Contrast SECURITY

The State Of DevSecOps Report

Cross-industry and Cross-persona Survey Finds That Application Security Creates Friction and Delivers Suboptimal Results

Table of contents

01 | Executive Summary

This report is based on a survey of development, operations, and security professionals—including C-level executives who lead them—across a wide range of industries. It explores development practices and the state of application security at organizations of all sizes. Survey results indicate that despite great strides in accelerating the application development process, security processes continue to create roadblocks:

- Application security testing scans take at least five hours for nearly two-thirds of organizations—with over one-third indicating eight or more hours.
- • Once the scan report is generated, it takes the application security team an average of one hour to triage and diagnose each alert. For those that are true vulnerabilities, over half of developers spend more than four hours locating the cause of the vulnerability and fixing it. After that, developers spend six hours per week verifying remediations.
- For applications in production, each alert consumes more than three hours of work for the security operations (SecOps) team, and each vulnerability requires 10 hours of unscheduled developer time for emergency remediation.

Despite these significant disruptions in the name of security, application security outcomes at the vast majority of organizations leave much to be desired:

- 79% admit their average application in development has an average of 20 or more vulnerabilities
- More than 99% say that applications in production average at least four vulnerabilities
- Only 5% of organizations avoided successful application attacks in the past year, and 61% experienced more than three
- More than two-thirds of organizations suffered an attack that resulted in the loss of critical data or operational disruption

As the demands on developers intensify and attackers increasingly target applications, organizations desperately need true observability into vulnerabilities and attacks. This necessitates a move beyond legacy application security tools toward an integrated application security architecture featuring instrumentation. This enables continuous monitoring and vulnerability scanning from within the application and results in continuous observability across the software development life cycle (SDLC)—virtually eliminating security-related coding delays while providing more complete protection against vulnerabilities and attacks.

Key Findings

57% of organizations have increased DevOps budgets due to COVID-19—35% by more than 10%

79% say the DevOps team is under increasing pressure to shorten release cycles

79% say the average application in development has 20+ vulnerabilities

99+% say the average application in production has 4+ vulnerabilities

91% say vulnerability scans take 3+ HOURS; 35% say 8+ hours

73% say each security alert consumes 1+ HOURS of application security time

71% say each vulnerability identified consumes 4+ HOURS of developer time

55% of organizations sometimes skip security scans to meet deadlines

61% of organizations experienced 3+ successful exploitative attacks; only 5% experienced zero

72% lost critical data; 67% experienced operational disruption; 62% saw brand degradation

Contrast SECURITY

02 | Introduction

As Microsoft CEO Satya Nadella asserted in 2019, "Every company is now a software company."[1] Digital tools and processes have permeated sales, manufacturing operations, supply chain management, and customer service at virtually every organization—part of a larger phenomenon that is sometimes called digital transformation. This trend was well underway even before the COVID-19 pandemic transformed global business overnight in early 2020. Since then, the process has only accelerated.[2]

Sizable companies in virtually every industry—and more than a few small and midsize businesses—now have their own in-house applications. This software is built by both in-house and outsourced development teams, and those teams have a tangible impact on the bottom line. Methodologies like Agile and DevOps and a growing use of open-source code[3] have accelerated the development process, enabling companies to deliver digital transformation at scale.

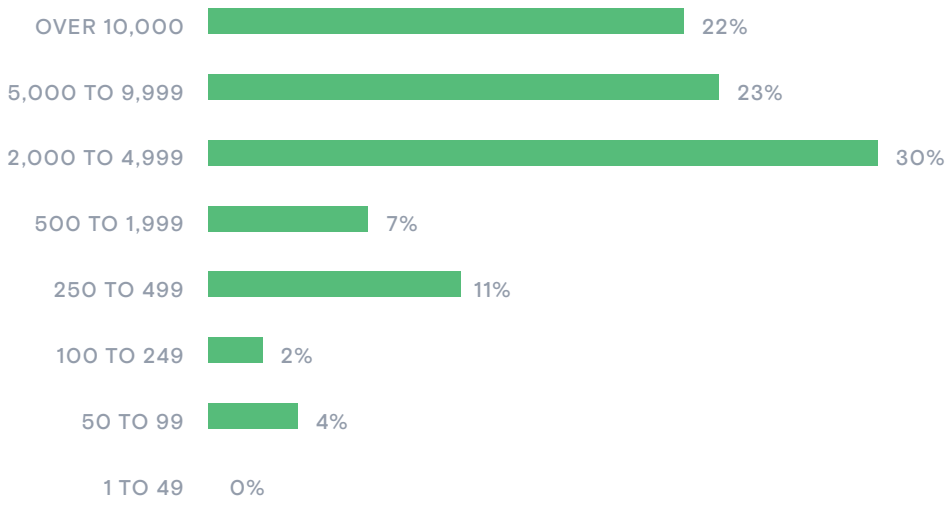
Unfortunately, the breakneck speed at which applications are now developed can present security risks to organizations. Legacy application security tools and processes were designed for slower, more methodical approaches to software development and struggle to adapt to today's pace. At the same time, software is a more compelling target for cyber criminals than ever before. The most recent Data Breach Investigations Report from Verizon found that 43% of data breaches this past year were the result of a web application vulnerability—a figure that more than doubled over the previous year.[4]

METHODOLOGY FOR THIS STUDY

This report is based on a comprehensive survey of practitioners and business leaders who touch the application development and security functions in various ways. Conducted in September 2020, the survey sought to gauge the importance of software development, as well as the state of application security, in a variety of industries. The results of each question were analyzed for the whole cohort, and some answers were also grouped by background data like company size and job title. From this analysis, we identified several insights about application development across multiple industries.

FIGURE 1

What is the size of your company?

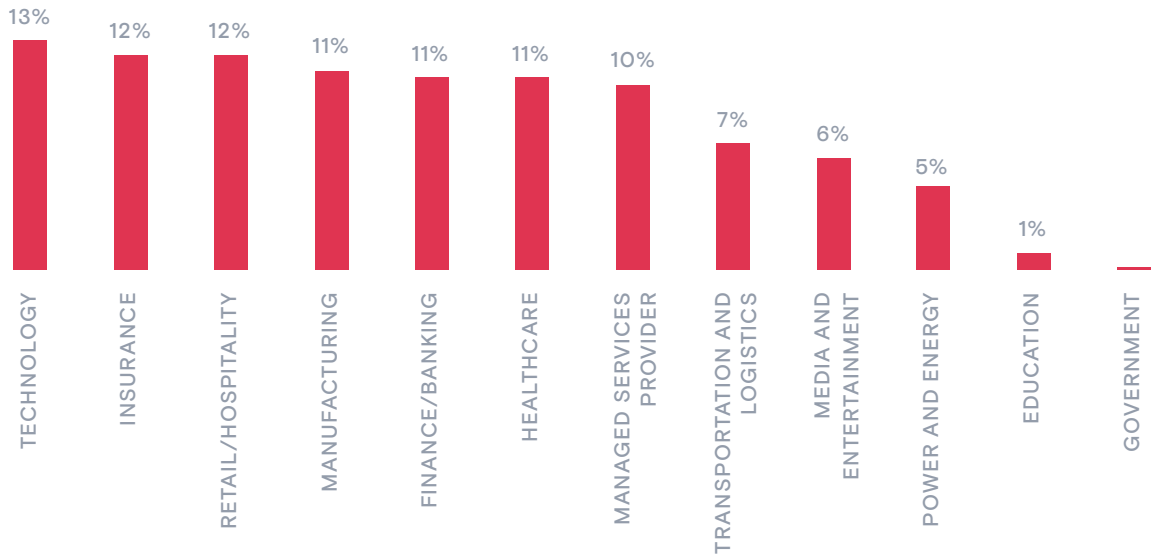


A DIVERSE POOL OF RESPONDENTS

Respondents come from organizations of varying sizes and in a variety of industries. Three-quarters work at companies with 2,000 or more employees (Figure 1)—often referred to as enterprises—while one-quarter are from smaller organizations. Respondents were part of a diverse array of industries, including technology, financial industries, retail/hospitality, manufacturing, and healthcare (Figure 2).

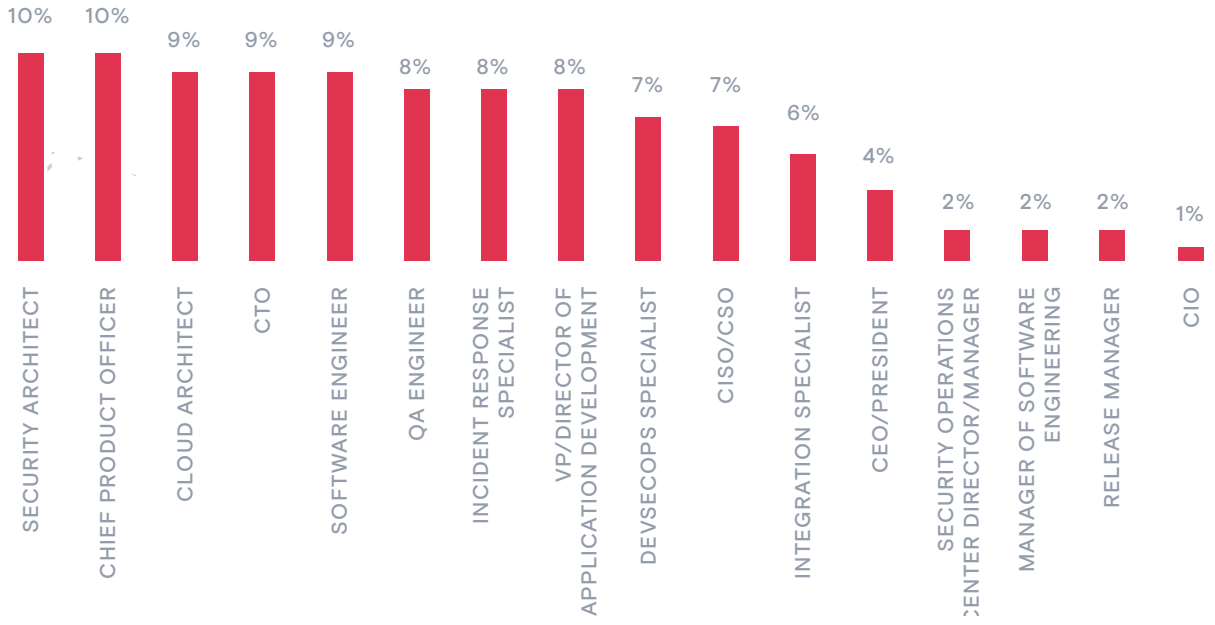
FIGURE 2

What best describes your industry?



