2018

Cybersecurity
INSIDERS

APPLICATION SECURITY REPORT

SECURITY INNOVATION

INTRODUCTION

Business applications are critical business resources for companies of all sizes — and they're increasingly under attack. To gain deeper insights into the state of application security, Cybersecurity Insiders conducted an in-depth study in partnership with the 400,000 member Information Security Community on LinkedIn.

This report is the result of a comprehensive survey of 437 cybersecurity professionals designed to reveal the latest application security trends, how organizations are protecting applications, and what tools and best practices IT cybersecurity teams are prioritizing to find, fix and prevent vulnerabilities in next-gen applications.

Among the key findings of this research are that many organizations are fairly confident in their application security posture, but still have a ways to go to reach an appropriate level of security maturity. They're facing a number of barriers that keep them from adequately defending against cyberthreats, and are concerned about protecting data and keeping up with the rising number of vulnerabilities.

The threat to applications is real, with malware, distributed denial-of-service, and other attacks putting applications at risk. Organizations are trying to counter by leveraging controls for securing applications, such as vulnerability scanning, anti-malware software, penetration testing, and identity and access controls. They're also actively monitoring applications to collect and respond to threat intelligence, and using a variety of methods to monitor applications.

We would like to thank Security Innovation for supporting this unique research.

We hope you will enjoy the report.

Thank you,

Holger Schulze

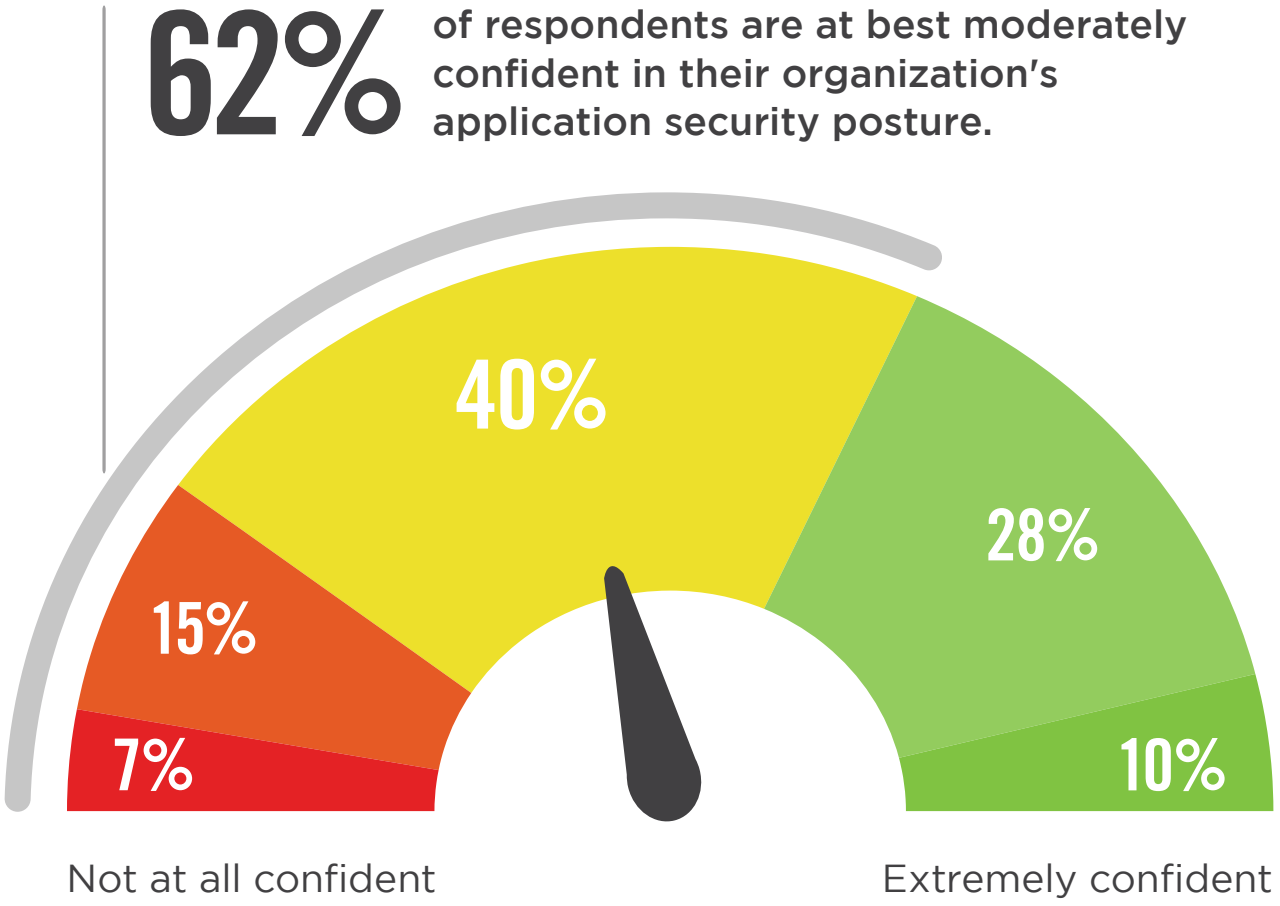
Holger Schulze
CEO and Founder
Cybersecurity Insiders
Holger.Schulze@Cybersecurity-Insiders.com

Cybersecurity INSIDERS

APPLICATION SECURITY CONFIDENCE

Survey respondents are at best moderately confident in their organization's application security posture. (62%). Only 38% said they are very confident or extremely confident.

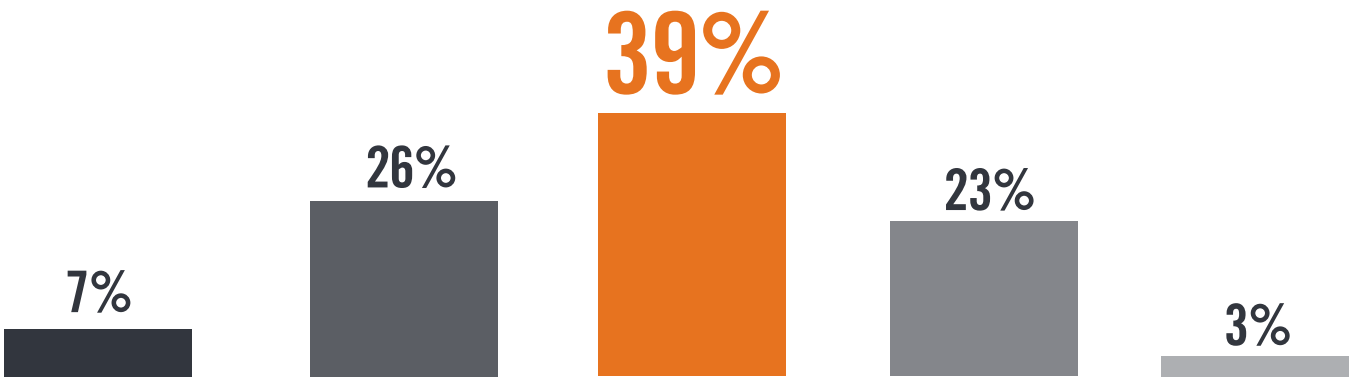
How confident are you in your organization's application security pos?



APPLICATION SECURITY MATURITY

When it comes to the maturity level of application security strategies, many organizations still have a long way to go. Nearly a third (26%) of organizations are doing little to nothing for application security. Only 7% of respondents said their organization is on the cutting edge of application security, while 26% characterize their company as being mature.

How mature is your application security strategy?



Not sure other 2%

BARRIERS AGAINST CYBER DEFENSES

A number of barriers are inhibiting organizations from adequately defending against cyberthreats, and none of them has to do with security technologies directly. At the top of the list are two "people issues": low security awareness among employees (37%) and lack of skilled personnel (37%). Next are lack of budget (35%), lack of management support and awareness (33%), lack of collaboration between departments (29%), and too much data to analyze (24%).

Which of the following barriers inhibit your organization from adequately defending against cyberthreats?

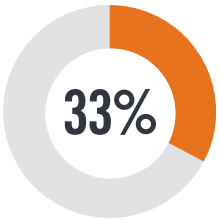
37%

Low security awareness among employees

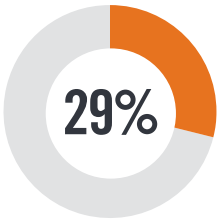
37%

Lack of skilled personnel

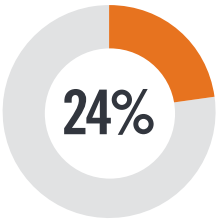
Lack of budget



Lack of management support/awareness



Lack of collaboration between separate departments



Too much data to analyze

Lack of investment in e ective solution 23% | Poor integration/interoperability between security solutions 22% | Inability to prioritize vulnerabilities based on risk 20% | Lack of contextual information from security tool 13% | Inability to justify additional investment 13% | None 6% | Not sure/other 10%

BIGGEST APPLICATION SECURITY CONCERNS

What are organizations' biggest concerns about application security? Not surprisingly, it's protecting data, cited by about half of the respondents (49%). And given the fact that hackers are constantly finding new ways to attack, it's also not a surprise that keeping up with the rising number of vulnerabilities also scored high (45%). Another top concern is security applications developed internally, cited by 42% of respondents.

What are your biggest application security concerns?

