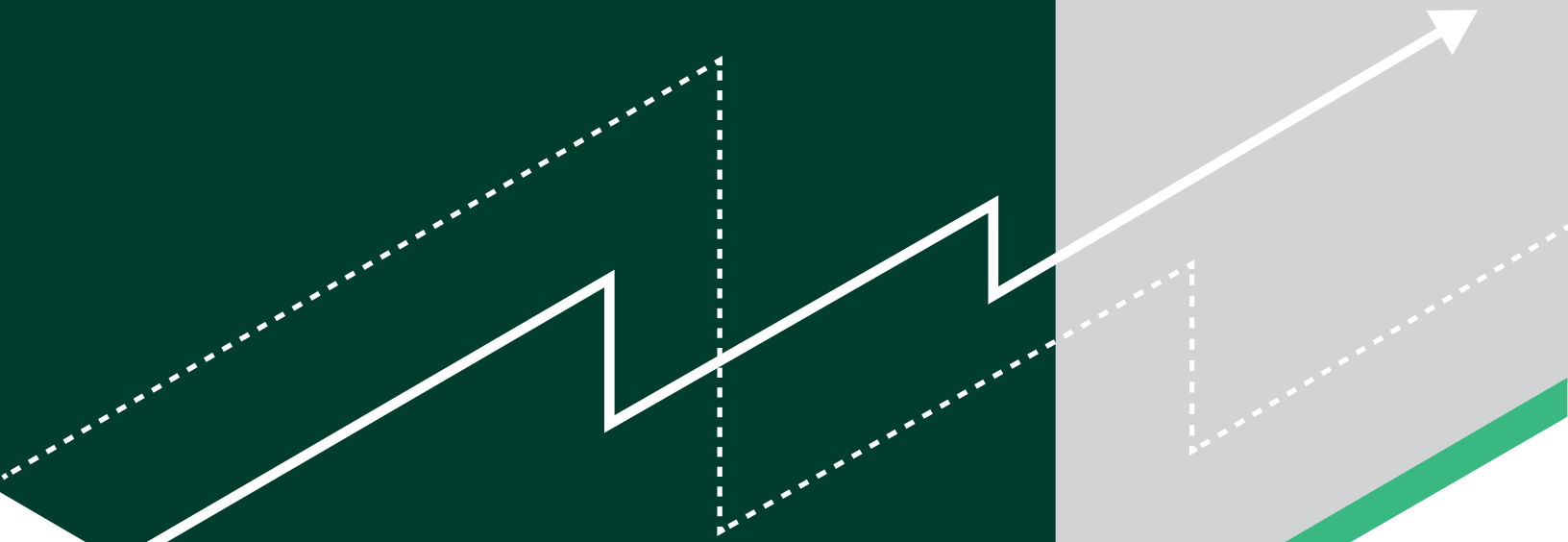
A Forrester Consulting
Thought Leadership Spotlight
Commissioned By VMware

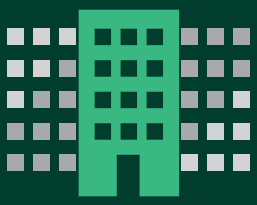
September 2021

Security At The Forefront: A Spotlight On Zero Trust

Zero Trust Results From The September 2021 Thought Leadership Paper, “Bridging The Developer And Security Divide”



FORRESTER®



Executive Summary

As organizations continually work to create agility and security at scale, many have turned to a Zero Trust framework, which is a "never trust, always verify" security model, to be more secure, promote business continuity, and reduce risk.[1]

VMware commissioned Forrester Consulting to evaluate how organizations are working to ensure a strong security posture via Zero Trust. 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.

