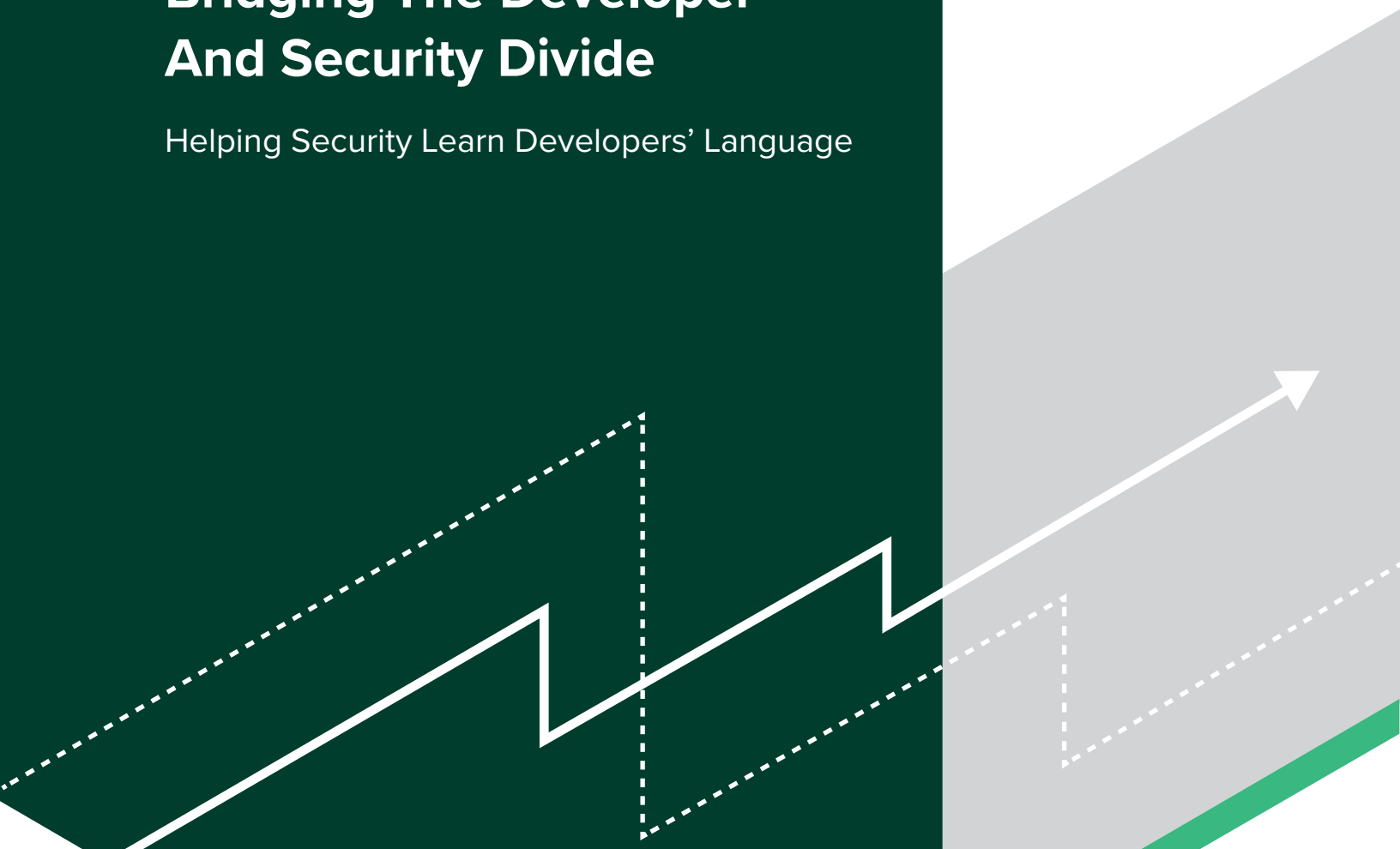
A Forrester Consulting
Thought Leadership Paper
Commissioned By VMware

September 2021

Bridging The Developer And Security Divide

Helping Security Learn Developers' Language



FORRESTER®

Table Of Contents

Project Director:
Emily Drinkwater,
Senior 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®

Executive Summary

As security professionals work to create a secure environment for organizations, developers are often left out of security planning processes but are then tasked with carrying these procedures out. This creates a fractured relationship between development and security. While senior leaders are more focused now on development and security relationships, one in three don't effectively collaborate or work to strengthen relationships. The relationships between these teams have a major impact on organizations with many benefits, including increased collaboration, more secure applications, increased agility, and continuous compliance. Security teams need to rethink their processes to further embrace the teams they support.

