Red Hat

The state of Kubernetes security report

2024 edition

A Red Hat® report

Executive summary

Cloud-native technologies are changing the way organizations develop, deploy, and scale applications. The inherent scalability, agility, and flexibility of cloud infrastructure lets businesses speed time to market, improve efficiency, and enhance innovation. However, as cyberattacks become increasingly sophisticated, robust security measures are key to safeguarding sensitive data, protecting against breaches, and complying with regulatory standards across hybrid cloud environments. In response, many IT organizations are investing in advanced security platforms and implementing collaborative, security-focused processes to protect critical systems, workloads, and data. In fact, IT security is a top funding priority for nearly 50% of companies.[1]

With a focus on container workloads and Kubernetes, Red Hat and Illuminas surveyed DevOps, engineering, and security professionals around the world in organizations ranging from small companies to large enterprises. Based on this data, the 2024 edition of the State of Kubernetes security report examines some of the most common cloud-native security challenges and business impacts that organizations experience today. We investigate specific security risks that most concern organizations—including software supply chain and application runtime vulnerabilities—and the steps organizations take to mitigate them. We identify the types and frequencies of security incidents that organizations experience in Kubernetes environments. We look at the distribution of Kubernetes security responsibilities across development, security, and operations teams to reveal the latest trends in DevSecOps adoption. And, finally, we provide guidance for reducing risks throughout your application life cycles.

Although challenging, comprehensive container and Kubernetes security can help you speed innovation and deliver more value for your organization. Using our survey results, you can evaluate your own Kubernetes security to find areas of improvement and gain insights for reducing security gaps. By continuously refining your security measures, you can protect critical business assets and create a culture of proactive security, ensuring the integrity and resilience of your infrastructure and applications.

Read on to discover 13 key findings from our survey.

*1 Red Hat report. "**2024 global tech trends**," February 2024.*

About this report

For the 2024 edition of this report, Red Hat sponsored a survey of 600 DevOps, engineering, and security professionals in the United States (U.S.), the United Kingdom (U.K.), and the English-speaking Asia Pacific region (APAC) to understand emerging trends in containers, Kubernetes, and cloud-native security. Data was gathered through 21-minute online and phone interviews with respondents sourced from online panels and 3rd-party databases. The survey was conducted in December 2023 and January 2024.

Respondent profile:

- IT professionals focused on applications, platforms, infrastructure, operations, security, or software architecture or development
- From companies with more than 100 employees
- From companies that have an internal application development team
- From companies that currently use containers

Respondent demographics

600
total reponses gathered

DevOps professionals

Engineering professionals

Security professionals

25% 100-499 employees
24% 500-999 employees
52% >1,000 employees

26% Technology
25% Financial services
24% Telco, media, and entertainment
26% Other industries

Key findings

Once again, our survey generated a lot of insight into how organizations approach Kubernetes security. Here are the highlights:

67% of organizations delayed or slowed down deployment due to Kubernetes security concerns.

46% of organizations lost revenue or customers due to a container or Kubernetes security incident.

42% of respondents cite security as a top concern with container and Kubernetes strategies.

42% of respondents report having DevSecOps initiatives in an advanced stage in their organization.

48% of organizations have early-stages DevSecOps initiatives, with teams collaborating on joint policies and workflows.

33% of respondents believe that their existing container and Kubernetes security solution slows down development.

30% of respondents identified vulnerabilities as the biggest worry for their container and Kubernetes environment.

Keep reading to discover more about these findings.

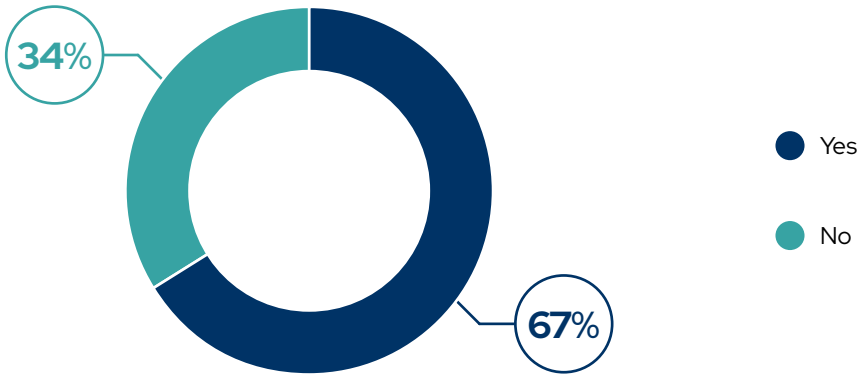
Finding 1:

Security issues continue to impact business outcomes

Security issues forced 67% of companies to delay or slow down application deployment.

Worldwide, organizations adopt cloud-native technologies like Kubernetes and microservices-based architectures to transform how they build, run, and scale applications. While some organizations develop all new software as microservices, many refactor existing applications using container-based technologies. In either case, containers can speed development and release cycles while increasing flexibility to run and manage applications across hybrid environments. However, incomplete security throughout the application life cycle—from development to deployment and maintenance—can diminish these valuable benefits. In fact, our survey found that 67% of respondents have delayed or slowed down deployment of container-based applications due to security concerns.

Have you ever delayed or slowed down application deployment into production due to container or Kubernetes security concerns?



Q27. Have you ever delayed or slowed down application deployment into production due to container or Kubernetes security concerns?
Base size: Total = 600

Percentages may not add to 100% due to rounding.

Finding 2:

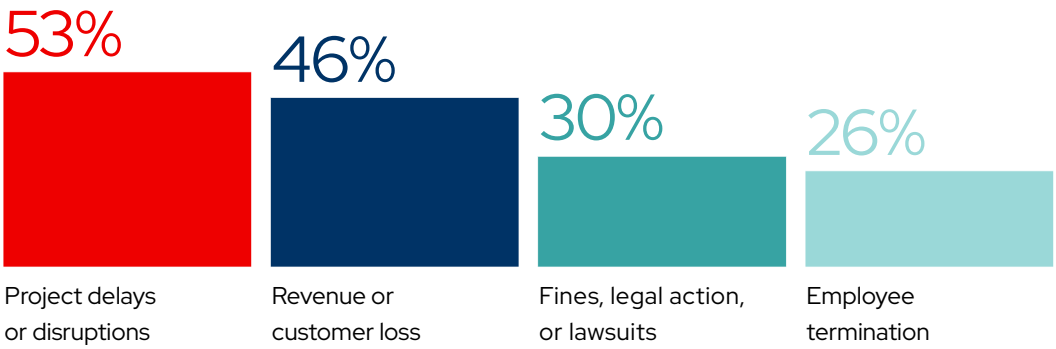
Security breaches affect everyone

Security incidents lead to broad consequences, including employee termination and loss of revenue.