49%

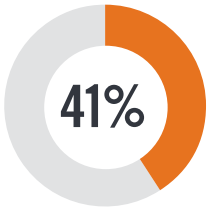
Protecting data

45%

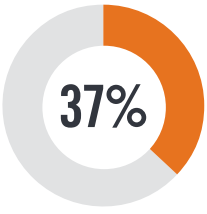
Keeping up with the rising number of vulnerabilities

42%

Securing applications we develop

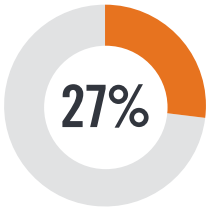


Threat detection/ breach detection



Securing cloud apps

Malware



Securing mobile apps

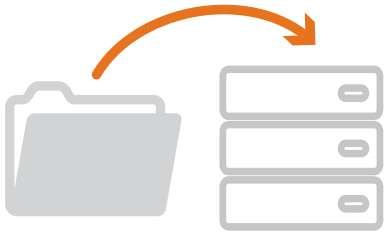
Meeting regulatory/compliance requirements 26% | Effective threat modeling 26% | Effectively prioritizing and remediating vulnerabilities that pose the most risk 26% | Securing open source software 23% | Securing business apps (ERP, etc.) 23% | Meeting customers' security needs and requirements 21% | Securing commercial off-the-shelf software 19% | Securing Embedded/ IoT/ hardware 18% | Securing Blockchain 7% | Not sure/other 6%

APPLICATIONS AT RISK

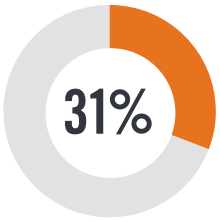
Not all applications are alike with regard to security risk. Those that present the highest security risk to businesses are customer-facing web applications and legacy applications, each cited by 41% of the survey respondents. Mentioned less frequently as security risks are mobile apps (31%), desktop applications (29%), business applications such as enterprise resource planning and supply chain management (28%), and internal-facing web applications (23%).

Which types of applications present the highest security risk to your business?

41% Customer-facing web applications

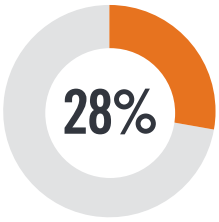


41% Legacy applications

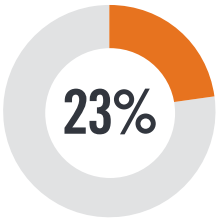


Mobile applications

Desktop (client applications)



Business Applications (ERP, SCM, MES, HR SRM, etc.)



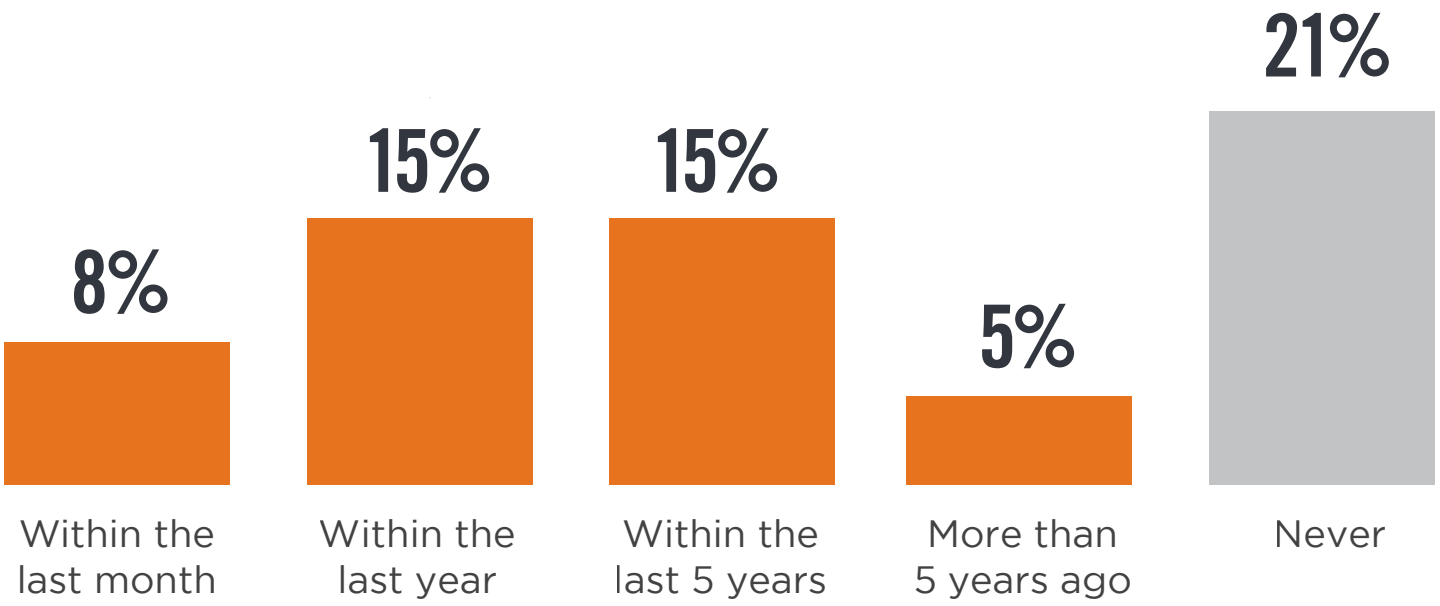
Internal-facing web application

Embedded/IoT software and firmware 26% | Securing Blockchain 7% | Not sure/Other 13%

COMPROMISED APPLICATIONS

43% of surveyed organizations have experienced application breaches or compromises in the past, and of those 8% had been attacked just within the last month. The unsettling news is that more than one third (36%) are not even sure if they've undergone a security attack against applications.

When was the last time that one of your company's applications was breached/compromised?



Don't know/unsure 36%

TYPES OF SECURITY ATTACKS

Recent years have seen rapid growth in malware variants and attacks, and the survey reflects this trend. Malware was the most common type of security attack against applications over the past 12 months, cited by 31% of the respondents. The next most common risk was application misconfiguration (23%), followed by distributed denial-of-service attacks (22%). Other key types of attacks include stolen credentials (19%). software vulnerabilities (17%), and information leakage (16%).

Which of the following security attacks against applications has your organization experienced over the past 12 months?

31%

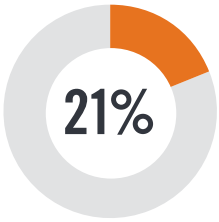
Malware

23%

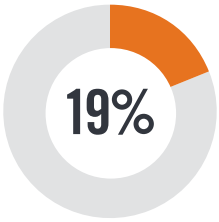
Application misconfiguration

22%

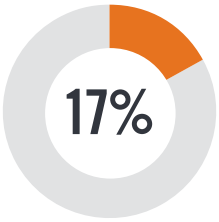
DDoS



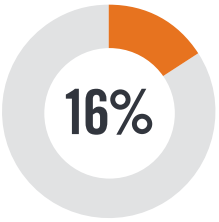
None



Stolen credentials



Software vulnerability exploite



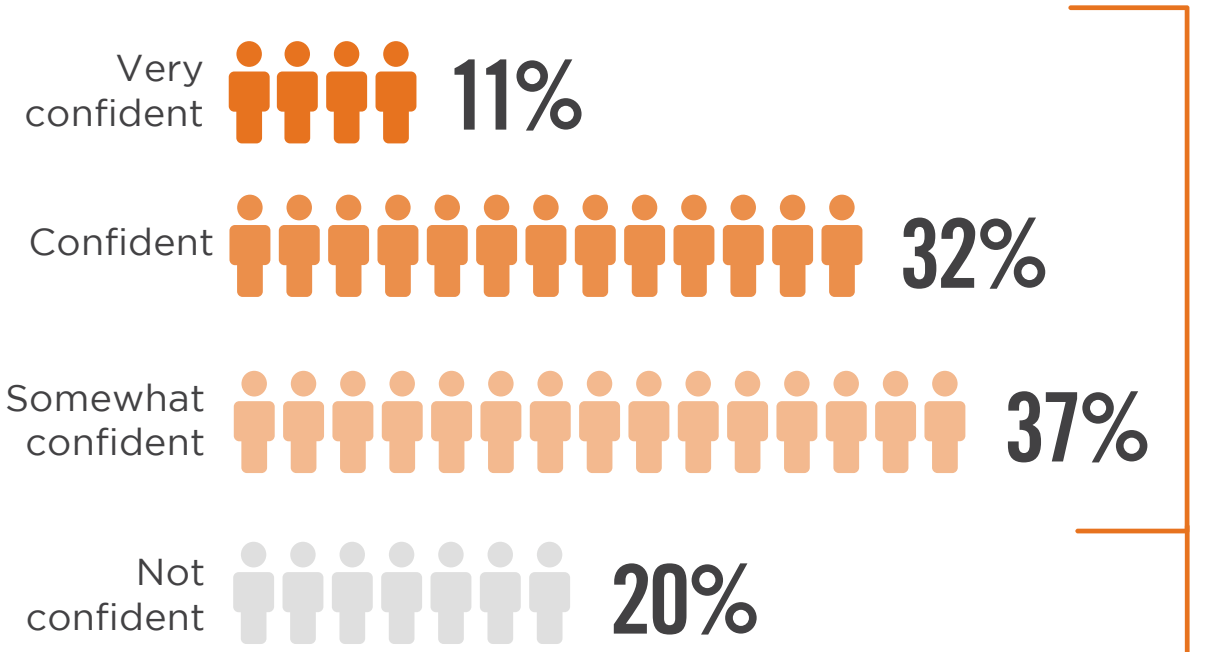
Information leakage

Unpatched library 15% | SQL injectio 14% | Brute Force 14% | Cross-site scripting 12% | Web Fraud 12% | Content spoofing 11% | Clickjackin 7% | Cross-site registry 6% | MitM/MitB 6% | Not sure/Other 13%

APPLICATION AWARENESS

Even with the emergence of "shadow IT" (in which departments, groups, and even individual users deploy business applications without the authority or knowledge of central IT management), apparently many organizations know their applications. More than three quarters of respondents said their organizations feel somewhat to very confident that they know all applications in use. Only 20% said they are not confident about knowing all the applications.

How confident are you that you know all applications used in your organization today?