Respondents come from organizations of varying sizes and in a variety of industries. Three-quarters work at companies with 2,000 or more employees (Figure 1)—often referred to as enterprises—while one-quarter are from smaller organizations. Respondents were part of a diverse array of industries, including technology, financial industries, retail/hospitality, manufacturing, and healthcare (Figure 2).

What is your job title?



03 | Insights from Development and Security Professionals

ANALYSIS OF THE SURVEY RESULTS REVEALS FIVE INSIGHTS FROM THE PERSPECTIVE OF BOTH CORPORATE LEADERS AND FRONT-LINE WORKERS INVOLVED IN SOFTWARE DEVELOPMENT AND APPLICATION SECURITY:

INSIGHT: DEVOPS IS GROWING IN IMPORTANCE, AND THIS PUTS PRESSURE ON DEVELOPERS

As the digital economy grows, speedy application development has become increasingly critical to companies in all industries. This trend has accelerated as a result of the changes in business priorities due to COVID-19.5 A solid majority of respondents (57%) report that their organizations have increased budgets for DevOps activities as a result of the pandemic (Figure 4), and 35% said that budget increase is more than 10% (Figure 5).

FIGURE 4

Will your organization place more emphasis and budget on devops As a result of the business changes of covid–19?

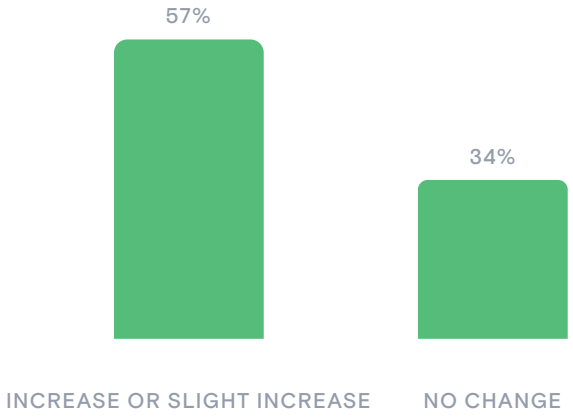
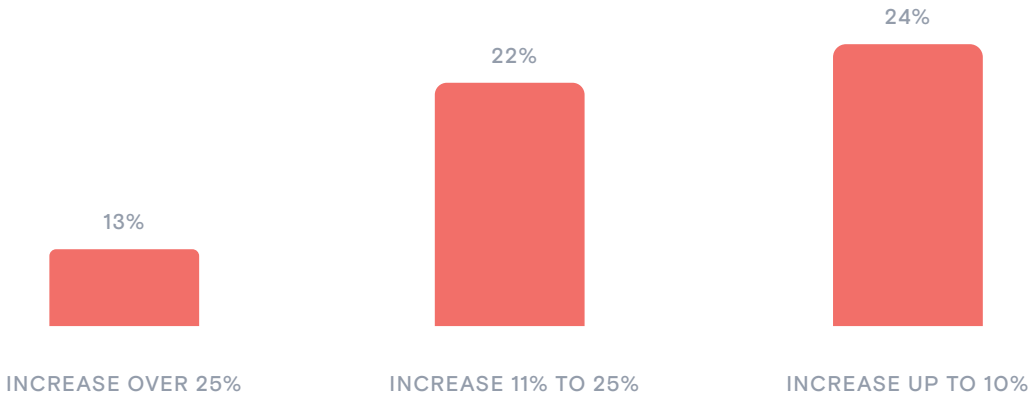


FIGURE 5

How much do you anticipate your devops budget to Increase as a result of covid–19?



Contrast SECURITY

GROWING DEPTH IN DEVOPS OPERATIONS

Survey results indicate that most organizations have relatively mature DevOps programs—not surprising given that DevOps has been in the mainstream for several years. More than three-quarters (78%) of respondents say that the methodology is in use for at least half of applications (Figure 6), and 88% report utilizing more than 500 application programming interfaces (APIs) (Figure 7). And 80% of teams deploy code to production at least multiple times per week (Figure 8).

FIGURE 6

What is your level of open-source library and framework adoption?

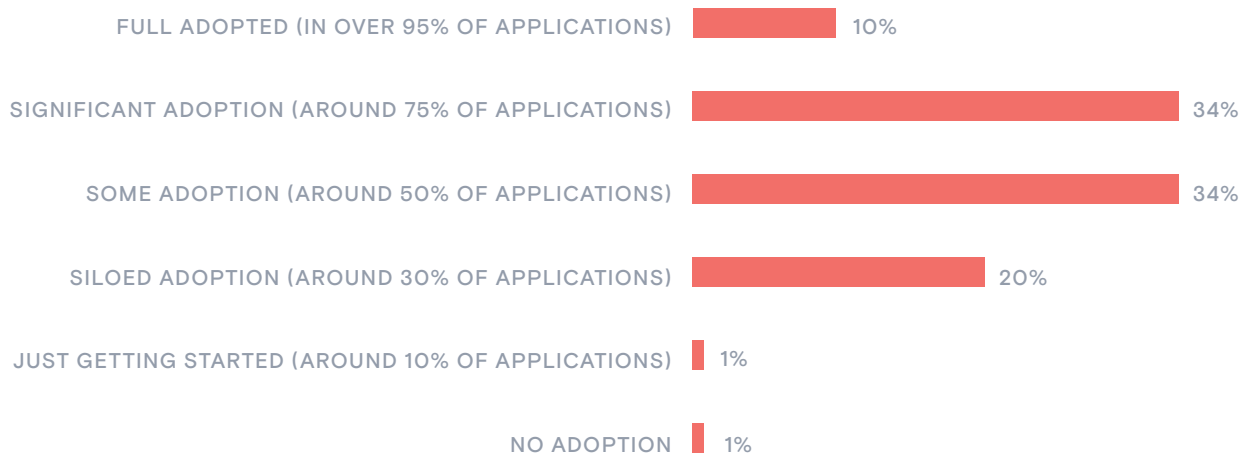


FIGURE 7

Approximately how many apis are used across all of your applications?

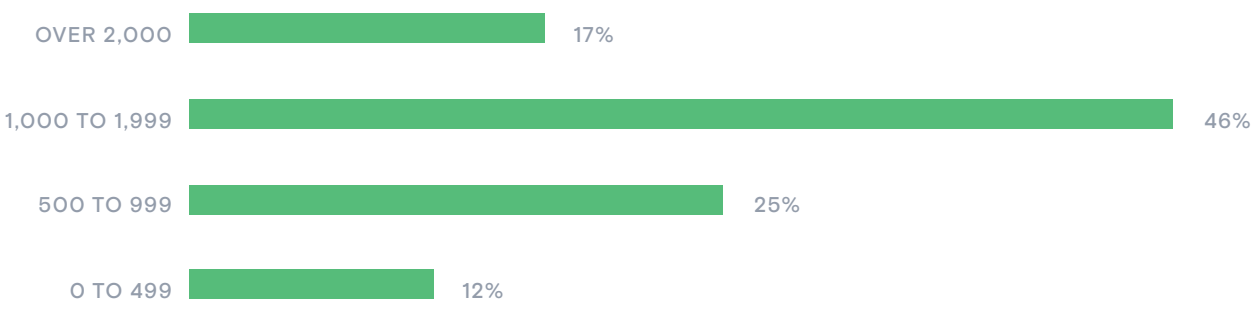
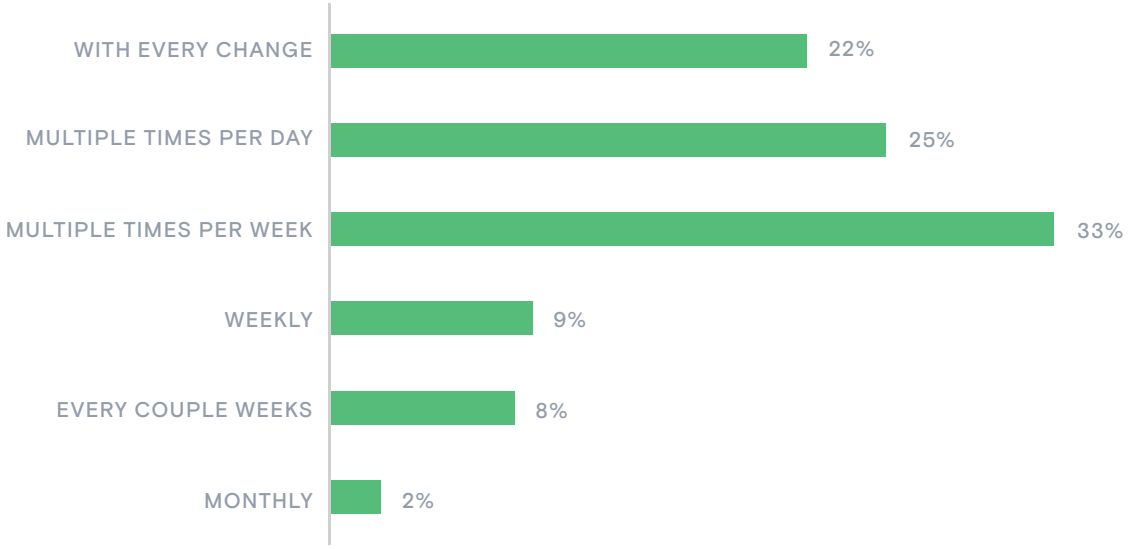


FIGURE 8

On average, how often do you deploy to production?