The impact of container and Kubernetes security issues can go well beyond delayed application deployments. 26% of respondents said that a security incident led to employee termination, while 30% reported that their organization was fined as a result of the incident. In these situations, the loss of valuable talent, knowledge, and experience can significantly impact operations, while fines and negative publicity can place significant financial burdens on businesses.

46% of respondents also revealed that their organization experienced revenue or customer loss as a result of a security incident. Security breaches can slow business growth when teams delay projects or product releases while they work to remediate issues. And as customers lose trust in a business's data protection abilities, they may turn to competitors that engage in more secure practices.

In the past 12 months, have you experienced any of the following impacts to your business as a result of containers/Kubernetes security or compliance issues or incidents?



Q29. In the past 12 months, have you experienced any of the following impacts to your business as a result of containers/Kubernetes security or compliance issues or incidents? Base size: Total = 600

Finding 3:

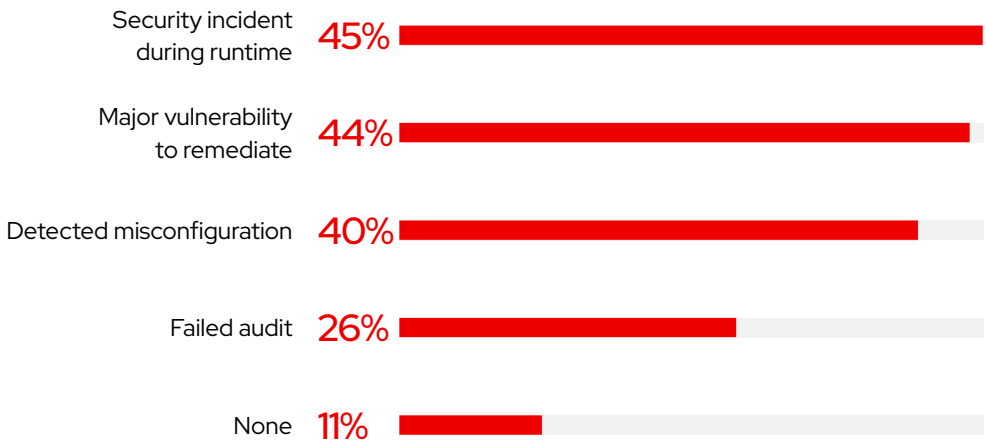
Security incidents occur in all application life cycle phases

Nearly 9 in 10 organizations had at least 1 container or Kubernetes security incident in the last 12 months.

Security incidents are not confined to running applications. Instead, container- and Kubernetes-related security incidents can impact all phases of the application life cycle. While 45% of respondents reported that their organizations experienced runtime incidents in the last 12 months, an almost equal number (44%) said they encountered issues in build and deployment phases, citing major vulnerabilities to remediate. At the same time, 40% said their organization detected misconfigurations in their container or Kubernetes environments, and 26% reported that their organization failed an audit.

Containers and Kubernetes technologies can increase productivity through cross-functional features and simplified operations. While Kubernetes provides mechanisms like network policies and role-based access control (RBAC) to enhance security across your cluster, some features are overly permissive or disabled by default and require additional configuration to ensure sufficient protection. Additionally, while security controls like **SELinux** can significantly increase application security, they can be challenging to customize and integrate into an operational environment. These difficulties frequently surface as security incidents, vulnerabilities, and misconfigurations at different stages of the application life cycle. Our survey results show that many organizations still struggle with the complexity of securing container-based Kubernetes environments, as 89% reported at least 1 related security incident during the last 12 months.

In the past 12 months, what security incidents or issues related to containers and/or Kubernetes have you experienced?



Q28. In the past 12 months, what security incidents or issues related to containers and/or Kubernetes have you experienced? Base size: Total = 600

Finding 4:

Current container security strategies present concerns

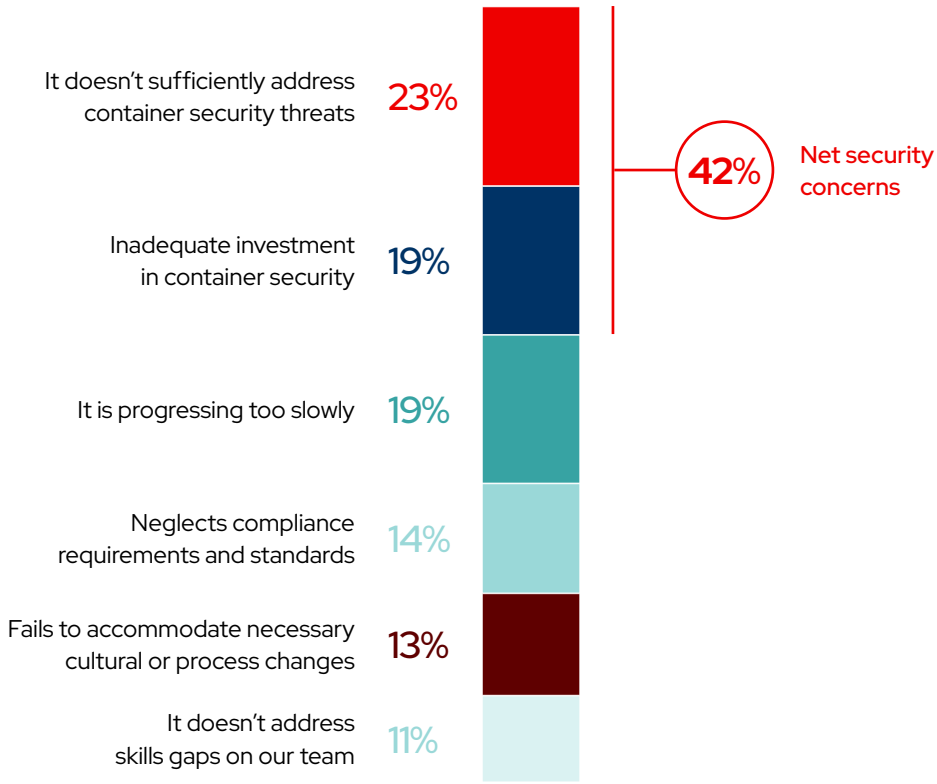
42% of respondents believe that their company does not sufficiently invest in container security or address related threats.

