DARKREADING
REPORTS

April 2024

Next

How Enterprises Secure Their Applications

Organizations are boldly embracing AppSec practices and focusing on their software security posture, but age-old problems of insufficient funding and security resources — as well as a disconnect between developers and the security team — remain major roadblocks.

Sponsored by opentext™

Brought to you by informa tech

TABLE OF CONTENTS

Figures

Sponsored Content

OPENTEXT PERSPECTIVES

By Stan Wisseman, Chief Security Strategist, OpenText Cybersecurity

Emerging Challenges: The Rising Risk of API-Based Cyberattacks

Securing the gateways of digital innovation: best practices for robust API security.

The growth of cloud computing, mobile applications, and the Internet of Things has accelerated the widespread adoption of application programming interfaces. APIs are fundamental components of modern applications, empowering developers to swiftly integrate third-party services, enrich functionality, and drive innovation. Whether in extending healthcare services or powering e-commerce, APIs have become seamlessly woven into the fabric of our digital existence. Consequently, malicious actors are exploiting vulnerabilities in APIs as they conduct cyberattacks.

API-Based Cyberattacks

Here are several instances showcasing the potential risks when APIs are inadequately secured.

- **Quest Diagnostics:** A significant data breach occurred at one of the United States' top clinical laboratory service providers, Quest Diagnostics, due to a vulnerability in a third-party API. Attackers exploited this vulnerability within the third party's Web payment page, which was accessible through an exposed API. This breach led to unauthorized access to the medical records of approximately 11.9 million patients.

- **Latitude Financial:** This Melbourne-based company, offering personal loans and credit cards in Australia, faced a significant breach in March 2023, resulting in the compromise of more than 14 million records. The compromised data included nearly 8 million driver's licenses, 53,000 passport numbers, and monthly financial statements.

- **Dropbox:** In a Nov. 1, 2022, incident, cybercriminals successfully infiltrated Dropbox's internal code repositories hosted on GitHub. This unauthorized

DARKREADING REPORTS

access encompassed 130 internal code repositories, some of which held API keys and user data. The attackers executed a phishing campaign by sending deceptive emails resembling CircleCI, a widely used continuous integration/continuous delivery (CI/CD) pipeline platform. Recipients were directed to a counterfeit CircleCI webpage, where they were prompted to enter their GitHub credentials. Subsequently, they received a one-time password request, adding to the deception.

- **Peloton:** In May 2021, a security researcher discovered a vulnerability that could enable unauthenticated requests to be made to Peloton's back-end APIs, which were integral to its exercise equipment and subscription services. This allowed for direct access to Peloton API endpoints, potentially exposing substantial volumes of personally identifiable information (PII) and affecting the privacy of Peloton's customers. The Peloton Web and mobile applications, designed to complement Peloton exercise equipment, relied on these back-end APIs for offering workout statistics and class scheduling. Peloton eventually resolved the API vulnerabilities, although the extent of PII exposure for Peloton customers remains uncertain.

Strengthening API Security

As a result of increasing API-based breaches, organizations are showing a growing commitment to bolstering their understanding and control of API-related risks. Here are some API security testing tips:

- **Extensive API security assessment:** Taking a comprehensive approach to API security testing, encompassing both dynamic analysis (DAST) and static analysis (SAST), enables the detection of vulnerabilities and security flaws in APIs across various phases of the development lifecycle.
- **Authentic real-world testing scenarios:** Many APIs require authentication for accessing sensitive data or executing vital operations. Conducting tests on APIs without authentication can lead to a false sense of security. Possessing the capability to manage various API authentication methods (including multifactor authentication, or MFA), facilitating the emulation of authentic real-world situations, will enhance the accuracy and relevance of security testing.

- **Evaluation of API attack surface:** A thorough grasp of the APIs incorporated into an application enables security testers to comprehensively evaluate the application's attack surface. This ensures that no potential vulnerabilities or entry points go unnoticed.

- **Data flow analysis:** APIs hold a pivotal role in governing the movement of data within an application. SAST data flow analyzers find security issues that involve tainted data that is put to potentially dangerous use. This analysis enables the precise identification of many types of security problems

- **Evaluation of third-party risks:** Many applications depend on third-party APIs and services. The identification of these dependencies holds paramount importance for evaluating the security risks linked with third-party elements. A vulnerability or security weakness in a third-party API can directly affect the overall security of the application.

- **Assessment of secure configurations:** APIs may require specific configurations to operate securely. Assessing whether these configurations are correctly implemented helps reduce the risk of misconfigurations leading to security issues.

Conclusion

The rise of API-based cyber threats is a growing concern as APIs continue to play a pivotal role in modern application architectures. The ease of integration and rapid innovation they enable have made them indispensable in various industries, from healthcare to finance. However, this increased reliance on APIs has also made them attractive targets for malicious actors seeking to exploit vulnerabilities.

The few high-profile incidents cited in this article serve as stark reminders of the risks associated with inadequately secured APIs. These breaches have resulted in the exposure of sensitive information, emphasizing the need for robust API security measures. The need to expand the scope of application security programs to include API security is more important than ever.

About the Author: Stan Wisseman is Chief Security Strategist for North America with OpenText Cybersecurity. In the information security field for over 30 years, Stan has applied security best practices to operating systems, networks, systems, software, and organizations. Before his current position, Stan served as the chief information security officer for Fannie Mae. He has also worked in various roles for the NSA, Oracle, Cable & Wireless, Cigital, and Booz Allen Hamilton.

About the Author

Jai Vijayan
Dark Reading

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He specializes in writing on information security and data privacy topics. He was most recently a senior editor at Computerworld. He is a regular contributor to Dark Reading, CSO Online, and other security publications.

EXECUTIVE SUMMARY

Organizations continued to shore up their application security defenses in the last year in response to rising concerns over software supply chain security issues, vulnerability exploits, and other threats to application security. A high percentage of organizations adopted a formal programmatic approach to secure internally developed apps while deploying a range of other mechanisms to protect commercial, third-party, and open source applications.

Dark Reading's 2024 survey of 107 IT, security, and application development professionals shows broad improvements in enterprise patch management practices and in testing and assessing business-critical apps, third-party apps, and Web applications. The growing use of containerized applications, microservices architectures, and application programming interfaces (APIs) to connect applications and services is fueling new security concerns and attempts to address them in many organizations. A relatively small, but notable, percentage of organizations are using software bills of materials (SBOMs) for a variety of use cases, including vulnerability management, risk assessments, and incident response. Many also are ramping up efforts in identifying, assessing, and addressing risks stemming from direct and indirect code dependencies.

Most respondents appear confident about their AppSec capabilities despite several red flags such as a relative lack of focus on issues that present the biggest threats: a growing gap between IT security teams and application developers on AppSec matters and a lack of funding and resources.

Here are key takeaways from the survey:

- 44% of organizations have been practicing formal, programmatic application security for one to five years.
- 23% of respondents say their biggest application security risk is attackers with deep knowledge of application vulnerabilities.
- 72% of organizations focus primarily on securing business-critical applications.
- 55% of organizations keep up to date on patching their most important applications.
- 74% consider their dependency scanning/software component analysis (SCA) practices very or somewhat effective.

Previous Next

Table of Contents

SYNOPSIS

RESEARCH

Survey Name: Dark Reading 2024 Secure Applications Survey

Survey Date: January 2024

Number of Respondents: 107 IT, cybersecurity, and application development professionals. The margin of error for the total respondent base (N=107) is +/- 9 percentage points.

Methodology: The survey queried IT and cybersecurity professionals and app developers on the current state of application security practices at their organizations, the biggest drivers for change, and obstacles to achieving them. Respondents include individuals with job titles such as CIO, CSO, CISO, CTO, IT manager/director, and vice president of IT or of security.

Respondents were recruited via email invitations containing an embedded link to the survey. The email invitations were sent to a select group of Informa Tech's qualified database; Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

ABOUT US

Dark Reading Reports offer original data and insights on the latest trends and practices in IT security. Compiled and written by experts, Dark Reading Reports illustrate the plans and directions of the cybersecurity community and provide advice on the steps enterprises can take to protect their most critical data.

Dark Reading Reports

DARKREADING REPORTS

State of Enterprise Application Security Practices

Concerns over the safety and integrity of the software supply chain have driven a heightened focus on application security. Organizations in Dark Reading's survey seem more aware of the need to implement end-to-end controls for protecting commercial and third-party apps, internally developed applications, and open source code. Yet the adoption of containers, microservices, cloud-native, and hybrid application environments are complicating the challenge for many organizations while heightening the need for better application security.

One manifestation of the heightened focus on application security in Dark Reading's survey is the growing adoption of formal, programmatic application security practices among organizations that develop at least some applications in-house. Programmatic security integrates security into the software-development lifecycle and application code, typically in an automated and policy-driven manner. This baked-in approach emphasizes the use of formal security policies, threat modeling, continuous testing and monitoring, automated code scanning, API testing, and shifting security more to the left by addressing it earlier in the software development lifecycle.

Nearly a quarter (23%) of organizations in the 2024 survey have been using a formal, programmatic application security model for five or more years, suggesting they have a relatively high degree of familiarity with these concepts **(Figure 1)**. Forty-four percent have been on the journey for only one to five years, and 8% have been at it for less than a year. Many of these organizations likely got started in the aftermath of incidents like the breaches at SolarWinds and Kaseya — which provided the impetus for the Biden administration's May 2021 executive order on cybersecurity — and more recently, breaches like Progress Software's MOVEit file transfer software and Atlassian's Confluence collaboration platform. In fact, 58% of the respondents in Dark Reading's survey say their organizations are at higher risk of a data breach via a third-party app because of breaches like the one involving MOVEit **(Figure 2)**.

DevSecOps models that integrate security practices into DevOps methodologies are a critical component of a programmatic application security environment. Nearly seven in ten organizations in Dark Reading's survey have implemented a DevSecOps approach to

Figure 1.

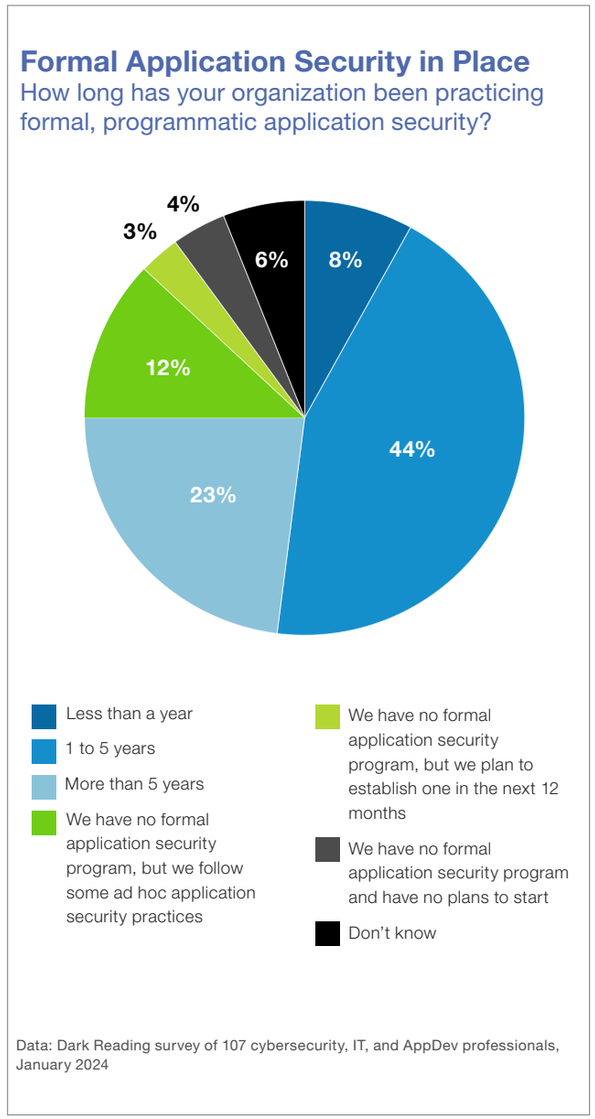


Figure 2.

