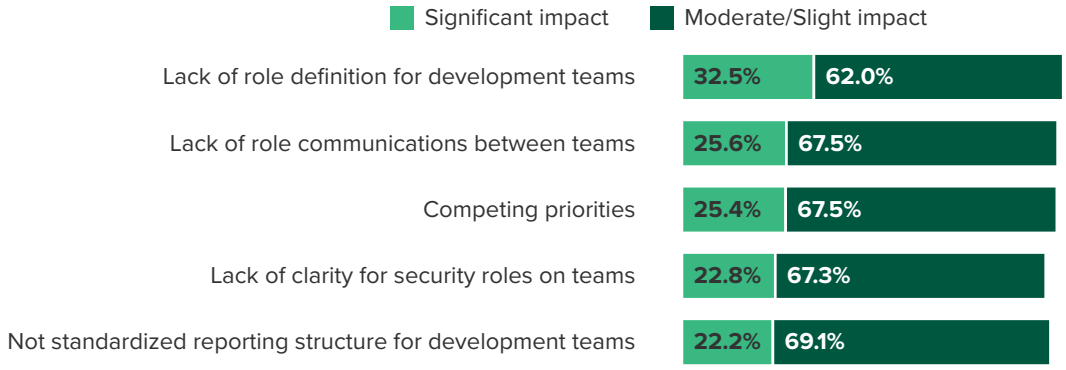
Positive relationships are critical to carrying out key security tasks and improving development cycles, but how can they be improved? Our research yielded these recommendations:

RECOMMENDATION 1: HAVE A STRONG VISION FROM THE TOP TO REDUCE COMPETING PRIORITIES AND EMPOWER TEAMS WITH THE TOOLS AND PROCESSES THEY NEED

- **Find common ground on a team level through shared KPIs.** Both security and development teams generally support the same high-level priorities. These two teams listed increasing operational efficiency, preventing security breaches, increasing revenue streams for the business, and improving user experience as four of their organizations' top five priorities. A strong vision and alignment among leaders supports shared goals. However, things start to break down at the team level when there is a lack of communication about roles and responsibilities among teams in addition to priorities that are in conflict. These gaps have a significant impact on collaboration across teams (see Figure 4).

Figure 4

"How do the following gaps impact collaboration across IT, development, and security teams?"



Base: 498 IT, 500 security, and 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

One practical way to get teams on equal footing is to have shared KPIs across teams. Examples include accelerated release velocity, reduced security incidents, and decreased mean time to patch/update. A unified purpose fosters positivity and trust across teams, giving them a positive goal rather than forcing teams to work together when policies are rolled out. For example, sharing the KPI of accelerated release velocity allows security teams to enter the world of development, learn their procedures, and implement security controls that meet security goals and work with development to not stifle their innovation. Security teams should measure the security of releases in context of release velocity, enabling the development teams to release more secure apps and features at the same speed. Similarly, having a shared KPI of reduced security incidents would cause developers to take security issues more seriously and increase collaboration with the security team.

- **Radiate strength of vision from leadership to reduce competing priorities.** To reduce silos and improve relationships, strength of vision from the top is critical. Leadership that is focused on collaboration, goal consolidation across teams, and the empowerment of practitioners helps move organizations in the right direction. As one CTO at a healthcare organization noted:

"**IT, security, and development don't have conflicting priorities anymore, but they did.** In our case, it wasn't because of the reporting structure. They were not reporting to different places. They are reporting into the CIO which was still the case before I arrived on the scene. **It comes down to strength of vision** and direction versus whether you're doing something more independent. The importance of things like scaled agile, DevOps, DevSecOps [development and security operations], integrated planning, automation of deployment — all of that stuff was not a thing at a global level for the CIO organization until I changed that."

Having a leader that can consolidate the focus for the organization is the first step and, from there, the tools and processes needed to empower the individuals to accomplish those goals will follow.

- **Create a unified reporting structure to reduce stumbling blocks.** Development teams typically do not have a unified reporting structure. We found that development professionals, such as those that cover site reliability, CI/CD pipelines, application delivery and development, software development, and more, have no consistent place to report, whether to IT, security, or R&D. Further, only 4% of respondents had all their development professionals reporting to the same team. This can be a stumbling block as teams are not well integrated: Only 28.3% said their security and development teams are significantly integrated. This lack of integration and the fact that developers have a scattered reporting structure can create inconsistency and lack of role definition across the enterprise. A unified development reporting structure standardizes software architecture, streamlines security processes, enables cross-selling opportunities, reduces complexity in the environment, and empowers developers to become enablement teams. Two professionals noted:

"A unified development team enables us to do things in a more standardized way. We are agile and our team is viewed as an enablement team. Rather than giving a DevOps engineer to each team, they bring requests to us and we work to hook them up. We look to do that in a way that provides some consistency and solves problems for more than one team." added:

VP of DevOps in FinServ

"I'm responsible for product engineering, infrastructure, operation, security engineering, and data and dev ops. **All of the developers roll up to me. It allows us to standardize our CI/CD process, which creates much more efficiency for our developers and allow them to innovate.** It also **allows us to manage compliance and security in a way where we deploy once and manage everywhere**...