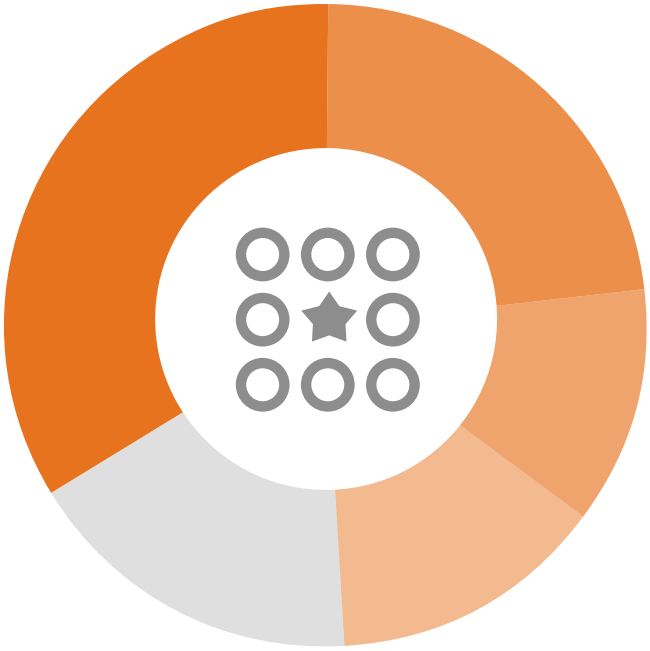
more 3/4 of respondents

feel somewhat to very confident they know all applications

NUMBER OF APPLICATIONS

Half of the respondents said their organization has more than 100 applications, and about one quarter said they have more than 500 unique applications in their IT environment. Some 14% of the organizations actually have more than 1,000 applications deployed. Only one third of the organizations surveyed have less than 100 unique applications.

How many unique applications are in your environment?



34%
< 100

23%
101-500

12%
501-1,000

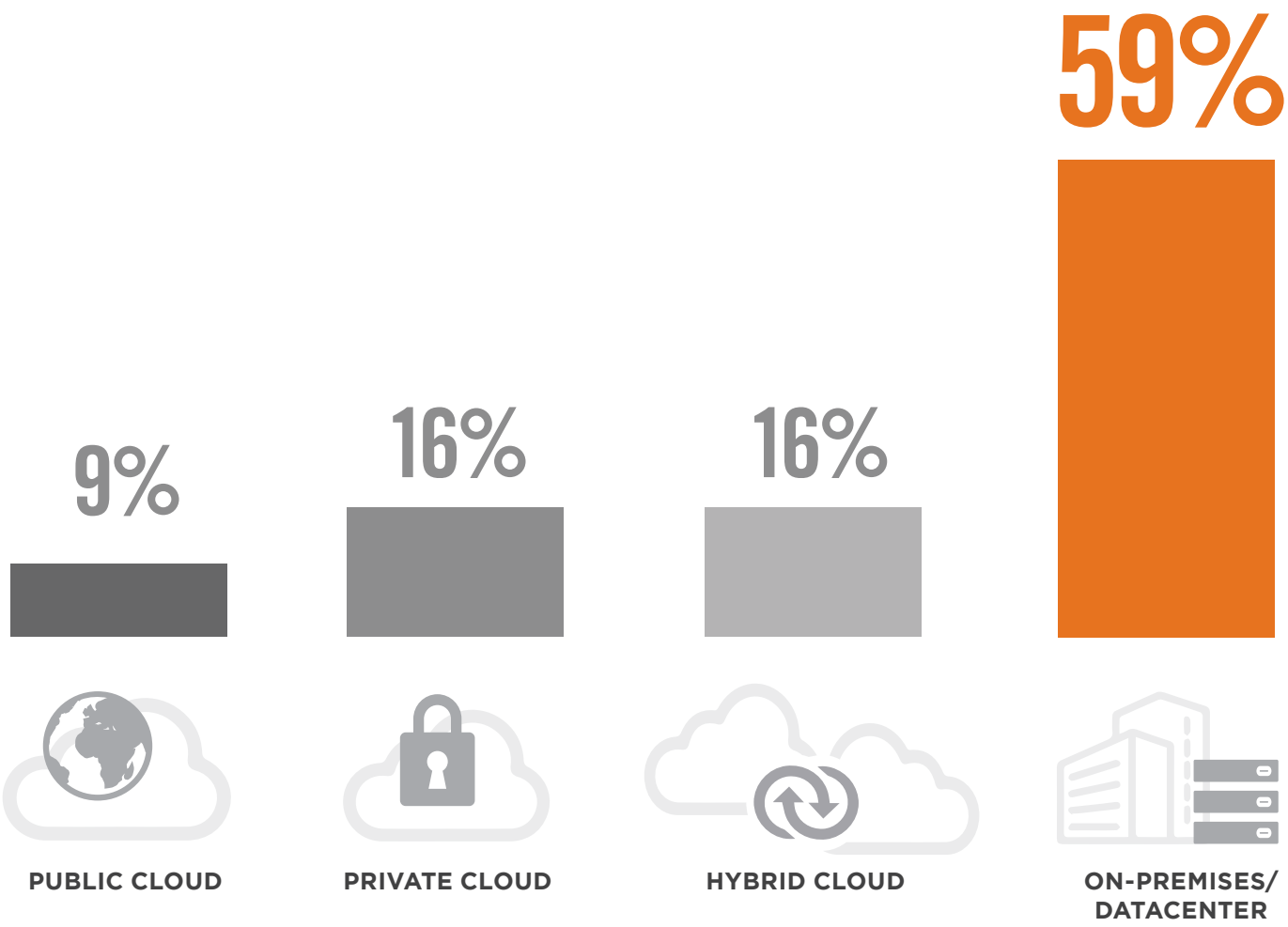
14%
> 1,000

17%
Don't know/ unsure

APPLICATION LOCATION

Even with all the focus on moving data and workloads to the cloud, including offerings such as software-as-a-service (SaaS), many organizations are keeping most of their applications inhouse. A majority of those surveyed (59%) said most of their applications are hosted in an on-premises data center. A relatively small share of applications are hosted in private clouds (16%), hybrid clouds (16%), or public clouds (9%).

Where are the majority of your applications hosted?



APPLICATION SECURITY PROGRAM

For those organizations that have an application security program in place, in-house management is the favorite option. Two thirds of the respondents said their organization has an in-house application security program, while 23% outsource the function or obtain it through a managed service. Another 14% said they have no dedicated application security program in place.

If you already have an application security program in place, is it:

66%

In house

23%

Outsourced/ Through a managed service

14%

No security program in place

Don’t know/unsure 9%

THIRD-PARTY APPLICATION SECURITY POLICY

Third-party applications can be the source of numerous security threats and vulnerabilities, so it makes sense that companies would want to identify and test all such software. Indeed, 41% of the organizations surveyed are doing this via a security policy related to application adoption. On the other hand, 27% of the organizations have a policy but do not enforce it. Even worse, 19% of the organizations have no policy in place for third-party software.

Do you have a security policy for adoption of third party applications your organization?

41%
Yes, we identify and test all third party software

27%
Yes, we have a policy, but no enforcement

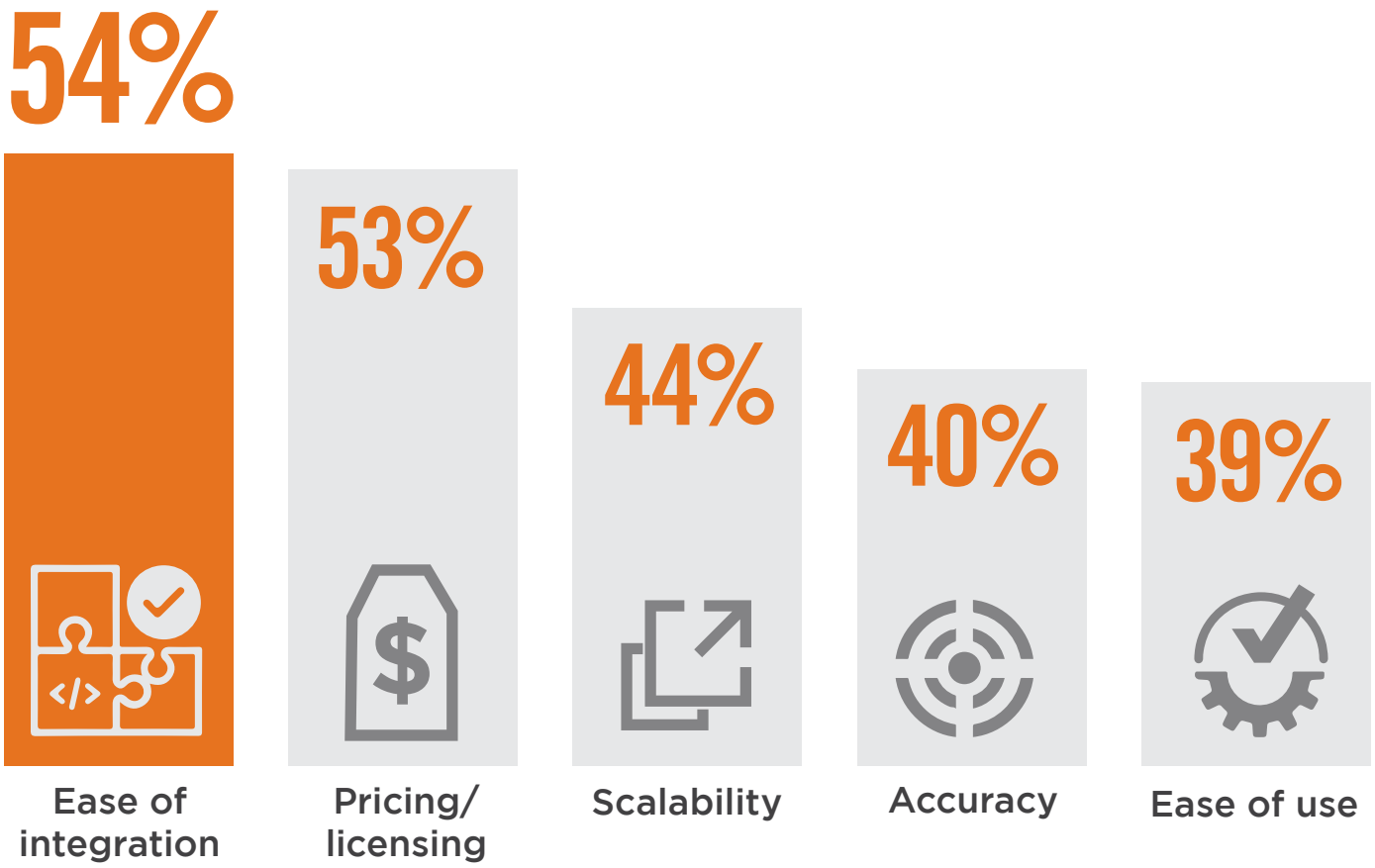
19%
No, we do not have a policy for third party software

13%
Not sure/other

APPLICATION SECURITY TOOL SELECTION

Ease of integration is the most important criteria for organizations when selecting an application security tool or service, according to 54% of the respondents. This is closely followed by pricing/licensing (53%), scalability (44%), accuracy (40%), and ease of use (39%).

