

Why Automation and Security are Critical to Successful Cross-Functional Teams – DevSecOps

July 2022 EMA Research Report

By Will Schoeppner
Research Director



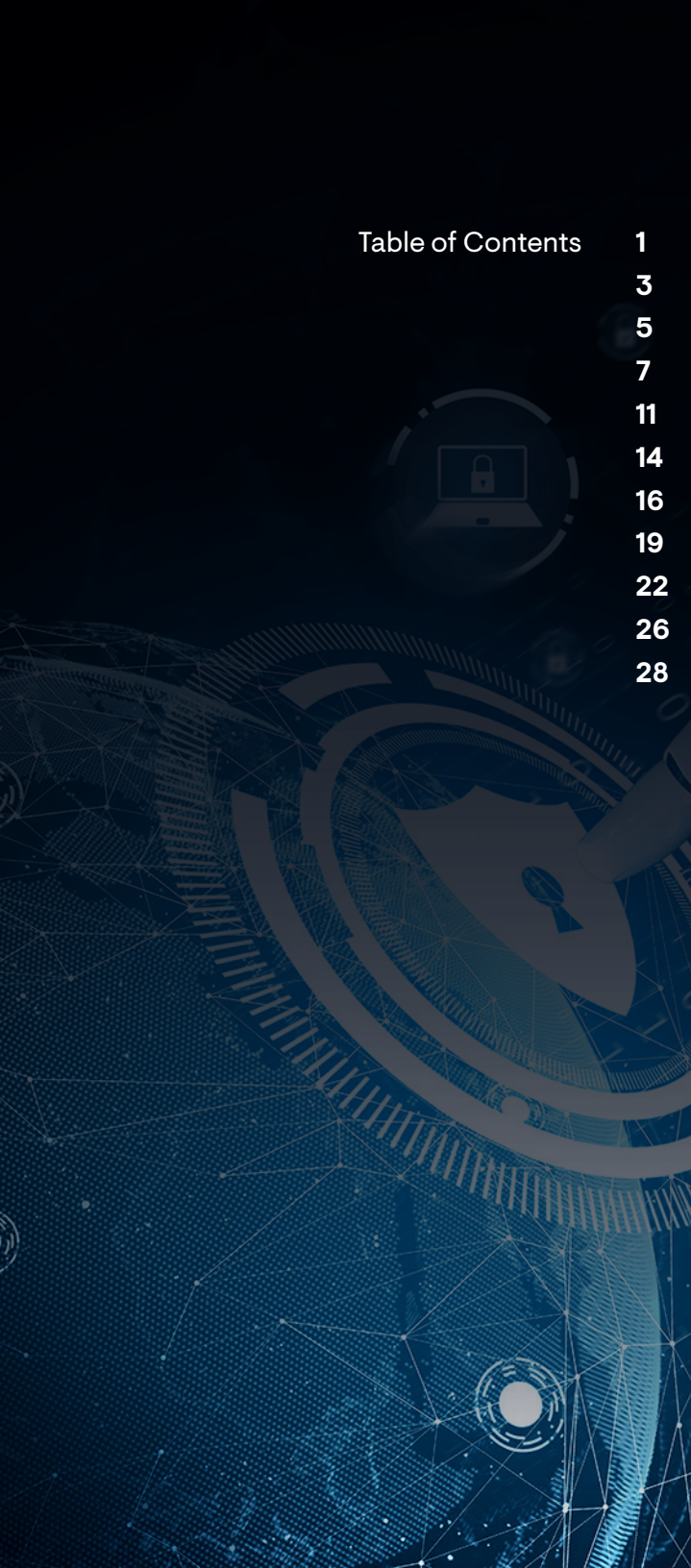


Table of Contents

1	DevSecOps in 2022
3	About the Study – Demographics
5	Executive Summary
7	The Structure Around a Successful, Collaborative Environment
11	The First Pillar – People
14	The Second Pillar – Processes
16	The Third Pillar – Technology
19	Trends in Cross-Functional Teams
22	The Dependence on Security and Automation
26	Conclusion
28	Case Study: Treating Security Like a Product at the U.S. Army Software Factory



DevSecOps in 2022

Today's business relies on faster, more reliable delivery from internal technical teams. This has led to an increase in collaboration between information technology teams over the past few years with DevOps teams, then with the addition of security teams to create a DevSecOps practice. This coordination focused on eliminating silos that are known to plague technical teams for years. However, for companies to realize the successes of these cross-functional teams, there must be a focus on three key pillars. The first includes people, then individuals, skillsets, and dynamics of the team members. The second pillar is process, with repeatable, documented procedures for all team members to follow. Finally, the third pillar is tools. Collaboration and development tools have advanced significantly in the years to allow cross-functional teams to be able to share ideas, communication, priorities, and responsibilities in a unified location, creating a seamless environment driving success. Organizations need to become nimble in providing fast, secure, reliable technology products and services throughout their increasingly complex, integrated enterprises. Research proves that demands on customer experience, the ever-growing challenge of staying ahead of risk and market swings, and employee engagement are the driving factors for these shifts.

As a result, the ability of organizations to implement cross-functional teams directly impacts organizational maturity. In concert, with the focus in agile and continuous integration and continuous delivery (CI/CD), customer experience is essential and is a term that has exploded in popularity recently. Having a business strategy centered on customer experience has become much more than just a trend. However, companies struggle to realize the true benefit of having a customer-focused strategy without focusing on all layers of the organization, including cohesive technology teams, and breaking down institutional silos. This strategy begins at multiple areas of the organization. A strong culture and strategy driven from the organization's leadership, all the way to a highly functional technology infrastructure layer with fully integrated workflow automation processes, make it possible to realize business impact throughout the organization and ultimately drive customer experience to see gains in revenue and customer retention.