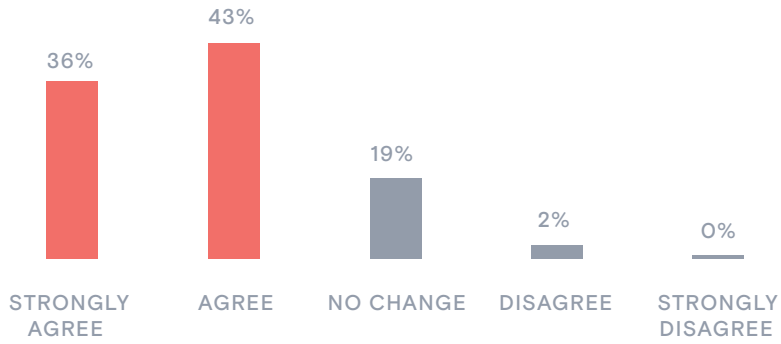


INCREASED SPEED REQUIREMENTS ON DEVELOPERS

From the perspective of developers, the great strides they have made in speed and efficiency in recent years is simply not enough for their management. Nearly 8 in 10 respondents (79%) say their DevOps team is under increased pressure to shorten release cycles and commit more code (Figure 9)—including more than 90% of CEOs, CIOs, CTOs, release managers, and security operations (SecOps) managers.

FIGURE 9

Is your devops team under increased pressure to Shorten release cycles and commit more code?



42% Of companies that suffered a breach attributed the cause to a known but unpatched vulnerability.

Source: “the state of vulnerability management in the cloud and on-premises,” ponemon institute and ibm, august 2020.

MORE LEADERSHIP FOCUS ON APPLICATION SECURITY

Cybersecurity is increasingly a priority for leaders such as boards of directors and the C-suite, and application security is an increasingly important part of that mix. Research by Verizon found that 43% of data breaches in the past year were the result of a web application vulnerability—a figure that more than doubled over the previous year.6 And recent research by Contrast Labs found more than 13,000 attacks per application per month.7 As a result, it is not surprising that a solid majority (56%) of respondents report that application security is discussed at each quarterly board meeting (Figure 10), and application security is a C-suite performance measurement at 72% of organizations (Figure 11).

FIGURE 10

Is application security risk a topic at board of director meetings?

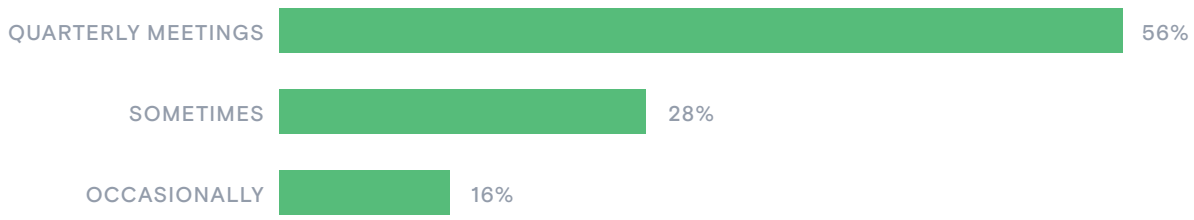
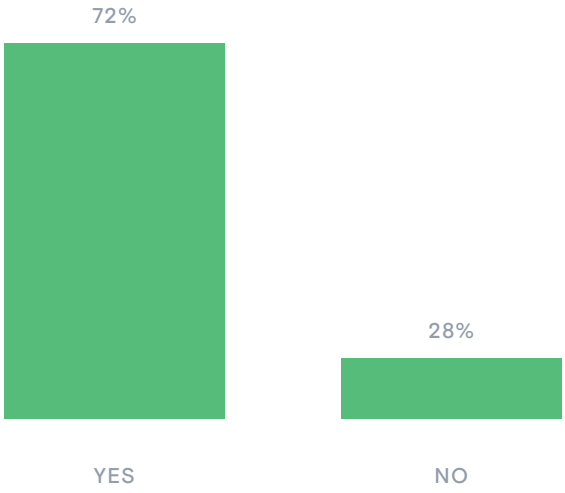


FIGURE 11

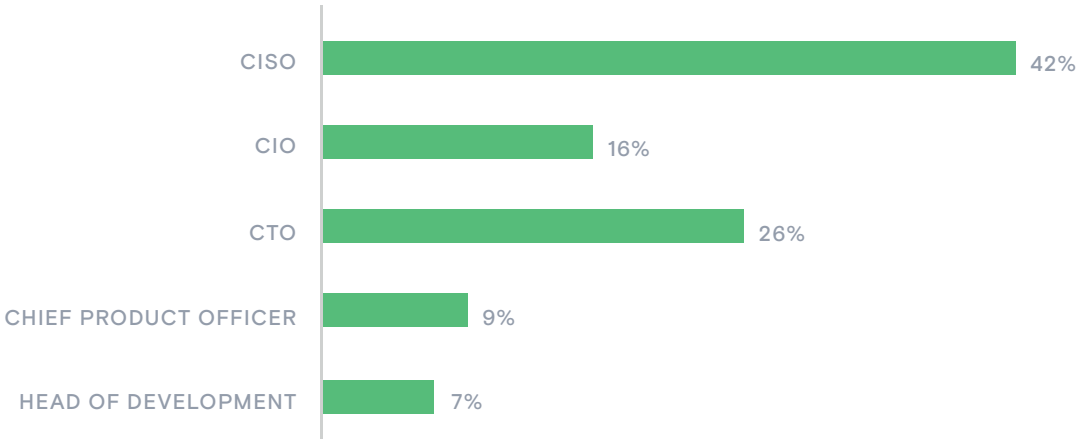
Is application security risk a c-suite measurement?



Given the importance of application security to executive management, it makes sense that 84% of organizations leave the final decision for DevSecOps investment to someone in the C-suite. Close to half (42%) leave that decision to the CISO (Figure 12).

FIGURE 12

Who is responsible for final devsecops decisions in your organization?

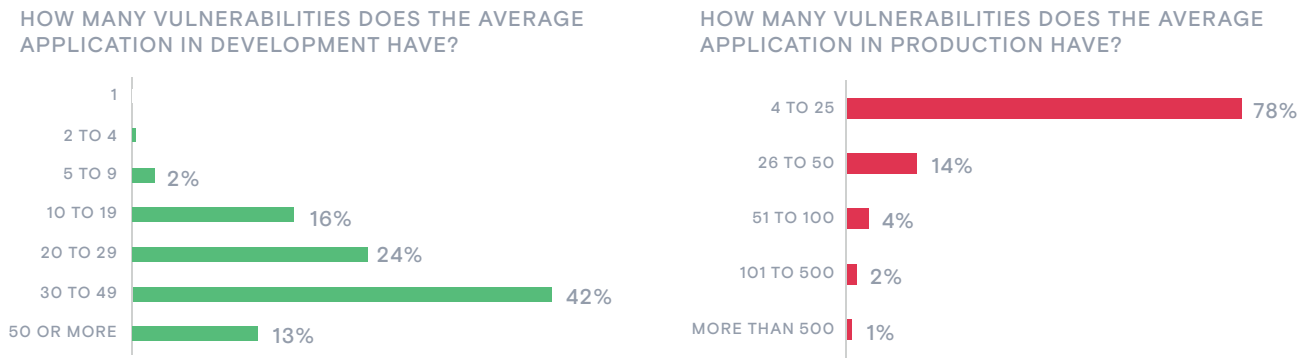


> "Ideally, our developers work at a high speed, and the security team investigates and analyzes vulnerabilities as they occur. But when we have a rush of work, this is not actually happening."
>
> – Survey Respondent, Cloud Architect, Technology Industry

INSIGHT: APPLICATIONS HAVE MANY VULNERABILITIES, AND MOST ORGANIZATIONS USE DEDICATED HEADCOUNT TO ADDRESS THEM

Vulnerabilities continue to be an issue with applications in development. Nearly 8 in 10 respondents (79%) say that the average application has 20 or more vulnerabilities (Figure 13). And the problem does not end when applications are deployed into production. More than 99% of respondents say the average application in production has at least four vulnerabilities.

FIGURE 13



When asked to rank a list of vulnerability types by the risk they pose to their organizations, types most cited in the top four were SQL injection, cross-site scripting (XSS), and broken authentication (Figure 14).

But interestingly, command injection was the second most common choice as the highest-risk vulnerability type. While this attack type is rare, the consequences of such an attack would be devastating, as an adversary could accomplish a complete remote takeover of a host.

This prioritization of vulnerability types differs somewhat from rankings by the Open Web Application Security Project (OWASP). SQL injection and command injection both belong to the number one item on the OWASP Top 10—injection vulnerabilities (Figure 15). XSS is ranked seventh by OWASP, and broken authentication is ranked second. The latest Contrast RiskScoreTM ranks XSS and SQL injection with the second- and third-highest scores, while broken authentication is number 15 in terms of rank.

FIGURE 14

What vulnerabilities pose the biggest risk to your organization (rank top 4)?