What are your most important criteria for you when selecting an application security tool or service?



Comprehensiveness of capabilities 37% | Time required to get the tool up and running in my environment 31% | Credibility (Established vendor) 29% | Enterprise-class support 27% | SaaS option 16% | Not sure/Other 13%

Survey participants could select more than one response, resulting in a total greater than 100%.

SECURITY CONTROLS

Organizations leverage several security controls and programs for protecting applications. Easily the most common is vulnerability scanning, cited by 69%. That's followed by anti-malware software (61%), penetration testing (54%), and identity and access controls (50%).

What are your organization's primary measures and controls for security applications?

69%

Vulnerability scanning

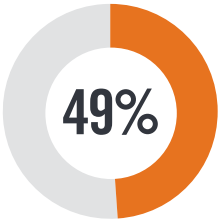
61%

Anti-malware software

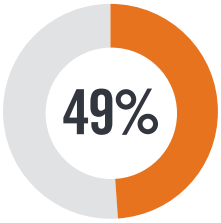
54%

Penetration Testing

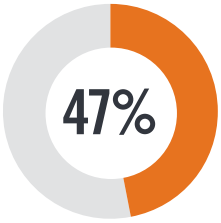
Identity and Access Controls



Security architecture and design



Web Application Firewall (WAF)/ Next-generation firewall



Security monitoring

Code reviews 36% | Secure coding guidelines 34% | Developer training 29% | Threat Modeling 22% | SAST (Static Application Security Testing) 21% | Container security 21% | DAST (Dynamic Application Security Testing) 18% | Web fraud detection 16% | Bug Bounty programs 11% | RASP (Run-time Application Security Protection) 10% | We require our software vendors to secure code before it enters our environment 10% | IAST (Interactive Application Security Testing) 8%

Survey participants could select more than one response, resulting in a total greater than 100%.

APPLICATION MONITORING

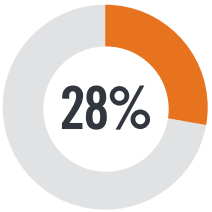
A majority of organizations (54%) are actively monitoring applications running in production to collect and respond to threat intelligence. They're using a variety of methods to monitor applications, including web application firewalls to protect applications (39%), a feedback loop to share incidents and identified vulnerability information back to development teams (28%), and code signing in deployment of applications (26%).

How are you currently monitoring applications for security issues?

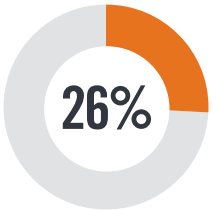
54%

We actively monitor applications running in production to collect and respond to threat intelligence

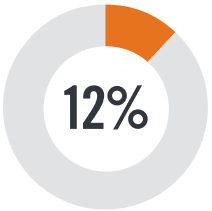
We use a web application firewall (WAF) to protect our applications



We have a feedback loop to share incidents and identified vulnerability information back to our development and design teams



We use code signing in deployment of our apps



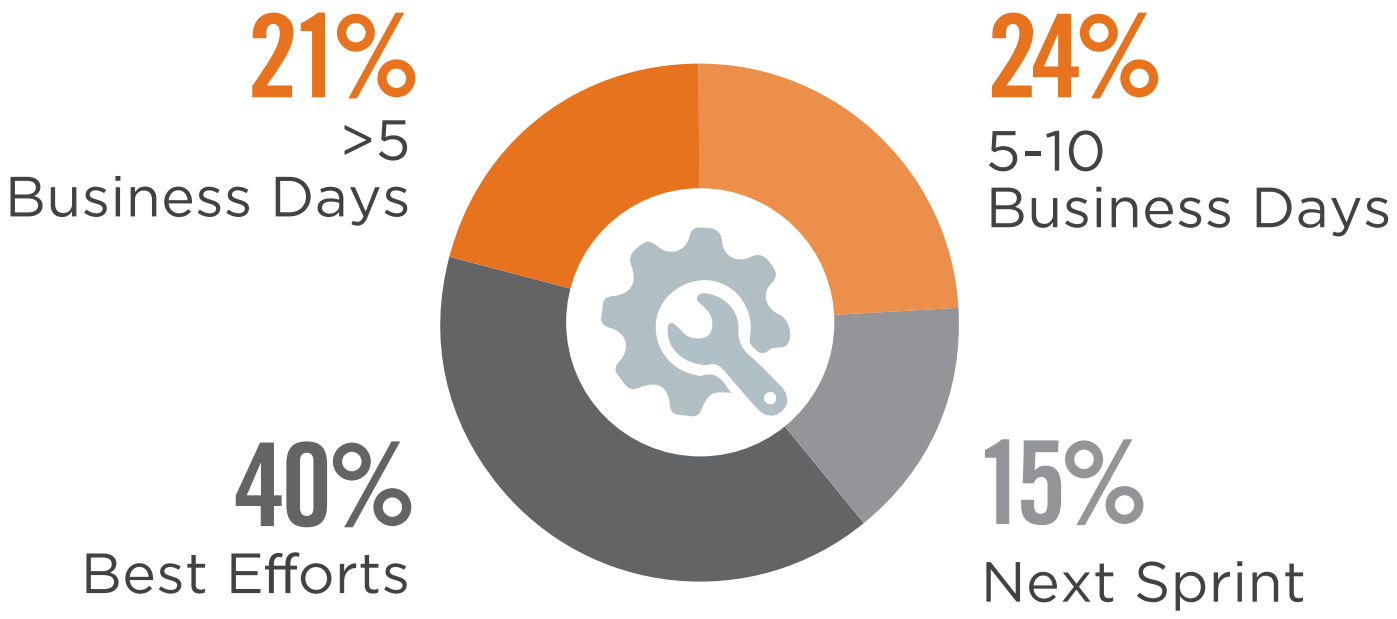
None of the above

Not sure/other 17%

SLAS FOR REMEDIATION

When asked what kind of service level agreement (SLA) their organizations have established around the remediation of high-severity issues, most respondents said "best efforts" (40%). This was followed by "five to 10 business days" (24%), "more than five business days" (21%), and "next sprint" (15%).

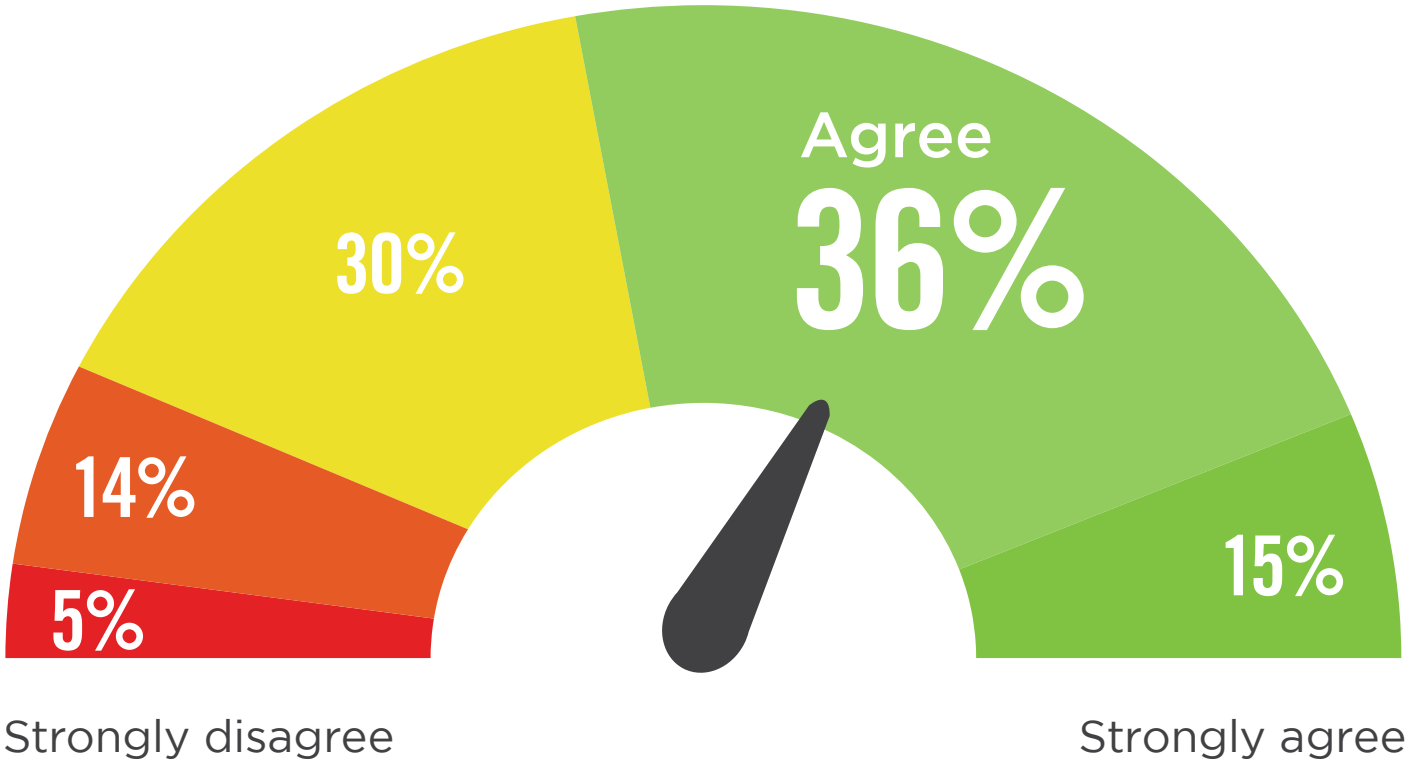
What kind of SLA have you established around remediation of high severity issues?