VMware commissioned Forrester Consulting to evaluate the relationship between IT, security, and development teams and how organizations are working to ensure a strong security posture via Zero Trust, which is a "never trust, always verify" security model.[1] 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:

- **Involve developers in security planning early and often.**
- **Learn to speak the language of the development team rather than asking development to speak security.**
- **Share KPIs and increase communication to improve relationships.**
- **Automate security to improve scalability.**

Security Is No Longer A Specialization

In surveying 1,475 IT, security, and development decision-makers, we found that in order to achieve positive business and security outcomes, organizations should:

- **Make sure security is no longer a specialization at your organization.** Rather than a few individuals within the organization being responsible for security, security tasks should be embedded across people (teams), processes, and technologies. For example, the convergence of development, security, and operations (dubbed DevSecOps) allows security teams to collaborate with development (dev) teams to build security into their processes.[2] Rather than slowing dev teams down, this ultimately helps them improve productivity and quality. There is a triangulated dependency loop in which embedding security across the teams sets the tone for how effectively security is embedded in processes and technologies. By starting with people, the processes and technologies will follow much easier — but many security teams start with processes and technologies and view the people as an afterthought rather than treating security as a team sport. Despite it no longer being a specialization, security is often still responsible for implementing and configuring security on their own.
- **Build better relationships to yield faster releases.** It is often said that security is everyone's responsibility, and the evidence shows that when this is the case, results follow. Focusing on the relational aspect of security is not a nice-to-have, but a must-have as increased collaboration across teams increases both security and agility. Everyone has to be on board and collaborate across teams for the security tools and procedures the security team implements to be most effective, enhancing the security posture of the organization. Increased collaboration also helps the development team meet its goals, since security and development teams with positive relationships can complete the software development lifecycle five business days faster than teams with negative relationships. Given the average number of releases each team will do in a given year, this will provide significant time savings over time. Particularly in fast-paced environments, such as cloud-native environments, when developers may be shipping code multiple times per week, it is critical to avoid a prohibitive five business day delay.
- **Make the right thing the easy thing to aid innovation.** With the adoption of cloud and other technologies that underpin modern applications (such as containers), it is no secret that developers are major drivers of business revenue. However, security challenges tied to cloud and containers still prevail. Survey respondents noted their top two most challenging tasks are:

  1. Ensuring security in the cloud (78.6%)
  2. Securing workloads and containers (70.5%)

Additionally, over half of developers (52.4%) felt security policies stifle their innovation. When security is so simplified and accessible that development teams don't even realize it's there, then security not only meets its traditional goals of reducing risks but — more importantly — becomes a business enabler by allowing development teams to be more innovative while increasing compliance and business revenue. A solutions strategist at a tech services organization noted:

"**Our security team's top priority is always about colleague experience**. And whether that colleague happens to be a developer, someone in finance, or a salesperson in the field, what we're looking for is this: '**How do we make security so simple and easy that they don't notice it?**' Or security that is easier to comply with than it is to find a way around. We've been focused on that for the last four or five years now. You know what it's like with security — **if you put a security roadblock in the way, people find innovative ways to get around it.**"

Security is so much more than just an insurance policy — it can empower development teams to accomplish their goals in the most secure and successful ways rather than hindering innovation and creating security hurdles to bypass. Our research yielded several important recommendations to help address these issues.

Over half of developers agreed that security policies sometimes stifle innovation.

Recommendation 1: Involve Developers In Security Planning Early And Often

› **Make security an embedded service.** Organizations expect developers to be more involved with security tasks in the future, particularly among cloud and workload tasks. However, developers currently aren't very involved in security strategy planning or execution (see Figure 1). 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.

Figure 1

Development Team's Involvement In Planning And Executing Their Organization's Security Strategy (Showing "Agree")

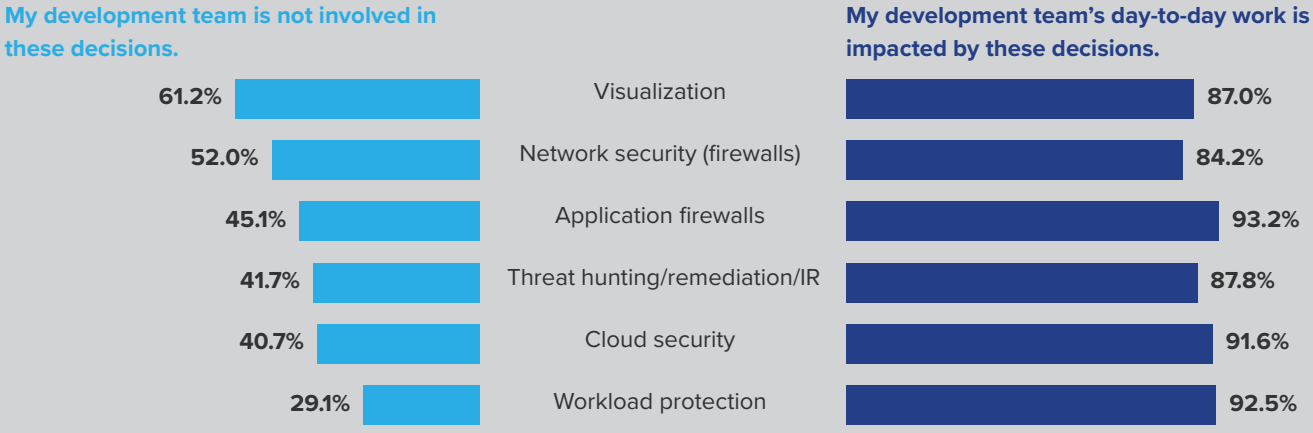
Developers are even less involved in security strategy planning than they think they are.

Base: 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

The security team makes decisions about key applications and tools that impact the development team's work, but the development team is often not involved in these decisions (see Figure 2). In fact, the tools and technologies that impact developers' work the most are the items they aren't involved in choosing.