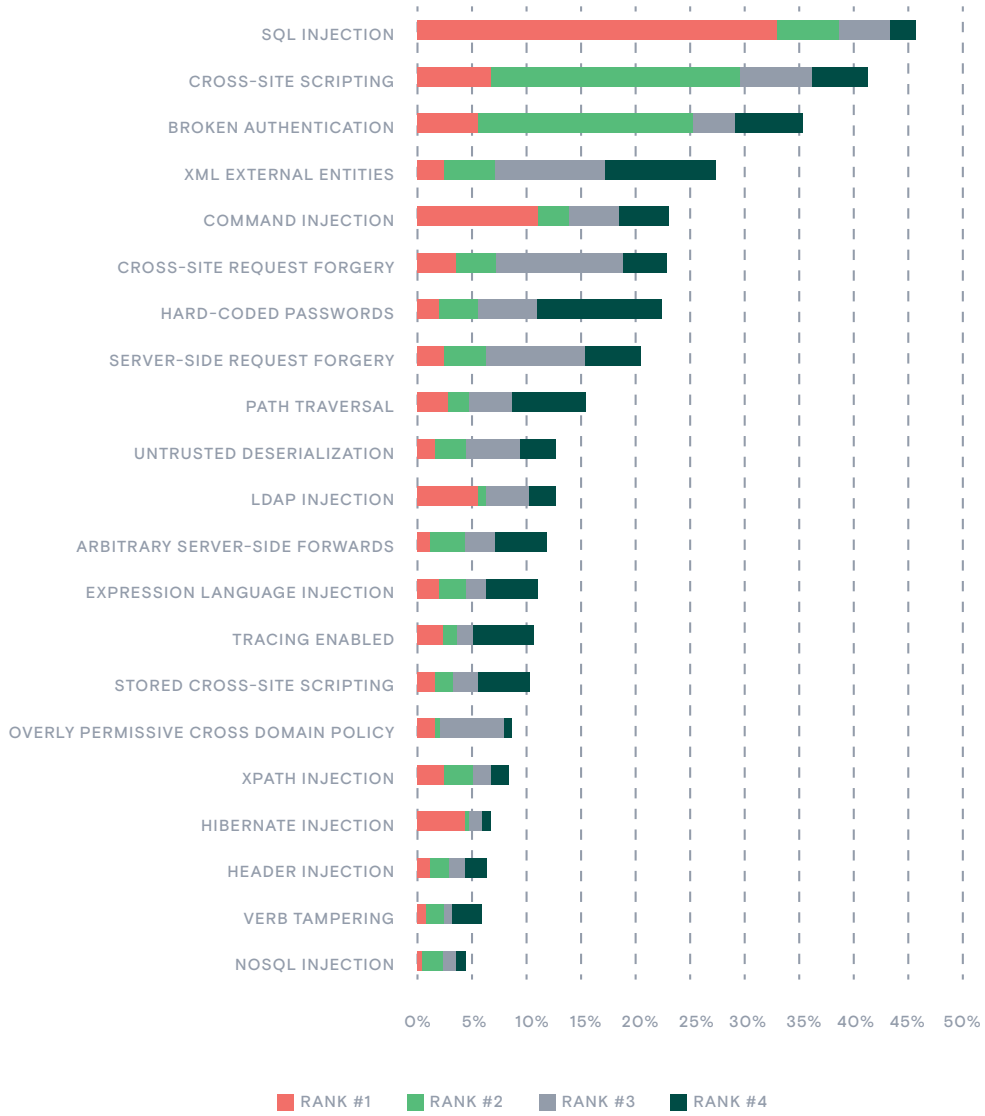
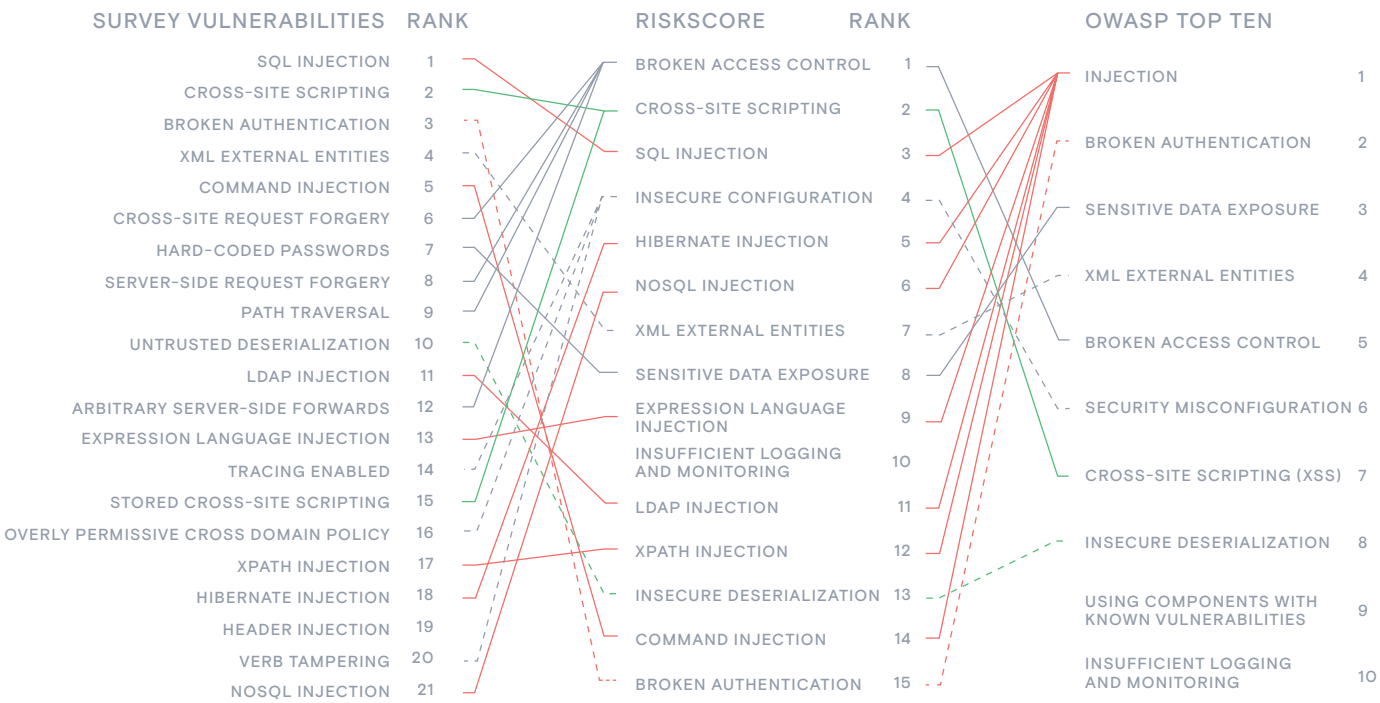


FIGURE 15



SECURITY STAFFING AND TOOLS

Given this prevalence of vulnerabilities in applications, it is perhaps not surprising that two-thirds (67%) of organizations have dedicated headcount for application security (Figure 16). These specialists are a part of the security team in approximately half of cases, and on the development team in the other half. Looking at this data by industry, it becomes clear that the answers to this question are not uniform. Insurance companies (90%), managed services providers (81%), and power and energy (75%) are more likely to have dedicated headcount than the group as a whole. On the other hand, finance and banking (56%), healthcare (56%), and manufacturing (57%) are less likely. And in organizations that have dedicated headcount, they are more likely to be on the security team at managed services providers (58%) and transportation and logistics companies (50%). This headcount is more likely to reside on the DevOps team in insurance (70%), media and entertainment (50%), and technology companies (41%) (Figure 17).

Another Contrast Labs survey8 that focused on the technology industry found that a similar percentage of firms had dedicated application security headcount, but almost all who had such headcount housed it on the security team. Here, including application security as a responsibility of the CISO and her or his team seems to be a trend with leading-edge companies.

FIGURE 16

Do you have a dedicated headcount responsible for application security?

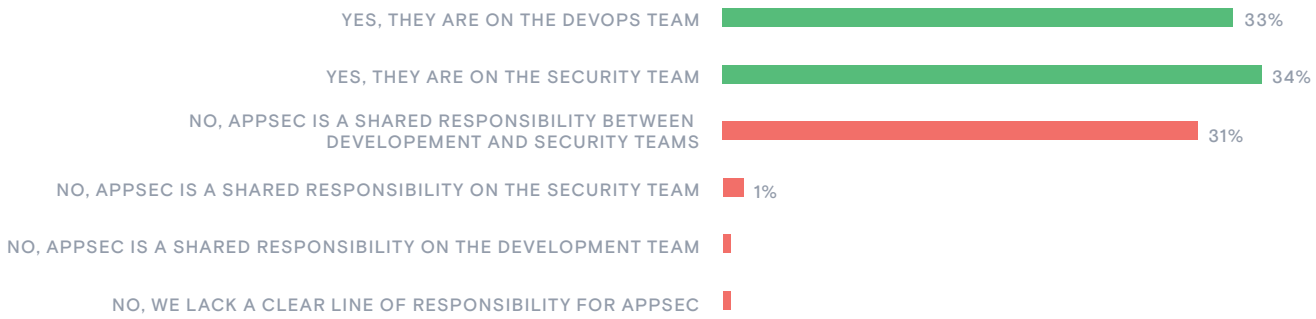
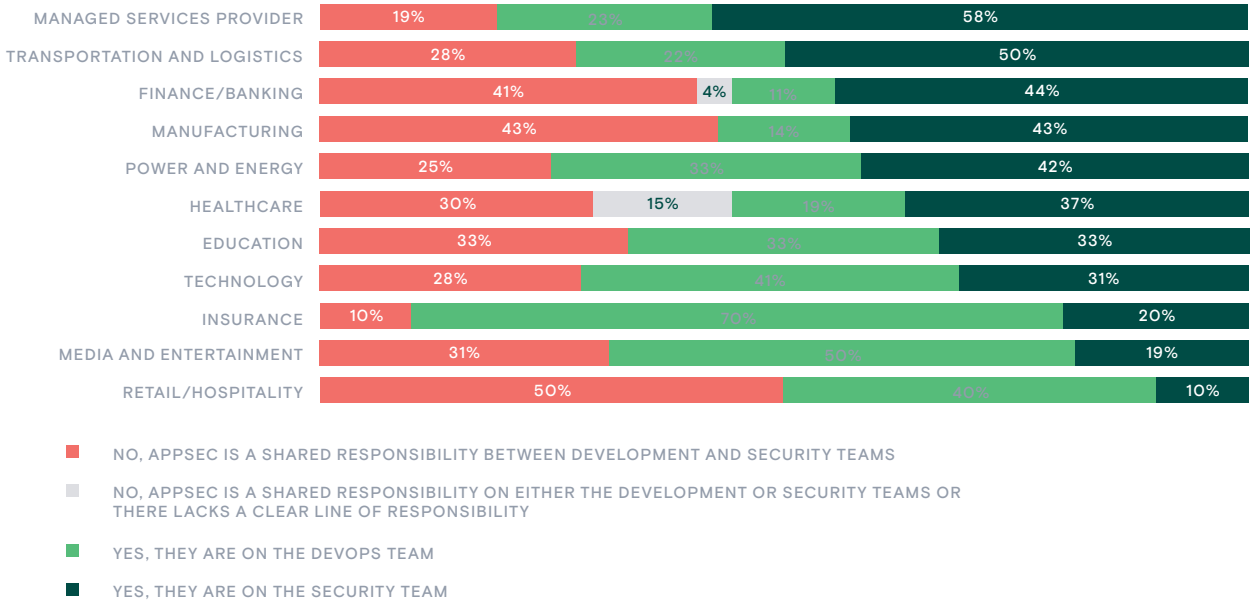