As organizations adopt container environments to streamline application deployment and scalability, they must also adapt their security processes to these dynamic and distributed systems. Kubernetes and containers introduce new software layers that can increase complexity and introduce additional security risks to critical infrastructure. With added potential entry points for cyber

threats, robust security measures are needed to protect against vulnerabilities, unauthorized access, and data breaches. Even so, some respondents are skeptical of their company's container strategy. In fact, 23% believe that their organization's strategy does not sufficiently address container security threats, while 19% think that investment in container security is inadequate.

Comprehensive container and Kubernetes security starts with understanding the complexity and potential security risks of modern environments. By implementing controls that encompass all layers of the software stack—including the underlying infrastructure, Kubernetes control plane, network, and container images and registries—you can begin to minimize risks to your cloud-native applications.

What is your biggest concern about your company's container strategy?



Q7. What is your biggest concern about your company's container strategy? Base size: Total = 600

Percentages may not add to 100% due to rounding.

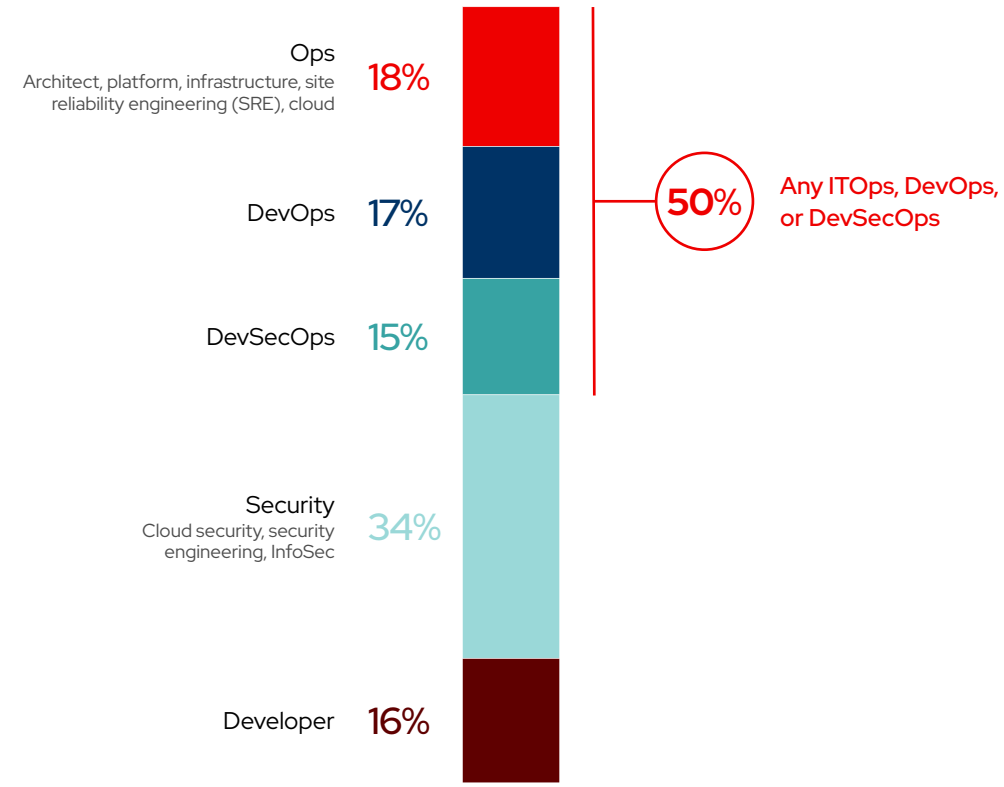
Finding 5:

Responsibility for security is highly decentralized

Only 1/3 of respondents say their security teams are responsible for Kubernetes security.

In many organizations, multiple groups collaborate to build and deploy workloads in container-based Kubernetes environments. Our survey results show that there is no single role responsible for Kubernetes security across organizations.

What role at your company is most responsible for container and Kubernetes security?



Q9. What role at your company is most responsible for container and Kubernetes security? Base size: Total = 600

In fact, only 34% of respondents overall say that security teams are most responsible for container and Kubernetes security within their organization. Various operations roles, including ITOps, DevOps, and DevSecOps, are responsible for security at 50% of organizations. Interestingly, APAC organizations are more likely to have a DevSecOps role most responsible (21%).

Advanced Kubernetes security technologies and processes can promote close collaboration between diverse teams and remove barriers that isolate domain experts. Developers can create and integrate custom software, open source components, and container images. Security experts can define and implement policies and controls across cluster resources. And operations teams can manage cluster infrastructure, access controls, and authorization mechanisms—all using a single set of common security solutions.

Finding 6:

DevSecOps practices are common across organizations

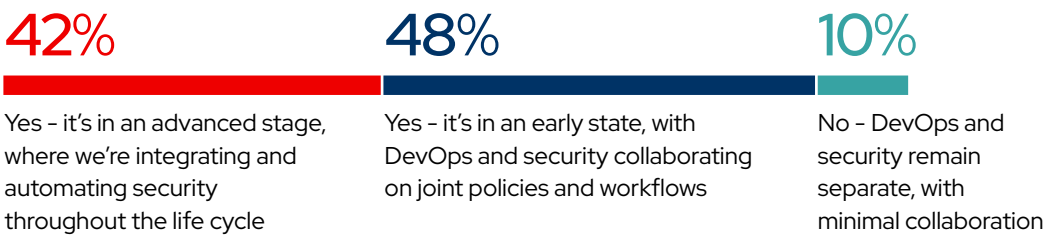
42% of respondents have a DevSecOps initiative in an advanced stage within their organization.