UNDERSTANDING APPLICATION RISK

Respondents were asked whether the application security data their organization collects is sufficient to understand the level of application risk, and prioritize remediation efforts. More than half (51%) either agree (36%) or strongly agree (15%) that the data is sufficient. Only 19% disagree or strongly disagree.

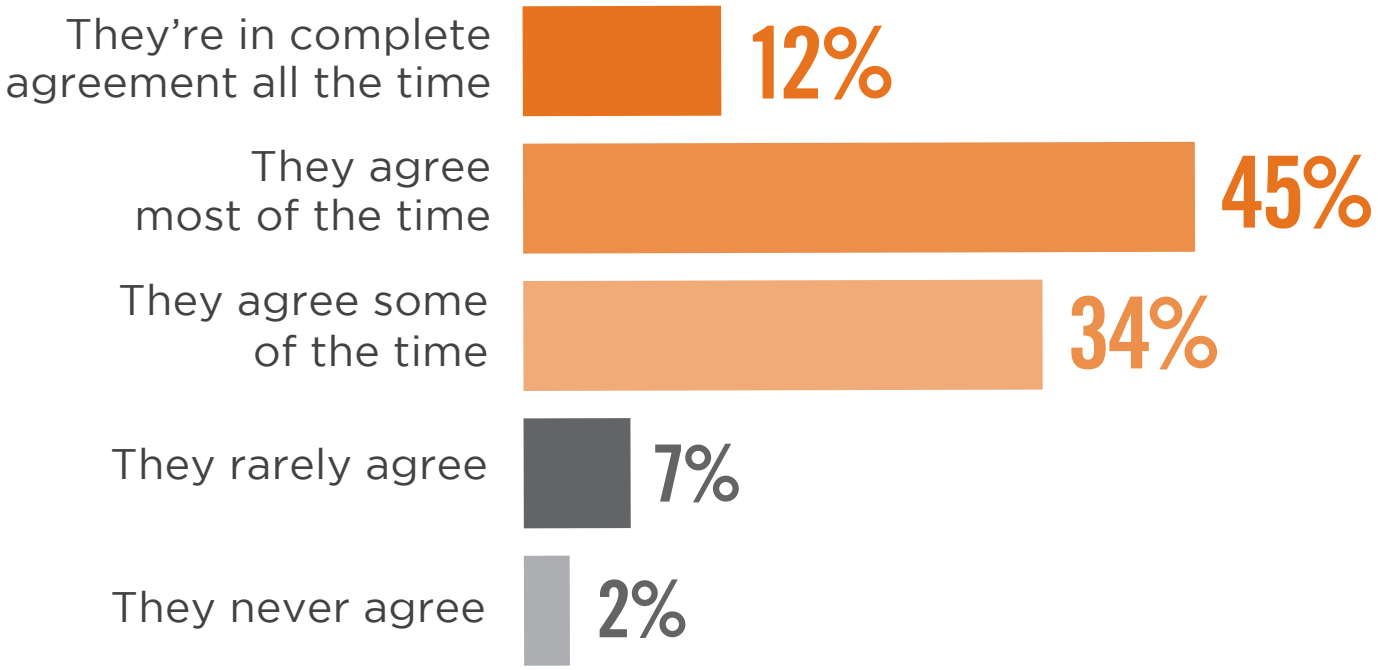
The application security data my organization has is sufficient to understand our level of application risk and prioritize the team remediation efforts:



VULNERABILITY PRIORITIZATION

Application security and development teams within organizations don't always see eye to eye on issues. But when it comes to determining which application vulnerabilities need to be fixed, they're largely in agreement. A huge majority (91%) of the respondents said teams are in agreement at least some of the time (34%), most of the time (45%), or all the time (12%). A mere 9% said the rarely or never agree.

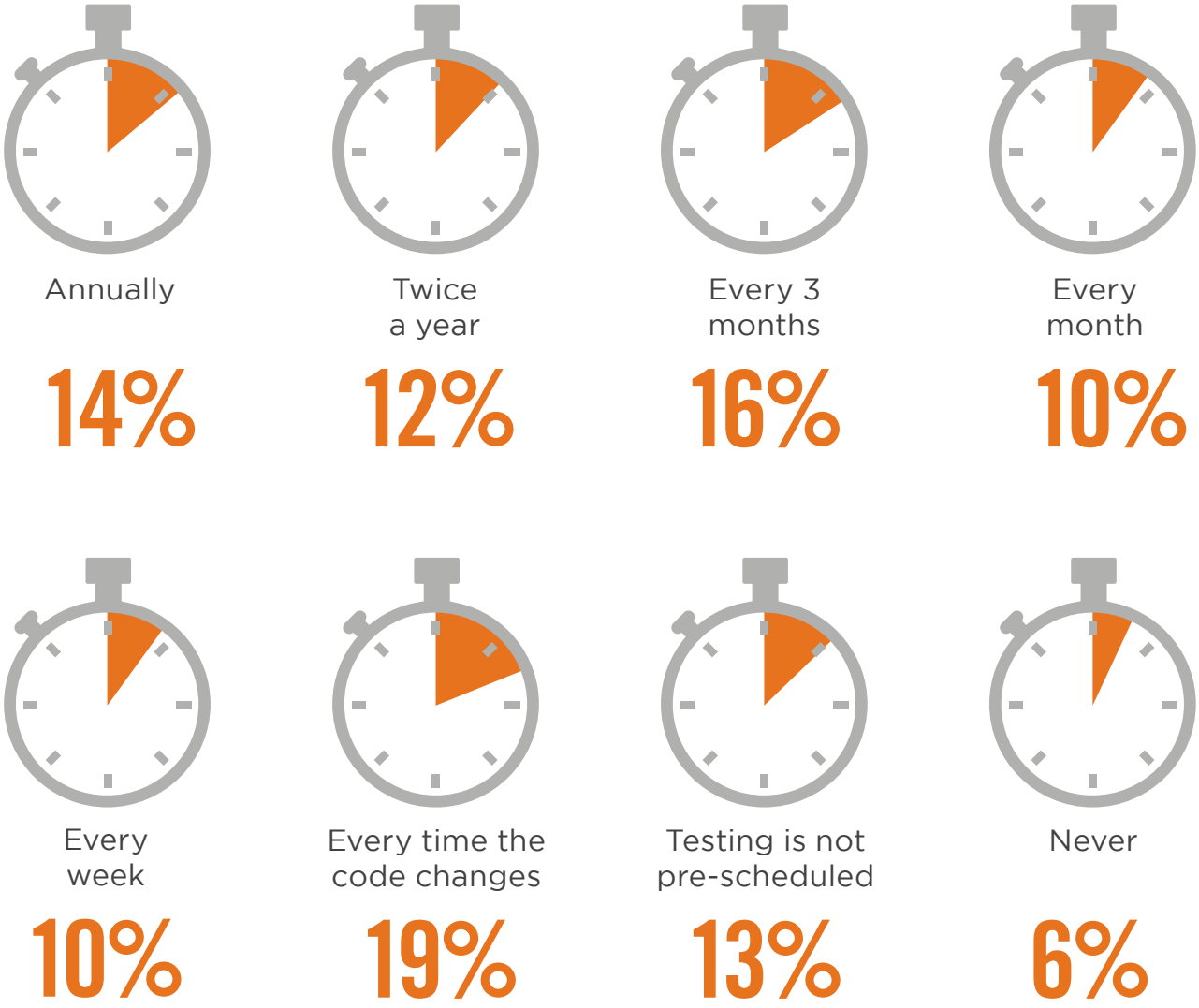
To what extent do the application security and development teams in my organization agree on which application vulnerabilities need to be fixed?



APPLICATION TESTING FREQUENCY

Organizations are all over the map when it comes to the frequency of testing applications for threats and vulnerabilities. The most cited frequency is every time the code changes (19%), followed by quarterly testing of applications (16%). Only 6% of respondents said they never test applications for threats and vulnerabilities.

How often does your organization test applications for threats and vulnerabilities?



PENETRATION TESTING

Organizations perform penetration testing for a number of reasons. The most commonly cited reason is that pen testing is part of the secure software development lifecycle (47%). Next highest on the list of reasons is that organizations need it for regulatory compliance (33%), and the need to prove that application security issues have been fixed (32%).

Why do you perform pen testing?

47%

It's part of our secure software development lifecycle

33%

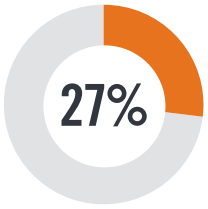
We need it for regulatory compliance

32%

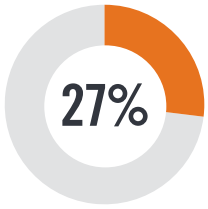
We need to prove application security issues have been fixed

We need to comply with PCI

Risk assessment for our 3rd party vendors



Customers need it for regulatory compliance reasons



Improves appsec

Customers ask for it 24% | We need to comply with HIPAA 19% | Avoid Bad Press 15% | Sales asks for it 4% | Other 3%

PEN TESTING CHALLENGES

The most challenging aspect of penetration testing applications is that it's hard to find and hire people with the right skillset, according to 22% of the respondents. This is followed by cost barriers preventing organizations from pen testing applications as frequently (18%) and comprehensively (15%) as desired.