FIGURE 17

Do you have a dedicated headcount responsible for application security?



COLLABORATION BETWEEN DEVELOPMENT AND SECURITY TEAMS

Ideally, an organization's development and security teams should be in frequent contact and work together to ensure that applications are delivered into production without vulnerabilities. This is true regardless of which team delivers front-line application security. In a freeform question, survey respondents were asked to describe the relationship between the security and development teams at their organizations (Figure 18). In an analysis of the open-text answers, 43% of respondents used terms like integrated, collaborative, and coordinated—concepts that would describe a well-functioning relationship. Unfortunately, this may mean that 57% of organizations still have work to do in this regard.

FIGURE 18

How would you describe the relationship between your Security and development teams?

"Creating a balance and synergy between the security and development teams is the easiest and most economical way to achieve software security. It contributes a great deal to the growth and development of the whole organization."

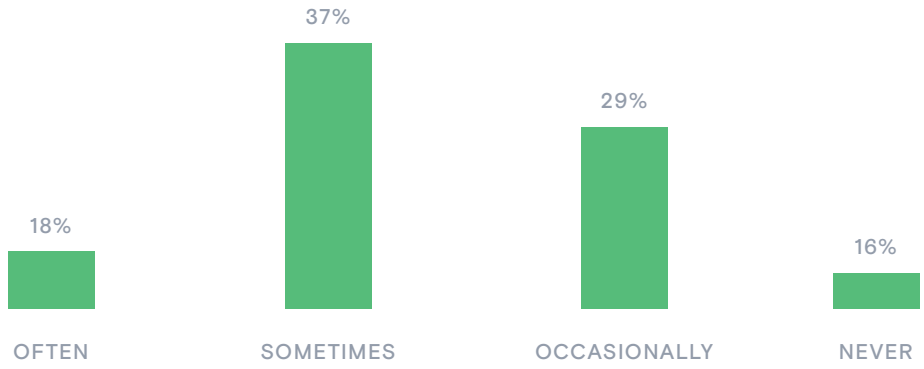
– Survey Respondent, CEO, Healthcare Industry

INSIGHT: APPLICATION SECURITY PROCESSES CONTINUE TO SIGNIFICANTLY SLOW DEVELOPMENT CYCLES

When asked detailed questions about application security processes, respondents tell a story of repeated delays to the development process—which can threaten the timely delivery of software for critical business objectives. In fact, 40% of respondents report that their teams sometimes or often skip security processes in order to meet deadlines. This can backfire when vulnerabilities are missed as a result, slowing delivery of the application at a later point in the process and putting the application and organization at risk if they are released into production (Figure 19).

FIGURE 19

Do your developers skip security scans to meet release cycle deadlines?



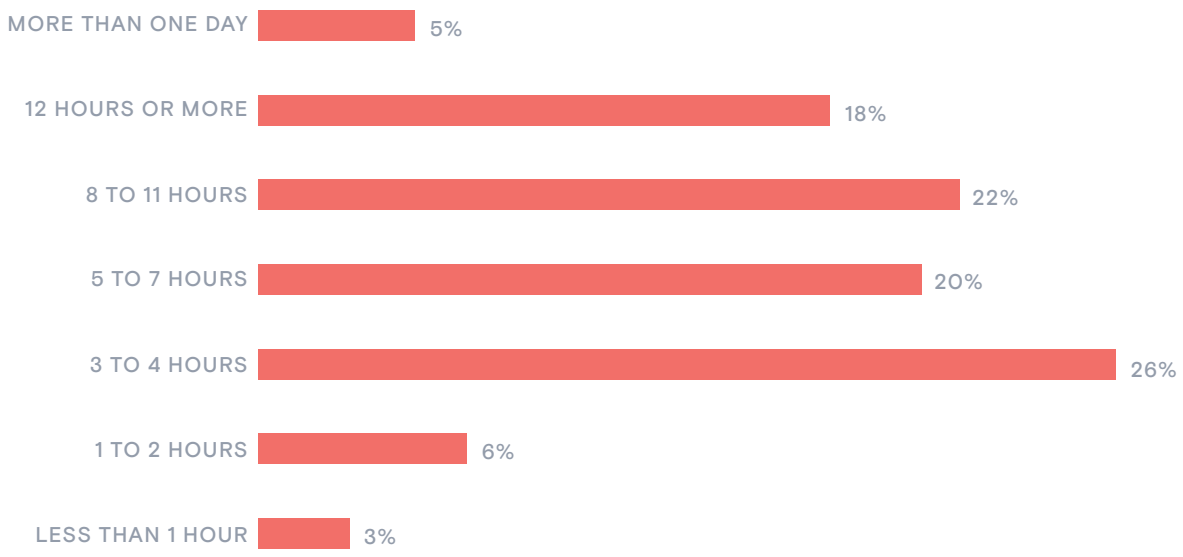
INEFFICIENCIES FOR APPLICATION SECURITY PROFESSIONALS

Vulnerability scans done by application security testing solutions cause significant delays for the security team. One big time sink is the time it takes to complete vulnerability scans. Nearly two-thirds (65%) of respondents said that these scans take at least five hours each time they are done—and 35% say that figure is eight hours or more (Figure 20). Since development often continues while scans are being run and the results are analyzed, even the first steps of remediation can be delayed until after additional layers of code have been added.

Once the scan is complete, application security professionals must pore over a long report to make note of all alerts, identify legitimate vulnerabilities, and trace their source. The majority (63%) say this process takes one hour per alert with a legacy static application security testing (SAST) tool (Figure 21). Slightly fewer respondents (61%) estimate this task takes approximately one hour with a legacy dynamic application security testing (DAST) approach.

FIGURE 20

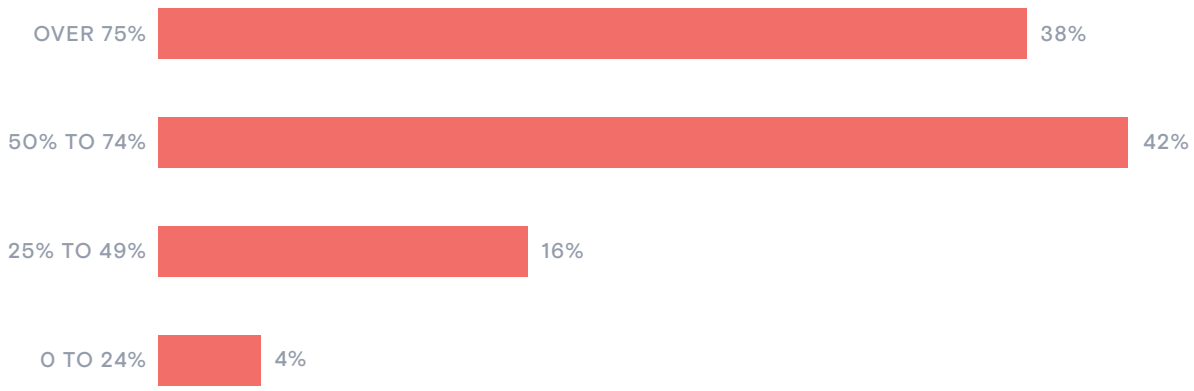
How long does it take to complete each static application security scan on average?



Of course, these figures are multiplied by the number of alerts, often in the hundreds for each scan. Many of them turn out to be false positives, for which both SAST and DAST solutions are notorious. Eight in 10 respondents report that at least half of the alerts generated by their scanning tools are false positives, and 38% put that ratio above three-quarters (Figure 21). This translates into many hours of wasted time for security team members.