Organizations continue to adopt DevSecOps practices to identify and mitigate security risks earlier in their container and Kubernetes deployment processes. In fact, 42% of respondents say their organization integrates and automates security throughout entire application life cycles using DevSecOps processes and tools like automated testing, continuous monitoring, and code reviews.

At the same time, 48% report that their organization understands the value of DevSecOps and is in the early stages of adoption, with development, operations, and security teams collaborating on joint policies and workflows. This is a significant increase from last year, when only 39% of respondents were at this

stage. For the remaining 10% of organizations, separate DevOps and security teams may lead to reactive processes that only address vulnerabilities at deployment or runtime, resulting in decreased efficiency, speed, and software quality, along with slower application delivery.

Do you have a DevSecOps initiative in your organization?



Q25. Do you have a DevSecOps initiative in your organization? Base size: Total = 600

Finding 7:

Kubernetes environments bring new security challenges

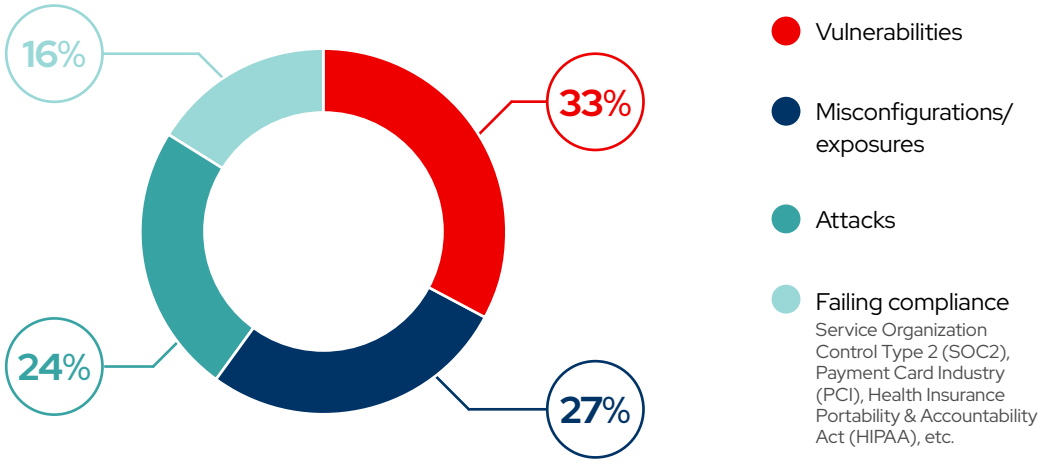
60% of respondents worry about vulnerabilities, misconfigurations, and exposures in their container and Kubernetes environments.

Mitigating vulnerabilities in complex, dynamic Kubernetes and container environments can be challenging. Because containers share host resources like operating system kernels, a single container vulnerability can impact multiple containers. And a vulnerability in a host itself can affect all containers deployed on the system. Respondents are clearly aware of this challenge, as 33% are most worried about vulnerabilities in their container and Kubernetes environment.

A top concern for 27% of respondents, incorrectly configured components—including base images, libraries, and dependencies—can introduce critical security issues across entire environments. If not properly validated and maintained, these components can serve as potential attack points and compromise the integrity and confidentiality of critical applications and sensitive data.

While these concerns are warranted, they can be mitigated with thorough security processes. For example, implementing automated, continuous security scanning can help you detect and fix common vulnerabilities and ensure correct configuration of security-sensitive components.

Of the following risks, which one are you most worried about for your container and Kubernetes environments?



Q10. Of the following risks, which one are you most worried about for your container and Kubernetes environments? Base size: Total = 600

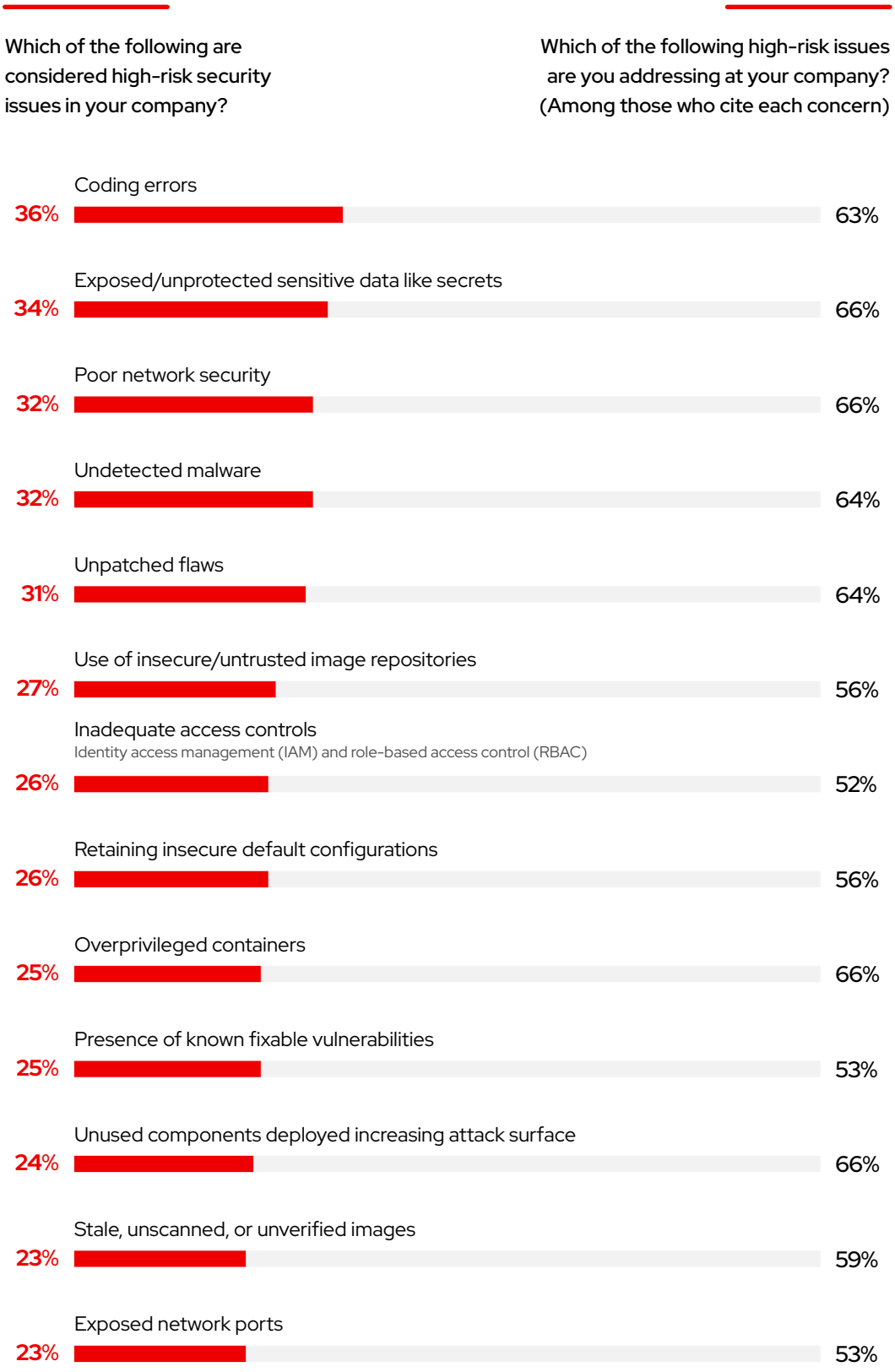
Finding 8:

Organizations are actively addressing high-risk issues

Coding errors, unprotected sensitive data, poor network security, and undetected malware present the highest security risks.

Overall, organizations do not have a single top security risk; instead, they are almost equally concerned about a range of potential issues. From coding errors (36%) and exposed sensitive data (34%) to poor network security (32%) and undetected malware (32%), these security risks highlight the need for comprehensive strategies to mitigate vulnerabilities and safeguard against cyber threats. Comprehensive analysis of Kubernetes and container components can identify vulnerabilities and misconfigurations to help you implement targeted remediation measures across your container environment. Robust security measures tailored to application requirements can effectively mitigate risks, protect sensitive data, and defend against threats. And user-friendly security controls integrated throughout the entire application life cycle can improve compliance and mitigate the risk of human error.

Based on our survey results, organizations are actively working to reduce high-risk issues across their container and Kubernetes environments. In fact, more than half of companies surveyed are focusing on every potential high-risk security issue. At the same time, 66% of organizations are addressing threats related to exposed sensitive data, poor network security, overprivileged containers, and unused components.



Q13. Which of the following are considered high-risk security issues in your company? Base size: Total = 600

Q14. Which of the following high-risk issues are you addressing at your company? Base size: Among those who cite each concern = 139 - 213

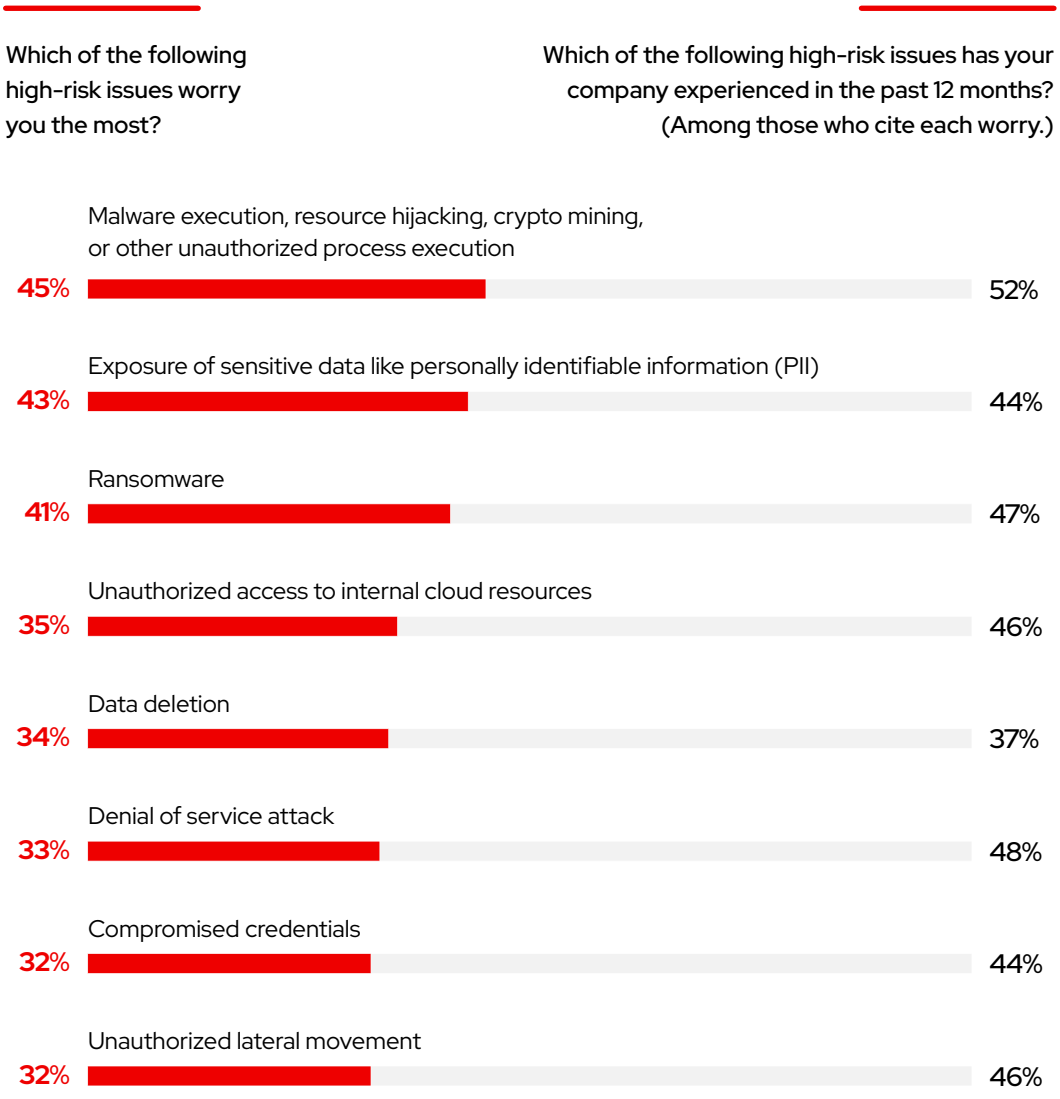
Finding 9:

Security issues can lead to serious consequences

More than half of organizations found unauthorized process execution in their environments.