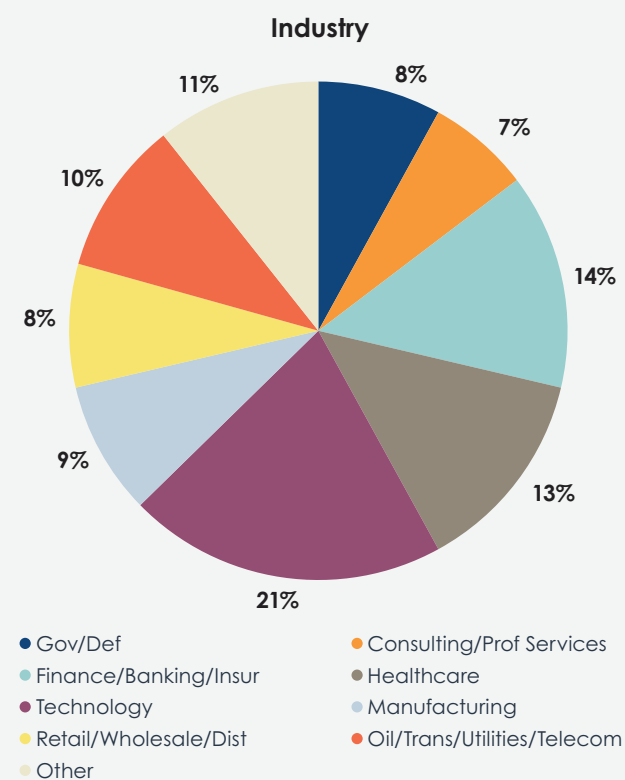
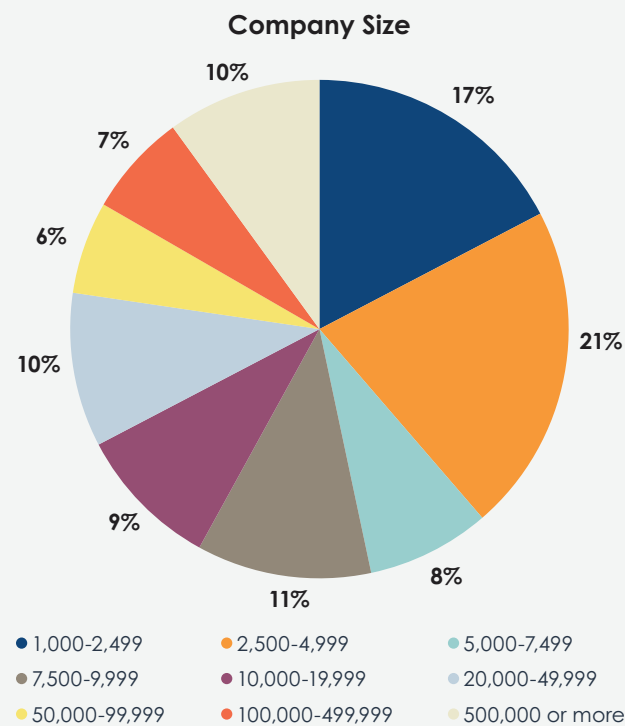
EMA research focused on where organizations can build on the successes of cross-functional teams by incorporating key functions and understanding how organizations can benefit from "shifting left" of critical operations in the development lifecycle, including security and automation.



About the Study – Demographics

The focus of this research, conducted in partnership with AppDynamics and VMware, was to understand the success of DevOps collaboration, how companies can build on the outcomes, and what is required for this success to continue in a complex, hybrid, multi-cloud environment. This study was conducted in the United States, United Kingdom, France, and Germany. The study collected results from 150 participants across multiple industries and job functions to capture a comprehensive landscape of cross-functional team collaboration and operations.

- Total Qualified: 150
- Company Size: 1,000+
- Location: 51% - U.S.
49% - Europe (UK, Germany, and France)





Executive Summary

The research delivered several fascinating key findings detailed throughout the report. Some of these key findings are:

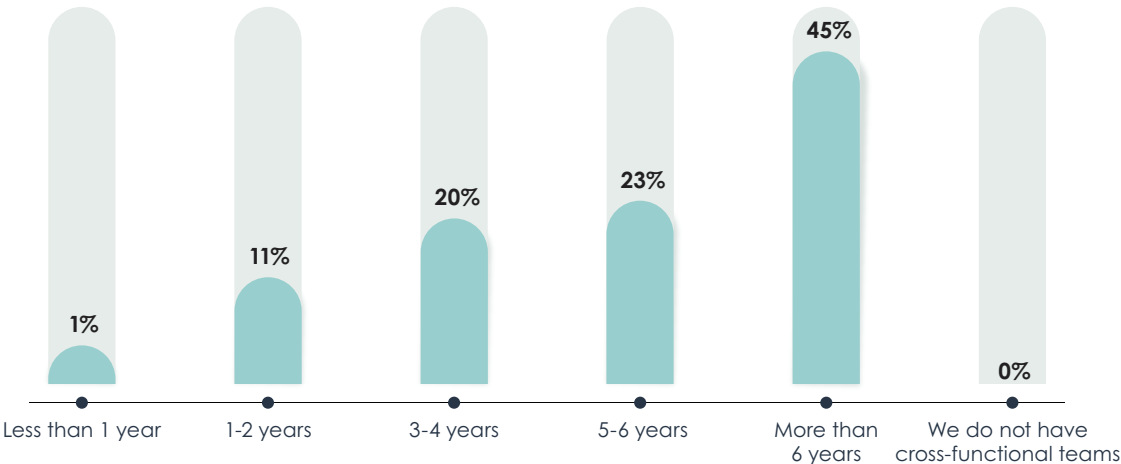
- Cross-functional teams, including DevOps, have been realized by 45% of organizations for over six years.
- The US (63% six years or more) has integrated technology teams longer than European countries (36% six years or more). However, European countries (90% agree) are seeing a greater benefit over the US (83% agree).
- Competing goals and priorities (33%) is the number-one reason overall for silos. The top reason in the US is competing goals and priorities (35%) and responsibilities in separate tools (30%). For European countries, it's competing priorities (32%) and lack of resources (21%).
- 73% of organizations have integrated DevOps teams. Only 38% of organizations have integrated DevSecOps teams.
- The greatest benefit of cross-functional teams is greater overall project success.
- 70% of organizations are satisfied with their cross-functional team production and collaboration tools, but only 19% are very satisfied.
- Only 27% of cross-functional teams use the same tools for collaboration.
- Companies are fairly to very concerned with vulnerabilities in open-source services (74%).
- Over half (52%) of companies rely on automation to update infrastructure code and application software from vulnerabilities most of the time.
- 50% of respondents feel security is an afterthought in the application delivery ecosystem.



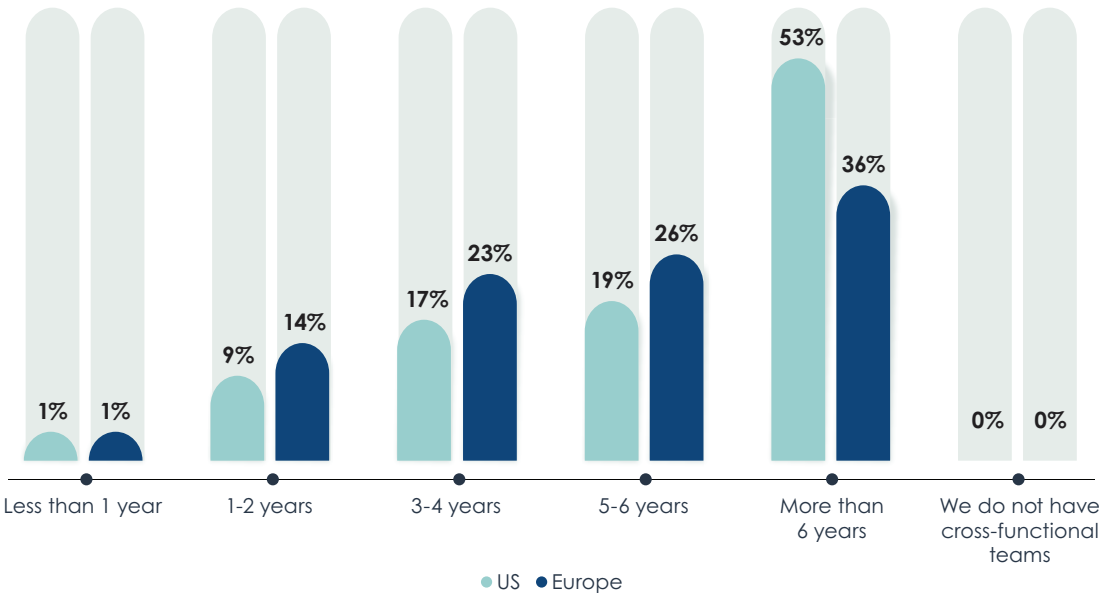
The Structure Around a Successful,
Collaborative Environment