FIGURE 21

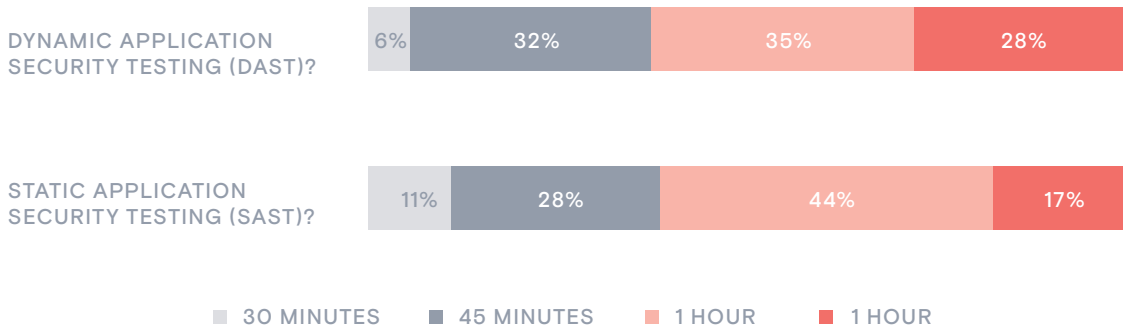
What percentage of security alerts identified by scanning tools turn out to be false positives?



Application security professionals must go through each item line by line, and more than half of respondents (61% for SAST tools and 63% for DAST tools) say that the process of triaging and diagnosing each security alert takes an hour or more (Figure 22).

FIGURE 22

How much time do security specialists spend triaging and diagnosing security alerts identified in a scan using ...



INEFFICIENCIES FOR THE DEVELOPMENT TEAM

Constantly facing pressure to deploy code quickly, developers need focused blocks of time to get their work done, but security needs tend to constantly interrupt. A solid majority of respondents (62%) say that developers stop coding to remediate vulnerabilities at least every two or three days (Figure 23)—and 27% do so daily.

How often this is done is a process choice aimed at maximizing efficiency, but if the number of vulnerabilities is large, it is easy to fall behind if remediation is less frequent. One leading SAST vendor found that organizations must do daily scans—and presumably daily remediation—in order to keep their median time to remediate close to 60 days, thus minimizing security debt.[9]

FIGURE 23

How often does your development team need to fix vulnerabilities?

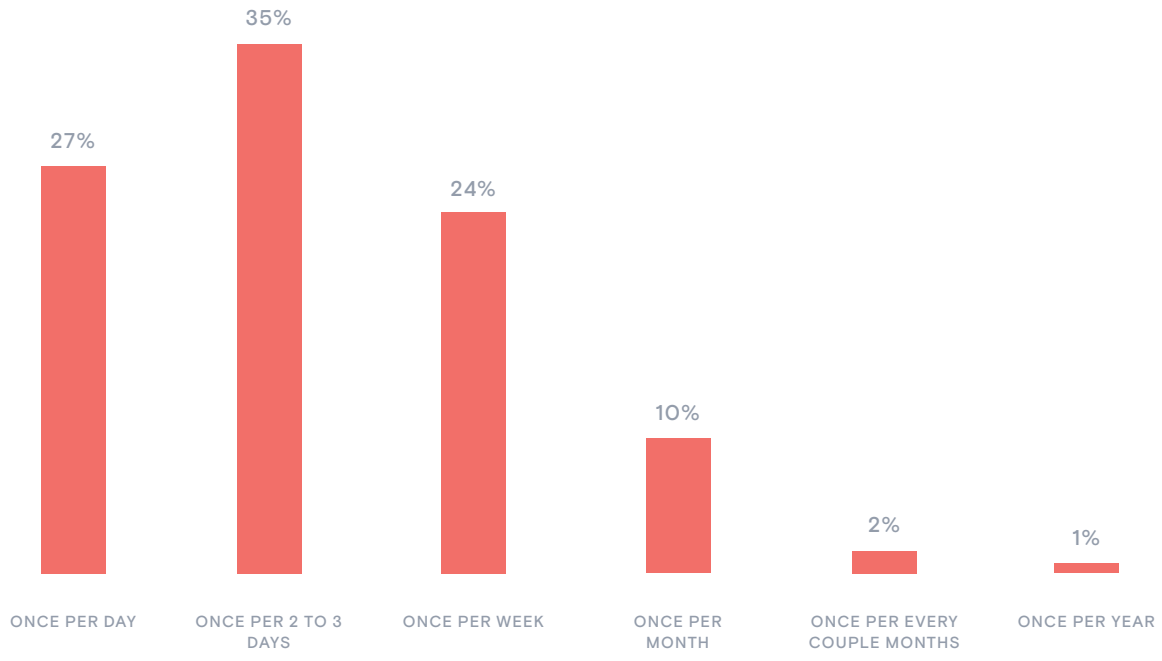
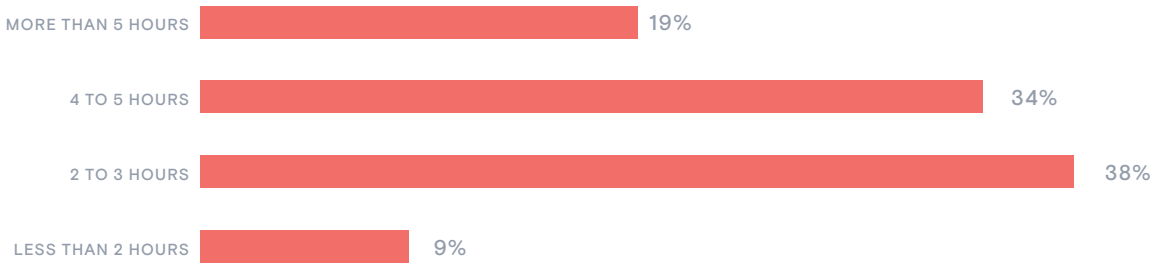


FIGURE 24

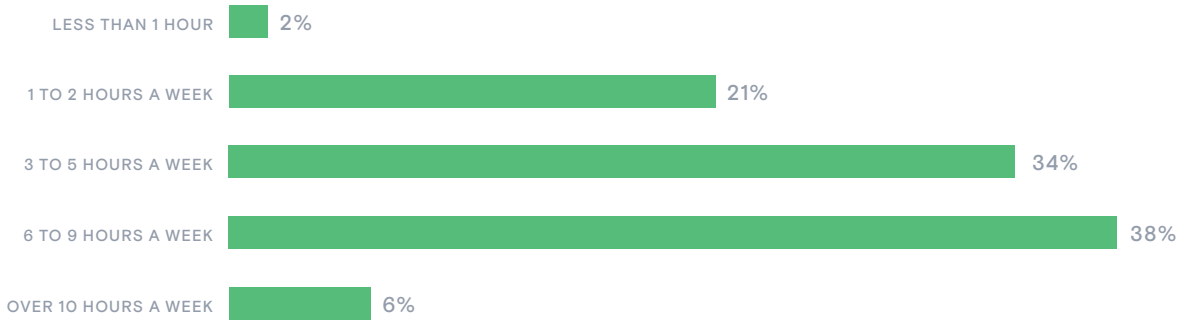
How much time on average does your development team spend Remediating each vulnerability found in development?



Once the security team completes the triage and analysis of alerts, they pass their findings back to developers for remediation. Almost all respondents (91%) report that remediation requires at least two hours of developer time for each vulnerability—and more than half (53%) put that number at four hours or more (Figure 24). The verification step itself can be complicated for organizations using legacy application security testing solutions: More than three-quarters (78%) of respondents said that individual developers spend at least three to five hours per week verifying remediations (Figure 25). Once those steps are taken, teams typically must perform another time-consuming scan to provide final verification of the fix.

FIGURE 25

How much time do security specialists spend triaging and diagnosing security alerts identified in a scan using ...



INEFFICIENCIES FOR APPLICATIONS IN PRODUCTION

The SecOps team in the security operations center (SOC) also sees significant inefficiencies from application security processes once applications are released into production. Well over half of respondents (73%) say their SecOps team spends at least three hours per security alert in triaging, correlating, risk rating, writing up, and retesting (Figure 26).

When risky vulnerabilities are found after a program is already in production, fixing those problems is both urgent and time-consuming. For developers, this creates issues because the work was not planned in advance and the result can be delays for the project on which they are currently working. Unfortunately, half of respondents reported that the average remediation in production requires at least 10 hours of work, and 71% said it takes at least five hours (Figure 27).

FIGURE 26

How much time on average does your security team spend triaging, correlating, risk rating, writing up, and retesting each vulnerability fix found in production?

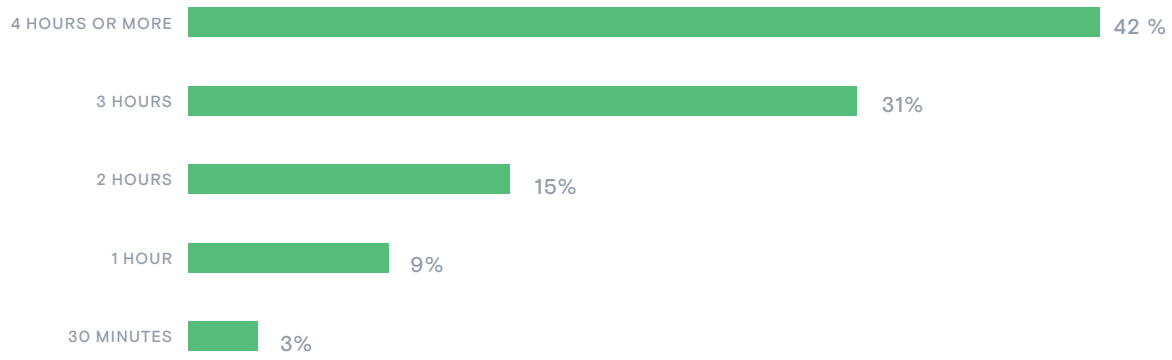
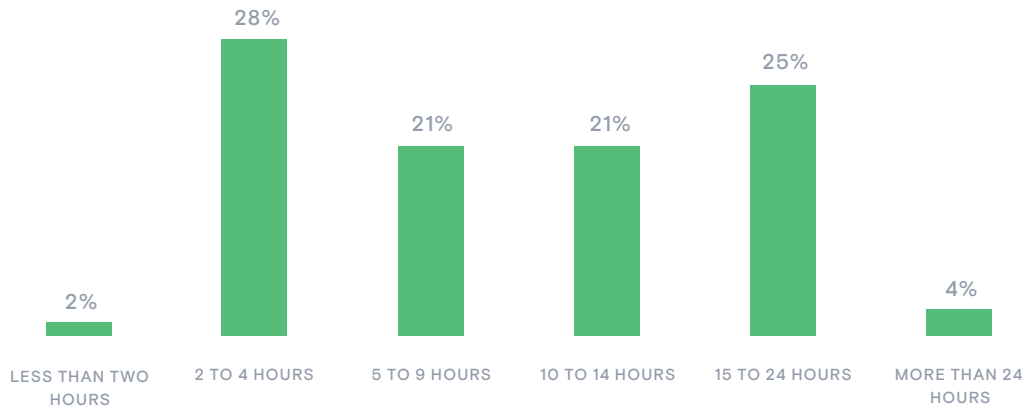


FIGURE 27

How much time on average does your development team spend Remediating each vulnerability found in production?