KEY RECOMMENDATIONS BASED ON FINDINGS

- **Recognize Zero Trust is a continual process, not a laurel to rest on.**
- **Involve development teams early in the security strategy process.**
- **Learn to speak the language of development rather than asking development to speak security.**

Introduction To Zero Trust

As organizations work to build and maintain security and agility at scale within their enterprises, many have turned to a Zero Trust model – a philosophy that you should 'never trust, always verify'. In surveying 1,475 IT, security, and development decision makers about Zero Trust, we found that organizations should:

- **Rebalance priorities based on shifting needs due to COVID-19.** Organizations are very focused on cloud and security, even more so since the onset of COVID-19 (see Figure 1). In looking at the top priorities for the next 12 months, it is clear that collaboration and cloud security are top of mind for organizations.[2] Make sure that your organization reevaluates priorities as your needs shift. Include a rebalance of the budget to align with those priority shifts.

Figure 1

Organization Priorities For Next 12 Months And Changes Since COVID

TOP 6 ORGANIZATION PRIORITIES	% Of Respondents Who Said The Level Of Importance Increased Since Onset of COVID
1 Implement cloud security (68.8%)	75.0%
2 Move infrastructure and applications to the cloud (65.3%)	67.5%
3 Drive collaboration/alignment between IT and security teams (61.4%)	54.9%
4 Drive collaboration/alignment between IT and development teams (59.7%)	65.2%
5 Integrate our front- and back-end systems (58.6%)	39.9%
6 Drive collaboration/alignment between security and development teams (58.1%)	56.1%

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

› **Keep resilience top of mind.** During critical times, security teams focus on risk identification, prevention, detection, and response to promote business continuity and concentrate on cyber resilience. A CTO at a healthcare organization noted:

"In the security space, **our top investment for the year is the combination of preventing ransomware and promoting business continuity**. If you really want to be protected these days **you need to have a better hygiene program.** You need to have stronger controls in terms of what devices actually get access to your internal network. You need to have a more robust protection against ransomware."

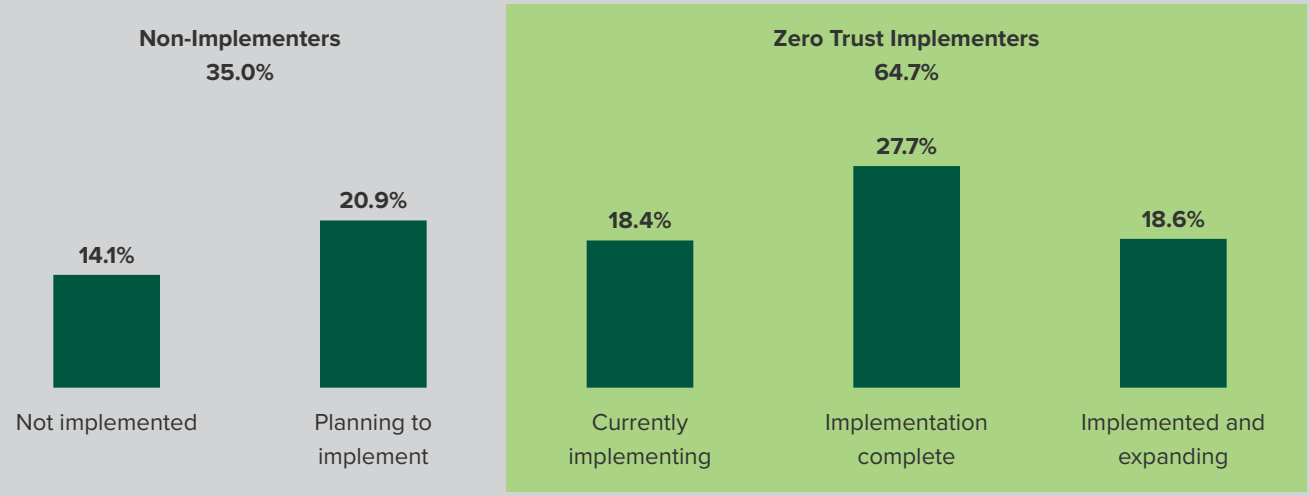
Zero Trust can greatly improve resilience when rolled out effectively across an organization. Because Zero Trust typically brings a decrease in the total number of security incidents and less severe breaches, teams can adapt and respond much faster. As companies look to improve their resiliency, Zero Trust should serve as the foundation for the strategy.