Also, **we wanted to start cross-selling products.** If your products are on different technology stacks, it's very hard to provide customers with cross-selling options. That was going to terribly impact our infrastructure costs for maintaining a bunch of disparate environments.

Last, but certainly not least **from a compliance and security standpoint (like GDPR, CCPA, cybersecurity, security scanning, etc.) having different ways for doing this was just driving up the complexity of managing our environment**."

CTO in Travel Technology

RECOMMENDATION 2: EMBED SECURITY ADVOCATES INTO DEVELOPMENT TEAMS RATHER THAN PUSHING SECURITY DOWN FROM THE TOP

- **Include development teams in the security strategy and planning.** When asked if development was involved in security strategy planning, 45.1% of development respondents said they were involved, but only 37.8% of security respondents said they involve development teams. This indicates that developers are even less involved in security strategy planning than they think they are. This often leaves the development team with new security policies that have been pushed down from the top that don't actually make sense in their environment or stifle their innovation. In fact, over half of developers (52.4%) feel security policies stifle their innovation. And, of course, sometimes the issue happens in reverse.

  Without an embedded security advocate on the team, the development teams often move forward with the creation of a new application and then expect security to secure it as an afterthought. Security must be a two-way street. The solution is to embed security professionals that are involved throughout the development process on development teams rather than a separate team that needs to be consulted.

- **Engage with development teams now as they will be more involved with security in the future.** Organizations believe development teams will be responsible for more security tasks in the future — especially with cloud and workloads. However, this increased involvement will be a challenge as security policies are not very clear to development teams and they often don't believe they are responsible for carrying out security procedures (see Figure 5). Engaging now and improving relationships lays the foundation for increased security demands in the future.

Over half of developers feel their innovation is stifled by security policies.

Figure 5

Development Team's Understanding Of Security Procedure Responsibilities
(Showing "Strongly agree")

Only 22% of developers have a clear understanding of which security policies they are expected to comply with.

Base: 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

- **Embed security advocates and bake security into the process.** Only one in three (38.6%) of developers said they have a security advocate on their team. Developers feel disconnected, don't know how to comply, and don't think they have responsibility for the security of what they develop. An embedded security advocate on development teams can break down relationship barriers and allow security teams to truly understand the developers' needs. When that trust is built, the security advocate can make security roles and responsibilities clear to the development team as an enabler rather than as a separate team that is somewhat blindly pushing down new policies and procedures.
- **Focus on trust-building exercises as most teams lack complete trust.** Only 16.1% of respondents said that there is complete trust between the security and development teams at their organization. Because trust is one of the most critical buildings blocks of a positive relationship, it is imperative that organizations work towards cultivating it to fix the problems among the people before throwing additional processes and technologies at the problem. A trusting relationship must be in place for success. To do this, the security team shouldn't leave development out of its planning and processes. Teams that do have trust indicate that a security mindset, security education, and collaboration to resolve risks are drivers of trust. These drivers should be made top goals of companies so that the relationships can improve.

RECOMMENDATION 3: SPEAK A COMMON LANGUAGE WITH DEVELOPERS TO EASE FRICTION BETWEEN TEAMS

› **Gain a thorough understanding of development tools/platforms to avoid impeding progress.** This is critical because development teams are often key drivers of revenue for the organization. One way that security can empower developers is giving them tools that can scan containers and Kubernetes configuration files early in the development lifecycle, automate the application of security policies, discover image vulnerabilities, and provide secure registries, Kubernetes access, and app/container catalogs that enable developers to build secure applications but are tools for which security and operations are able to set policies. This cross-team collaboration enables each group to effectively meet their goals while not impeding innovation.

The senior director of DevOps at a tech services organization said that his development team is almost always left out of the security planning processes. As a result, they put policies and procedures on things that don't make sense because they are not educated on the technology. He noted:

"From a security standpoint, it seems like **there's a bit of confusion about what it means to be secure in a containerized environment**."

After working through a myriad of issues with his team, he adapted the security policies to fit his need. However, it required much manpower effort that could have been prevented with appropriate education.