Figure 2

Development Team's Involvement In Security Decision-Making For Critical Items And Its Impact On Their Work



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

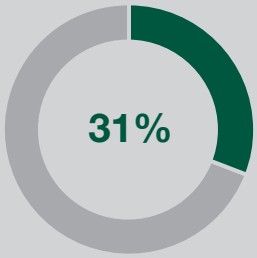
FORRESTER®

Right now, security teams often roll out new procedures without consulting development, and development teams often create new applications for security to verify compliance right before production deployment. Security has to be a two-way street from the start. The solution is to embed security professionals on development teams rather than create a separate team that gets consulted at the eleventh hour. Security teams should view other teams across the organization, especially developers, as their own customers. They should focus on making these customers (developers) more productive and effective, while maintaining high levels of communication and collaboration.

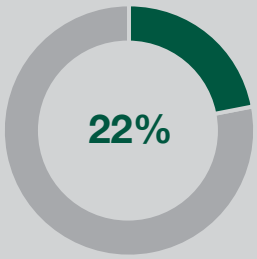
- **Make security responsibilities clear as some security duties shift left for developers.** Many organizations are preparing for some ownership of security tasks to shift left, increasing the development team's future involvement in some security tasks.[3] This increased involvement is a challenge because security policies are often not designed with developers in mind. This often leaves developers feeling as if they are not responsible for security tasks and don't have a clear understanding of how to comply (see Figure 3). Increased collaboration brings increased compliance and improved agility. It is important for security and development teams to work together so that development teams are clear which policies to comply with and which tools are approved. For instance, developers can work with security teams to automate the security of open source libraries, reducing both risk and the effort required for the teams to keep this up to date. This type of automation also helps define roles by making it clear which team owns the tasks. By improving relationships, increasing collaboration, and making security responsibilities clear, teams can better support their overarching goals of improving business and security outcomes.

Figure 3

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



It is clear to my development team how to appropriately comply with security procedures.



It is clear to my development team which security policies we are expected to comply with.

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

FORRESTER®

It is unclear who owns the responsibility for security tasks adding to the confusion and strain across teams. In fact, a VP of DevOps at a financial services organization noted:

"The **developers are not ultimately responsible** for the security issues with the things they develop. I would say it is a shared responsibility between security and IT, but not really the developers."

Meanwhile, a CTO at a healthcare organization expressed quite the opposite:

"**I don't think a developer understands that their individual action might take everything down, but that's a fact — it might**. They think of impact in terms of their part of the world. 'Hey, I'm working on this non-critical application, I can do whatever I want,' without realizing that, in the world we now live, they really can't because **we're no stronger than the weakest link in the armor**."

- **Empower developers to be involved in security decisions.** Security must move beyond just presenting developers with a security plan. Instead, engage them and connect them with the purpose of improving overarching business outcomes as well as the team goals on increased security and agility. Make developers feel connected and influential to empower them. Allow them to design their own security policies, suggest tools and processes they are comfortable with, and contribute feedback to policies in the form of a request for comment process (RFC) before the policies go live as the domain experts. Consider assigning a security resource to developer standups so developers get more familiar with security personnel.

  Right now, developers feel disconnected, don't know how to comply, and don't think they have responsibility for the security of what they develop. 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.

Recommendation 2: Learn To Speak The Language Of The Development Team Rather Than Asking Development To Speak Security

› **Make education a two-way street.** It is a fairly common practice for security teams to make primers for the rest of the organization about security procedures and policies. The problem? Security speaks a different language from the rest of the organization. Security teams must learn to speak the language of the development team rather than asking development to speak security. 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**."

There is room for growth in security education programs as only about half of developers (54.3%) said there is a formal education process for new/updated security policies within their organization. Security teams should build trust by trusting development teams to be good security ambassadors through a thorough education process. Unfortunately, a common practice is for security to roll out new policies and not realize its far-reaching impacts until it is already in progress. Two developers noted:

"W**e are not consulted about security tools, technology, or procedures** — pretty much anything across the board — **until after it's been put in effect and starts to impact productivity**."

- Senior Director of DevOps in Tech Services

"**When the security team rolls out something new, they roll it out and leave it to us to figure out how it impacts our work**. They're rarely coming out and talking with us about these things beforehand."

- VP of DevOps in FinServ

Development and security don't have the same language.

Furthermore, a shockingly low one in three (38.4%) of developers reported that they are thoroughly educated on the security procedures they are expected to execute. Having security advocates embedded within teams would help alleviate many of the education woes, but is not a common practice. Only 38.6% of developers said they have a security advocate embedded in their development team. Embedded security team members improve security compliance, and allow security teams to understand the innerworkings of development teams. A senior developer of DevOps at a tech services organization said:

"We actually have **a few security people that are really good at explaining why something** is bad rather than just saying they can't do this. **It's storytelling that educates rather than just policy**."