› **Activate your Zero Trust strategy to reduce risk and solve people, process, and technology issues.** Nearly two in three respondents reported their companies have at least started their Zero Trust journey (see Figure 2). For many organizations, this increased focus on business resilience has spurred the adoption or acceleration of a Zero Trust framework within their organization. There is a substantial group of laggards who have yet to begin their journey.

Two in three companies have at least started their Zero Trust journey.

Figure 2

Implementation Status Of Zero Trust Security Framework



Base: 498 IT, 500 security, and 477 development managers and above with responsibility for development and/or security strategy and decision-making
Note: Not showing "Don't know"
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

FORRESTER®

With security, tools and processes are not always the primary issues. Of those non-adopters, there are some significant 'people' problems that might be inhibiting their adoption. Only 25% of non-adopters have increased their organizations' development team staff dedicated to security in the past 12 months. The relationship between security and development teams as a whole is significantly more negative for non-adopters (56% negative) than adopters (48% negative). There is also a lack of Zero Trust education for the non-adopters that could prevent them from adopting this framework. Only four in 10 understand why a Zero Trust framework is important and 41% understand the impacts Zero Trust could have on their organization. Through improved relationships and an increased awareness of Zero Trust and its impact on accomplishing their security goals, these non-adopters could come to understand the value of Zero Trust within their organization.

Only 4 in 10 understand why a Zero Trust framework is important.

- **Adapt your messaging about Zero Trust to make its importance clear to all teams.** Over eight in 10 (81.8%) of Zero Trust adopters said that their organizations' adoption of a Zero Trust framework has been moderately or significantly effective. However, many within the organization are still unclear about the importance of Zero Trust and how it is implemented. To be more effective, educational programs must be improved and the relationship issues must be solved. The recommendation to embed security advocates on teams is critical to a successful Zero Trust rollout as it keeps security top of mind, not as an afterthought.[3] Consider embedding security advocates onto each team across the organization to aid in this messaging. By building stronger relationships and having a more thorough understanding of the unique needs of each team, security advocates can make sure roles, responsibilities, and priorities around Zero Trust are clear.

Benefits Of Zero Trust

Zero Trust provides organizations with the agility and security they desire. We found that organizations should:

› **Activate Zero Trust to improve data protection, threat detection, and the overall quality of work.** Zero Trust can have profound benefits across teams that support their goals. Security professionals noted that a Zero Trust framework helped their organizations reach their goals of better authentication, detection, and resolution (see Figure 3).

Figure 3

"How does/would a Zero Trust framework impact your work?"

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%

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

Recent Forrester research also notes that in addition to promoting a positive security culture, "implementing Zero Trust gives employees more choice, reduces friction in accessing key information resources, and improves technology performance."[4]

› **Create a robust Zero Trust rollout and education plan to greatly reduce security issues.** A Zero Trust mindset that is well executed includes key stakeholders from the beginning and is rolled out with proper education in place is successful at reducing overall security issues within the organization. A CTO at a travel technology organization implemented a successful rollout of Zero Trust and commented:

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

The continuous application of a Zero Trust mindset helps companies accomplish their overall security goals.

Key Recommendations

How can you maximize the benefits of Zero Trust? This study yielded several important recommendations:

RECOMMENDATION 1: RECOGNIZE ZERO TRUST IS A CONTINUAL PROCESS, NOT A LAUREL TO REST ON

› **Use Zero Trust to address your security and compliance needs.** Many adopters of Zero Trust cited drivers of adoption as increased cloud security, network access control, and wake-up calls from others in the industry. Industry professionals had these thoughts about their Zero Trust adoption:

"Things are moving towards Zero Trust. I think **it's largely like cloud-driven.**"

VP of DevOps in FinServ

"From our standpoint, **a zero-trust policy was something that we initially looked at for network access** like VPN connectivity from home where we wanted developers to get access to on-premises tools before we moved to the cloud. For us, it was more a question of what was going to be the best way in which we could do that, no matter if it was a user or a device to prove that they were who they said they were before they could get access to anything."