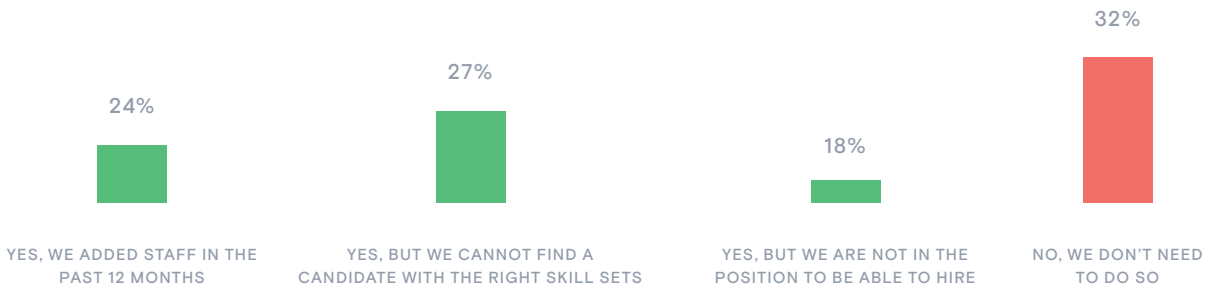


INEFFICIENCIES DD PRESSURE TO INCREASE STAFF

These inefficiencies have increased pressure on organizations to add application security staff. This is because legacy application security tools require experts to read and interpret the reports from increasingly frequent scans.10 Unfortunately, the cybersecurity skills shortage makes this difficult. Among respondents, nearly one-quarter (24%) have managed to add staff for their DevSecOps efforts (Figure 28). On the other hand, 45% say they need staff but cannot hire, due to either a lack of candidates or a lack of budget.

FIGURE 28

Have you needed to add more security staff to deal with devsecops issues?



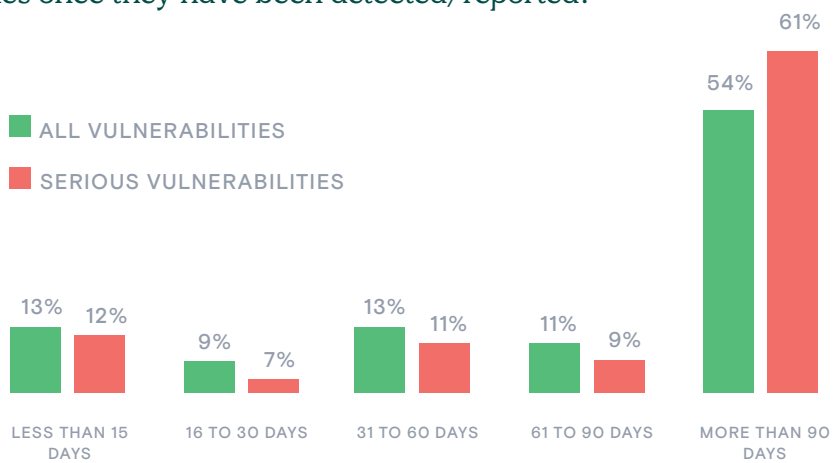
> "With the software development ground shifting, it's time for application security teams to get a move on—from appsec after the fact to secure code throughout the software development life cycle."
>
> Source: John P. Mello Jr., "The State of Application Security Testing: The Shift is on to Secure Code," Techbeacon, May 11, 2020.

INSIGHT: REMEDIATION TIMELINES SUGGEST STRUGGLES WITH PRIORITIZATION

Despite the constant interruptions to development and the vast amount of time consumed by scanning, identifying, and fixing vulnerabilities, organizations report unacceptably slow timelines for getting through this process. More than 6 in 10 respondents (61%) say that it takes more than 90 days to remediate the average serious vulnerability (Figure 29). And 54% say that is their average timeline for all vulnerabilities. This suggests difficulties with the prioritization of vulnerabilities, as organizations would ideally be faster at repairing serious vulnerabilities than non-serious ones. It also reveals a process problem, as a 90-day feedback loop for security reduces efficiency and increases cost.

FIGURE 29

On average, how long does it take to remediate Vulnerabilities once they have been detected/reported?



Analyzing these results by industry shows significant gaps. Two industries—finance and banking and healthcare—performed the best, with 58% and 57% of organizations, respectively, in those industries reporting that they resolve the average serious vulnerability in less than 90 days (Figure 30). On the other end of the spectrum, only 25% or 26% of organizations in two industries—media and entertainment and manufacturing—have met that benchmark.

Asked about how long it takes to reach the remediation of milestones of 25%, 50%, and 75% of vulnerabilities, a significant plurality of respondents (34%) took between 61 and 90 days to resolve even 25% of vulnerabilities (Figure 31)—but 50% of respondents require less than 61 days. But no fewer than 94% of respondents took more than 60 days to resolve half of their vulnerabilities, and 65% require more than 90 days to resolve three-quarters of their vulnerabilities.

FIGURE 30

On average, how long does it take to remediate serious vulnerabilities once they have been detected/reported?

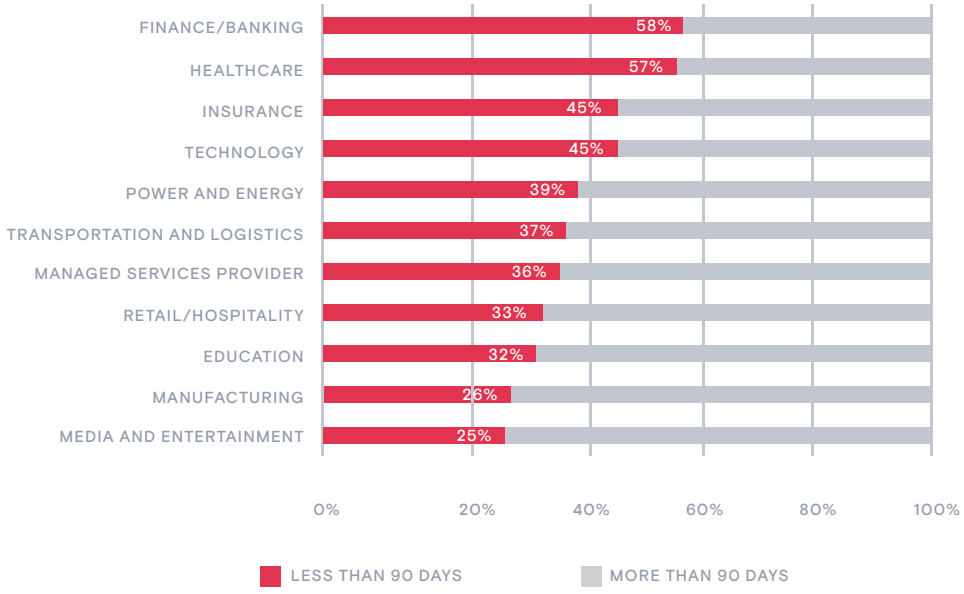
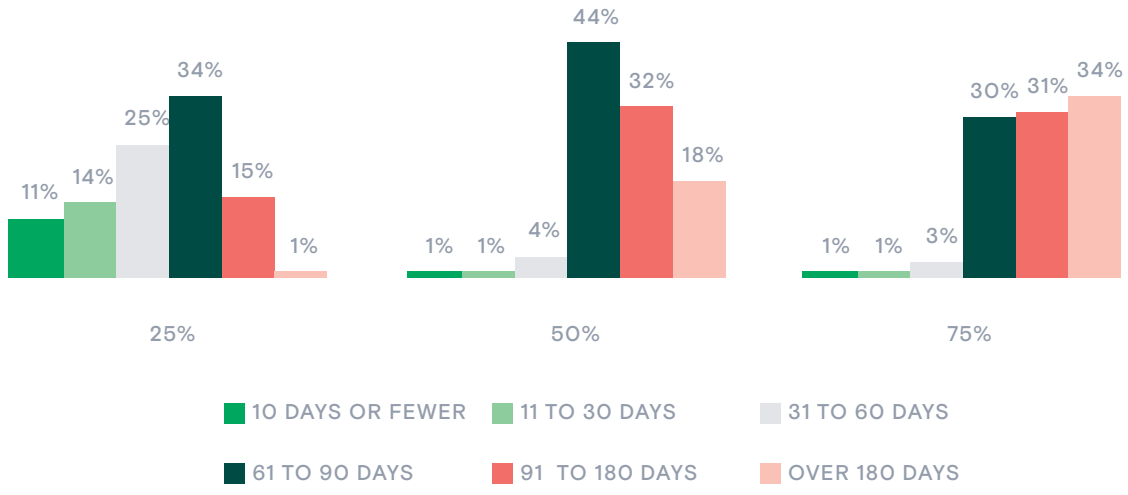


FIGURE 31

How long does it take you to reach these remediation milestones?