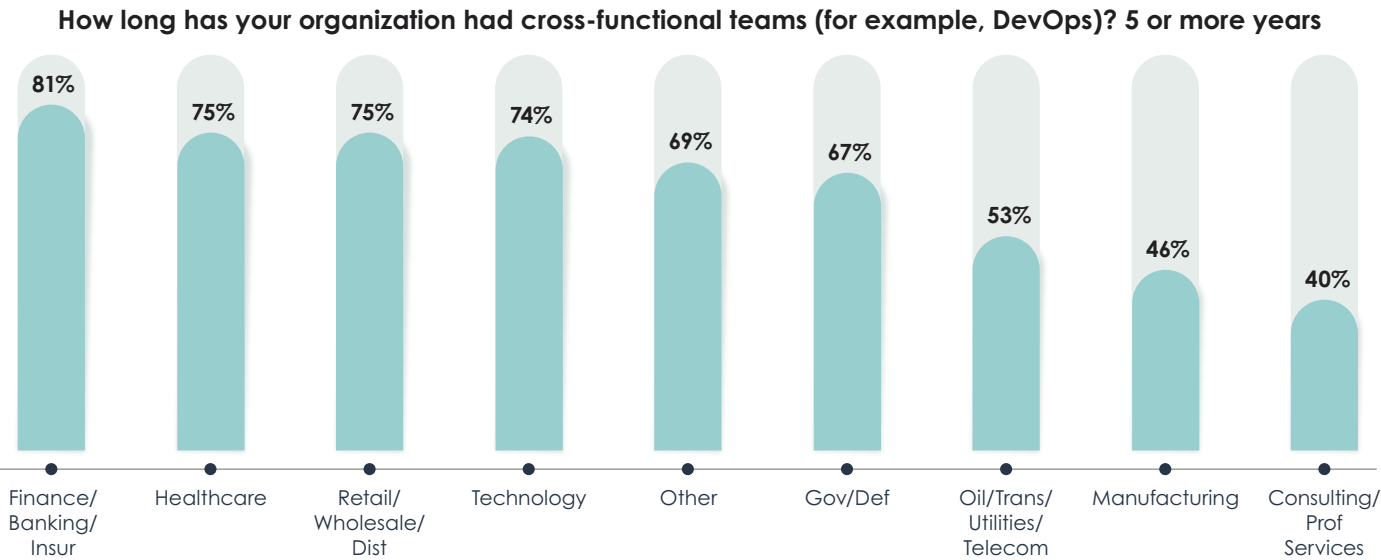
To understand the DNA of an organization that has integrated cross-functional teams, EMA asked survey respondents how long they have had DevOps teams in their environments. DevOps integration isn’t new, and the data shows that 45% of organizations have DevOps integrated in their application development ecosystems for more than six years. Interestingly, the US showed this adoption earlier, with 53% of companies surveyed having DevOps integration for six years or more and European countries with only 36% of respondents indicating having DevOps teams for six years or more. From the graphics, it is evident that finance, banking, and insurance, followed by healthcare, retail, and technology companies, were quicker to adopt cross-functional teams in their application development processes.

How long has your organization had cross-functional teams (for example, DevOps)?



How long has your organization had cross-functional teams (for example, DevOps)?

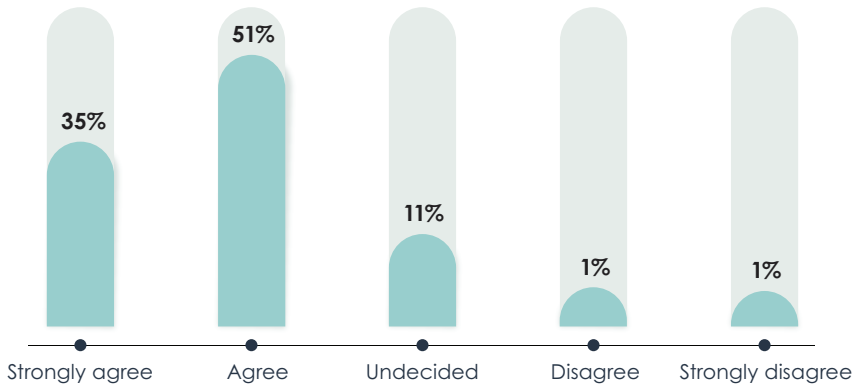




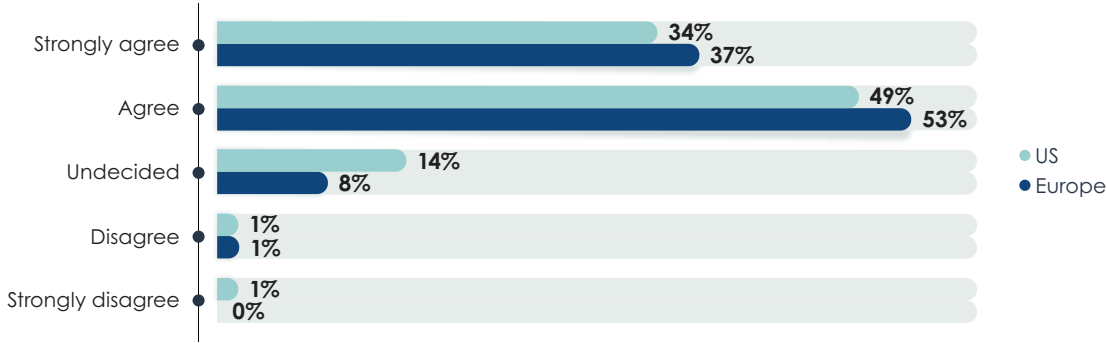
It should not come as a surprise that most respondents (more than 86%) indicated that they are seeing a direct impact of having cross-functional teams. However, an interesting data point in the research showed that even though European countries adopted cross-functional teams more recently, they are seeing a greater impact to business outcomes at 90% in comparison to US respondents at 83%.

When respondents were asked what the greatest challenges are to creating silos in the organization, the number-one reason given was due to competing goals and priorities.

Are you seeing a direct impact to business outcomes from having cross-functional teams?



Are you seeing a direct impact to business outcomes from having cross-functional teams?



What is the greatest challenge that's creating silos within the organization?