› **Learn to speak the language of development rather than asking development to speak the language of security.** When the security team makes primers on security for the rest of the organization, it is almost always written in the language of security with little input, if any, from the teams it is meant to help. However, this makes compliance even more difficult as other teams have a different language to speak about the issues. Security teams should make security easy and relatively unnoticeable by learning to speak the language of the other teams, including development. Having a security advocate who asks the right questions and takes the time to get to know the development teams will go a long way to building trust between teams. A CTO in healthcare noted:

"**The relationship between development and security is strained, but not strained due to malicious intent, strained because they just don't have the same language to talk about the problem.** They're just not understanding each other. Everybody wants to protect the place. Everybody wants to get stuff done. Everybody wants to run stable systems. **We're just not speaking the same language and we don't have enough understanding of each other's fields of expertise.**"

"The relationship between development and security is strained ... because they just don't have the same language to talk about the problem"

Speaking the language of developers makes it easier for the development team to comply with security policies, but this does not replace the fact that security is the responsibility of all individuals. Developers must take strides to help bridge the gap as well by including security teams in their processes and working with security advocates to ensure the security of the applications they create.

› **Focus on education — a stepping stone to trust.** A lack of security education for development teams means that security lives in a silo and is not an embedded part of developers' daily actions. Only 38.4% of respondents agreed their organizations' development teams are thoroughly educated on security procedures they are expected to execute. Security teams work endlessly to create their security policies and procedures but are failing to execute the follow-through and actually educating employees on how to comply. Open, streamlined communications and embedded teams avoid the strained relationships and increase the effectiveness of educational efforts.

Benefits of Increased Collaboration

By following these recommendations, organizations will see improved relationships and the benefits that come with it:

› **Foster increased collaboration to build trust.** By increasing collaboration across teams, such as embedding a security advocate and improving educational programs, teams will find that there are benefits much farther reaching than just the people alone. The increased collaboration fosters more secure applications and increased agility because it empowers and enables teams to tackle technology and process issues (see Figure 6). Collaboration solves the critical problems that the development and security teams are facing. Yet the relationship and collaboration challenges prove that sometimes the hardest step to take is actually the most needed action.

Figure 6

Benefits Of Increased Collaboration Across Teams

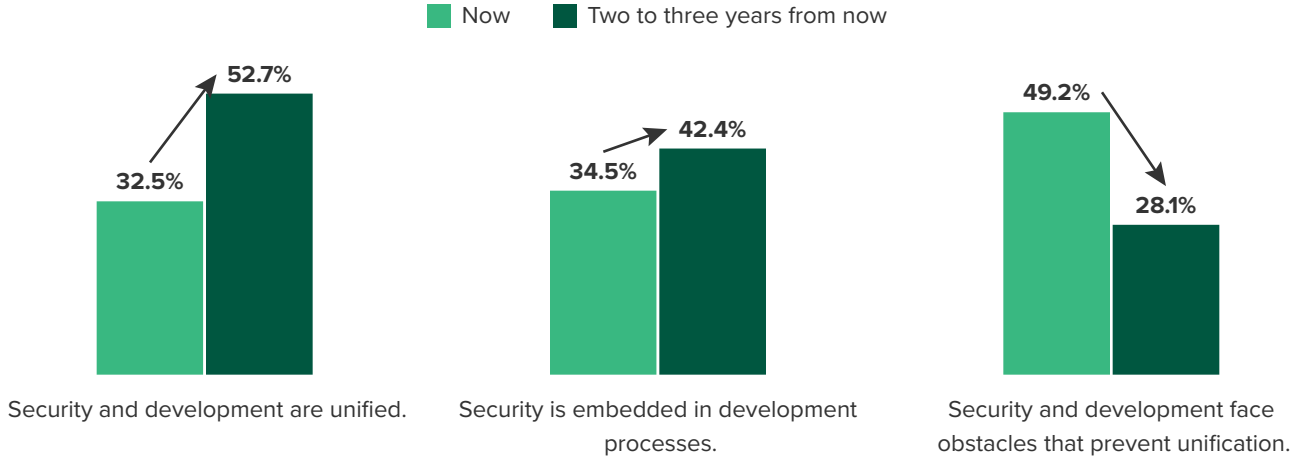
Base: 498 IT, 500 security, and 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

FORRESTER®

› **Be prepared because, ready or not, collaboration is on the horizon.** The time to tackle collaboration and trust issues is now, before the unification of teams is even more prevalent. You can't build trust in a day, so don't wait. In the next two to three years, some companies plan to overcome unification obstacles, have more unified teams, and have security embedded in the development process (see Figure 7). By embedding security into development teams and actively collaborating now, this process of team unification will come as a natural transition in the future.