CTO in Travel Technology

"We're trying to take that next step to get beyond just the basics of zero trust. How do we really do this well? How do we become the gold standard for zero trust? **A lot of that was triggered by a major security event at another organization. I think that caused a big wake-up in our company.** This was a company that, technically, wasn't impacted. The org themselves weren't hacked, their product was hacked and used to island hop, and yet they've taken the full brunt of the impact. There's an awareness now in our business that, **if something similar happened to us it would be catastrophic**, so we're doing a lot of work to make sure that kind of stuff is as protected as possible."

Security Solutions Strategist in Tech Services

Whether driven by your organization's move to cloud, a need for network access control, or a major security event, now is the time to bolster your organization's Zero Trust strategy to combat against security issues and proactively poise yourself to be ready for the future.

› **View Zero Trust as a journey, not a destination.** Zero Trust is a framework for behavior, not a mission can be completed. Because it is intended to be a change in the way that companies think about security as a whole and security needs are always changing, Zero Trust should be viewed as a continual process. This means simple adoption is not enough alone. Putting a strategy in place is the starting point, but Zero Trust must be a permanent focus and journey to be successful. In reflecting on the Zero Trust rollout at his organization, the CTO of a healthcare organization noted:

"**Zero Trust is not a state of being, it's a journey**. It is a thought model. If you think of it as a state and you try to lay out a plan on how to get there, you will actually miss the target. What it really is, is a different way of thinking about security problems.

Security problems keep evolving as our infrastructure solutions, user environment, and threat actors change. I personally don't subscribe to the idea that zero trust is a state, I actually violently disagree with that, but the pursuit of a Zero Trust mindset is absolutely advisable."

Contrary to some other security tools or processes that are implemented in one fell swoop, doing a Zero Trust rollout in one big burst will likely not yield you the results you are looking for.[5] A more strategic, gradual change over a one-to-two-year span that works with existing security capabilities is more likely to stick and be successful. A successful Zero Trust model is a continuous state of discovering, planning, acting, and optimizing with continuous improvements expected.[6]

A successful Zero Trust model is a continuous state of discovering, planning, acting, and optimizing.

RECOMMENDATION 2: INVOLVE DEVELOPMENT TEAMS EARLY IN THE SECURITY STRATEGY PROCESS

› **Involve developers early in the Zero Trust rollout to reduce resistance.** Some business units may initially resist a Zero Trust model as they fear it meddles in their jobs. Additionally, over half (52.4%) of developers reported thinking security policies can stifle their innovation. This is often the result of security pushing down new protocols and procedures without having a thorough understanding of how it will actually impact other teams.

When the security team doesn't have a thorough understanding of the tools and platforms other teams have in use, their protocols often impede progress. This highlights the need to involve other teams early on. As is, developers are often left out of the security planning process, leaving them to implement security policies that they don't understand or were not made properly with their needs in mind. The senior director of DevOps at a tech services organization noted:

"I think that **developers are definitely being left out** of the security education process."

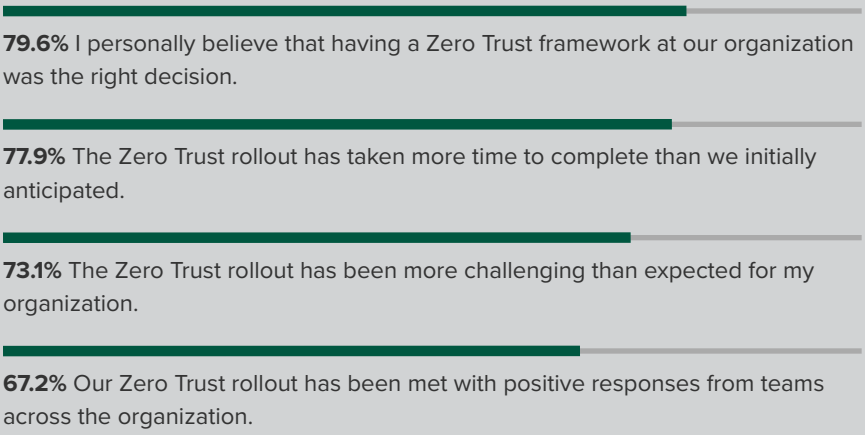
This highlights the need for security advocates to be embedded into development teams to ensure that development is involved early on. More and more security tasks are being shifted left for developers.[7] This means that they will only have increased responsibility for security in the future. However, this will be challenging unless developers understand the security strategy, involve themselves in the security decision-making, and influence the policies that impact their work. Have regular stand-ups with key team members from all teams across the organization to ensure that the unique needs of each team are addressed before rolling out new policies.