What is the most challenging thing about pen testing applications?

22% It's hard to find or hire people with the right skills

18% It's too expensive to pen test our applications as frequently as we want to

12% Tools and scanning services aren't effective and/or produce too much noise

15% It's too expensive to pen test as many applications as we want to

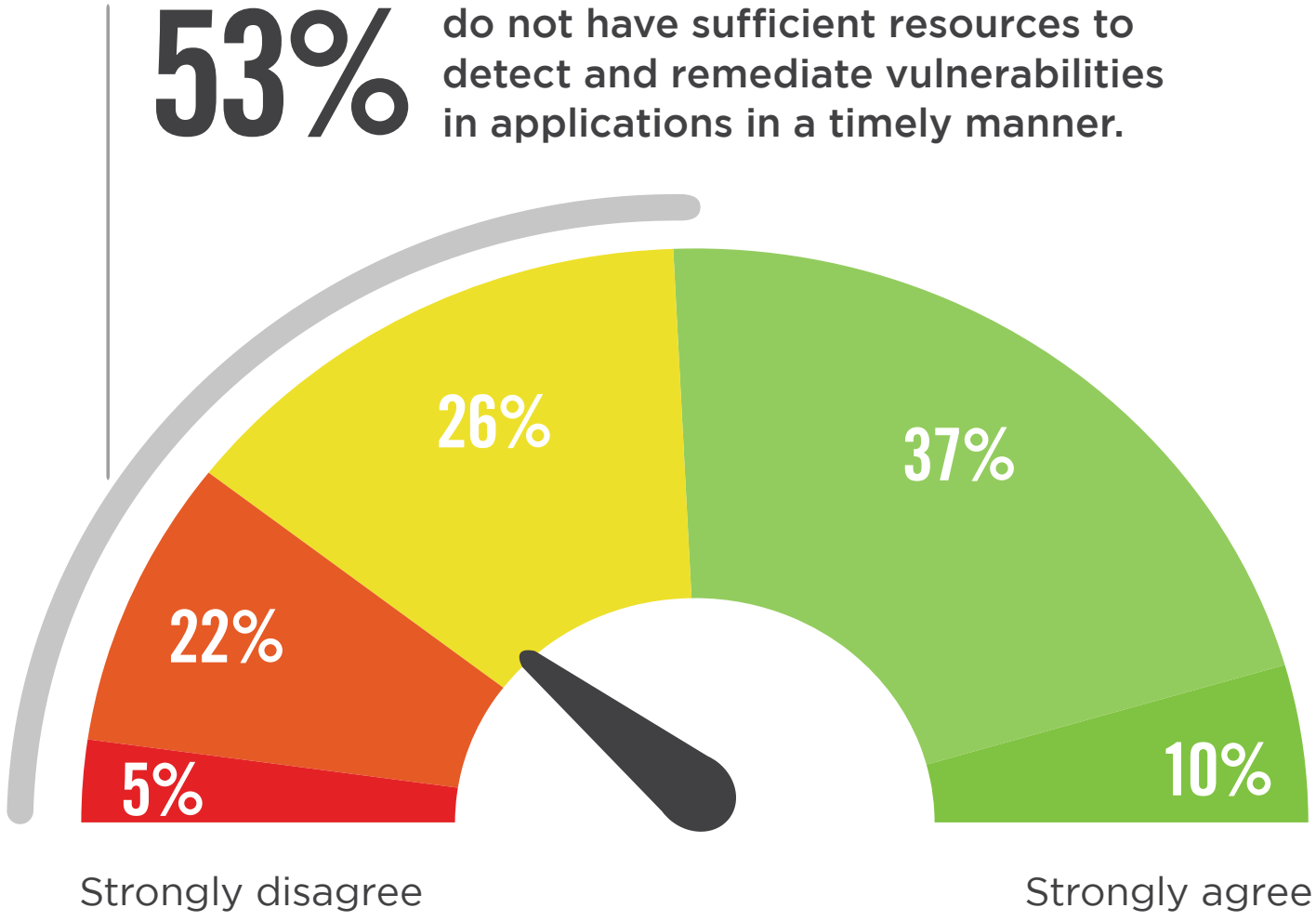
12% It's hard to get issues fixed

Lack of integration with the SDL 11% | Pen Test reports aren't easy to understand 6% | Other 4%

APPLICATION SECURITY RESOURCES

A majority of organizations (53%), do not have sufficient resources to detect and remediate vulnerabilities in applications in a timely manner.

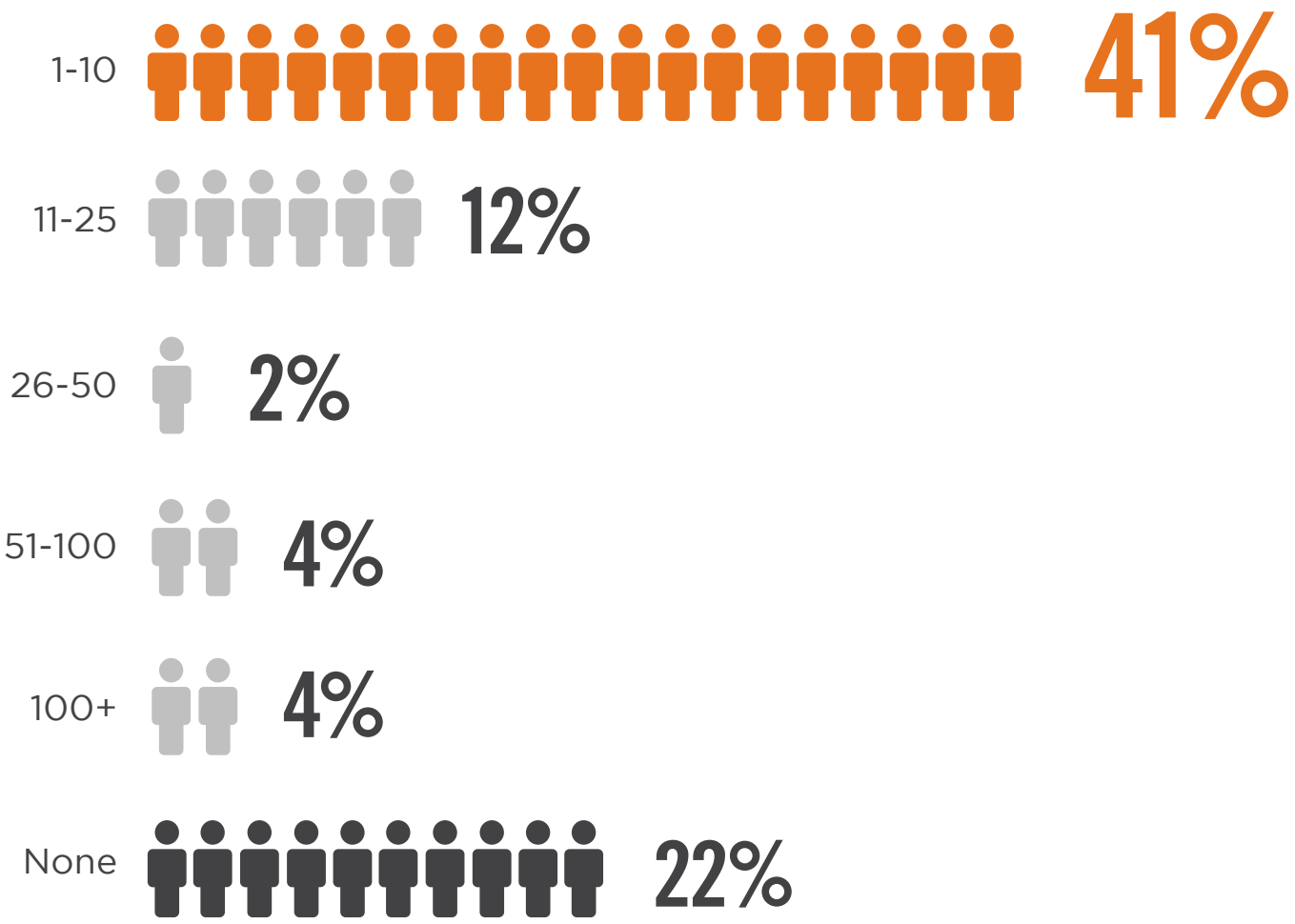
My organization has ample resources to detect and remediate vulnerabilities in applications in a timely manner.



APPLICATION SECURITY STAFF

The typical team of application security and penetration testers has anywhere between one and 25 staffers, according to the survey (53% of organizations). Few organizations have substantially larger testing teams: 2% have 26 to 50 testers; 4% have 51-100; and 4% have more than 100. Interestingly, 22% of the organizations do not have any full-time application security personnel.

How many full-time application security and pen testing people do you have in your company?



Don't know 15%

APPLICATION SECURITY BUDGET

Budgets for application security programs are generally trending up, with 50% of the respondents saying their budgets will increase over the next 12 months, and 33% saying they will stay the same. Only 17% of the organizations expect to see a budget decrease.

How is the budget for your application security program changing over next 12 months?