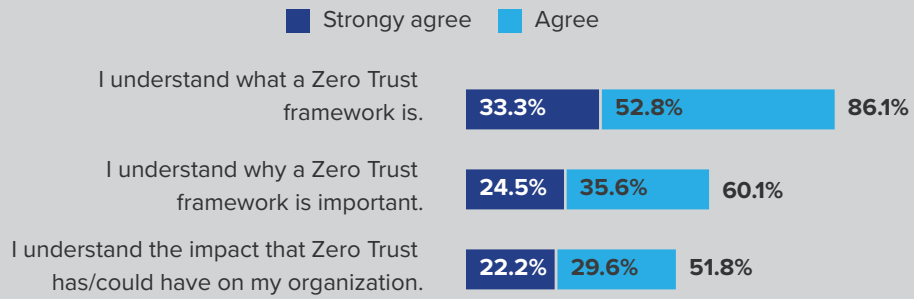
An embedded security advocate can do so much more than pass along a primer. They can be educated themselves, understand the nuances and needs of each team, and educate through storytelling rather than policy alone.

Only 38.6% of developers said they have a security advocate embedded in their development team.

- **Engage cross-functional teams on your Zero Trust strategy to be more effective.** Many organizations have recognized that traditional security approaches alone are not enough to protect against ransomware, breaches, and other major security incidents.[4] Zero Trust, which is a "never trust, always verify" model of security, recognizes the vulnerability of trust and makes security the core of all processes and strategies. About two-thirds (64.7%) of respondents reported their organizations have at least started their Zero Trust journey, but more education for developers is needed as many don't understand why it is important or the impacts it can have (see Figure 4). Some are resistant to the Zero Trust rollout, likely the result of poor communication and lack of effective engagement throughout the process. In fact, only 57.2% of developers said they have been educated about their organizations' Zero Trust framework, highlighting the great need for a mature education process. Development teams need to understand the who, what, how, why, and where of Zero Trust, which takes more than just basic education or a primer alone. It requires engaging developers in the Zero Trust journey from the beginning so they are equally invested in its success.

Figure 4

Development Team's Understanding Of Zero Trust



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

› **Adopt and activate Zero Trust to bring big improvements to your organization.** Zero Trust can bring big benefits, especially when all teams within the organization understand its value. Common benefits of deploying Zero Trust include a decrease in the total number of security incidents experienced and their overall severity, along with streamlined remote connectivity and identity and access management administration. This accelerates the velocity of internal teams and reduces the risk of data loss through intrusion. The CTO of a travel technology company noted:

"**The amount of ongoing security issues that we faced after we adopted a Zero Trust strategy dramatically decreased**. It simplifies our security architecture dramatically."

Security professionals indicated the top benefits of a Zero Trust framework include improved identity management, data protection, and overall quality of work (see Figure 5).

Figure 5

Development Team's Understanding Of Zero Trust

A Zero Trust framework would increase ...	
Identity protection	**73.0%**
Detection capabilities	**71.5%**
Data protection	**63.7%**
End-to-end security	**61.5%**
Overall quality of work	**57.9%**

A Zero Trust framework would decrease ...	
Total number of security incidents	**46.0%**
Risk of data breach	**34.7%**

Base: 500 security 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

Recommendation 3: Share KPIs and Increase Communication To Improve Relationships

- **Share KPIs across teams as a starting point for improving relationships.** Over half (58.1%) of respondents indicated it is a critical or high priority to drive collaboration and alignment between the security and development teams, and 72.5% agreed that their senior leadership focuses more on strengthening the relationship between development and security than they did two years ago, but relationships are still strained. In fact, one in three (36.5%) decision-makers reported their organizations' teams are not effectively collaborating or taking strides to strengthen relationships between security and development teams.

  Organizations are aware that the relationships need improvement and that it is an important goal, but they struggle to figure out how as improvement seems stagnant. When senior leadership is hyper-focused on an issue, it is typical for steps to be put in place quickly for the goal to be accomplished. However, contrary to process and technology goals, relationship goals can be difficult to accomplish in a workplace setting. It is clear that the lack of relationship improvement means that many don't even know where to start.

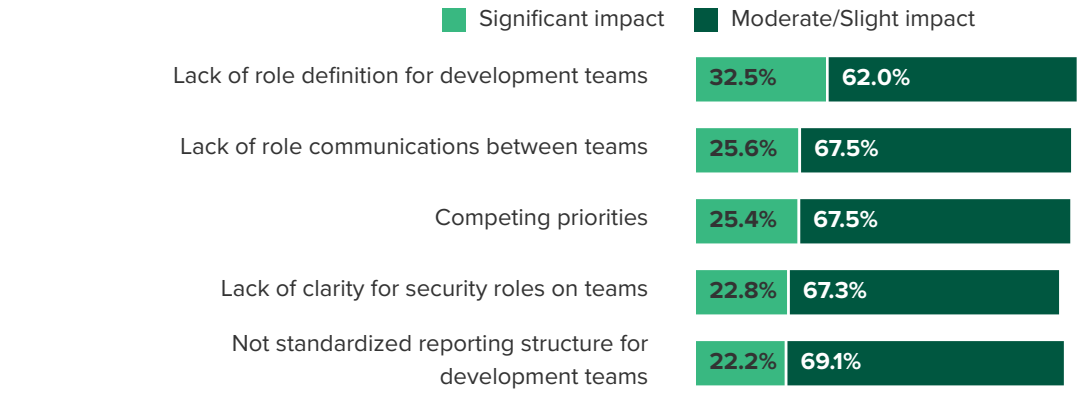
  One practical way for teams to begin the process of relationship improvement is to have shared KPIs, such as accelerated release velocity, reduced security incidents, and decreased mean time to patch/update across teams to give a unifying purpose. For example, sharing the KPI of accelerate release velocity pushes security to dive into the world of development, learn the mechanics, and implement security policies that both meet their 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.