Risks Evolving Over Time

How has the risk of third-party and supply chain compromises evolved over time for your organization, compared with other attack vectors?

	Significantly greater risk than one year ago	Slightly increased risk than one year ago	The risk is about the same as a year ago	The risk is less than a year ago	The risk is significantly less than a year ago	Not sure/not applicable
Attack via a third-party software component/dependency	29%	29%	25%	5%	2%	10%
Attack via a business application such as Microsoft Exchange	20%	29%	29%	7%	2%	13%
Attack via a breach at a cloud provider/platform	19%	35%	28%	1%	7%	10%
Attack via a poorly secured or weak API	18%	31%	29%	4%	5%	13%
Attack via a breached security tool	14%	28%	32%	8%	6%	12%
Attack via a compromised developer platform	12%	27%	35%	9%	3%	14%
Attack via a compromised IT platform	11%	30%	37%	6%	6%	10%

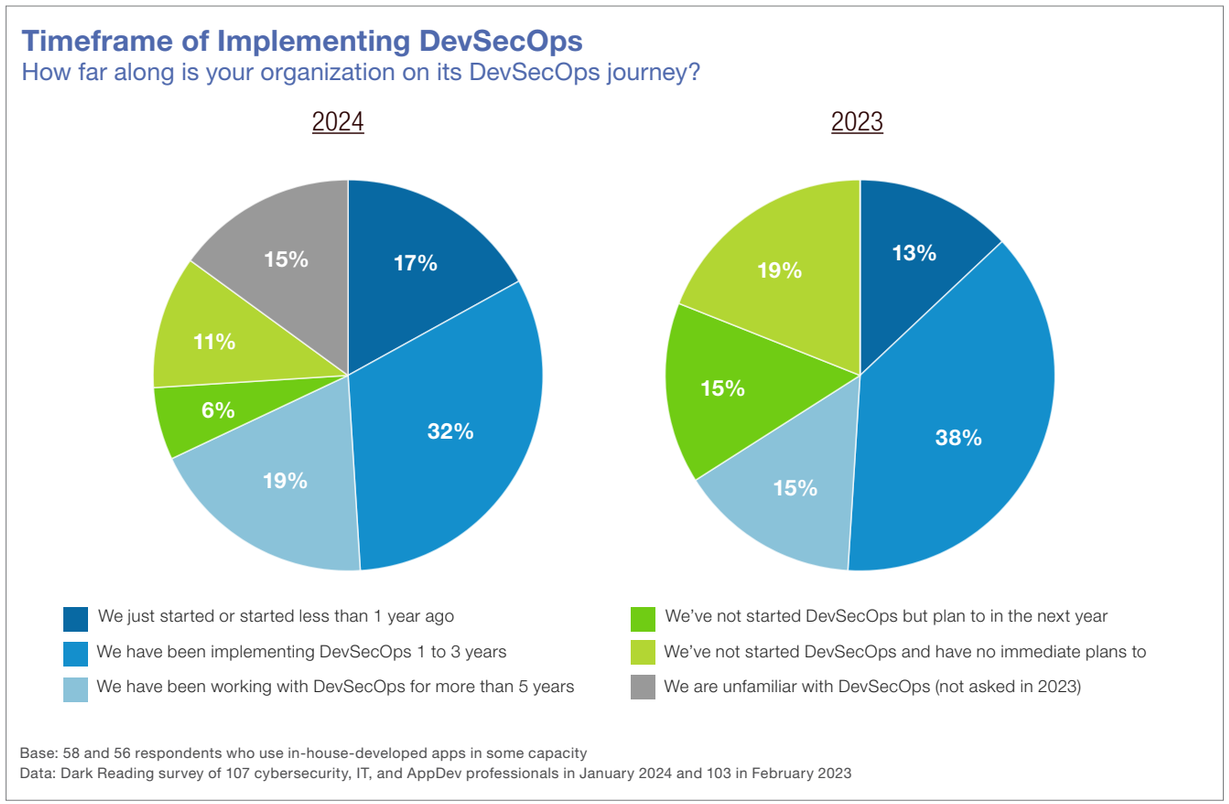
Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

application development, with some further along in the journey than others **(Figure 3)**. Nearly one-third (32%) have been implementing DevOps for one to three years, 19% have been doing so for more than five years, and 17% either just started or have been at it for less than one year. In total, 68% of organizations that develop application software in-house, up slightly from 66% last year, have made security an integral part of their software-development lifecycle.

Security experts have long advocated DevSecOps as key to reducing application vulnerabilities and risk, and 75% of organizations have implemented the practice for precisely that reason **(Figure 4)**. However, other factors are driving enterprise adoption of DevSecOps. Fifty-three percent of organizations, for instance, expect that implementing DevSecOps will help them improve business agility; 36% are doing it to meet compliance requirements; and 31% to drive down costs. The 11% of organizations in Dark Reading's survey that have no immediate plans for DevSecOps attribute their decision to a lack of DevOps and security skill sets — and the lack of a need for it due to the customized nature of their application environment.

The increased focus on internally developed applications is only part of the story. Almost all organizations use a mix of commercial off-the-shelf apps and third-party (contractor) developed applications as well, some to a greater degree than others. A plurality of 41%, for instance, employ a mix of off-the-shelf software and in-house-developed apps, while 40% rely entirely or very heavily on commercial apps because they do little or no in-house application development **(Figure 5)**. Fourteen percent of respondents say they only use commercial software for commodity functions, while relying on internally developed apps for key business needs.

Figure 3.

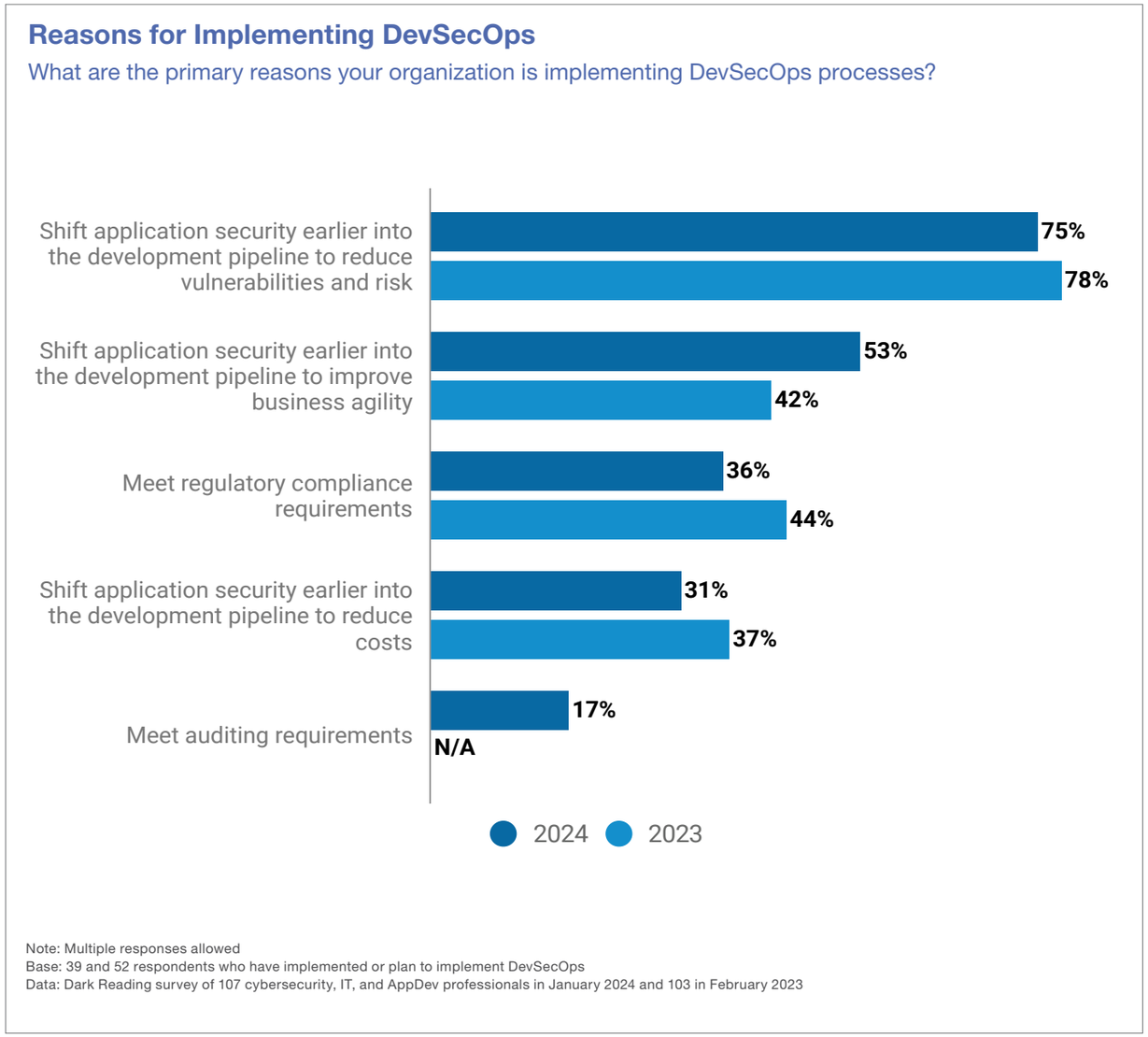


Over the past 12 months, IT, AppSec, and application development teams have bolstered security around commercial and third-party apps on a variety of fronts. This includes improved patching practices, greater use of Web application firewalls, and more regular testing and monitoring of third-party software, Web applications, and business-critical apps in general.

More organizations, for instance, have kept their business-critical commercial apps up to date with the latest patches over the past year, compared with the previous two years. Fifty-five percent of respondents in Dark Reading's 2024 survey claim their organizations apply important patches promptly after the vendor releases them. That number is up slightly from 53% in 2023 and notably from 46% in 2022. Paradoxically, though, the percentage of organizations that failed to keep up with the latest patches — though smaller — increased as well. This year, 31% express concern that they occasionally fall behind on their patching, an increase from 27% in 2023., However, this year, only 9% say their organizations are at risk because they are frequently behind on installing critical patches; that figure is unchanged from 2023. **(Figure 6)**.

The percentage of companies falling behind on their patches, even occasionally, is concerning because research has shown that unpatched vulnerabilities are often the cause of data breaches and are a favored attack vector for threat actors. Research that Cisco conducted last year showed that many of the vulnerabilities that attackers targeted frequently in 2023 were old flaws, including some that were more than 10 years old. In fact, nine of the ten most frequently targeted flaws in 2023 were from 2017 or prior years. Unpatched vulnerabilities are also a major contributor to enterprise security debt — or the backlog of security

Figure 4.