› **Increase communication to ease the challenges of your Zero Trust journey.** For adopters, the Zero Trust rollout was longer than anticipated, more challenging than expected, and not always met with positive responses (see Figure 4). But when asked if the security team collaborated and worked with other teams before the rollout, the answers were negative. Over half of teams (51.4% of development teams and 59.8% of IT teams) were not consulted about the adoption. It was simply rolled out to them and they were expected to comply with no initial involvement. This further underscores that security should not be a specialization, but an embedded part of teams so that security initiatives are baked into processes and made with the needs of other teams in mind. Think of developers as your clients, and that you are providing them with a service. Your team should build relationships with developers, embed yourselves into their processes, and provide solutions that work with their needs. By viewing the security team as a services team for the rest of the organization, goals are more aligned and teams are empowered to work together to achieve their goals rather than impeding progress and innovation.

Over half of teams were not consulted about the adoption of Zero Trust.

Figure 4

"Rate your level of agreement with the following statements."
(Showing "Agree" and "Strongly Agree")



Base: 955 IT, security, and 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

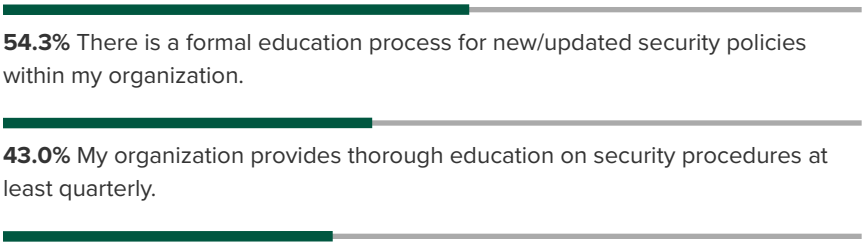
FORRESTER®

RECOMMENDATION 3: LEARN TO SPEAK THE LANGUAGE OF DEVELOPMENT RATHER THAN ASKING DEVELOPMENT TO SPEAK SECURITY

› **Make education a two-way street for your teams.** Historically, security teams have taken a "teach them security" approach rather than an "empathize and educate ourselves" approach. Even still, organizations have some major security education gaps with most developers never being fully educated on security procedures (see Figure 5).

Figure 5

"Rate your level of agreement with the following statements."
(Showing "Agree" and "Strongly Agree")



54.3% There is a formal education process for new/updated security policies within my organization.

43.0% My organization provides thorough education on security procedures at least quarterly.

38.4% The development teams are thoroughly educated on security procedures that they are expected to execute.

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

Right now, security and development teams are not always involved in each other's work when they should be. Professionals in the space noted:

"We're **trying to be better at involving stakeholders early**."

CTO in Healthcare

"**We are not consulted** about security tools, technology, 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

This can be solved by embedding a security advocate on teams, sending security to the teams rather than making the teams seek out and figure out how to comply with security. Unfortunately, only one in three developers (38.6%) reported having a security advocate embedded in their team. Security should be investing in understanding development teams by embedding a team member to improve relationships and increase compliance.