50%
Budget will increase

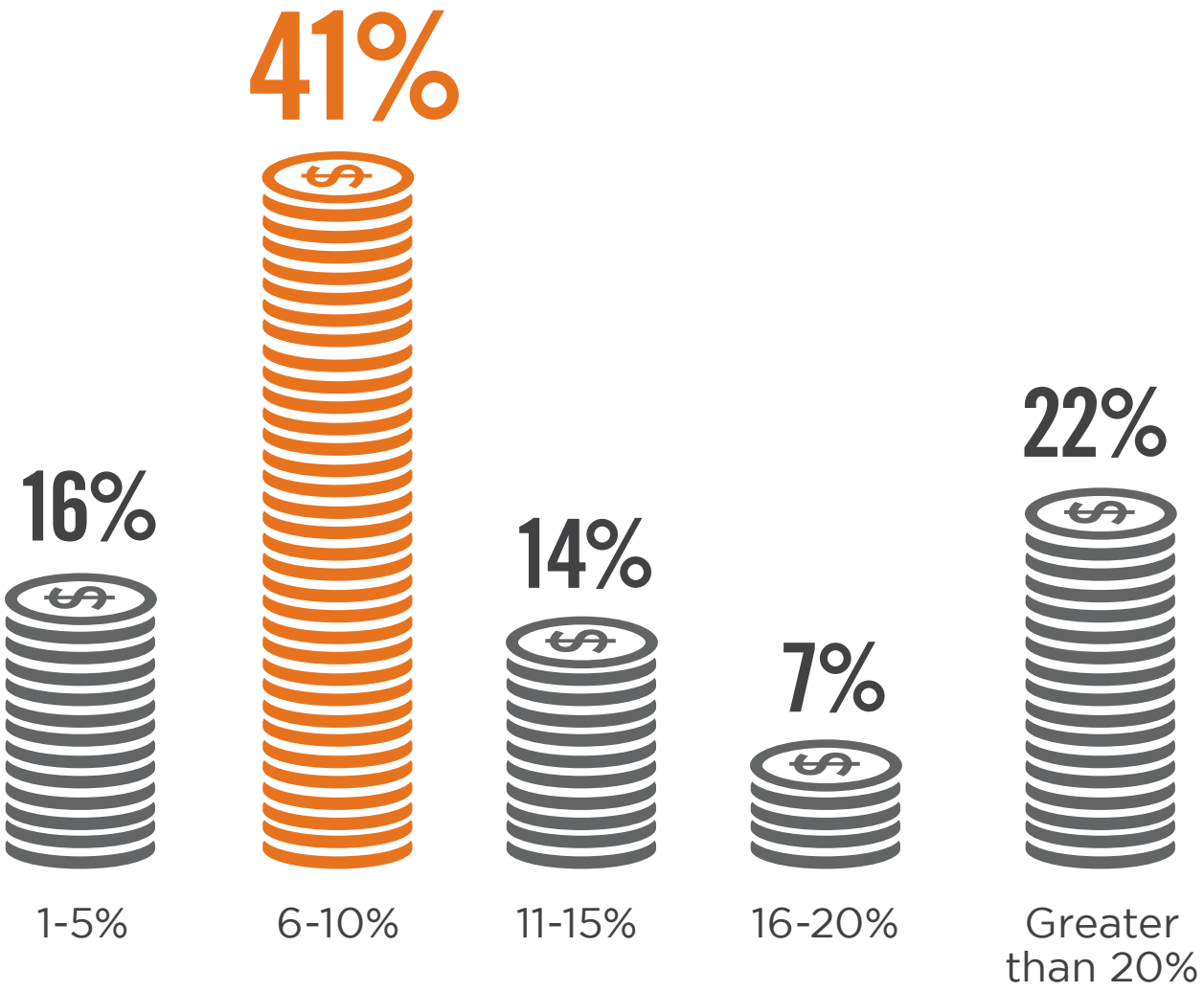
33%
Budget will stay the same

17%
Budget will decrease

SIZE OF BUDGET INCREASES

For those organizations that expect to see expanded budgets for application security programs, the increases will be fairly substantial. Fiftyseven percent of the respondents said budgets will rise by up to 10%, and 43% said they will increase by more than 10%. The largest share of respondents (41%) said the budget increase will be between 6% and 10%.

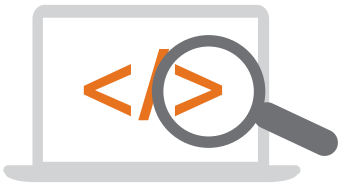
If the budget for your application security program will increase, indi by how much.



SECURE APPLICATION DEVELOPMENT

Organizations are employing several secure development initiatives. The most common is regular security code reviews on all code check-ins (cited by 39%). Others include a role-based security education program (35%), a process to track the usage and security of third-party or open source code (35%), and an established security gate to identify vulnerabilities in releases (34%).

What secure development initiatives do you currently employ, if any?



39%

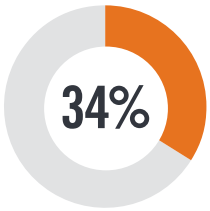
Regular security code reviews on all code check-ins

35%

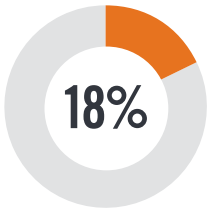
A role-based security education program

35%

A process to track the usage and security of third-party or open source code



An established security gate to identify vulnerabilities in releases



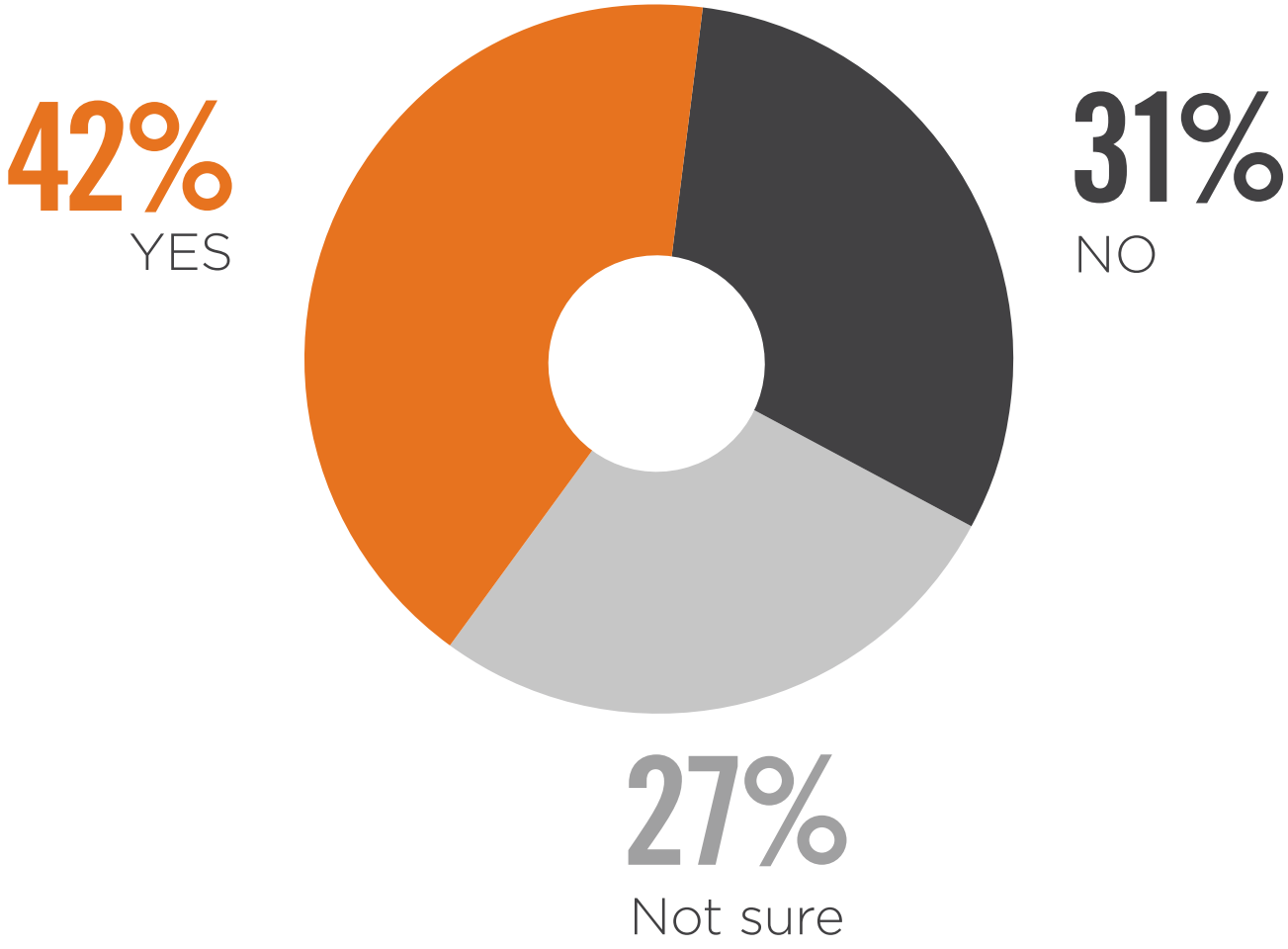
None of the above

Survey participants were asked to select all answers that apply.

SECURE CODING

It's common knowledge that many companies are facing market pressures to get new software out the door quickly. But does the "rush to release" cause application developers to neglect secure coding procedures and processes? The answer is yes, according to 42% of the respondents. Another 31% said it does not lead to neglect and 27% are not sure.

Does the "rush to release" cause application developers in your organization to neglect secure coding procedures and processes?



AUTOMATING SECURITY TESTING

Organizations are evenly divided among those that automate security testing in their software release lifecycle and those that do not, each at 43%. Another 14% of the respondents don't know if their organization automates security testing.

Do you automate security testing in your software release lifecycle?