1 in 3 are not effectively collaborating to strengthen security and development relationships.

› **Focus on enhancing communication to improve relationships.** The lack of communication and lack of clarity among roles has a major impact on collaboration across teams (see Figure 6).

Figure 6

"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

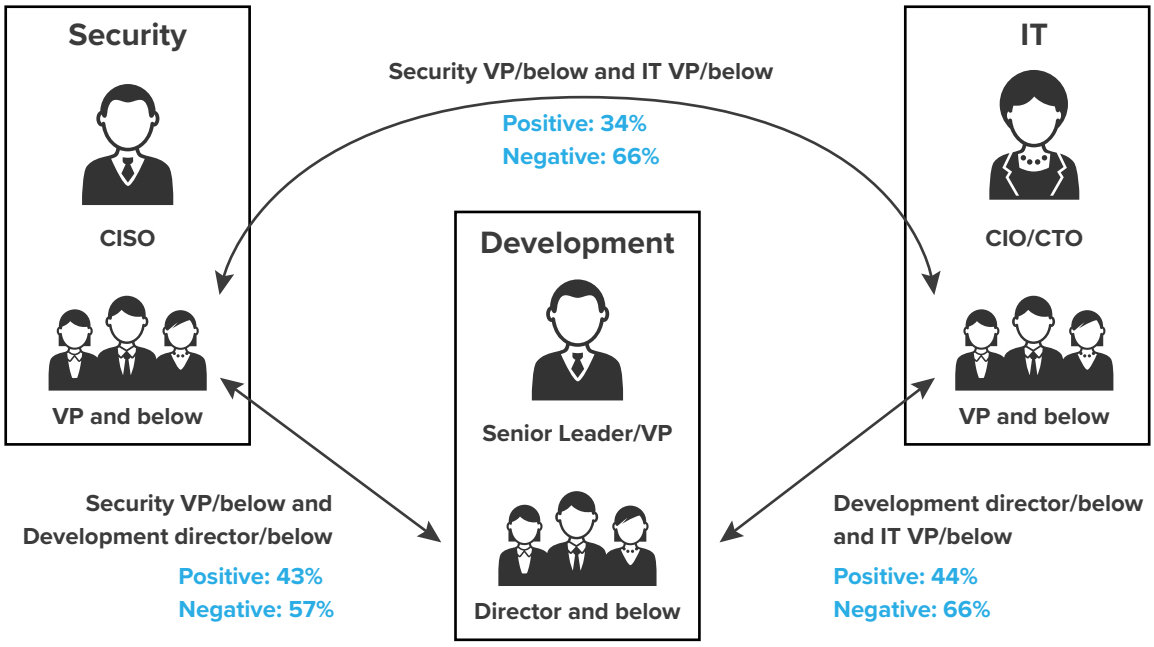
By communicating priorities and objectives across teams, collaboration can greatly improve through those broken-down silos. Having a security advocate embedded on teams or having a regular stand-up meeting with key members from each team allows companies to effectively collaborate rather than impede progress. A CTO at a travel technology organization noted:

"I think **our IT, security, and development team relationships are quite the opposite of strained**. My leadership team, which includes our head of security, has a daily standup where we go through the prioritization of product features with infrastructure apps and security apps. **There's complete transparency around the daily issues** that we run into across IT, security, and development.

There is debate on what we can and can't do, but it's done very transparently, and **we make decisions together** on how we prioritize things. We'll have a conversation together and obviously there's trade-offs between doing everything security wants versus building product features. We're very transparent about the things that we do together. The daily sprint planning or the bi-weekly sprint planning all the way through strategic alignment of our roadmaps across all three groups happens continuously. I think that starts with the top and works its way down to the underlying infrastructure, product engineering, and security teams."

› **Improve strained relationships, particularly for VP/below groups.** In an assessment of relationships from 2020 to 2021, it is clear that relationships have only improved slightly and have a long way to go to be positive.[5] The relationship between security and the other teams is particularly strained, especially for the VP/below groups (see Figure 7). This is likely fueled by competing priorities, lack of communication, and lack of role clarity.

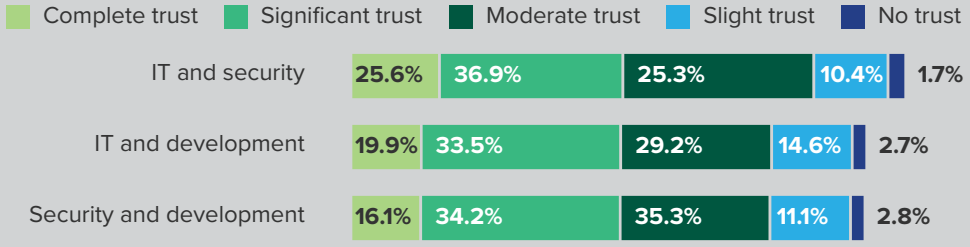
Figure 7: Relationships Between VP And Below Groups



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

› **Have an education, communication, and collaboration plan to improve trust between teams.** The lack of trust across teams is prevalent, fueling their negative relationships (see Figure 8). However, teams that do have some level of trust indicate that relationships can be improved and trust can be built through education, communication, and collaboration.