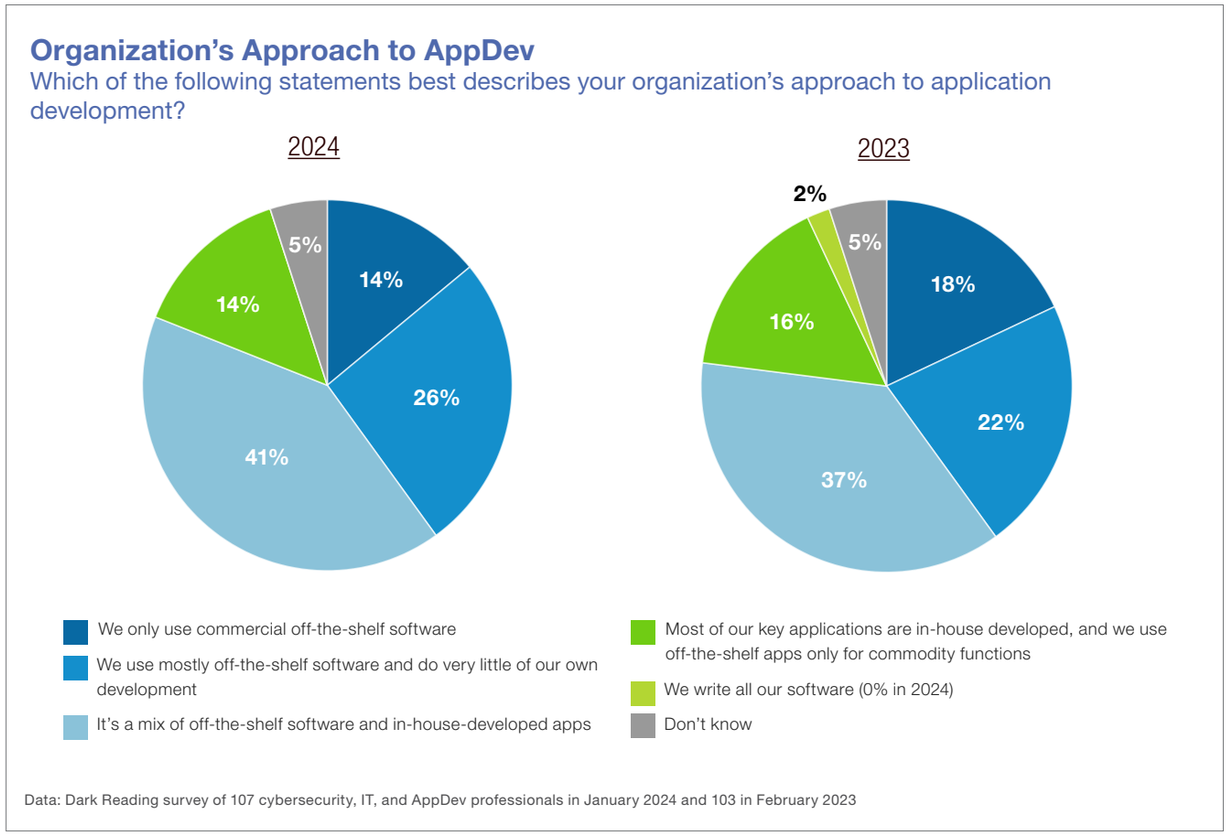


work that an organization needs to address to reduce cyber-risk. A study by Veracode found security debt stemming from unpatched vulnerabilities was present in a startling 42% of enterprise applications.

Over the past year, more organizations also have ramped up the use of Web application firewalls (WAFs) to protect key applications against threats. Twenty-one percent, up from 19% in 2023 and 14% in 2022, rely heavily on WAFs to protect against application vulnerabilities in lieu of patching **(Figure 7)**. While security analysts consider this a less-than-optimal practice, WAFs have proved useful as an application risk mitigation measure when deployed as part of a layered defense strategy. Many organizations have resorted to using WAFs in place of patches due to the complexity involved in finding and applying patches constantly across the enterprise application environment. Thirty percent of organizations, up from 21% in 2023's survey, used WAFs as a temporary precaution while they worked to patch vulnerable systems.

Continuous assessment and testing of business-critical, Web, and public cloud apps for security issues has been another major

Figure 5.



focus for many organizations over the past 12 months. Forty-six percent of organizations monitor and assess business-critical apps for security issues on a continuous and ongoing basis, and 16% do so at least once every month **(Figure 8)**. Similarly, 54% either always or often conduct security tests on Web and public cloud applications, and another 27% do so at least sometimes **(Figure 9)**. Nearly half (47%) perform similar tests on commercial apps that employees use, and 44% do the same with open source applications.

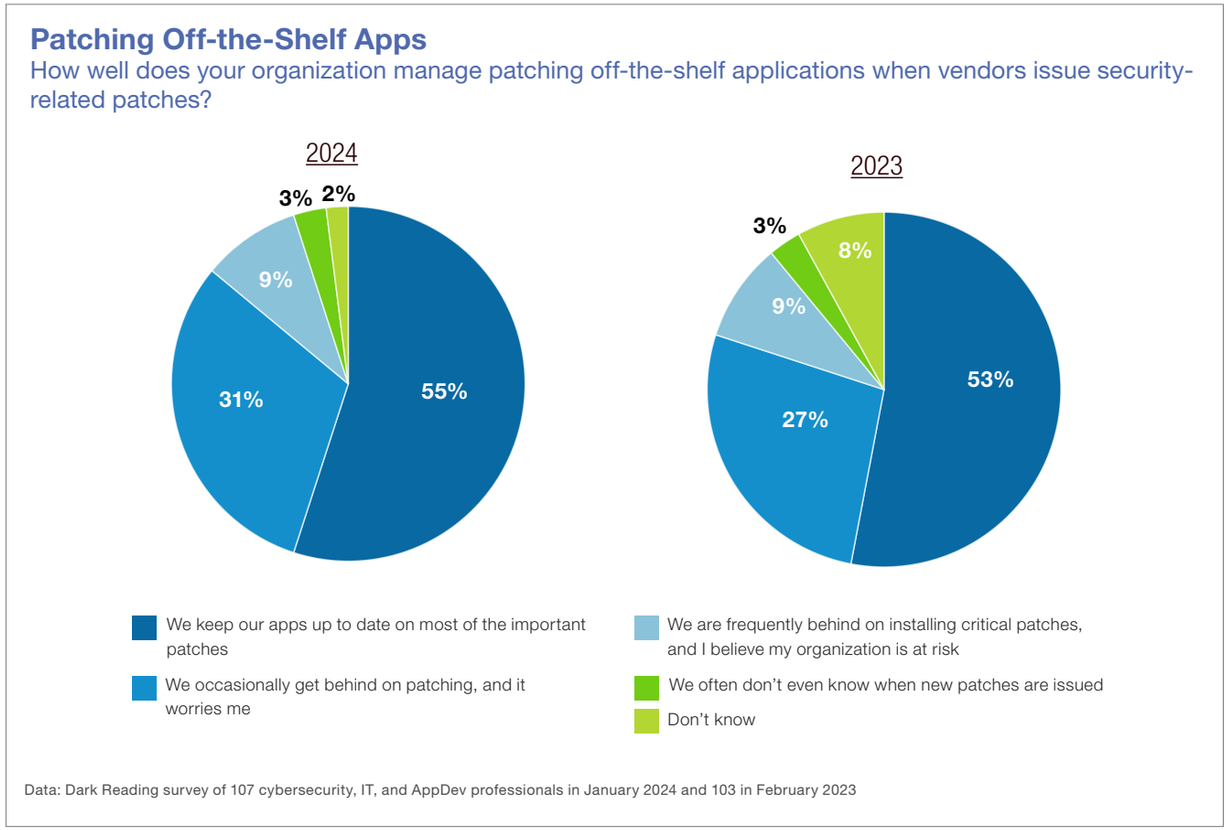
How Enterprises Respond to Emerging AppSec Challenges

The rising adoption of container technology fuels additional security concerns for stakeholders in enterprise application security. Nearly one-third (32%) of organizations using internally developed apps to some extent have used containerized applications frequently over the past 12 months, and 30% have done so infrequently **(Figure 10)**. More than one-fifth (21%) expect to deploy applications in container environments in the coming 12 months. If that pattern holds, more than eight in ten organizations will have containerized application environments by year-end.

Containers offer some security benefits, the primary one being application isolation. However, they also present a Pandora's box of security issues that organizations need to be cognizant of and address.

For 50% of the IT, security, and application development professionals in Dark Reading's survey, the biggest concern has to do with image vulnerabilities tied to the use of insecure libraries and other dependencies **(Figure 11)**. Vulnerable images give attackers a way to break out of a container and escalate privileges on the

Figure 6.

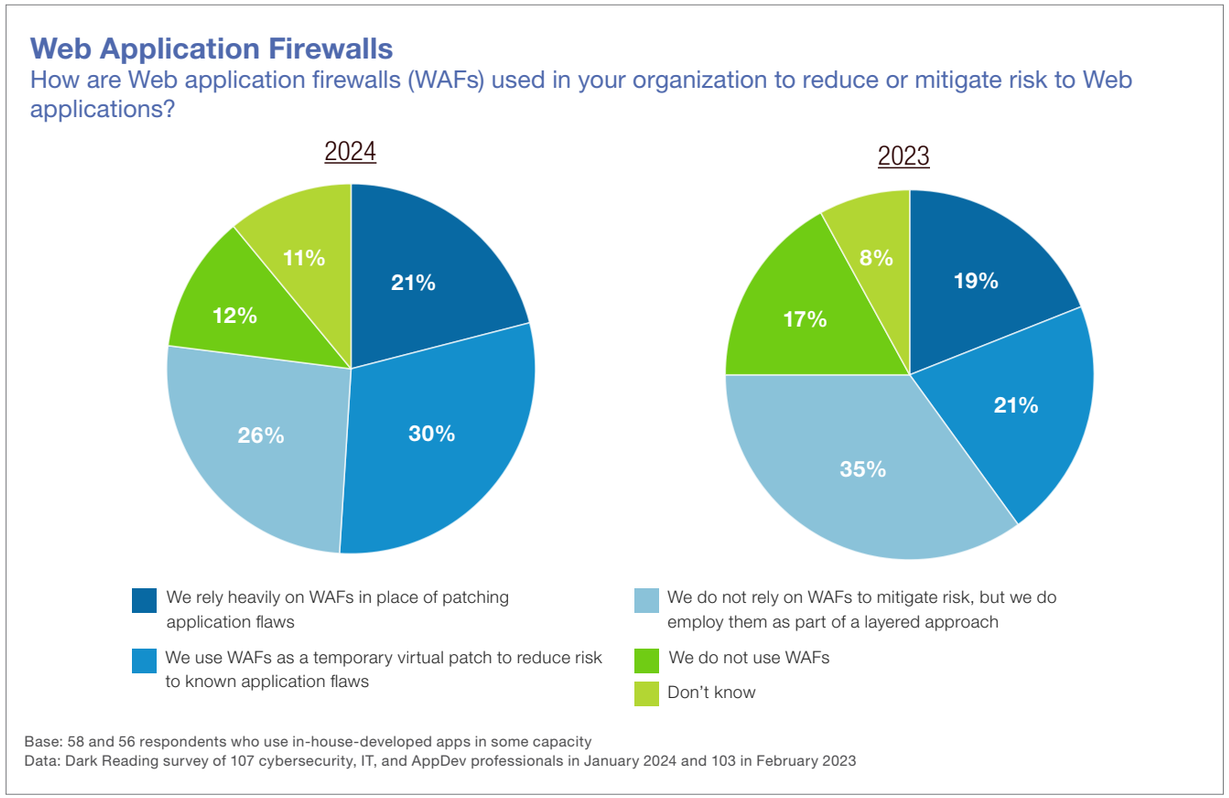


underlying host, to inject malicious code, access sensitive data and secrets, and carry out other malicious activity. Forty-three percent worry about application vulnerabilities leading to a container takeover and 39% about the risks associated with unchecked communications between computers. Thirty-six percent say containers put their continuous integration/continuous deployment environment at risk; 30% fear a container registry compromise; and 57% are concerned about cyberattacks that leverage the complexity and density of microservices.