43%
YES

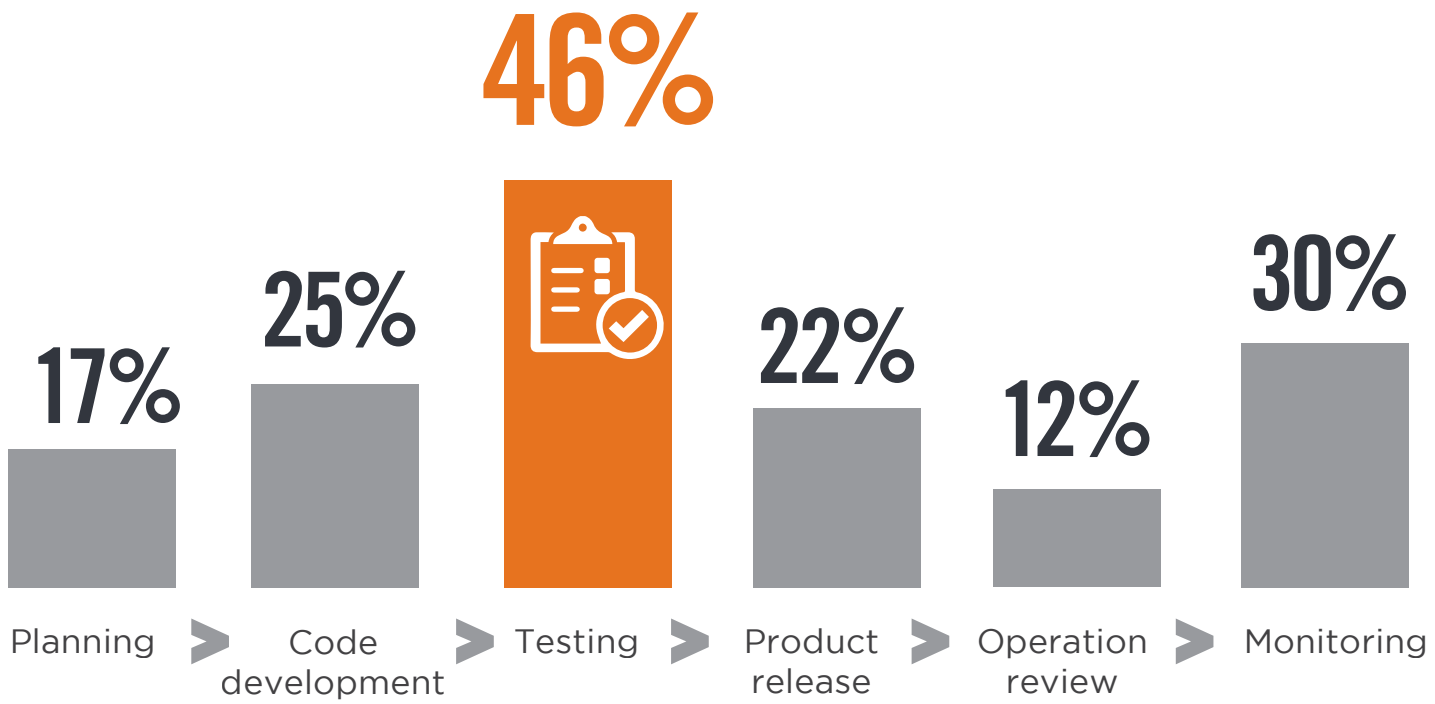
43%
NO

14%
Don't know

TESTING IN THE LIFECYCLE

Asked about where in their release lifecycle organizations automate security testing, 46% said during testing, easily the most common response. Others cited monitoring (30%), code development (25%), product release (22%), planning (17%), and operation review (12%). One third of the organizations do not automate any application testing.

Where in your release lifecycle do you automate security testing?



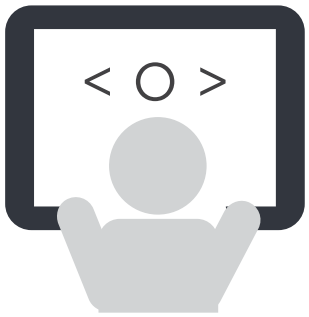
33% We do not automate any application testing

Survey participants could select more than one response, resulting in a total greater than 100%.

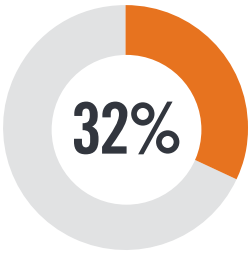
DEVELOPER TRAINING

A majority of nearly half of the organizations are using computer-based training to train their developers. Other methods include instructor-led training (ILT) or live, in-person training (28%), and interactive cyber ranges (19%). Nearly one third (32%) said they are not currently training their developers.

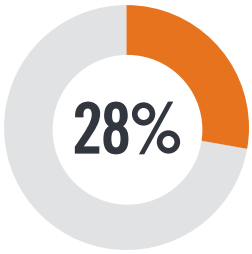
How are you currently training your developers?



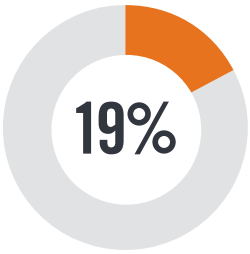
47% Computer-based training



We are not currently training our developers



ILT (or live, in-person training)



Interactive cyber ranges

SECURITY TRAINING CHALLENGES

The most challenging aspect of providing developers with security training is that training is perceived as too time consuming, and organizations can't afford to take developers off projects (cited by 47%). Other challenges include high cost of training (25%), difficulty to find the right training program (24%); and organizations don't see positive results of training (9%).

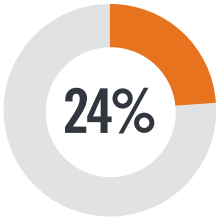
What is the most challenging thing about getting developers security training?

47%

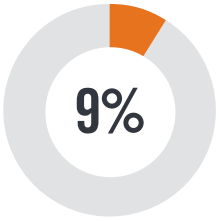
Training is too time consuming (can't afford take developers off projects)

25%

Costs is too high/ don't have the budget



It's hard to find the right training program

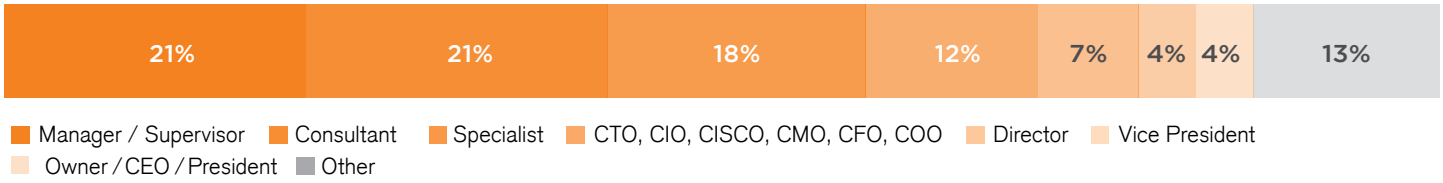


We don't see the results from training

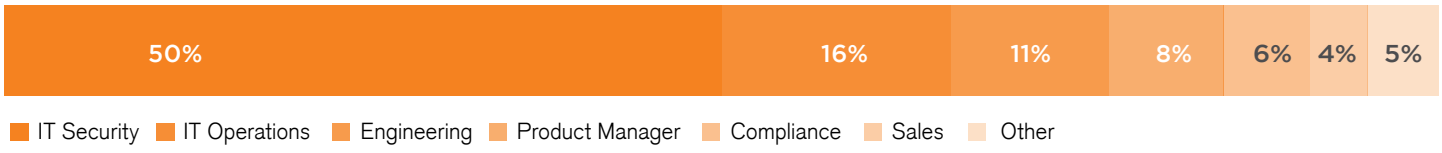
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of cybersecurity professionals to gain more insight into the latest application security threats faced by organizations and the solutions to prevent and remediate them. The respondents range from technical executives to managers and IT security practitioners. They represent organizations of varying sizes across many industries.

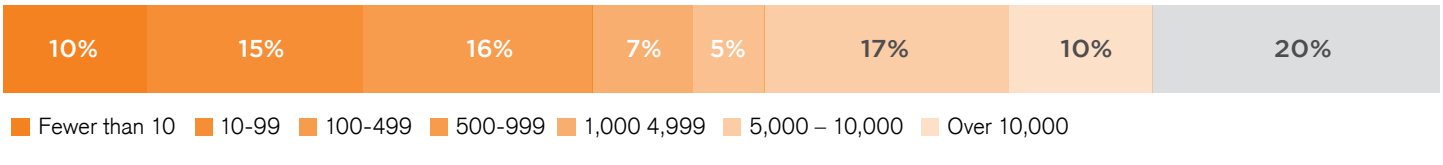
CAREER LEVEL



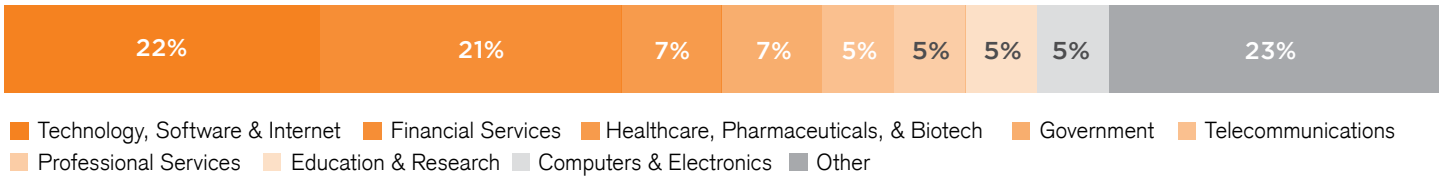
DEPARTMENT



COMPANY SIZE



INDUSTRY



SPONSOR OVERVIEW

Security Innovation | www.securityinnovation.com

Since 2002, organizations have relied on Security Innovation for our unique software security expertise to help secure and protect sensitive data in the most challenging environments - desktops, web applications, mobile devices and in the cloud.

A best in class security training, assessment and consulting provider, Security Innovation has been named to the Gartner Magic Quadrant for Security Awareness Training for four consecutive years. Security Innovation is privately held and headquartered in Wilmington, MA USA.