Many high-risk security issues—from unauthorized process execution (45%) to exposure of sensitive data (43%) to ransomware (41%)—concern respondents, reflecting the importance of protecting against a range of threats that can compromise the integrity, confidentiality, and availability of data and systems. Unauthorized process execution poses a significant risk, allowing malicious actors to infiltrate systems, disrupt operations, and access sensitive information. Exposure of sensitive data raises concerns about regulatory compliance and financial and reputational damage resulting from data breaches. And ransomware attacks can cause significant disruptions and financial losses for organizations.

These concerns are justified. For every high-risk security issue identified in our survey, more respondents actually experienced the issue than worried about it. For example, the top worry was unauthorized process execution, cited by 45% of respondents. However, 52% of respondents reported that their organization actually experienced some type of unauthorized process during the last 12 months alone. This discrepancy is even greater for unauthorized access to internal cloud resources, denial of service attacks, compromised credentials, and unauthorized lateral movement. 11-15% more organizations experienced than worried about these high-risk issues.



Q15. Which of the following high-risk issues worry you the most? Base size: Total = 600

Q16. Which of the following high-risk issues has your company experienced in the past 12 months? Base size: Among those who cite each worry = 189 - 270

Finding 10:

Risk management is critical for software supply chains

44% of respondents say software vulnerabilities are the highest-risk aspect of software supply chains, an increase of 9% from last year.

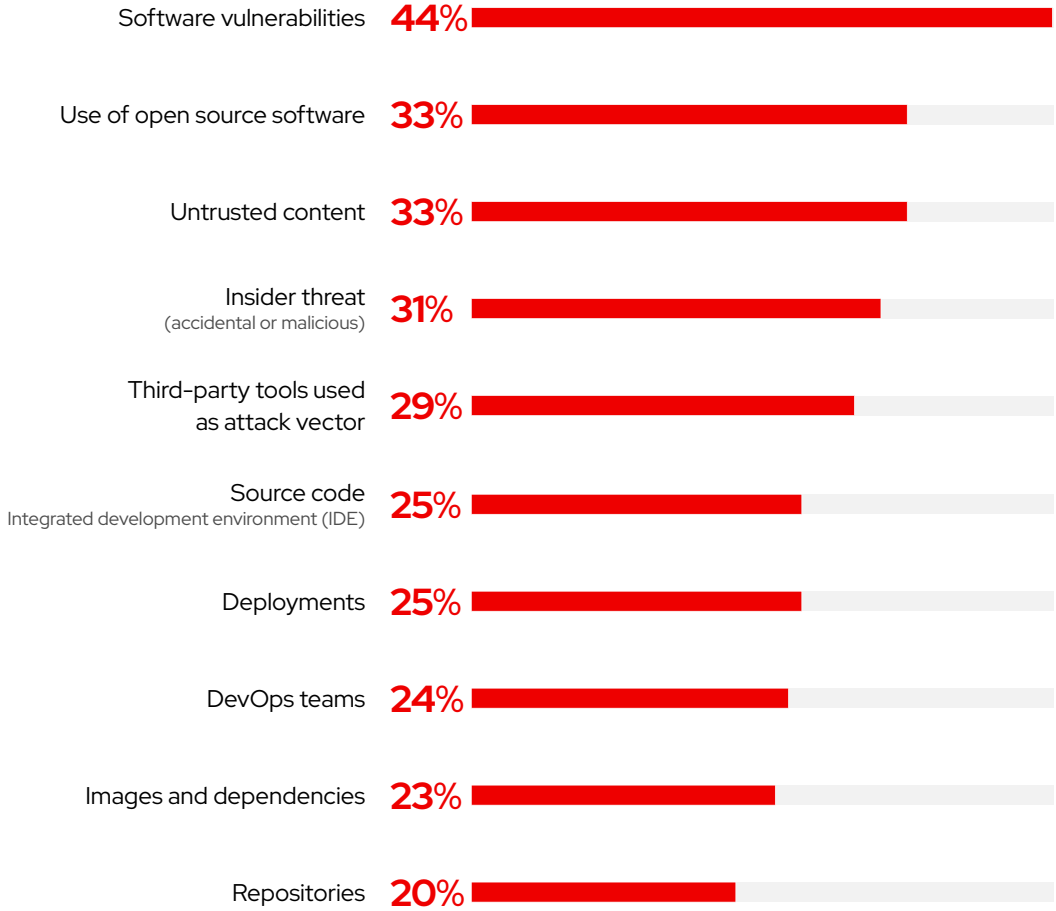
Securing software supply chains can be challenging due to their inherent complexity and global reach. Supply chains often integrate software from a variety of commercial vendors and open source projects, so it is crucial to ensure the integrity, authenticity, and security of each component.

We asked respondents to identify the highest-risk aspects of software supply chains. Software vulnerabilities (44%), open source software (33%), and untrusted content (33%) ranked at the top across organizations. This makes sense, as each of these aspects can lead to serious consequences. Software vulnerabilities can lead to security incidents like data breaches and malware execution. Open source software must be properly reviewed, scanned, and maintained to reduce the risk of incorporating new vulnerabilities. And untrusted content can compromise system integrity and allow unauthorized access.