Such worries have led to a broader reassessment of container security at many organizations. A survey by DZone last year found the percentage of organizations that perceived containers as improving application security fell sharply from 69% to 51% over the course of two years. Forty-four percent feel that the use of containers heightened application risks, up from just 7% a year ago.

Forty-nine percent of organizations have used container-specific monitoring tools to mitigate container risks over the previous 12 months **(Figure 12)**. These tools (from vendors such as Sysdig, Aqua, and Dynatrace) enable visibility into container processes, communications, vulnerabilities, suspicious activity, and other metrics. Thirty-five percent have deployed orchestration management tools to address security risks in their container environment, and 23% have used immutable (or unmodifiable) containers to maintain a known good state and to mitigate risks tied to configuration drift and unapproved changes. Other steps deployed by a high percentage of organizations in the past year for limiting container-related AppSec risks include limiting use of privileged containers (28%), using only trusted sources for images (37%), and implementing application programming

Figure 7.



interface (API) access controls on microservices (also 37%).

Somewhat troublingly, though, a focus on securing application programming interfaces continued to decline over the past year. API security has become critically important because organizations have begun using APIs extensively to open access to internal and external applications and services. Their role in fueling the digital economy makes them a popular target for attackers. A startling 94% of respondents in a survey by Salt Security last year said their organizations experienced an API-related attack in the year prior to the survey; 31% experienced a sensitive data exposure from these attacks; and 17%, a full-fledged data breach. Yet a mere 18% of organizations in Dark Reading's survey have a formal process for evaluating API security — and that's down from 20% last year and 24% in 2022 **(Figure 13)**. Only 36% this year, down from 46% in 2023, report treating API security the same as Web application security — something that analysts recommend. Nearly one in five (18%) don't perform any API security testing at all.

Software bills of materials (SBOMs) have become an essential component of application vulnerability management and for several other use cases, such as incident response, verifying open source license compliance, and risk assessment. Many security analysts liken it to a list of ingredients — or of all the open source and third-party components — that go into building an application. SBOMs provide information such as the name and version of each library, framework, and module in a software package; its origin and source; direct and indirect dependencies; license information; and other data. A Biden administration 2021 executive order requires federal agencies to obtain SBOMs from all software vendors and contractors from whom they purchase applications. Increasingly,

private companies have been requiring the same and are building SBOMs for the software they develop internally.

Dark Reading's survey data suggests that SBOMs are still just taking root at many organizations. Less than one in four organizations (23%) have used an SBOM for patch management in the last year, 22% for risk assessment, and 18% to identify vulnerabilities in the application environment **(Figure 14)**. A smaller percentage have leveraged SBOMs for continuous monitoring (16%), dependency tracking (14%), regulatory compliance (14%), component verification (12%), and incident response (12%). Other surveys, though, uncovered higher adoption rates, such as one from Sonatype that pegged the number at 76% who currently maintain an SBOM and 16% that plan to do so shortly.

Similarly, Dark Reading's survey found a low adoption of dependency-tracking practices among organizations. Fewer organizations than last year — 29%, versus 35% — require each developer or project to keep track of their own dependencies **(Figure 15)**. Similarly, just 38%, down sharply from last year's 52%, maintain a centralized repository with authorized dependencies for all projects. Twenty-four percent maintain a local repository to which anyone can add dependencies, and 20% have projects that can generate an SBOM. As with the other dependency-related metrics, those two numbers are lower than last year. The data suggests that many organizations are still at high exposure to threats like the Apache Log4j vulnerability, which many organizations found hard to fix because they could not find the vulnerable component in their application stacks.

The Drivers and Hurdles for Real Change

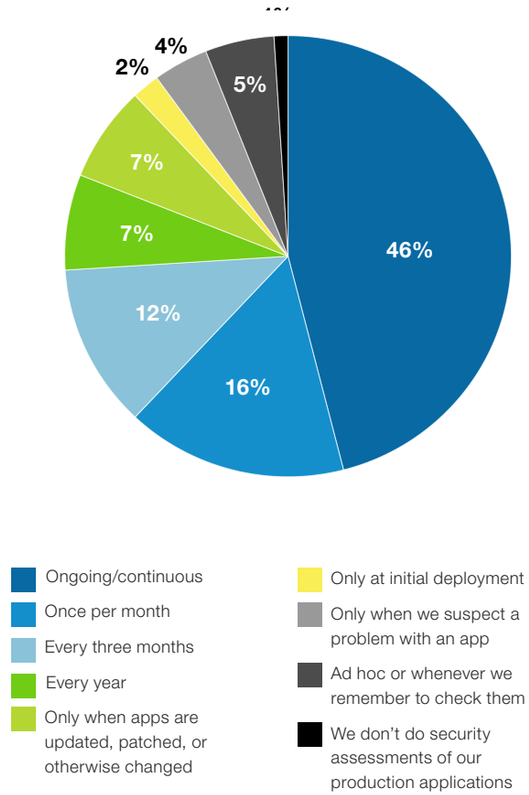
Multiple factors are driving the heightened focus on application security. The biggest concern for many organizations is the security of open source components and the security of APIs **(Figure 16)**. There also appears to be a high level of apprehension over both the accuracy and depth of the security testing practices that organizations use and the threats to cloud native applications.

A substantial percentage of organizations appears to be bolstering their AppSec practices due to a shortage of security staff, the widespread presence of open source code in their applications, and worries about attackers with deep knowledge of application flaws. When asked to check off their greatest pain

Figure 8.

Assessing Business-Critical Apps

How often does your organization thoroughly assess the security of its business-critical applications?



Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 9.

Testing Third-Party Applications

How often does your organization test the following application types for security flaws?

	Always perform security testing	Often perform security testing	Sometimes perform security testing	Do not perform security testing	Limited access/visibility to test	N/A
Web or public cloud applications used by employees	23%	31%	27%	10%	5%	4%
Web or public cloud applications used by customers/partners	21%	21%	22%	15%	13%	8%
Off-the-shelf applications used by employees	18%	29%	31%	11%	8%	3%
Open source applications	16%	28%	32%	12%	3%	9%
Off-the-shelf applications used by customers/partners	15%	28%	22%	15%	13%	7%

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

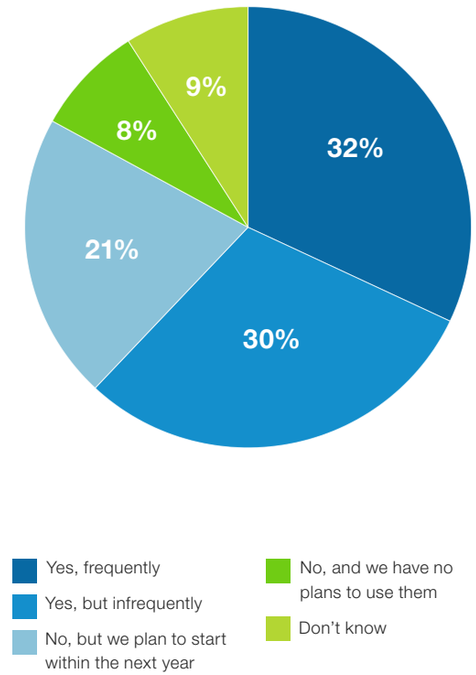
points regarding application security, 23% of respondents cite attackers with deep knowledge of application vulnerabilities, 20% inadequate security staff, and 19% frequent use of open source code libraries **(Figure 17)**. Less-cited risks to application security include inadequate security tools, security-illiterate developers, poor-quality application code, and misconfigured tools and systems.

Fears about attackers scanning code to find exploitable vulnerabilities have grown, with 50% of respondents pinpointing it as the biggest source of concern with application security **(Figure 18)**. Forty-four percent of organizations have shored up app security to mitigate threats to intellectual property, 41% to make it harder for threat actors to find and abuse keys and other credentials, and 39% to guard against the potential for a malicious actor to add an unauthorized package or component to an application. A substantial number are also concerned about attackers introducing malicious code into apps (35%) or hijacking a software-update mechanism —SolarWinds-style — to push out malware (28%).

Figure 10.

Use of Containers

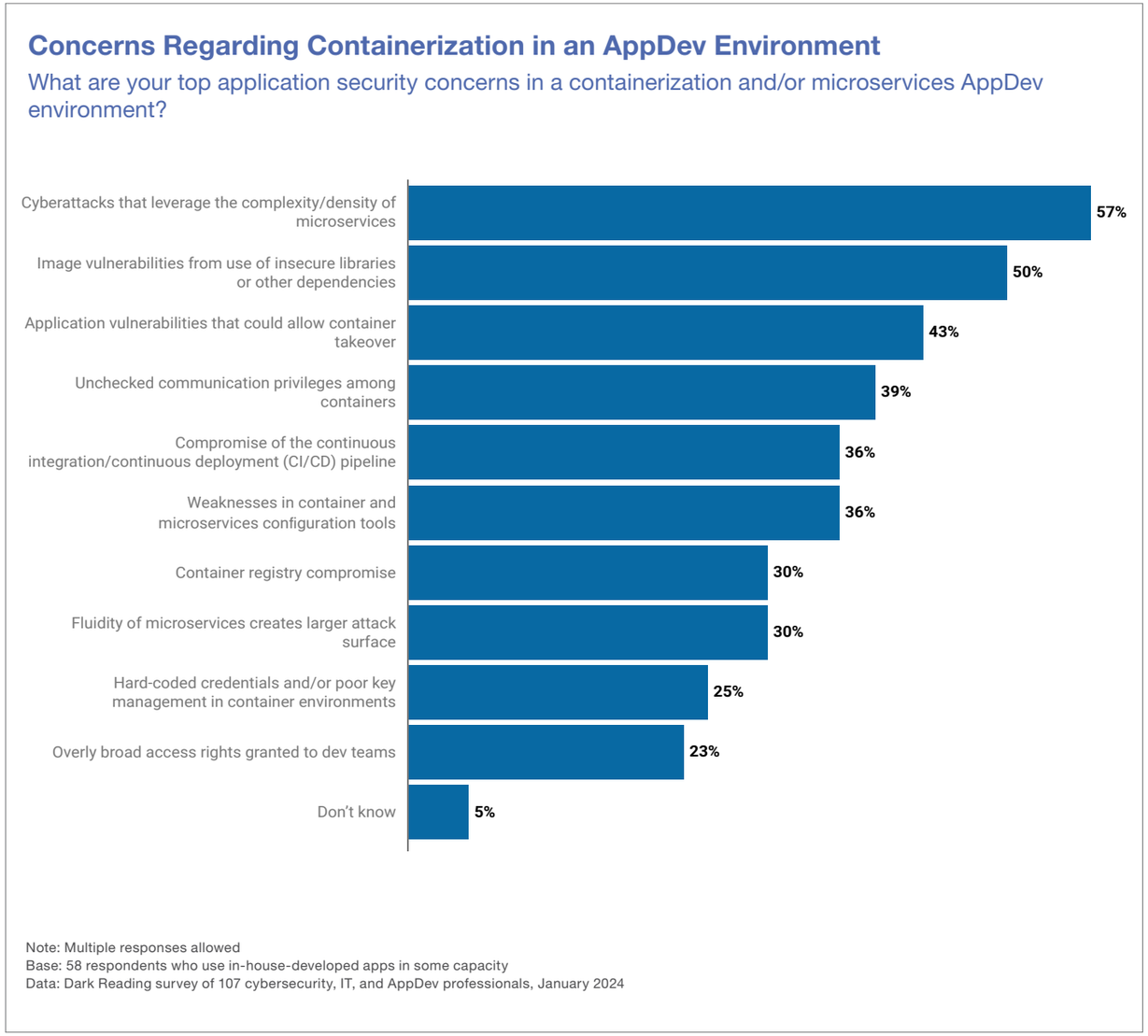
Does your organization use containers and microservices as part of its overall application development and deployment approach?