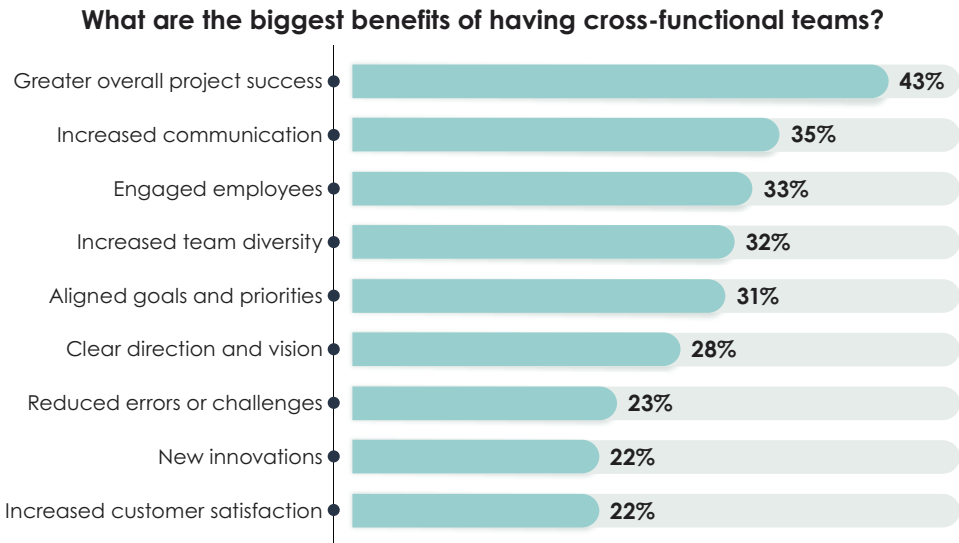
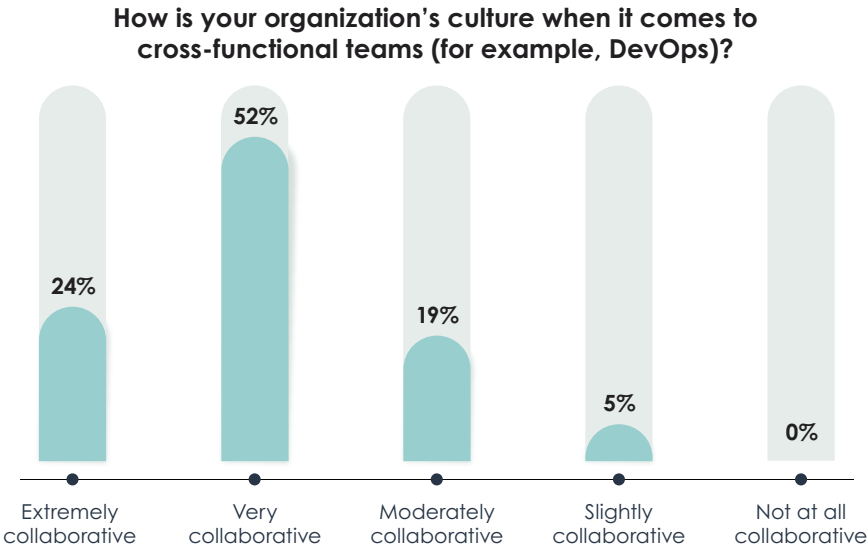




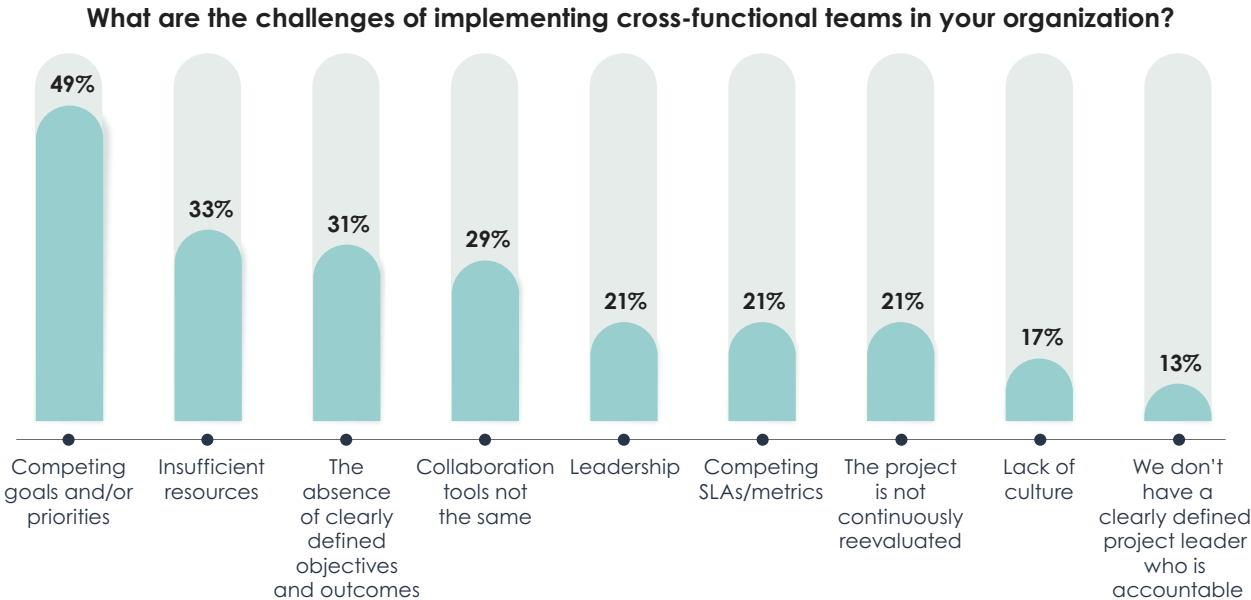
The First Pillar – People

Developing cross-functional teams begins with the individuals who make up the critical technology and business operations teams that are the success of any organization. Technology teams are inundated with ongoing day-to-day activities, ongoing technology projects, and ever-growing technology initiatives. The individuals who make up the teams may, at first, see developing cross-functional teams as another layer of complexity in an already complex environment. Therefore, EMA asked about the organization’s culture when it comes to cross-functional teams like DevOps. Results show that 76% of respondents felt their company’s culture was either extremely or very collaborative.

Another key to creating successful cross-functional teams is to bring in diverse talent to inspire innovation and growth within the organization. Not surprisingly, the data showed that one of the top benefits of having cross-functional teams was increased diversity.