Figure 8
Level Of Trust Between 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®

Teams with trust indicate that the following statements are true about their team dynamics:

- Security is top of mind (66.7%).
- Proper security education is in place (56.6%).
- Representatives from IT, security, and development teams collaborate in developing strategies that solve for risks and security gaps identified across the enterprise (53.3%).
- Roles and responsibilities across IT, security, and development teams are clearly defined and workflow is established (45.0%).
- Tasks/actions are not micromanaged across IT, security, and development teams (43.8%).

These statements indicate that education, communication, and collaboration are the building blocks of trust across teams. The most important thing to remember is that it is critical to teach security to understand development, not making development understand the language of security. It's not about fault, it's about empathy, culture, and aligning priorities.

Building a network of developer champions is one way this can be accomplished. When building a formal, funded champion program, make sure to identify and train developer security champions, support and reward the champions, and measure success. Forrester notes, "When you can't find direct developer experience, hire a person who empathizes with the role and pressures that developers experience."[6] This empathetic approach helps to bridge the gap between security and development and instills a culture of security.

Recommendation 4: Automate Security To Improve Scalability

- **Automate security processes to improve scalability.** In general, security teams have a smaller number of employees than IT and development teams, highlighting the need for automation. In this study, the average number of employees on IT teams (97) and development teams (86) far outweighed security teams (59). The VP of DevOps at a Financial Services organization noted:

  "The number of developers far outweighs the number of people on the security team, at least in organizations that I have been a part of. It makes it harder to have a high level of interaction and even further makes the case for automation on the security team."

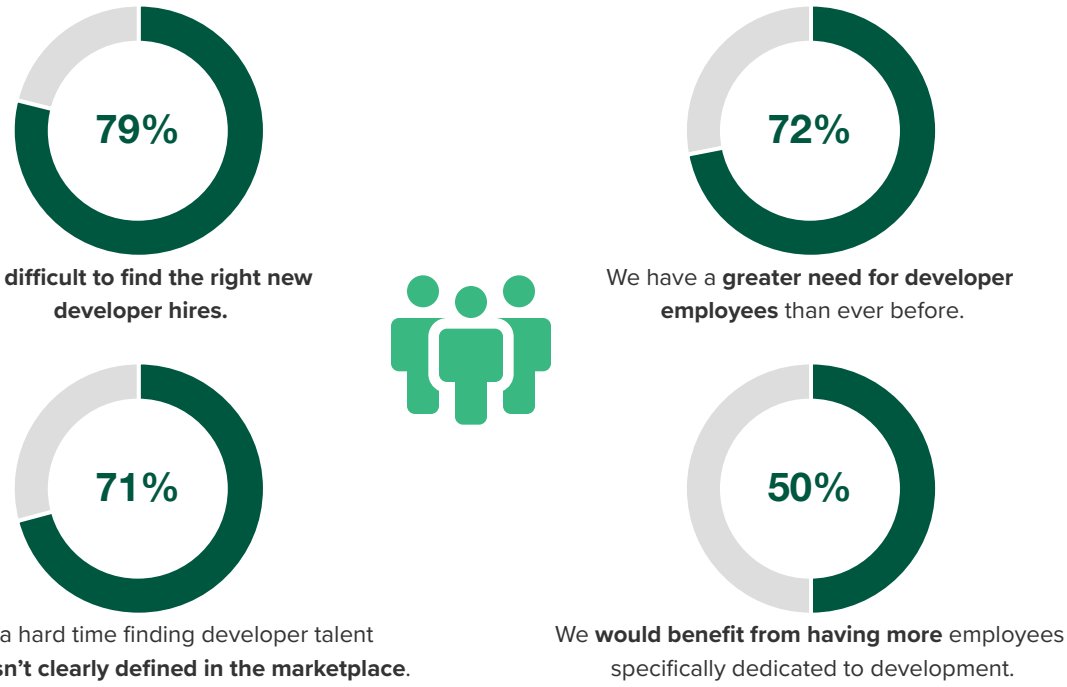
  Even though it's imperative for the security team to automate to scale to meet the needs of the enterprise, four in five (80.4%) security teams are only moderately focused, slightly focused, or not focused on this at all. Development teams specialize in automation, which is something the security team needs most. The lack of automation can have devastating consequences as the VP of DevOps at a financial services organization noted:

  "Our security ticketing system takes way too much time. **It kills productivity and it's not efficient for anyone**. Not only that, but worse. You still have to get the job done somehow. **People take really awful shortcuts** like extending the security of an existing group rather than creating a new one. This is rampant, just to get around the cumbersome and time-consuming system. People do that all the time."

  When automating security, it is important to remember that security should be a service. Security should research the development team's requirements, procedures, and vendors to provide them with automated processes that meet their needs. For developers, ease of use is critical to not impede progress. Treating security as a service can help avoid hindering agility with a rollout of policies that don't meet the development teams' needs.

- **Increase employee experience to help retain hard to find talent.** Teams are understaffed across the board: IT (65.9%), security (68.0%), and development (64.2%), and it is very difficult to find development talent in the marketplace (see Figure 9). The inability to find qualified staff highlights the need for increased automation when possible, along with a superb employee experience so that good talent can be acquired and retained.