Base: 58 respondents who use in-house-developed apps in some capacity

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 11.

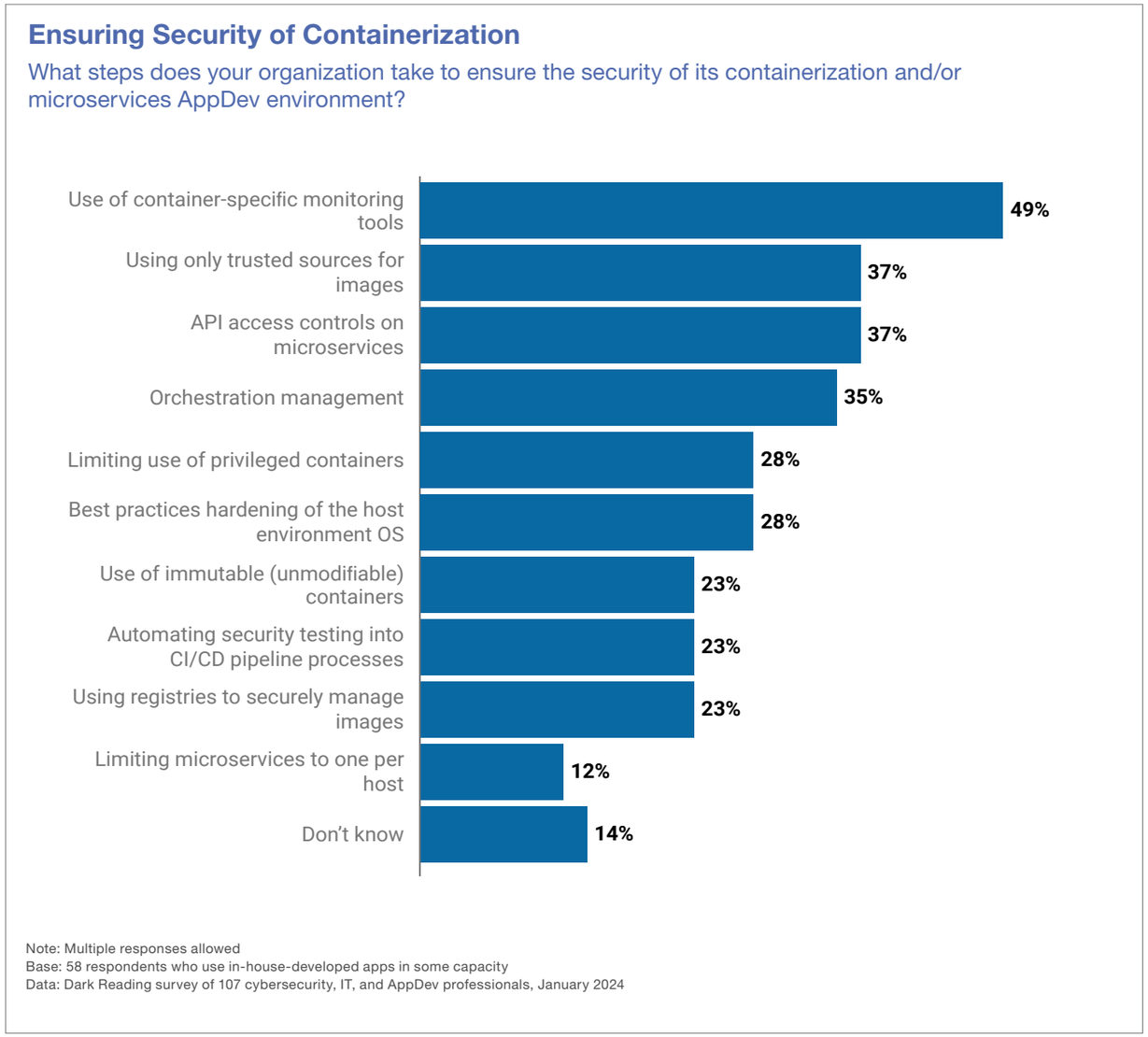


Breaches like the one involving Progress Software's MOVEit platform and numerous recent mass attacks on Microsoft Exchange Server vulnerabilities had a big influence on attitudes toward application security as well. Fifty-eight percent perceive attacks via trusted software suppliers such as Progress as increasing their risk exposure, 49% feel the same about attacks via business apps such as Microsoft Exchange, and 54% about breaches via a cloud provider or platform.

Even so, most of the information security and application developers in Dark Reading's survey (63%) express confidence in their organizations' ability to prevent compromises via the software supply chain; 59% feel the same about their ability to detect a supply chain compromise; and 50% say they have the necessary capabilities to ensure a secure software supply chain **(Figure 19)**.

Much of that confidence appears tied to a perceived effectiveness of the mechanisms that organizations have deployed to detect, monitor, and assess application security. Eighty-two percent of organizations that have conducted manual penetration tests on their applications feel those tests were highly effective at rooting out vulnerabilities in the environment **(Figure 20)**. Penetration testing is a requirement

Figure 12.



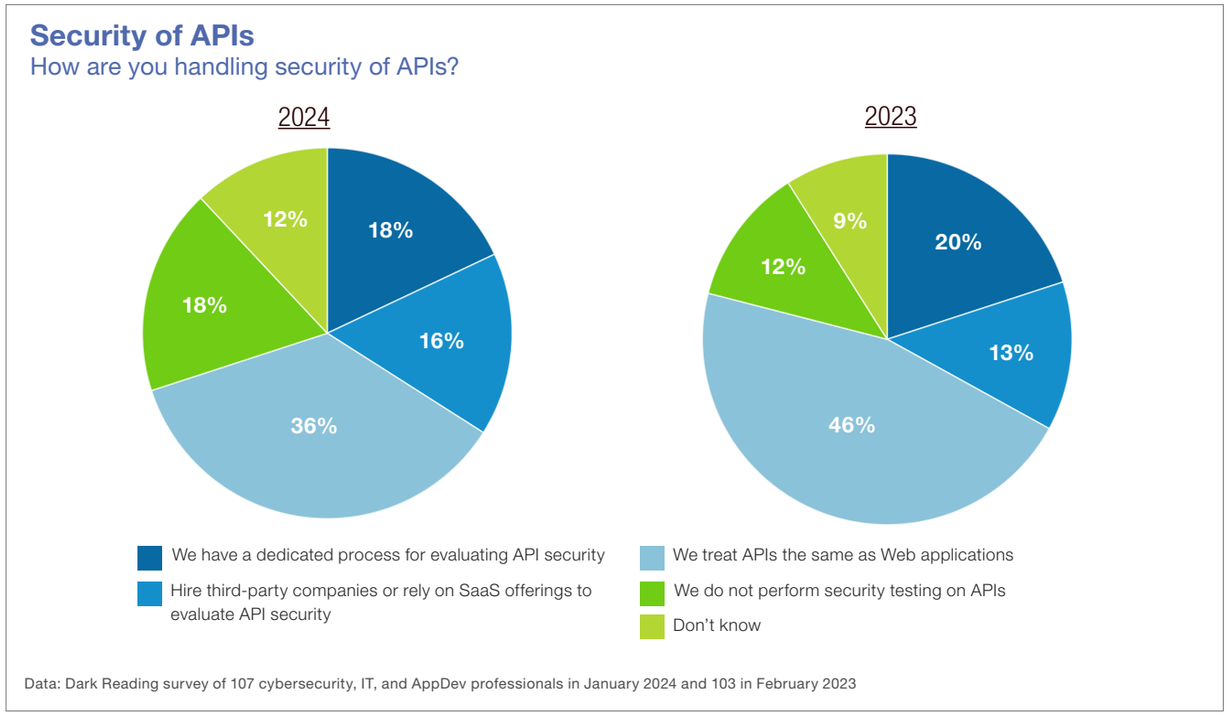
for regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and the EU's General Data Protection Regulation (GDPR). When done correctly, they can help organizations detect a range of vulnerabilities they might have missed otherwise. But when done incorrectly, they can cause damage and create a false sense of security.

Eight in ten organizations consider their static (80%) and dynamic (also 80%) AppSec testing processes effective. Similarly, 80% express confidence in the ability of their anomaly-detection tools to unearth application security issues. Seventy-five percent have high confidence in their dependency scanning/software component analysis (SCA) capabilities.

Dark Reading's survey also uncovered some potential red flags that suggest some of the confidence might be based on somewhat shaky ground.

First, there appears to be a growing disparity in knowledge of application security issues among information security teams and application developers. Nearly three-fourths (73%) of survey respondents consider the IT security team at their organizations "knowledgeable" or "very knowledgeable" on AppSec, and

Figure 13.



another 23% describe them as "somewhat knowledgeable" on those matters **(Figure 21)**. Those data points are notably higher than in Dark Reading's previous survey. At the same time, the percentage of application developers with very good knowledge of application security declined to 18% this year from 22% last year, and the percentage of those considered "somewhat knowledgeable" on AppSec dropped in that interval to 51% from 57% **(Figure 22)**.

Nearly double the proportion of respondents — 30% in 2024, versus 17% in 2023 — say their application developers are "not very knowledgeable" or "not at all knowledgeable" on AppSec matters.

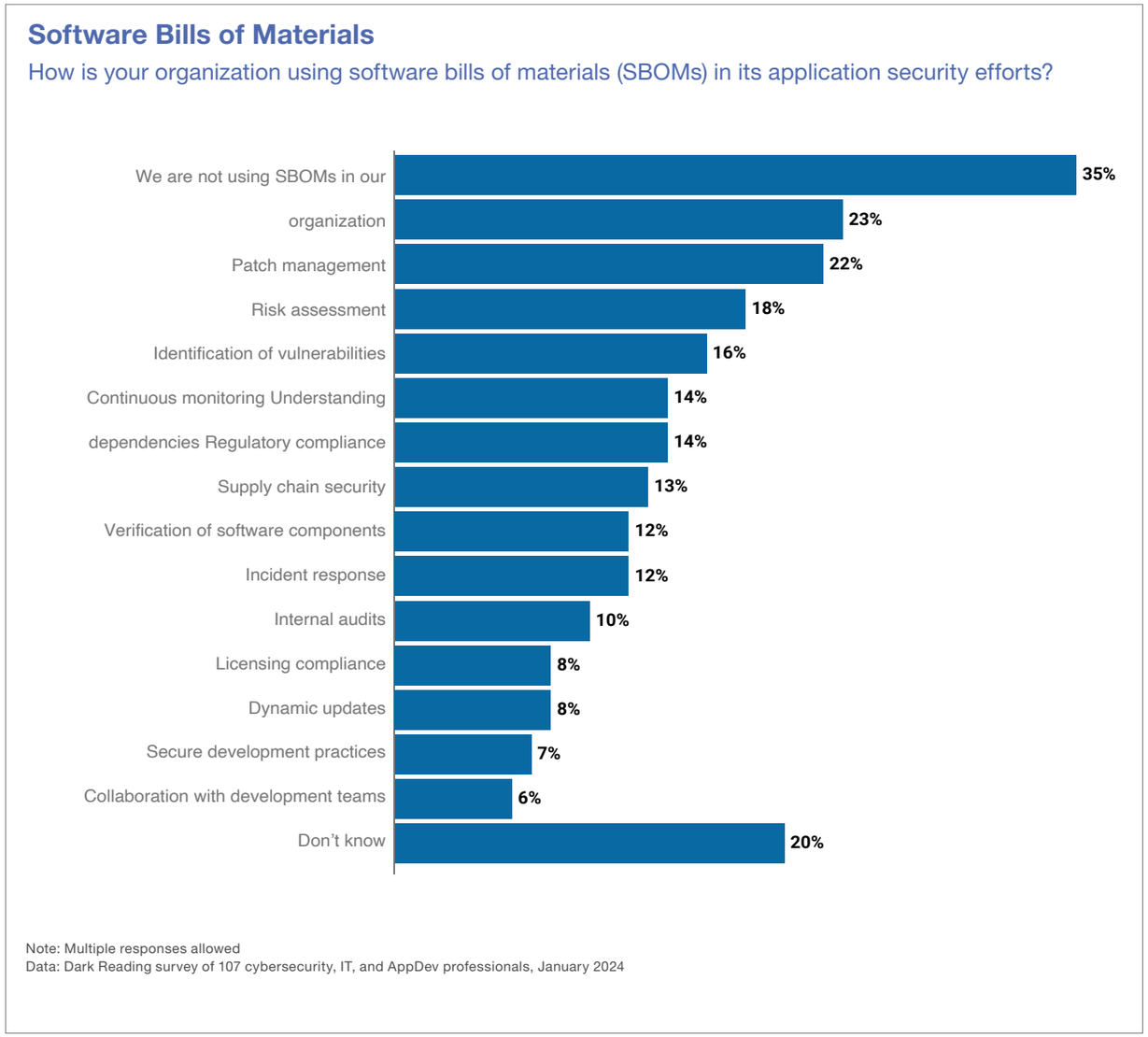
Our survey also reveals a troubling contradiction regarding the application categories that security teams mainly prioritize, compared with the applications they view as posing the greatest security threats to the organization. Nearly half (47%) say legacy applications present the biggest security risk to the enterprise (**Figure 23**).