"With the software development ground shifting, it's time for application security teams to get a move on—from appsec after the fact to secure code throughout the software development life cycle."

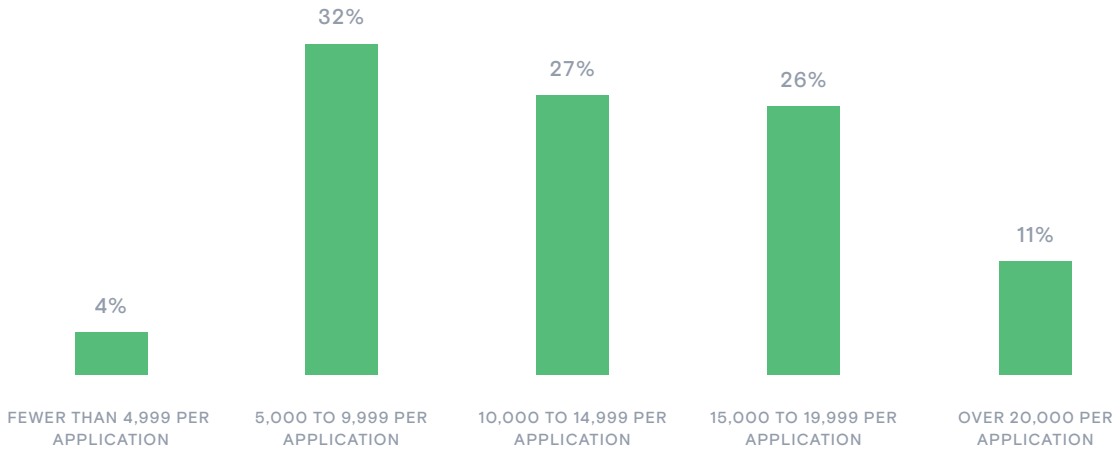
Source: John P. Mello Jr., "The State of Application Security Testing: The Shift is on to Secure Code," Techbeacon, May 11, 2020.

INSIGHT: ALMOST ALL ORGANIZATIONS HAVE SUSTAINED SUCCESSFUL ATTACKS, AND THEY HAD REAL CONSEQUENCES

Application attacks continue unabated even during a pandemic, and most respondents are experiencing hundreds of attack probes every day. In fact, 64% of respondents said individual applications in production received more than 10,000 probes per application per month in the past year, and 11% saw more than 20,000 (Figure 32). Some probes are simply trying to detect what technologies are used in the web application or API. But other probes are attempts to see if a vulnerability is present. Once confirmed, then real exploit attempts can start. This volume of probes is consistent with analysis of telemetry data from Contrast Labs analyzing probes and attacks on the Contrast Security customer base.[11]

FIGURE 32

On average, how many attack probes per application in production Runtime did you experience each month this past year?



REAL ATTACKS DAMAGE THE BUSINESS

The purpose of probes is to find applications that are candidates for actual attacks, and organizations represented in this survey were hard hit. Only 5% of respondents claim that they saw no successful attacks to applications in production in the past year, and a solid majority (61%) sustained three or more such attacks (Figure 33).

Many of these attacks were quite consequential to the business. Nearly three-quarters (72%) said business-critical data was exposed in at least one attack, 67% experienced operational disruption, and 62% saw brand degradation for their organizations (Figure 34).

FIGURE 33

How many successful exploited attacks on applications in production Runtime did you experience this past year?

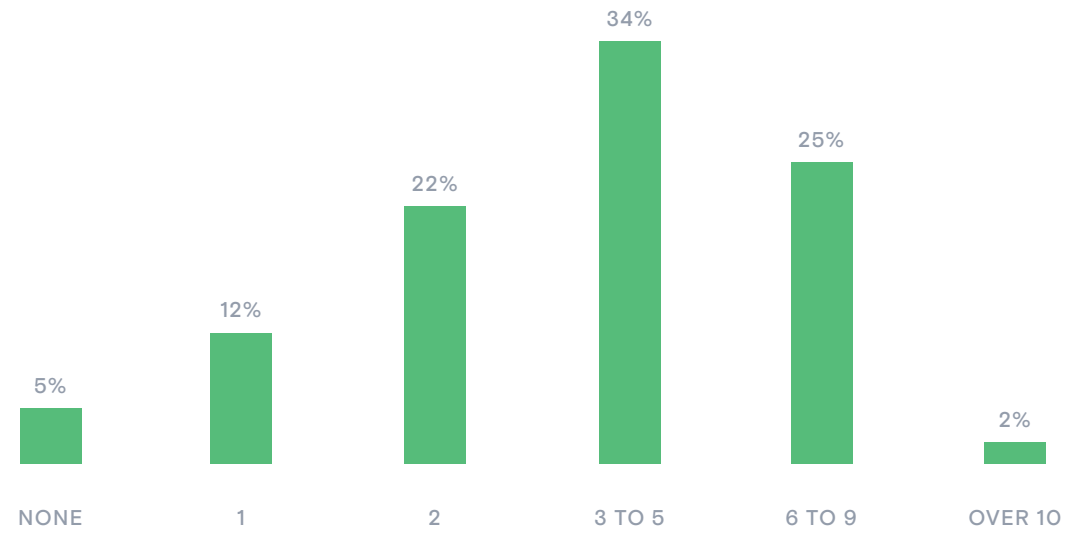
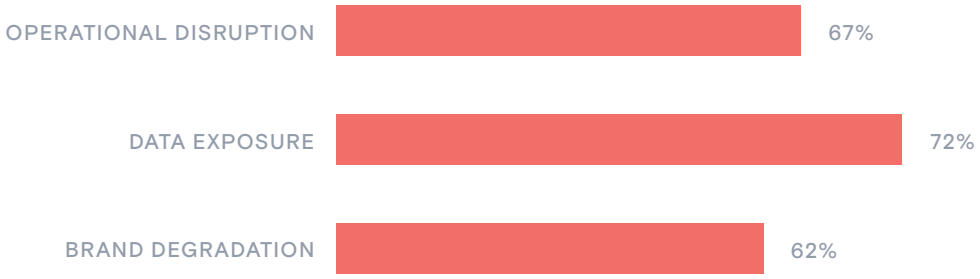


FIGURE 34

What were the repercussions of these attacks?



> "Given the pace of change and rate of attack cisos are often being called upon to deal with short-term, high-impact, issues on a daily or weekly basis."
>
> Source: "Research Report: Cybersecurity Technology Efficacy," Debate Security, October 2020.

04 | Conclusion

Digital transformation is no longer an optional step for businesses in any industry, and applications are a key part of any such strategy. As one observer put it, "Applications have become the business imperative, the key conduit to customers and the essential business enabler."[12]

Developers have risen to the challenge, dramatically improving their speed and efficiency in recent years. This survey found that 78% of organizations now deploy code to production at least multiple times per week, and nearly half do so daily. Despite this, the fast-changing marketplace makes further business acceleration a necessity. Nearly 8 in 10 organizations are pressuring their DevOps teams to develop code even faster, and more than half admit to skipping security scans to meet deadlines.

CONSTANT DELAYS TO DEVELOPMENT

The temptation to take shortcuts when it comes to security is understandable, as such processes consume a significant amount of time at most organizations. Almost everyone who responded to the survey admits that traditional application security testing scans take at least three hours each time they are run—and many say they take significantly longer.

According to a majority of respondents, each alert generated by these tools—including a large number of false positives—consumes at least an hour of time for the security team in triaging and tracing the source.

Each legitimate vulnerability takes more than four hours of developer time, and verifying those fixes consumes more than six hours per week for the typical developer. For applications already in production, a majority of respondents estimated that each alert consumes more than three hours of SecOps time and more than 10 hours of unscheduled developer time for emergency remediation.

> "Software engineering is not only about programming and developing, but also about the quality of the finished product. We need partners on the security team to accomplish that."
>
> – Survey Respondent, QA Engineer, Transportation and Logistics Industry

[1] Mark Holmes, "Microsoft CEO: 'Every Company is Now a Software Company'," Satellite Today, February 26, 2019.
[2] "COVID-19 Is Accelerating the Rise of the Digital Economy," BDO, May 2020.
[3] Forrester found a 40% increase in the use of open-source code in one year; see Amy DeMartine and Jennifer Adams, et al., "Application Security Market Will Exceed $7 Billion By 2023," Forrester, updated March 29, 2019.
[4] "2020 Data Breach Investigations Report," Verizon, April 2020.
[5] Maayan Manela, "Covid-19 cutbacks? No one told the software industry, salaries see a boost despite the pandemic," CTech, September 7, 2020.
[6] "2020 Data Breach Investigations Report," Verizon, April 2020.
[7] "2020 Application Security Observability Report," Contrast Security, September 2020.
[8] "Priorities and Challenges for Modern Software Developers," Contrast Security, September 28, 2020.
[9] "State of Software Security, Volume 11," Veracode, October 27, 2020.
[10] "How Legacy Application Security Requires Experts, Time, and Cost That Degrade DevOps Efficiencies," Contrast Security, July 27, 2020.
[11] "2020 Application Security Observability Report," Contrast Security, September 2020.
[12] Jo Peterson, "DevOps: The Secret to Doing More, Faster, Better and for Less Green," Channel Futures, February 23, 2018.
[13] Mukesh Soni, "Defect Prevention: Reducing Costs and Enhancing Quality," iSixSigma, accessed April 9, 2020.

Contrast SECURITY

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com