Figure 7

Future State Of Organizations

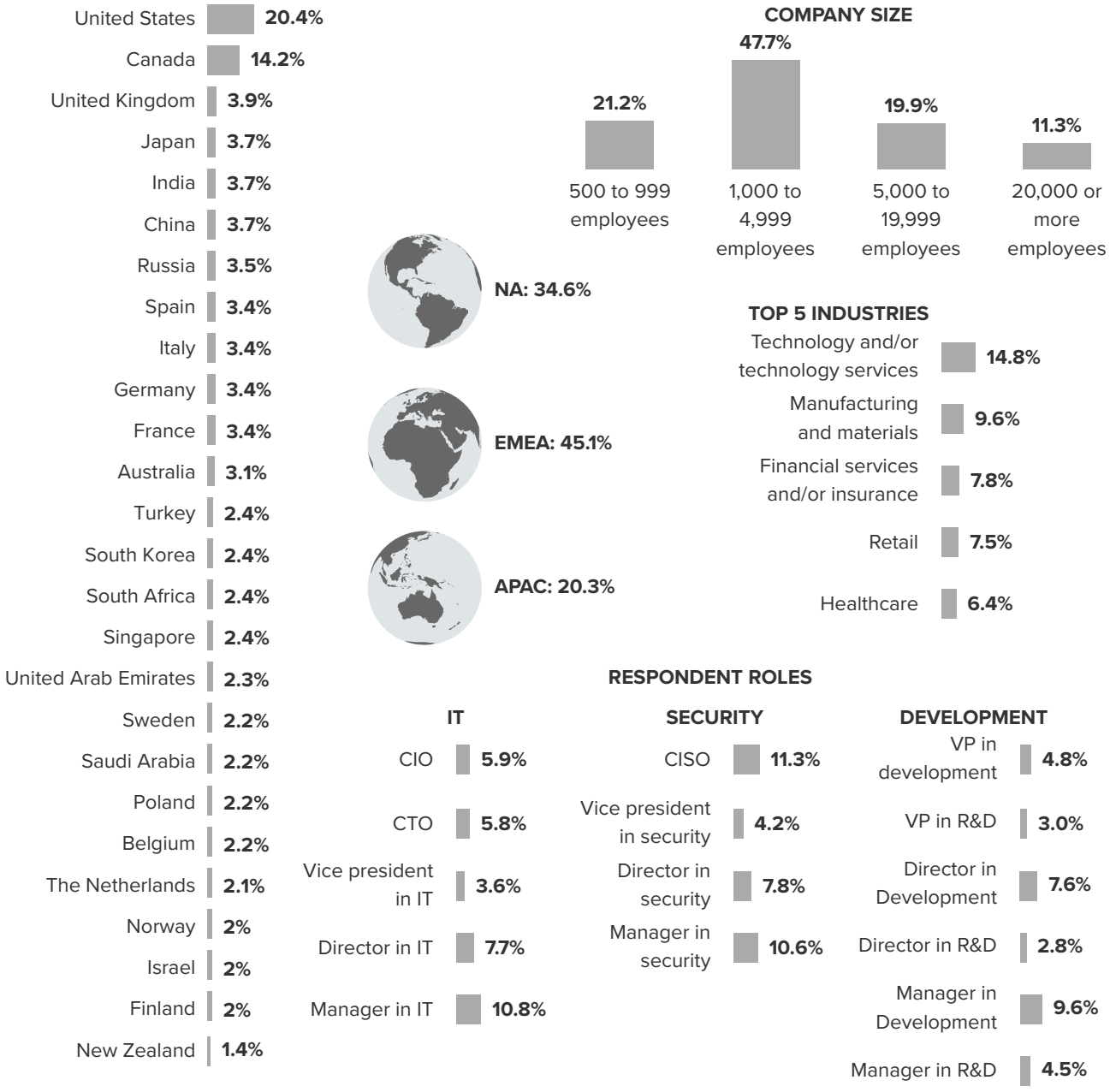


Base: 498 IT, 500 security, and 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

Appendix A: Methodology

In this study, Forrester surveyed 1,475 IT, security, and development managers and above (including CIOs and CISOs) with responsibility for development or security strategy decision-making. Forrester also conducted five interviews with directors and above in these roles. The purpose of this study was to evaluate the relationships between IT, security, and development teams, understand the role of security within development teams and DevOps pipelines, and explore the impact of Zero Trust frameworks on security teams and during the DevOps cycle. Questions provided to the participants asked about team collaboration, security strategy, and Zero Trust. Respondents were offered a small incentive as a thank-you for time spent on the survey. The study began in March 2021 and was completed in April 2021.

Appendix B: Demographics



Base: 1,475 IT and security managers and above with responsibility for security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

FORRESTER®

Appendix C: Endnotes

[1] Source: "IT and Security Insights By Role," a commissioned study conducted by Forrester Consulting on behalf of VMware, May 2020.

Project Director:
Emily Drinkwater,
Senior Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group