Notably, concerns about software vulnerabilities increased 9% from 35% in 2023 to 44% this year. And respondents in the technology industry ranked vulnerabilities even higher, at 51%. We also found that respondents from small companies ranked insider threats higher than average, at 36% versus 31% overall.

Organizations can address these challenges with a comprehensive approach to software supply chain security that includes rigorous supplier evaluations, security-focused coding practices, and continuous monitoring of software dependencies. By prioritizing security at every stage of the software supply chain, you can minimize risks, protect against cyber threats, and ensure the integrity of software delivered to your users and stakeholders.

What aspects of the software supply chain security represent the highest risk?



Q30. What aspects of the software supply chain security represent the highest risk? Base size: Total = 600

Finding 11:

Software supply chain security worries are justified

57% of organizations detected vulnerable application components in their software supply chain in the last 12 months.

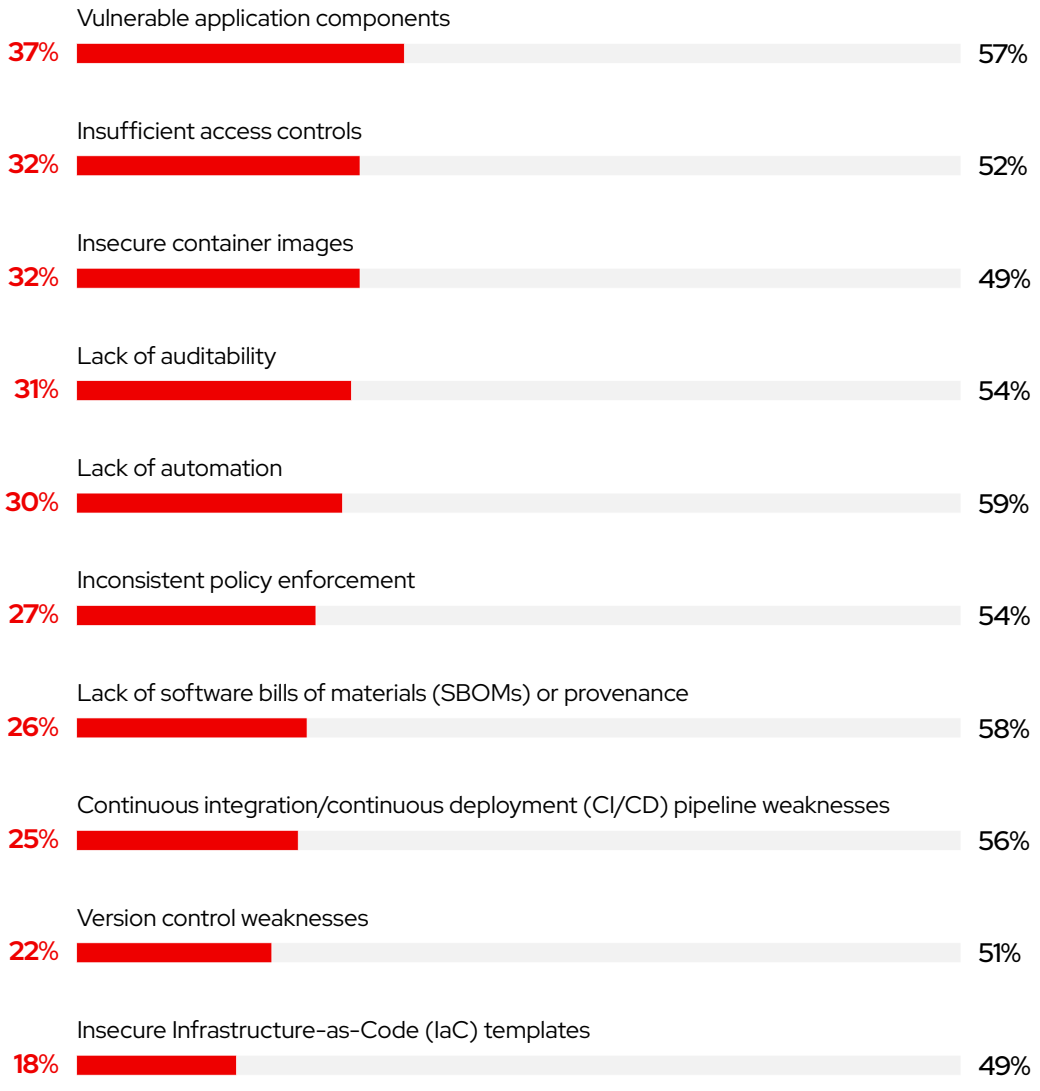
Software supply chain security helps ensure integrity, confidentiality, and availability throughout application life cycles. With robust security measures, organizations can mitigate the risk of supply chain attacks, unauthorized access, and data breaches to safeguard digital assets and maintain customer and stakeholder trust.

However, respondents expressed many concerns about the security of their organizations' software supply chains—including vulnerable application components (37%), insufficient access controls (32%), and insecure container images (32%). As with overall security issues (**Finding 9**), these concerns are warranted. Almost every issue identified in the survey was experienced by more than half of all respondent organizations, with vulnerable application components, lack of automation, and lack of software bills of materials (SBOMs) impacting nearly 60% of companies.

Additionally, at least 1.5 times more organizations experienced than were concerned about each issue. In fact, the 4 issues of lowest concern—lack of SBOMs, continuous integration/continuous deployment (CI/CD) pipeline weaknesses, version control weaknesses, and insecure Infrastructure-as-Code (IaC) templates—were experienced by more than twice as many organizations as were concerned about the issue.

Which of the following software supply chain security issues is your company most concerned about?

Which of the following software supply chain security issues has your company experienced in the past 12 months? (Among those who cite each concern.)