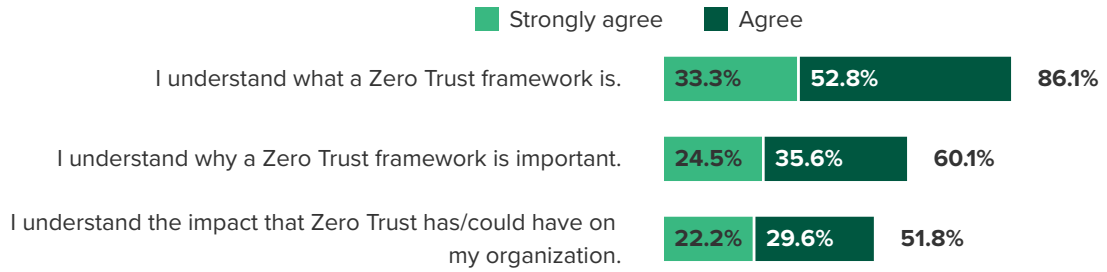
› **Create thorough education programs to make the importance of Zero Trust clear to developers.** Developers noted that they generally understand what Zero Trust is, but are still unclear why it is important, highlighting the need for further Zero Trust education (see Figure 6).

Because Zero Trust isn't just another tool from the security team, but a true change in the way people think, security teams must get buy-in from across the organization. It's important for security to build a network of champions and 'sell' the strategy internally to get buy-in to increase the likelihood of success.[8]

Only half (51.8%) of developers reported understanding the impacts that Zero Trust has on their organization.

Figure 6

Development Team's Understanding Of Zero Trust

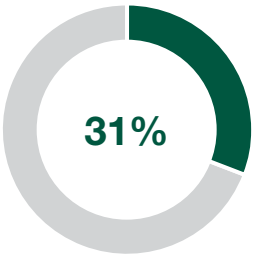


Base: 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

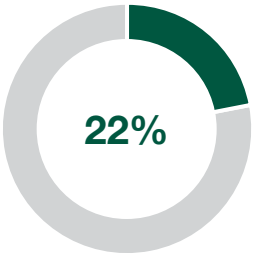
› **Set clear expectations about Zero Trust roles and duties to garner more involvement across the organization.** About half of developers said they do not feel they are responsible for the Zero Trust rollout (47.2%) or for carrying out their organizations' policies related to Zero Trust in their line of work (59.7%). This is very problematic as Zero Trust is a way of thinking for all individuals, not just the security team. These responses indicated that the development team's role is mostly undefined when it comes to Zero Trust. Because security is no longer a specialization, Zero Trust should be the responsibility of everyone in the organization. However, security policies are not very clear to development teams (see Figure 7).

Figure 7

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.

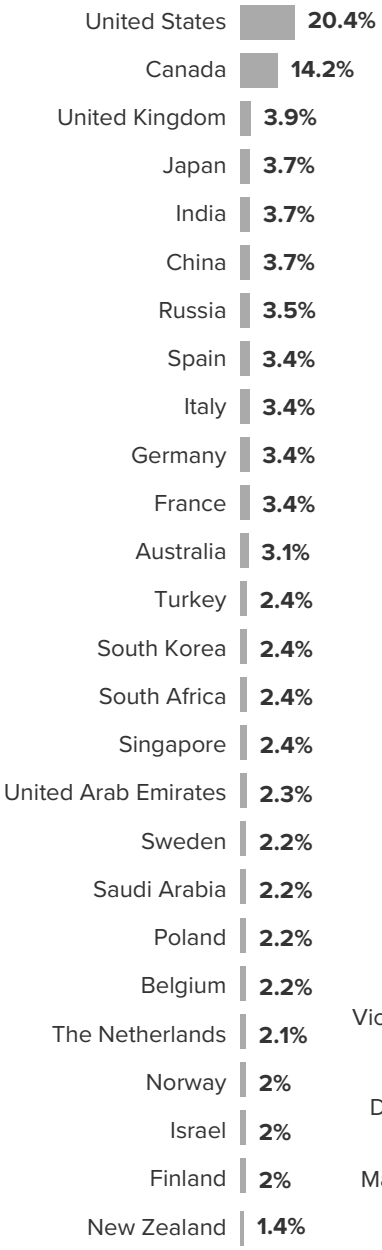
Base: 477 development managers and above with responsibility for development and/or security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, April 2021