The data suggests that many organizations are likely not paying the attention they should to legacy application environments. Older apps traditionally have been popular targets because they are based on outdated architectures and don't receive regular security updates and support. Often legacy apps are not visible to modern IT management tools.

The survey shows other contradictions in what companies focus on and what they see as the greatest application security risks. Although 72% cite business-critical applications as the category into which they are putting most of their security focus, only 27% say these apps pose the biggest security risk to their organizations. Forty-six percent of organizations thoroughly assess the security state of their business-critical applications continuously, 16% do so at least once every month, and another 12% once in three months.

A similar pattern appears in other application

Figure 14.

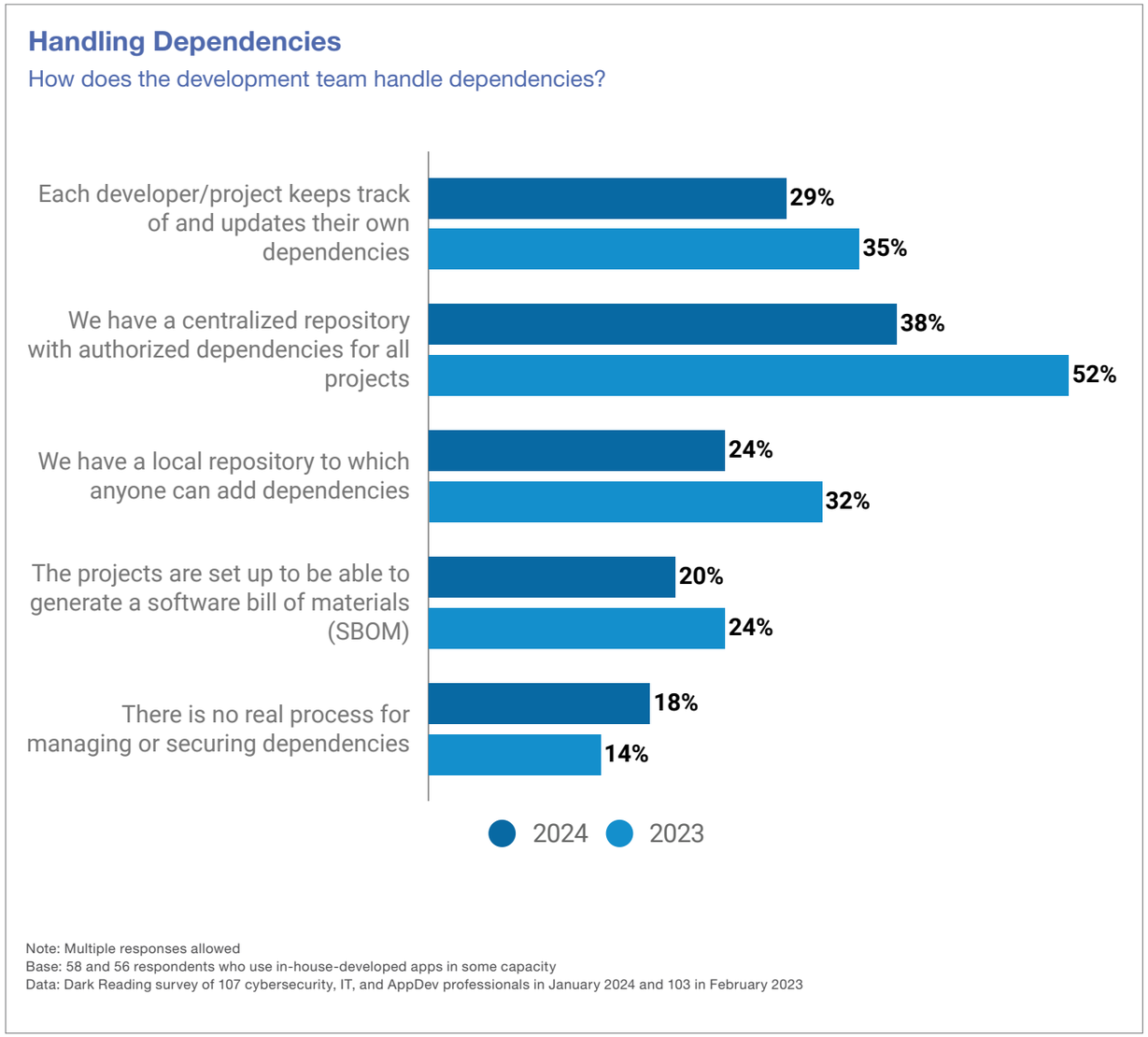


categories. More than six in ten organizations (65%) have made Web applications their top focus, and 61% have done so with cloud applications, while 35% say Web applications present the biggest risk and 26% point to cloud applications. However, one area of greater risk — third-party apps, with 41% — was a primary focus for 43% of respondents.

A similar pattern appears in other application categories. More than six in ten organizations (65%) have made Web applications their top focus, and 61% have done so with cloud applications, while 35% say Web applications present the biggest risk and 26% point to cloud applications. However, one area of greater risk — third-party apps, with 41% — was a primary focus for 43% of respondents.

Challenges to implementing application security programs at organizations include a lack of funding and security skills. Forty-three percent of organizations over the last year had to contend with inadequate funding and management support for application security initiatives; 33% did not have the technical resources to secure their production apps properly; and 32% had to deal with inadequate security skills **(Figure 24).**

Figure 15.



Conclusion

A high percentage of organizations have adopted formal and programmatic application security practices to address concerns over supply chain security, vulnerability exploits, and other threats to software security. IT, security, and application development teams have ramped up security efforts around internally developed applications, commercial and third-party software, and open source components.

Dark Reading's survey shows that more organizations than last year have adopted DevSecOps practices and improved their patch management capabilities. In addition, they are conducting more testing, monitoring, and assessments of their business-critical, third-party, and Web applications.

Most respondents appear confident about their application security posture. However, the survey shows a disconnect between what IT and security leaders perceive as the biggest app security risks and on what they are focusing. A lack of funding and security skills as well as a gap in application security knowledge between developers and IT security teams are undermining some of the progress organizations made last year.

APPENDIX

Figure 16.

Ranking Vulnerabilities

Where do you feel your organization is most vulnerable?.

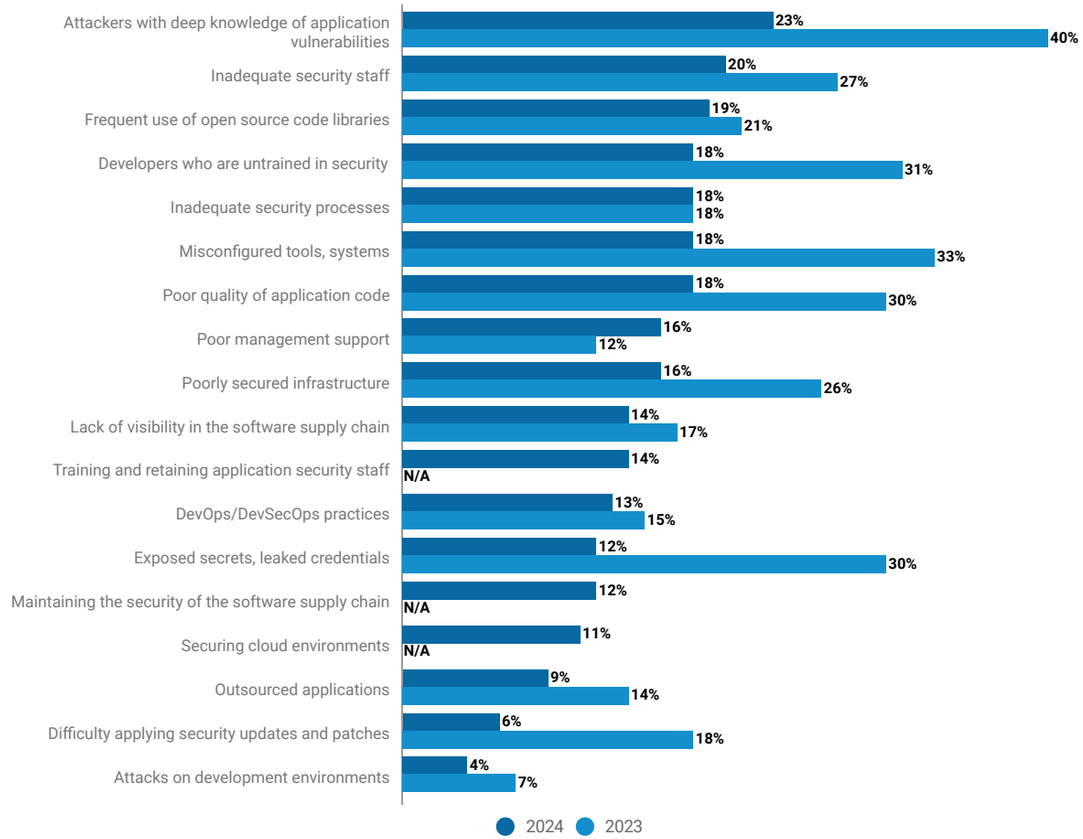
	Overall rank	Score
Security of open source components used in our code	1	247
Security of our APIs	2	232
Accuracy and depth of our security tests	3	228
Cloud-native applications	4	201

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 17.

Greatest Risks to Application Security

Which of the following are the greatest pain points when it comes to the security of applications (both third party and in-house developed) in your organization?