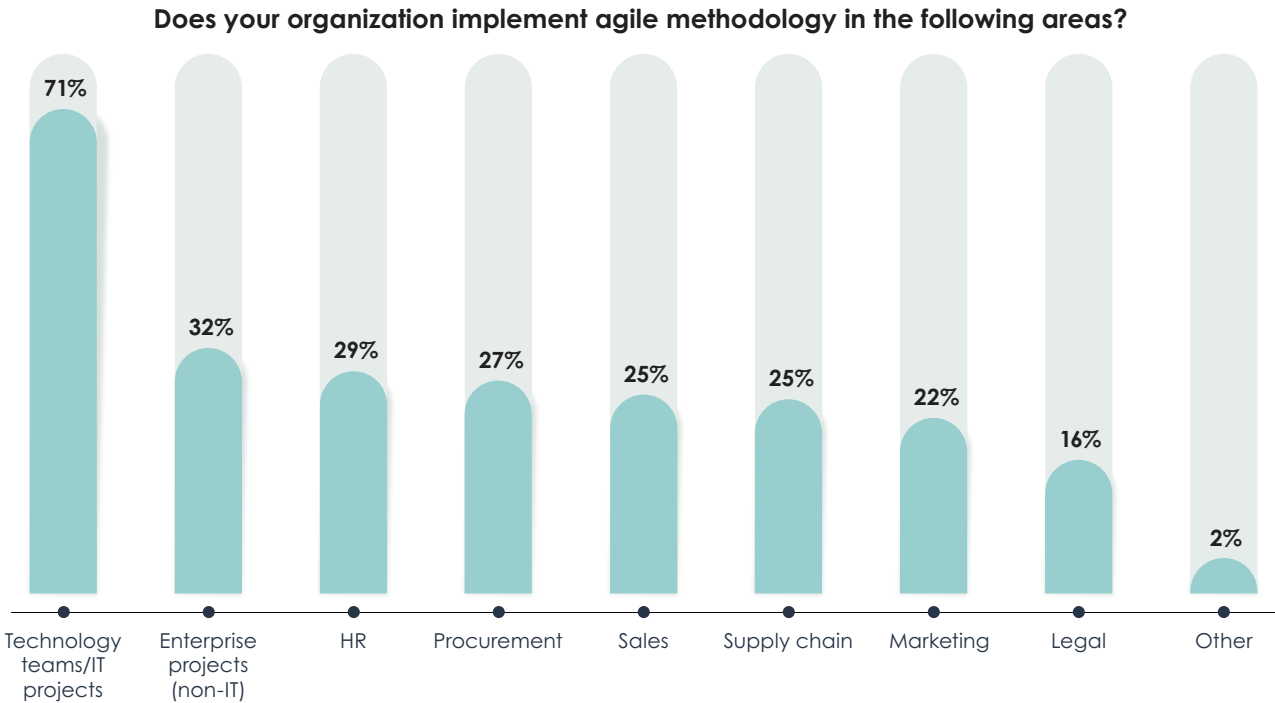
However, technology teams need the support and direction of the business leaders with a well-structured strategy that incorporates team integration at all levels and functions in the organization. This is evident by the finding when EMA asked what the challenges are of implementing cross-functional teams. Nearly 50% of companies stated that competing goals and priorities was number one, followed by 33% indicating insufficient resources.





The Second Pillar – Processes

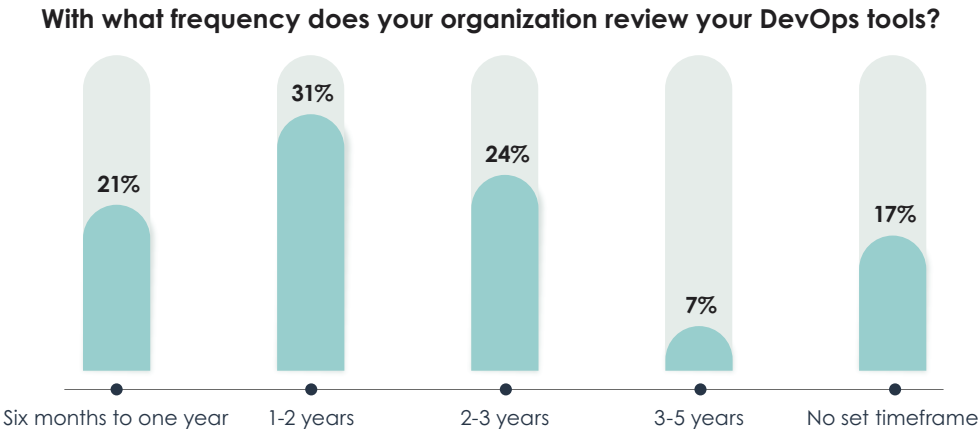
A strong hallmark of a mature enterprise with a strategy incorporating cross-function teams is the adoption of agile processes instituted in core business functions. A common limitation for technology teams adopting agile and DevOps in their development process is competing business processes, often seen when areas including supply chain, procurement, human resources, and non-technology initiatives are still using traditional processes. This can lead to confusion and competing priorities within the organization. EMA research shows that companies recognize this challenge and are incorporating agile methodology in core business functions outside of the information technology development teams. When respondents were asked if agile processes are used throughout the organization, 32% indicated that they use agile for non-IT projects and 29% of companies use agile in their HR teams, 27% of their procurement teams, and 25% of organizations sales and supply chain departments.





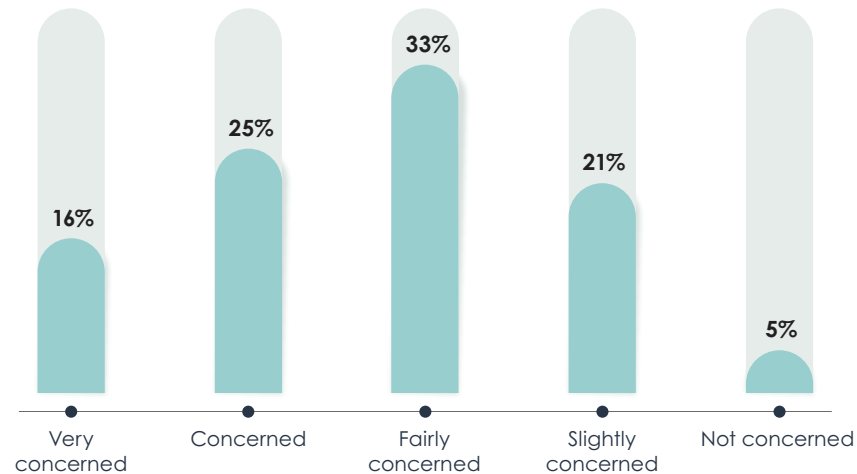
The Third Pillar – Technology

People and processes are two pillars critical to the success of cross-functional teams. The third pillar, technology, is the glue that brings these teams together. EMA research shows that 71% of companies are either somewhat or very satisfied with their current cross-functional production and collaboration toolsets. However, in today’s complex multi-cloud hybrid environment, technology teams need to evaluate their current tools at an even more rapid frequency, with 17% of respondents reviewing their toolset on a continuous basis with no set timeframe and 21% of respondents reviewing their toolset every six months to a year.