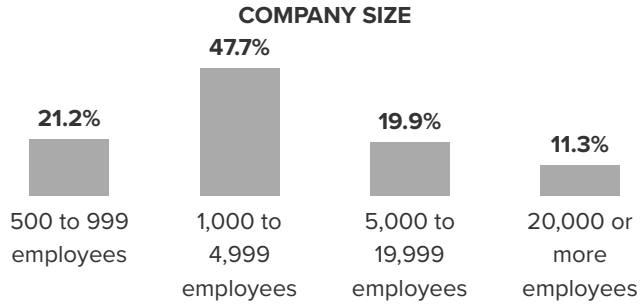
A two-way education is critical as development teams are often key drivers of revenue for the organization. When security policies are so automated that they don't slow down the development lifecycle, developers can continue to innovate and drive revenue growth, while keeping the business secure.

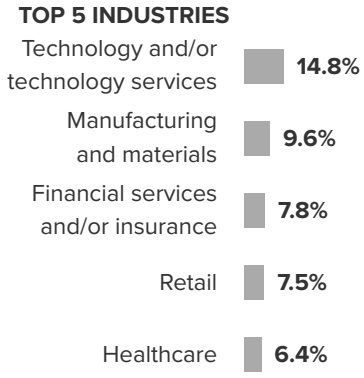
Appendix A: Methodology

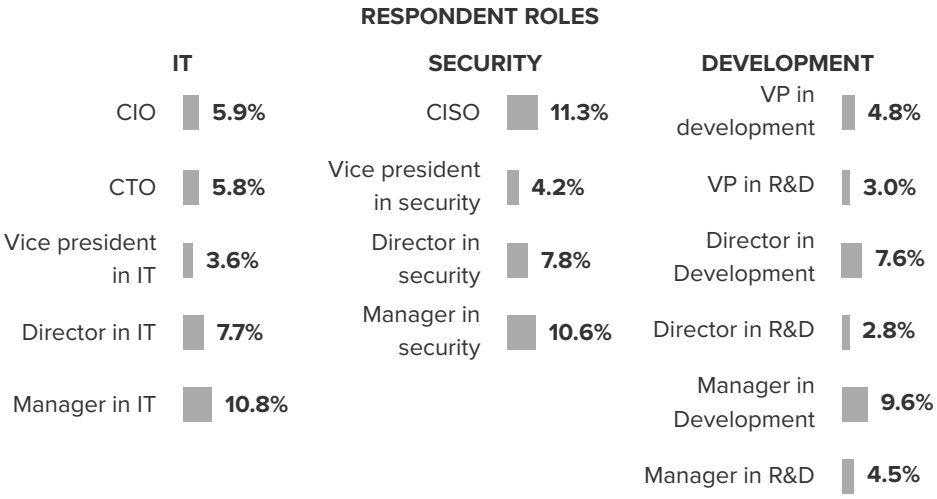
In this study, Forrester surveyed 1,475 IT, security, and development managers and above (including CIOs and CISOs) with responsibility for development or security strategy decision-making. Forrester also conducted five interviews with directors and above in these roles. The purpose of this study was 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] "Security And Development: A Spotlight On Relationships," a commissioned study conducted by Forrester Consulting on behalf of VMware, September 2021.

[3] "Bridging The Developer And Security Divide," a commissioned study conducted by Forrester Consulting on behalf of VMware, September 2021.

[4] Source: "Enhance EX With Zero Trust," Forrester Research, Inc., July 13, 2020.

[5] Source: "A Practical Guide To A Zero Trust Implementation," Forrester Research, Inc., March 3, 2021.

[6] Source: "Defend Your Digital Business From Advanced Cyberattacks Using Forrester's Zero Trust Model," Forrester Research, Inc., June 25, 2021.

[7] 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.

[8] Source: "Sell Your Zero Trust Strategy Internally," Forrester Research, Inc., June 23, 2020.

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®