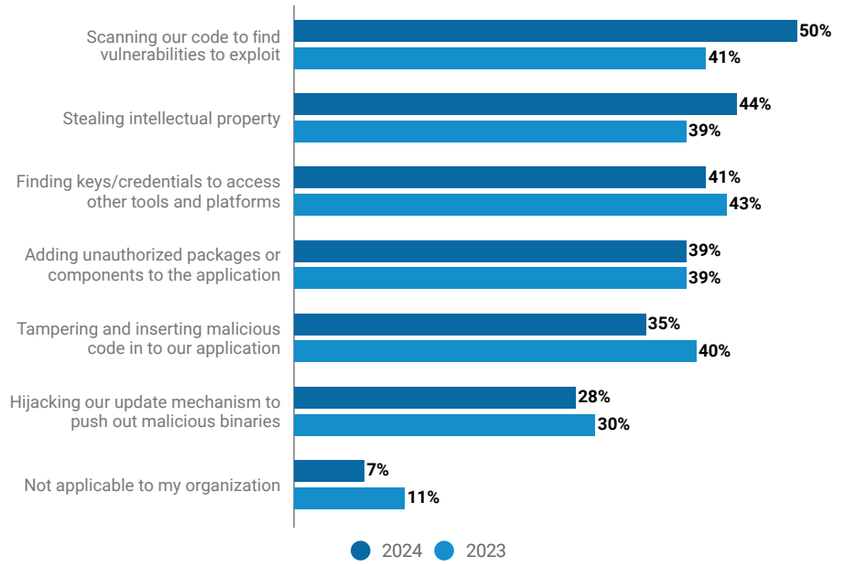
Note: Maximum of three responses allowed
Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals in January 2024 and 103 in February 2023

DARKREADING REPORTS

Figure 18.

Attacks on Source Code and Apps

Attackers are increasingly targeting source code and applications. Which of these issues are of concern to your organization?



Note: Multiple responses allowed
Base: 58 and 56 respondents who use in-house-developed apps in some capacity
Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals in January 2024 and 103 in February 2023

Figure 19.

Software Supply Chain

Rate your agreement with the following statements about the software supply chain.

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree	Don't know
My organization will be able to detect and respond to a software supply chain compromise	16%	43%	23%	12%	6%
My organization has the necessary knowledge and expertise to ensure a secure software supply chain	14%	36%	22%	14%	14%
My organization's existing defenses are effective at preventing software supply chain compromises	10%	53%	22%	5%	10%

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 20.

Effectiveness of Application Security Assessments

Rate the effectiveness of the application security assessments used by your organization.

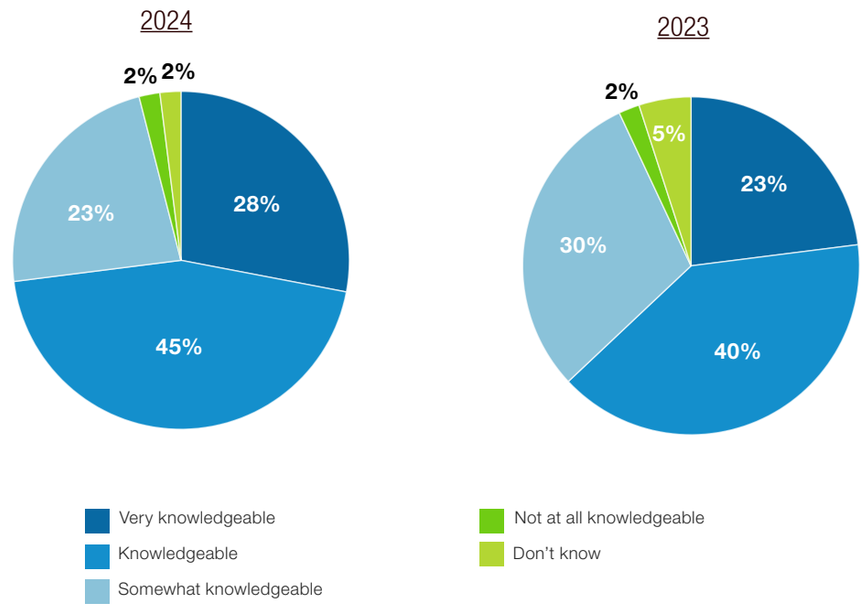
	Very effective	Somewhat effective	Not effective	Not used
Dependency scanning/software component analysis (SCA)	33%	41%	14%	12%
Manual application penetration testing	29%	53%	6%	12%
Dynamic code scanning/dynamic application security testing (DAST)	22%	58%	2%	18%
Static code scanning/static application security testing (SAST)	22%	58%	6%	14%
Mobile application security testing (MAST)	19%	38%	6%	37%
Interactive application security testing (IAST)	18%	41%	8%	33%
Anomaly detection tools	18%	62%	6%	14%

Base: 58 respondents who use in-house-developed apps in some capacity
Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 21.

Security Team's Knowledge About Emerging App Vulnerabilities

How knowledgeable is your security team about new and emerging application vulnerabilities security researchers are disclosing?

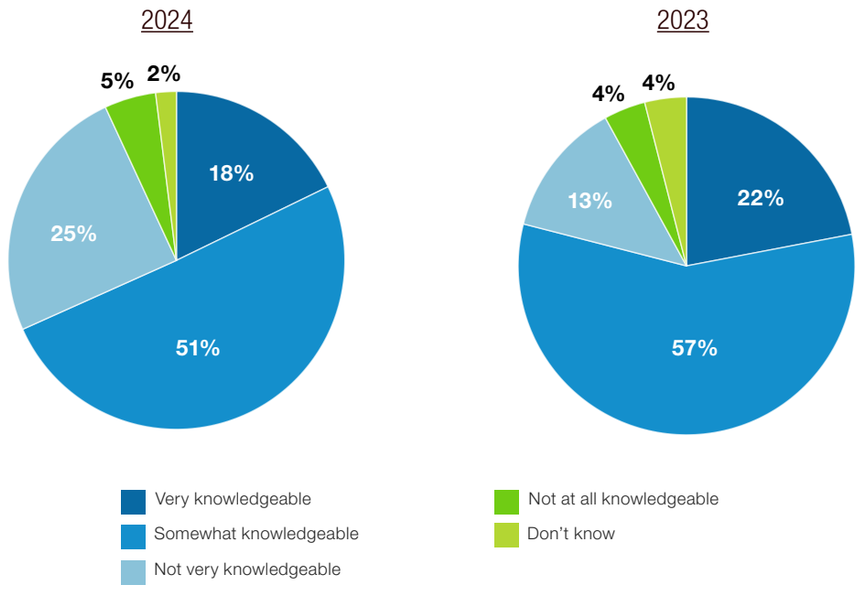


Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals in January 2024 and 103 in February 2023

Figure 22.

Application Developers' Knowledge About Security

When it comes to application security, how knowledgeable is the average application developer in your organization?



Base: 58 and 56 respondents who use in-house-developed apps in some capacity
Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals in January 2024 and 103 in February 2023

Figure 23.

Organizations' Focus on Top Security Risks

Which of the following application areas does your organization primarily focus on, and which pose the biggest security risks to your organization?

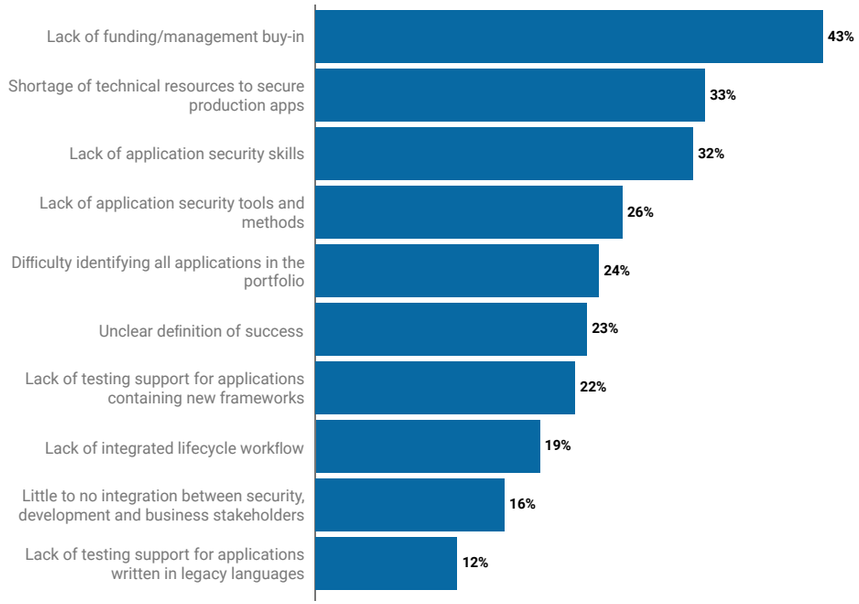
	My organization primarily focuses on these areas	Biggest security risks to my organization today
Business-critical applications	72%	27%
Web applications	65%	35%
Cloud applications	61%	26%
Legacy applications	47%	47%
Third-party applications	43%	41%
Mobile applications	38%	25%
Open source applications	30%	24%
Embedded (device-specific) applications	29%	16%

Note: Maximum of three responses allowed in each column
Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 24.

Obstacles to Application Security Program

What would you say have been the biggest obstacles to implementing an application security program in your organization? ?



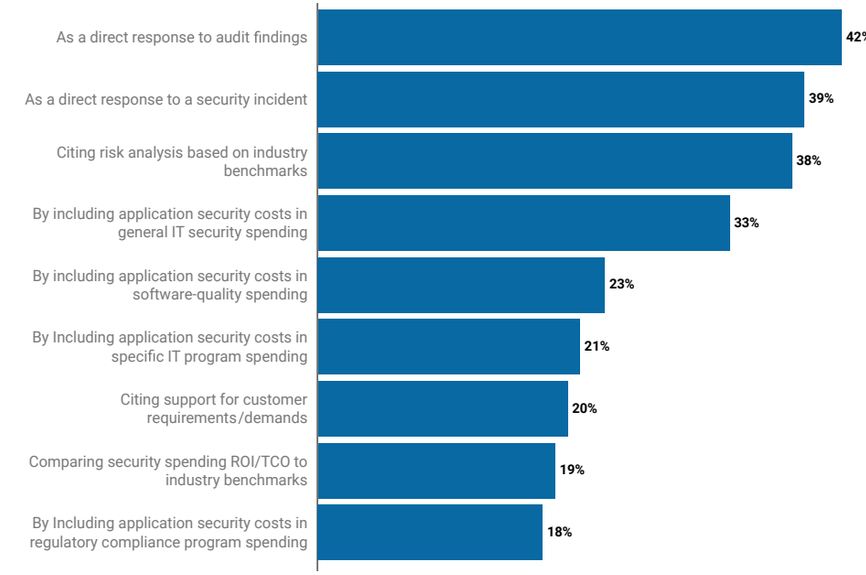
Note: Multiple responses allowed

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 25.

Justifying Application Security Spending

How does your organization justify its application security program spending?



Note: Multiple responses allowed

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 26.

Application Security Tools

Rate your level of agreement with the following statements about application security tools.