Figure 9
Challenges With Finding Development Talent



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

› **Integrate security systems to bake security into the application lifecycle.** Only one-third of respondents (32.9%) indicated that their organizations' security solutions are mostly or completely integrated with seamless sharing of data between products/tools or integrated with custom or off the shelf APIs. Because security solutions remain unintegrated, the challenges of ensuring security in the cloud and securing workloads/containers are exacerbated. The security team noted that their top 3 challenges are:

- Ensuring security in the cloud (77.2%).
- Securing workloads and containers (67.6%).
- Integrating security in the DevOps cycle (66.8%).

The results of these integration challenges can be detrimental, resulting in increased silos, decreased collaboration, higher risk of security breaches, increased complexity in managing tools, and a lack of agility. Integrated tools allow the proper pipelines to be in place to enable security teams to push critical updates across registries and to build processes. By integrating the tools, updates can be automated across those systems, baking security into the development process. To alleviate these integration challenges, the security team must consider integration as a top criterion when investing in new tools. A CTO at a healthcare organization noted:

"**There are lots of broken relationships across tools**. We have far too many different systems. **Nobody spends a lot of time thinking about pre-integration**. Most people stood things up and then they will post-integrate. That's not a great strategy for how you do get things done."

FORRESTER®

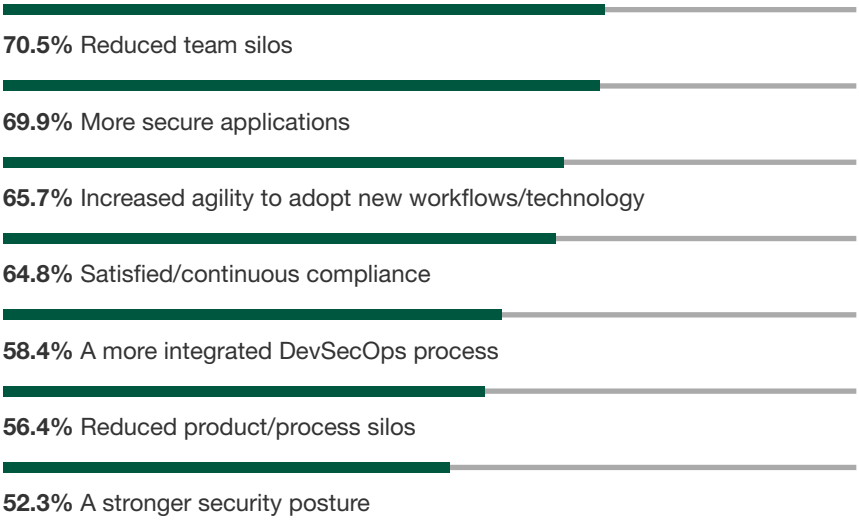
Conclusion: Support Unification Efforts To Increase Security And Innovation

As companies work to put these four recommendations into action, they are, of course, focused on the future of their organization. These organizations should:

- **Improve relationships to see increased innovation and more secure applications**. The goal of improving relationships brings benefits beyond just the relational aspects. It 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. Teams recognized increased collaboration could reduce silos, further secure applications, and increase agility — outcomes teams need the most (see Figure 10). Increased collaboration is the key to unlocking the door to improved security, innovation, and agility — three critical items to both teams.

Figure 10

Benefits Of Increased Collaboration Across Teams



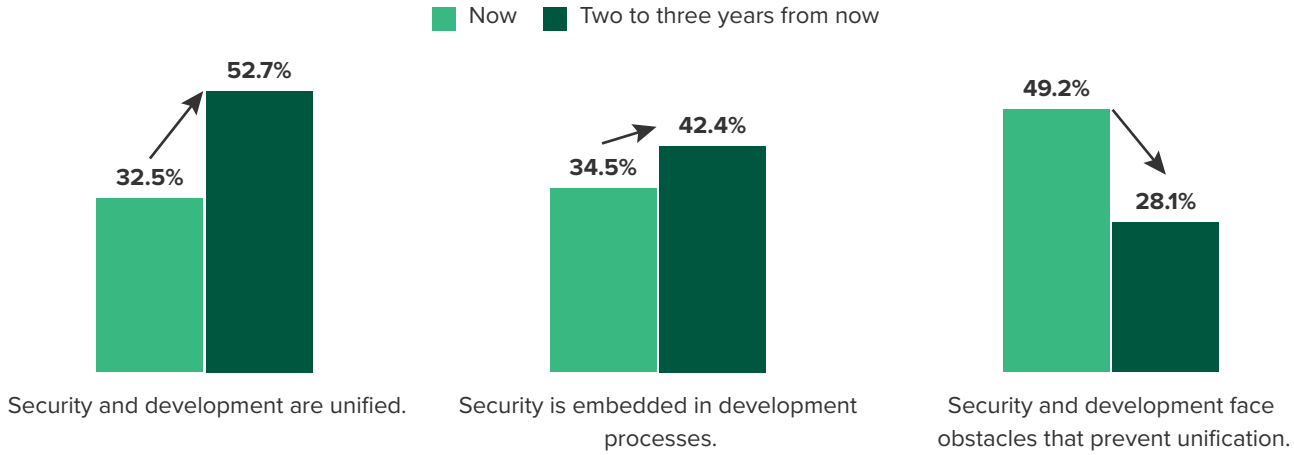
Base: 498 IT, 500 security, and 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

- **Resolve communication and relationship issues now for security and development teams to prepare for the planned unification in the future.** It is important to take active steps towards collaboration now, because more team unification is on the horizon. 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 11).