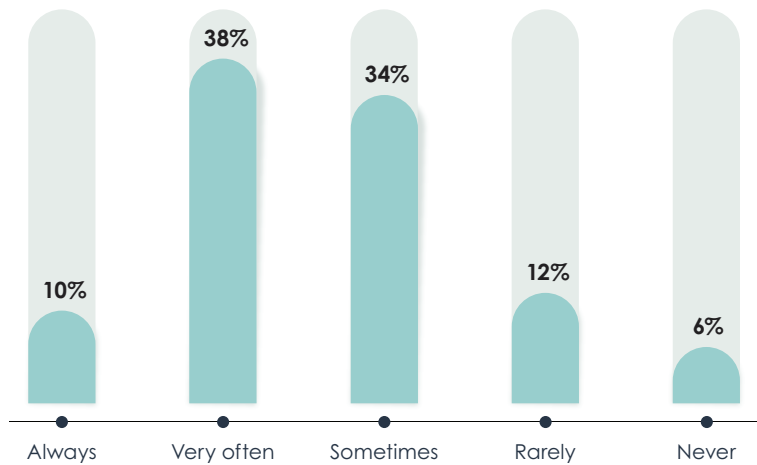


The developers and engineers faced with the complexity of a multi-cloud hybrid environment and increasing demands to meet business outcomes and customer expectations typically perform this frequent review of tools and products. Often, this group will explore open-source tools to stay ahead of constant change. However, these teams remain security-focused, with 74% of those surveyed indicating they are fairly concerned to very concerned about active vulnerabilities in their open-source services. Eighty-two percent reach out for support when it comes to active vulnerabilities.

How concerned are you about active vulnerabilities in your open-source services?



Do you rely on commercial support for your open-source services to prevent and respond to active vulnerabilities?





Trends in Cross-Functional Teams

The concept of cross-functional teams has been around for a while. According to the data, 73% of companies are currently using DevOps teams in their application development environments. We continue to see a growing trend to build on this success with adding functions more to the

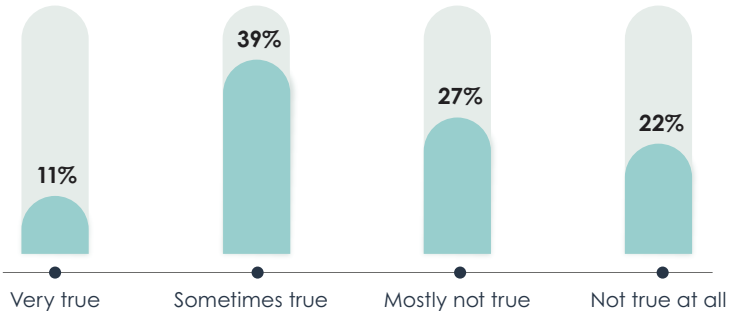
“left” of the application development ecosystem. One of the more interesting findings of this research showed that only 38% of respondents indicated that their organizations have DevSecOps integrated. Additionally, 50% of those surveyed indicated that security is usually an afterthought

in the application delivery ecosystem. However, there is hope, since two areas that will see the greatest growth over the next 12 to 24 months are in DevSecOps and DataOps.

Listed are common cross-functional teams. Which cross-functional teams are you currently seeing, do you plan to implement in the next 12-24 months, or do you have no future plans to implement?

	DevOps	DevSecOps	NetSecOps	SecOps	GitOps	NetOps	BizDevOps	NoOps	DataOps
Currently seeing	73%	38%	21%	30%	19%	31%	24%	15%	43%
Future planning (12-24 months)	15%	35%	37%	31%	37%	35%	30%	32%	32%
No future plans	12%	27%	42%	39%	44%	33%	46%	53%	25%

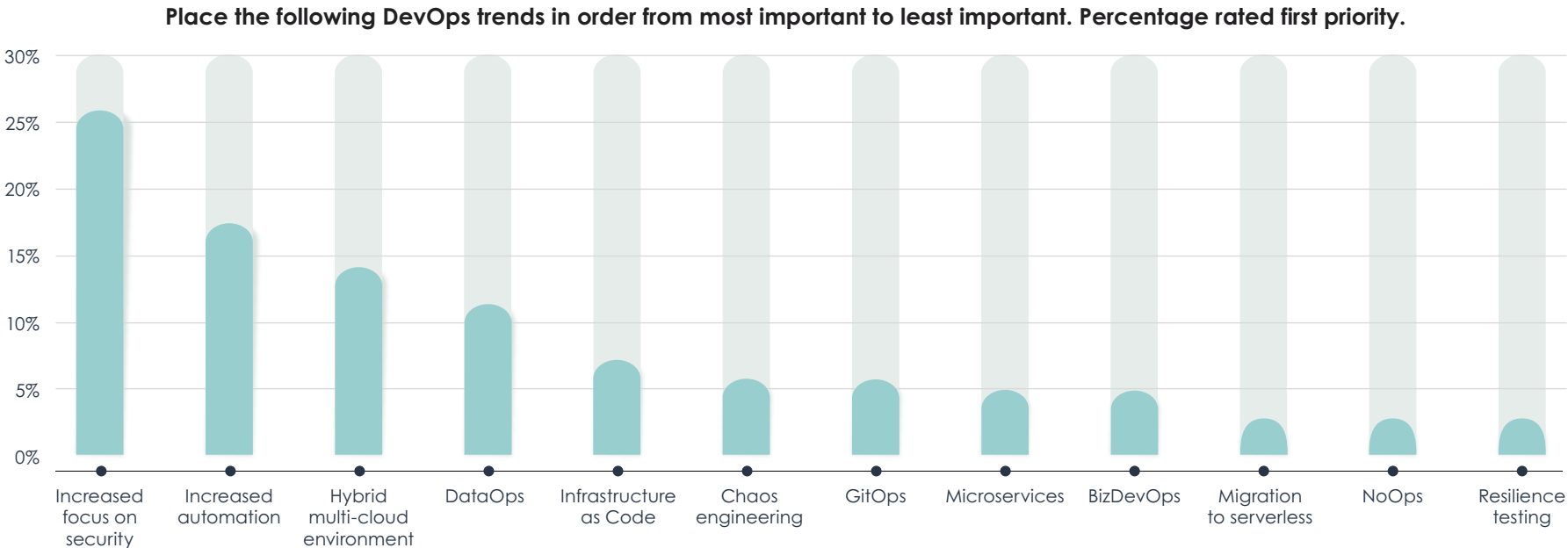
How true is this statement within your organization:
Security is usually an afterthought in our application delivery ecosystem.