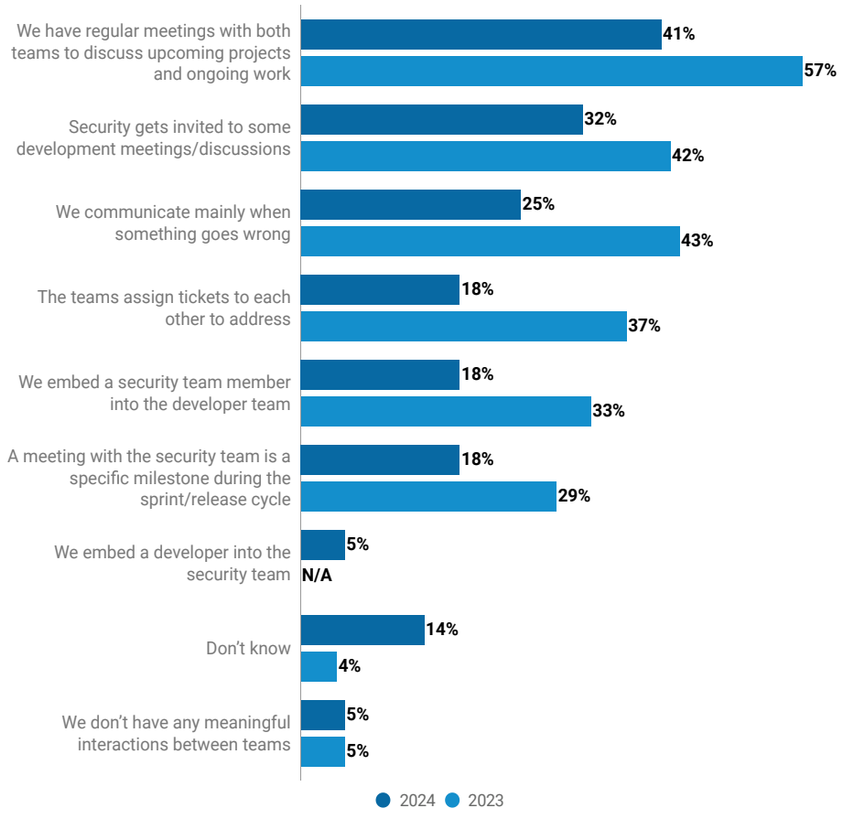
	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
We worry about finding false negatives	17%	41%	30%	12%	0%
Our tools are very accurate	14%	34%	41%	11%	0%
Our security tools just scratch the surface of all that we need to do	12%	44%	29%	13%	2%
We find more issues than we can remediate	12%	27%	34%	24%	3%
We find too many false positives	8%	39%	36%	15%	2%

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 27.

IT Security Team's Interaction With AppDev Team

How does the security team communicate or interact with your company's application development team for day-to-day activities?



Note: Multiple responses allowed

Base: 58 and 56 respondents who use in-house-developed apps in some capacity

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals in January 2024 and 103 in February 2023

Figure 28.

Effectiveness of Security Practices

How would you rate the effectiveness of the security practices your organization employs to safeguard applications?

	Very effective	Somewhat effective	Not effective	Don't use this security practice
Using verified, secure libraries/frameworks	39%	48%	7%	6%
Employing intrusion prevention/detection systems (IDS/IPS)	39%	44%	11%	6%
Performing regular compliance/audit reviews	26%	61%	6%	7%
Training developers in secure coding and development lifecycle practices	24%	48%	15%	13%
Virtual patching	23%	40%	15%	22%
Security design/architecture review	22%	65%	4%	9%
Establishing secure coding standards with regular reviews	22%	54%	13%	11%
Threat modeling	20%	41%	17%	22%
Software composition analysis (SCA) and/or pipeline composition analysis (PCA)	19%	39%	14%	28%
Participation in bug bounty programs	15%	17%	15%	53%

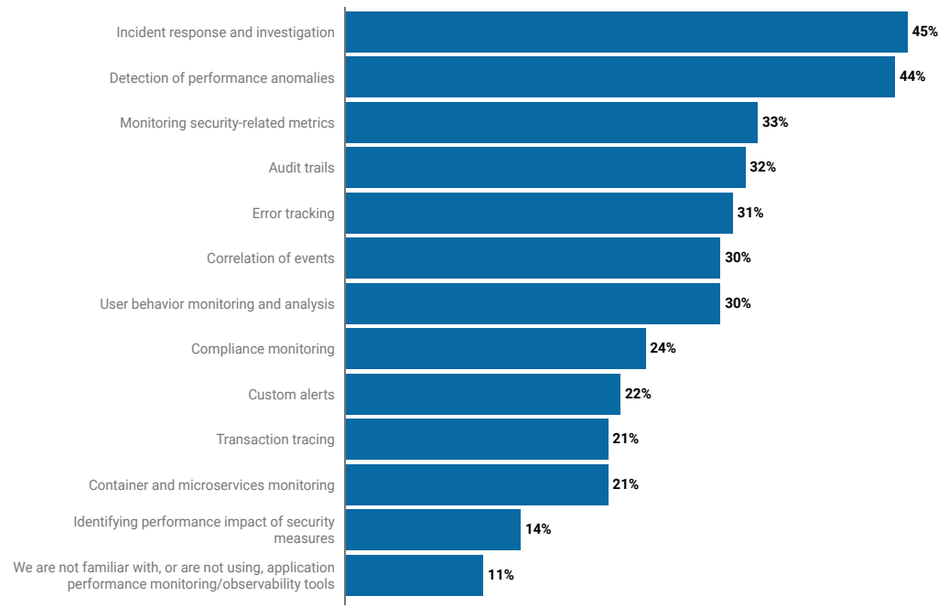
Base: 58 respondents who use in-house-developed apps in some capacity

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 29.

Use of APM

How is your organization using application performance monitoring in its application security efforts?



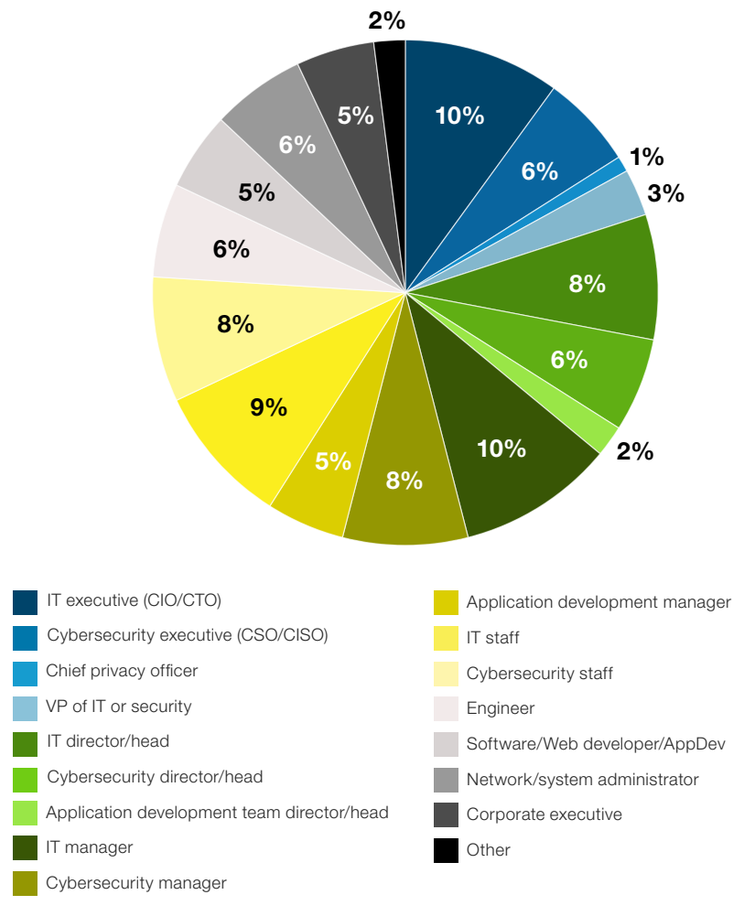
Note: Multiple responses allowed

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 30.

Respondent Job Title

Which of the following best describes your role in the organization?

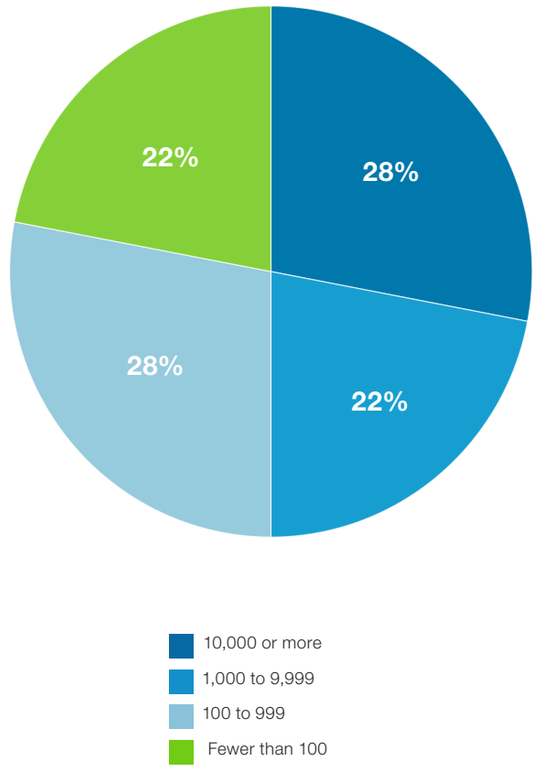


Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 31.

Company Size

How many employees are in your company in total?



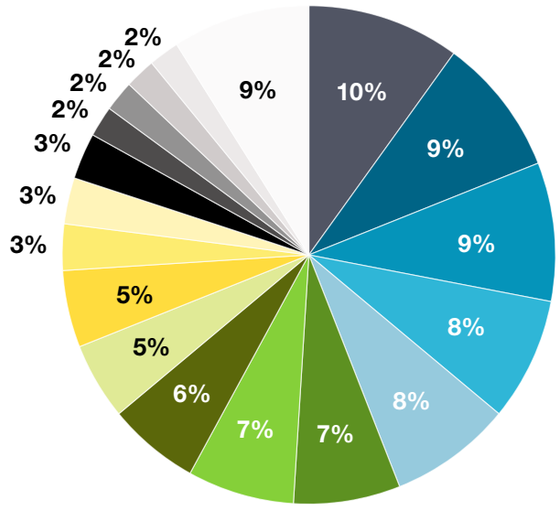
Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

DARKREADING REPORTS

Figure 32.

Respondent Industry

What is your organization's primary industry?



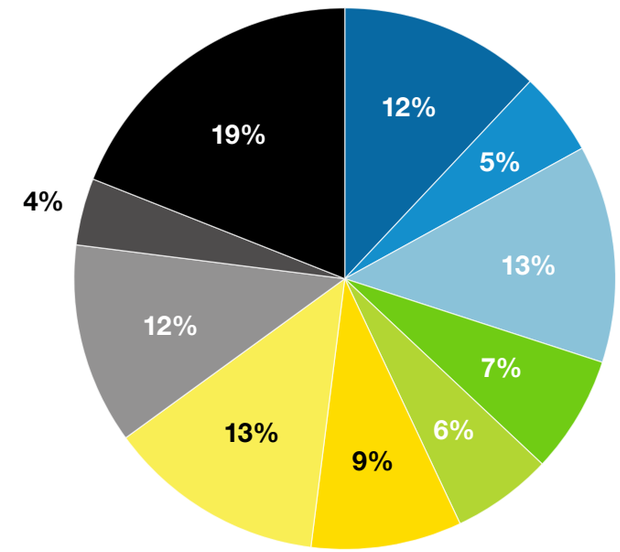
- Banking/financial services/VC/accounting
- Consulting/business services
- Manufacturing, industrial, process (noncomputer)
- Computer or technology manufacturer/tech vendor
- Education
- Media/marketing/advertising
- Solutions provider/VAR
- Construction/architecture/engineering
- Government
- Healthcare/pharmaceutical/biotech/biomedical
- Communications carrier/service provider
- Nonprofit/trade association
- Utilities
- Aerospace
- Agriculture/mining/oil/gas/energy
- Food/beverage
- Insurance/HMOs
- Other

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024

Figure 33.

Respondent Company Revenue

What is the annual revenue of your company?



- $10 billion or more
- $5 billion to $9.9 billion
- $1 billion to $4.9 billion
- $500 million to $999.9 million
- $100 million to $499.9 million
- $50 million to $99.9 million
- $6 million to $49.9 million
- Less than $6 million
- Government/nonprofit
- Don't know/decline to say

Data: Dark Reading survey of 107 cybersecurity, IT, and AppDev professionals, January 2024