FORRESTER®

Figure 11

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

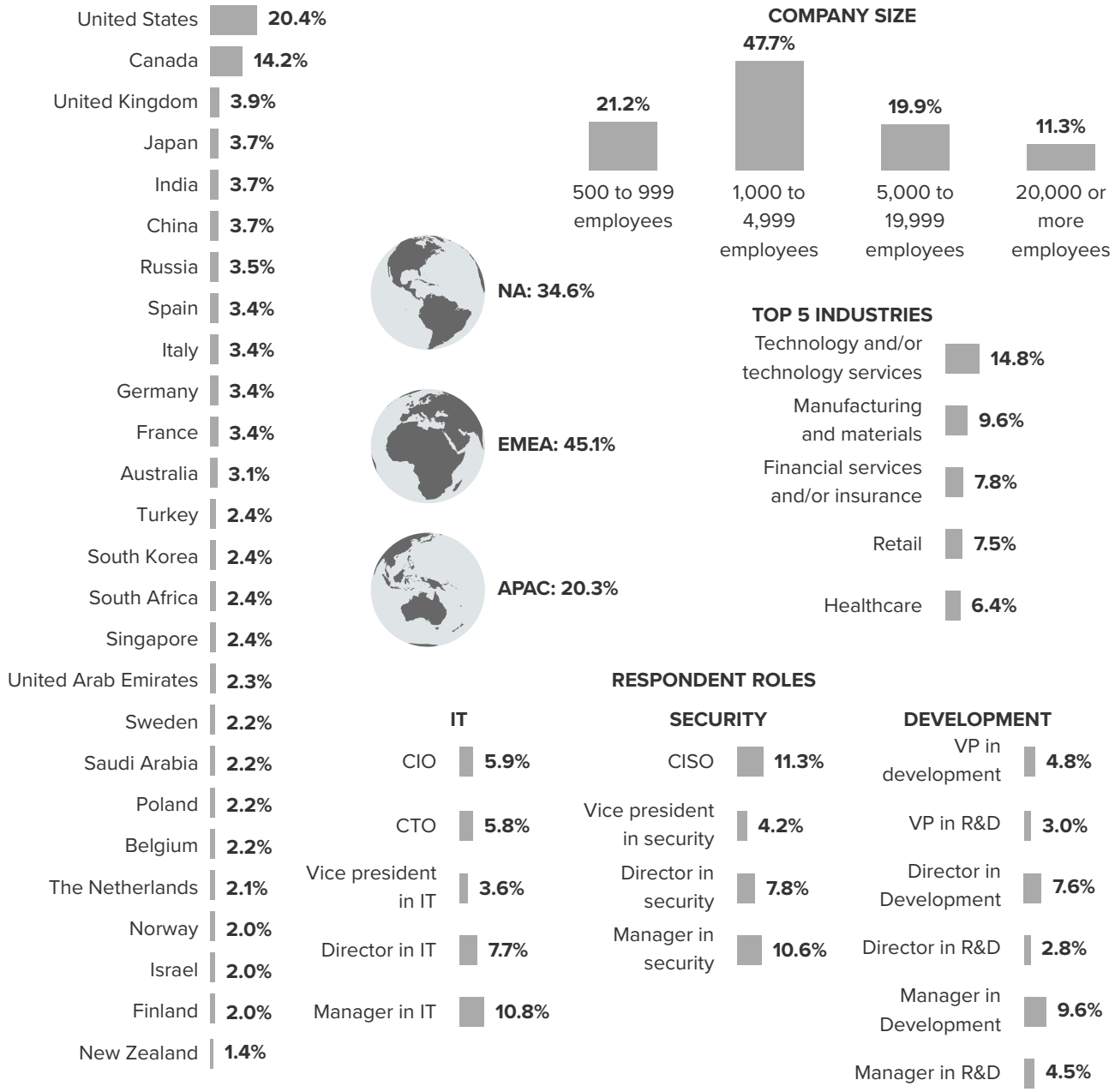
By embedding security into development teams and actively collaborating now, this process of team unification will come as a natural transition in the future. When security and development teams collaborate, embed team members, and work towards shared goals, both the security and development teams can better meet their objectives. Increased unification allows the security team to embed security processes into development processes and yield more secure applications. The unification allows developers to increase their innovation and agility by releasing code and applications faster and more securely.

As companies work towards this more unified state, it is more important than ever that they address communication, education, and relationship issues now to unify and collaborate in the future.

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: Chase Cunningham, "A Look Back At Zero Trust: Never Trust, Always Verify," Forrester Blogs (https://go.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/).

[2] Source: "Don't Ignore Security In Low-Code Development," Forrester Research, Inc., December 23, 2020.

[3] Shift left is a term used to describe the movement of tasks that once happened near the end of the software development life cycle (SDLC) to earlier in the cycle. Source: "Master The SDLC For Modern Application Delivery," Forrester Research, Inc., January 26, 2021.

[4] Source: Chase Cunningham, "A Look Back At Zero Trust: Never Trust, Always Verify," Forrester Blogs (https://go.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/).

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

[6] Source: "Build A Developer Security Champions Program," Forrester Research, Inc., June 12, 2020.