Two areas frequently on every CIO’s mind are security and how to achieve business outcomes with limited resources in a growing, complex environment. When integrating cross-functional

teams into the organization’s application development ecosystem, security and automation are paramount to meet today’s challenges. This is collaborated with EMA’s research, when

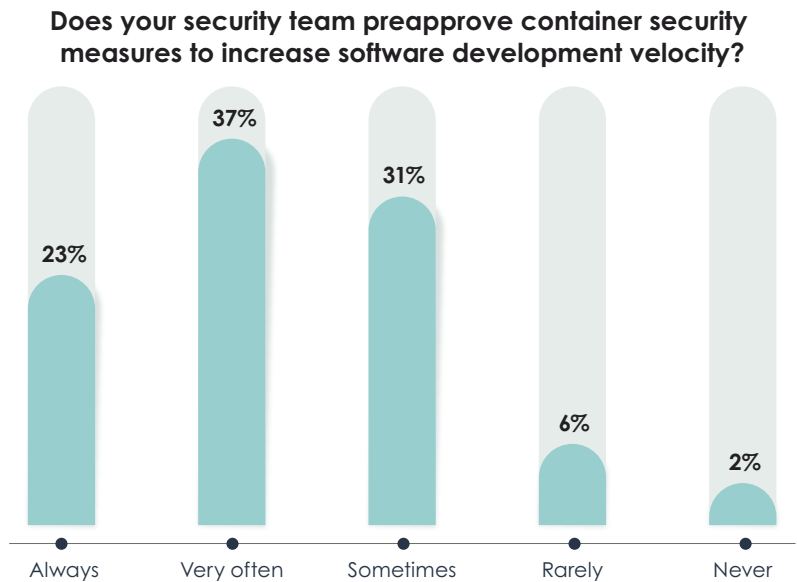
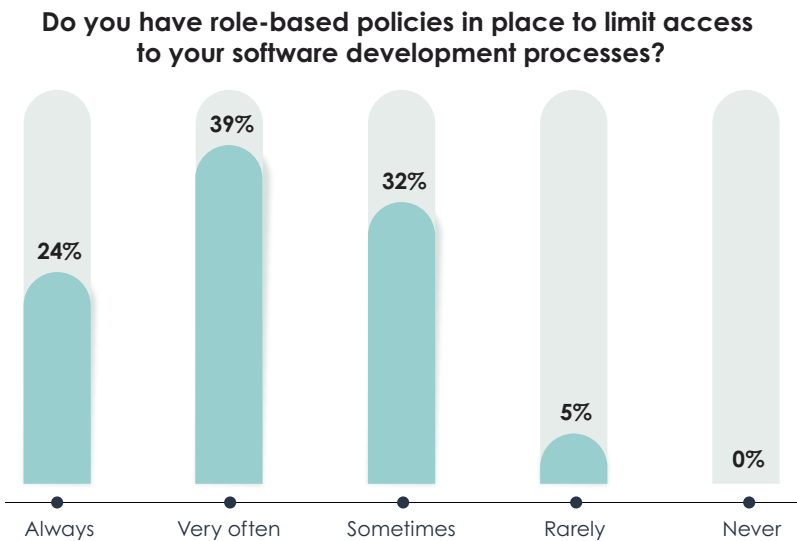
participants were asked to indicate their top priority of DevOps trends. The top two priorities were a focus on increased security and increased automation.



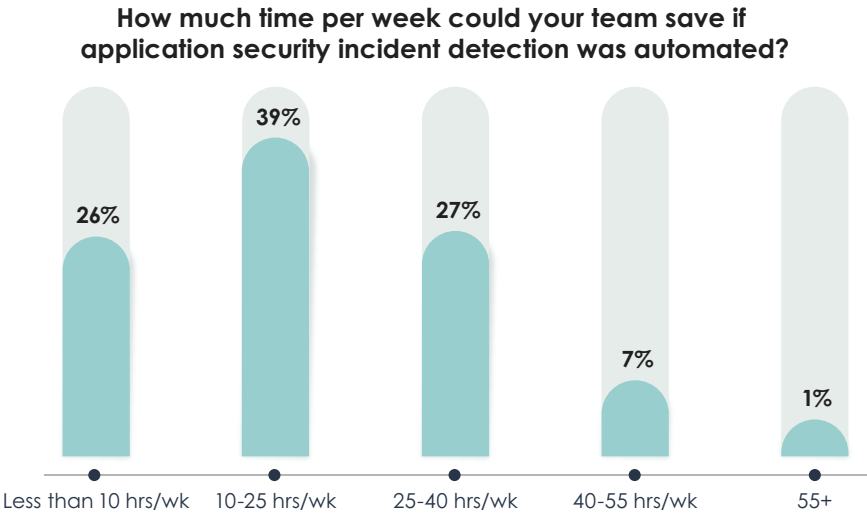


The Dependence on Security and Automation

Security has taken an increased role and is now a critical piece in every aspect of the build and development process. EMA research asked respondents if their organization has role-based policies in place to limit access during the software development process. Sixty-three percent stated that this occurs always or very often. Similarly, 60% of respondents indicated that security teams always or very often approve container security measures.

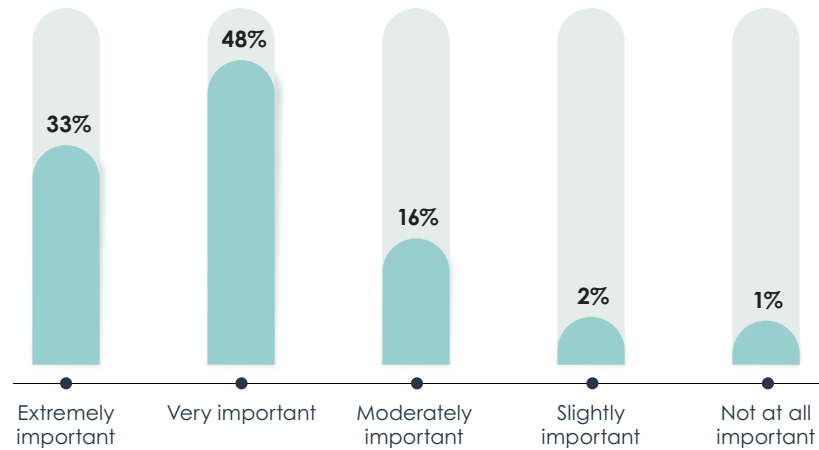


Technology teams are historically resource-constrained, and automation can often be critical to the success of a cross-functional team environment. For example, when asked how much time could be saved if application security incident detection was automated, 39% of respondents felt anywhere between 10-25 hours a week, and 27% believed that could be as much as 25-40 hours a week saved in valuable resource time.

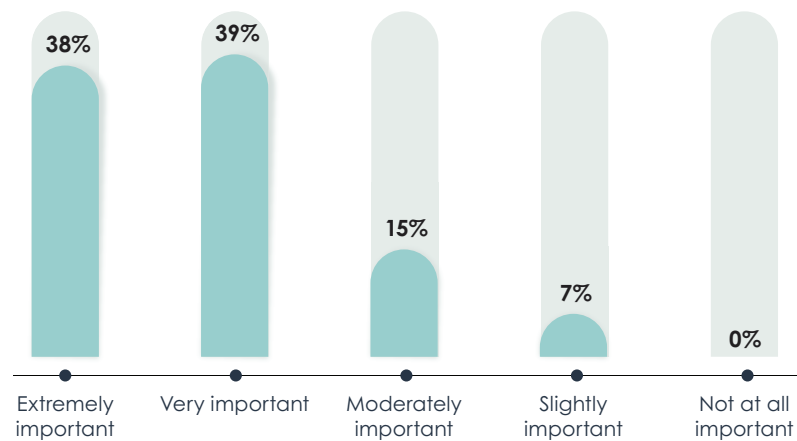


Not only are security and automation key components to the successful development of cross-functional teams, but also to the overall success of the business growth strategy. Eighty-one percent of companies indicated it is either very important or extremely important to have the ability to detect and block exploits automatically at runtime. Additionally, and not surprisingly, 77% believe that it is either very important or extremely important to have the business insights to accurately prioritize security incidents.

How important is it to your company's growth strategy to have the ability to detect and block exploits automatically at runtime?



How important is it to have the business insights to accurately prioritize security incidents?





Conclusion

The success of cross-functional teams with the introduction of DevOps into application development environments has been realized for some time. This collaboration led to the breakdown of silos and drives collaboration, speeding up production time and creating a seamless delivery process. The implementation of agile practices across organizations can help to mature software development processes and further break down organizational silos that stifle innovation. The increasing complexity of a hybrid, multi-cloud environment has rapidly become the standard, creating a necessity of increased collaboration. This begs the question: what core functions additionally need to “shift left” in the application development lifecycle?

There are two key findings driving the success of cross-functional teams in today’s environment. DevOps team(s) will need to cooperate with security to make the shift to DevSecOps, which includes a culture change and adopting tools and automation. Security can no longer be an afterthought in the application delivery ecosystem. DevOps teams will need to embrace security and work collaboratively with security teams within the organization to create a DevSecOps culture. With the ongoing threats companies face today, we are seeing security interwoven in every aspect of the development and delivery process. Companies slow to adapt to these changes will be at risk of increasing vulnerabilities and will continue to see bottlenecks in the build process, impacting business outcomes and the ability to deliver on customer expectations.

EMA research shows that the second key finding is the success of any organization’s strategic initiative: they must incorporate a strong strategy to drive automation at every layer of the organization. Automation of key processes will help by eliminating the possibility of human error, allowing for faster detection of security incidents to help de-risk technology investments. If the development of cross-functional teams is to be successful, the strategy needs to tackle the high demand of these teams to deliver on customer needs, resource constraints, increased security vulnerabilities, and increasing workloads. EMA believes automation is no longer a desired feature in an organization’s operational and development tool. This has become required and expected among customers because they evaluate their tools frequently. For companies to remain competitive in their respective markets, we are seeing a focus on automation across nearly every business and technology function within the organization.



Case Study: Treating Security Like a Product at the U.S. Army Software Factory

Security is a constant concern for businesses large and small, public and private. Data breaches and software supply chain attacks are occurring more and more frequently. A growing gap in the cybersecurity workforce is hampering security efforts in every type of organization. With the average cost of a data breach currently at \$4.24 million, leaders have significant motivation to look for new and innovative ways to mitigate cybersecurity risk in their organizations.

The U.S. Army is no exception. Alex Barbato, Solutions Engineer at VMware Tanzu Labs, worked with Hannah Hunt, Chief of Product at the United States Army Software Factory, to build a robust, compliant, and more resilient software development process to deliver applications to production.

The talent gap

As Hunt explained in a joint talk at SpringOne 2021, “Organizations are increasingly risk-averse and also unwilling to articulate their risk tolerance.” This has resulted in significant security and compliance struggles within organizations. Small organizations may underestimate their cybersecurity risk profile, leading to security breaches, and some lack the expertise needed to harden and secure their infrastructure. Enterprise organizations also struggle with ransomware attacks and attracting security talent. These problems are acutely felt in the U.S. federal space, where cybersecurity positions may be classified as IT specialist positions and staffed with underqualified or undertrained personnel. To overcome these challenges, according to Hunt, security needs to be treated like a product.

The problem with the Risk Management Framework

The U.S. federal government utilizes a set of guidelines called the Risk Management Framework (RMF), initially created for the Department of Defense, to assess risk in a cybersecurity posture. It is a prescriptive process that integrates physical security, privacy, cybersecurity, and risk management into the software development lifecycle. The seven steps within the process allow security personnel and developers to understand the risks and impacts of

a project and sort the risks into clear sets of controls, then assess their progress against these goals. However, the problem with this approach to cybersecurity is that adherence to these measurements leads to numerous spreadsheets and lengthy compliance documentation that eventually balloons out of control. Leadership starts to lean more and more heavily on the goals presented in the RMF. As a result, documentation becomes the central fixture of security rather than actual practice and implementation in secure software builds.

Using control insights to deliver software securely

Controllable input metrics are purposely chosen measurements based on leading indicators that result in the desired output metrics. Barbato believes that the controllable input for security is control insights. For software delivery organizations, control insights are responses to identified potential threat vectors in the software delivery system. These responses can be derived from any number of relevant frameworks or controls, like NIST 800-53, OWASP, or CIS benchmarks. Every organization needs to determine which control set works best for them and, most importantly, use feedback to adapt the framework and make it viable. Moreover, defining the controllable inputs is a way cybersecurity personnel can help contribute to desired business outcomes while maintaining a cybersecurity posture in application development.

Defining control insights is only the first step. Organizations also need to have measures for success based on business and security concerns. These measures can be established in many ways, including simulating business load, penetration tests, or running mock security breaches. Hunt and Barbato used roadmaps with objectives and key results (OKRs) to measure the success of their secure software delivery program. Another vital step in their process was implementing automation. They reduced toil by automating tests and scans, which helped maintain security and consistency in the software development cycle. Once established, they gathered feedback from stakeholders and used that to iterate on the process. Defining and using control insights with measures for success, automation of tasks, and integrating feedback loops allowed the organization to move toward more security-focused outcomes instead of focusing on complicated spreadsheets of risk management indicators.

Bridging compliance and development needs

Hunt and Barbato utilized a “team of teams” model, wherein the cybersecurity team worked together with the platform and user-facing application teams to get applications into production. Using this model, as an organization expands, they may add roles and teams to this larger team, like penetration testers and security assessment groups. However, in the U.S. Army Software Factory, the demand for a particular role arose due to a need to bridge the gap between application teams and compliance and security controls. To meet the need, they developed a position called the application security validation engineer (ASVE).

The ASVE is a code-first role with a focus on soft skills. This individual requires a high level of empathy to work between security, application development, and platform engineering teams. Often, miscommunication and misunderstanding occur between these teams due to competing goals, poor implementation practices, and misaligned incentives. The ASVE helps align teams and keep them moving toward a common goal while removing blocks and enabling collaboration and communication.

When input controls, measurements, and defined goals are integrated into application development, security becomes part of the overall process and the final product instead of an afterthought or roadblock. Treating security like a product garners buy-in from the application team to focus on security outcomes during app development. It makes security more tangible and usable. Hunt and Barbato leveraged their team of ASVEs along with OKRs and roadmaps to implement and scale secure application development. With balanced teams working toward the same goals, they’ve been able to deliver multiple applications, like MySquad, to production and prove that security doesn’t need to be a hurdle for organizations to stumble over.





About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com. You can also follow EMA on [Twitter](#) or [LinkedIn](#).

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2022 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.