Q32. Which of the following software supply chain security issues is your company most concerned about? Base size: Total = 600

Q33. Which of the following software supply chain security issues has your company experienced in the past 12 months? Base size: Among those who cite each concern = 107 - 223

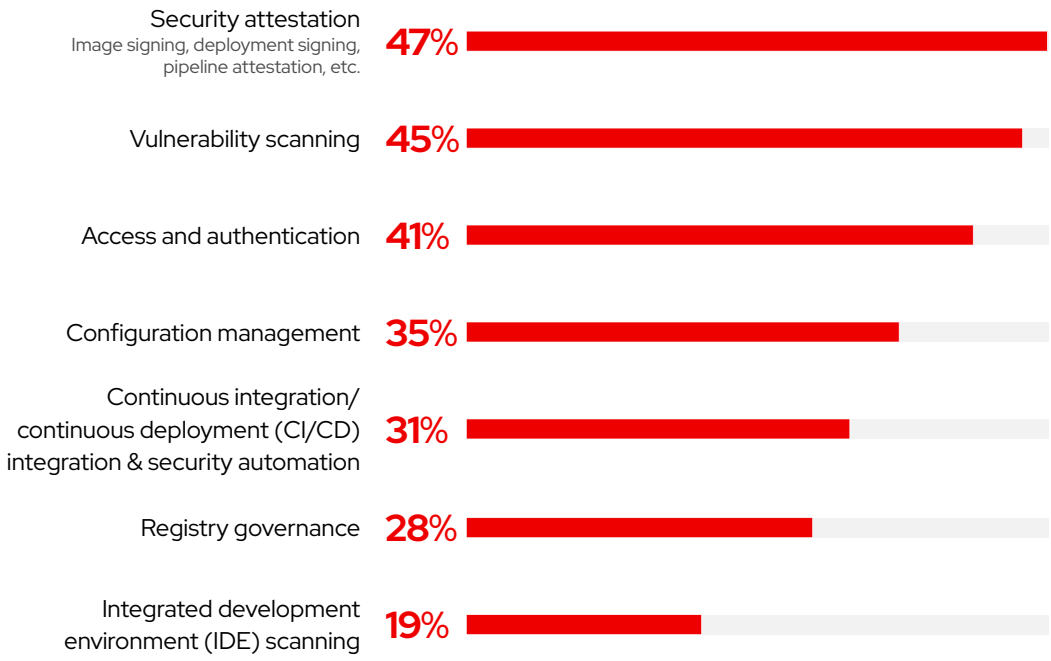
Finding 12:

Tools and processes support software supply chain security

Nearly half of respondents view security attestation as a key software supply chain security control.

Organizations mitigate vulnerabilities and protect critical software supply chains with a variety of advanced security tools and technologies—including security attestation (47%), vulnerability scanning (45%), and access and authentication mechanisms (41%). By verifying each software component's origin, authenticity, and compliance with security standards, security attestation helps you ensure the integrity and trustworthiness of applications. Vulnerability scanning lets you

Which of the following are most important when it comes to software supply chain security?



Q31. Which of the following are most important when it comes to software supply chain security? (Please select up to 3 most important aspects.)
Base size: Total = 600

proactively address security risks—before they can be exploited—by identifying and remediating potential weaknesses and vulnerabilities in your software supply chain. With access and authentication mechanisms like multifactor authentication (MFA) and RBAC, you can reduce the risk of unauthorized access to sensitive software components and data.

Finding 13:

Organizations use open source tools for Kubernetes security

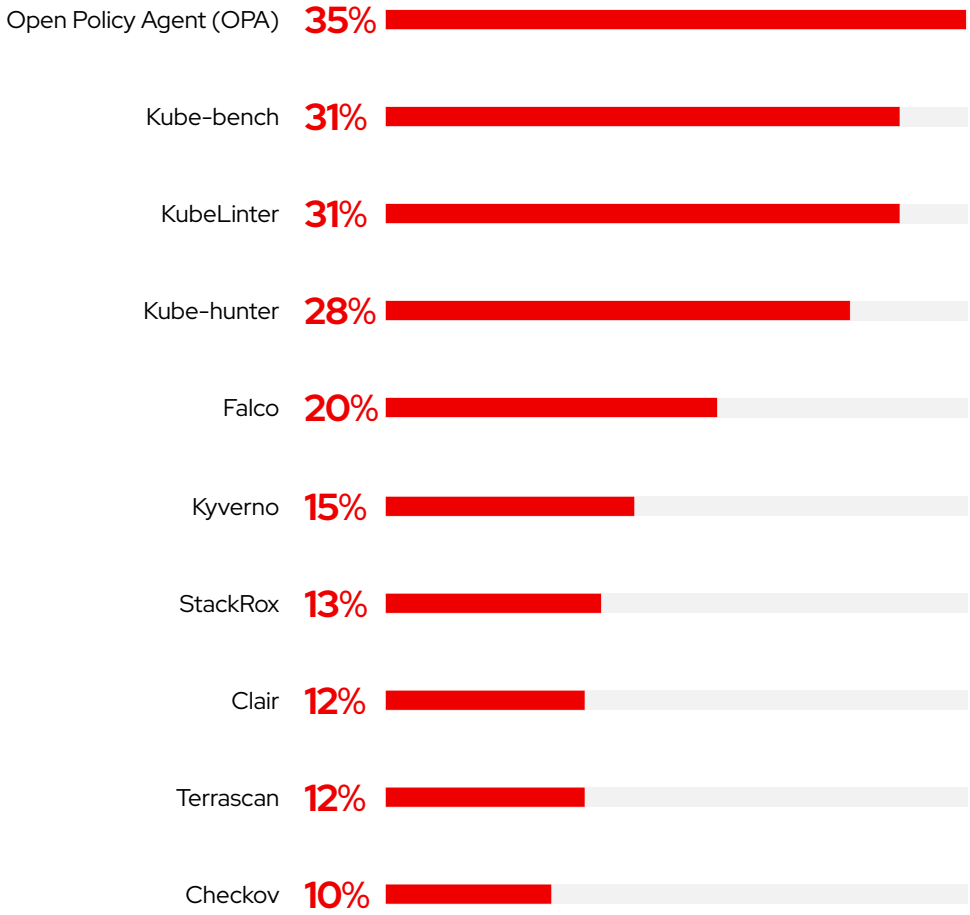
Open Policy Agent, Kube-bench, and KubeLinter are popular open source Kubernetes security tools.

A comprehensive ecosystem of open source tools—with advanced technologies developed by dedicated contributors—provides a range of security solutions for containers and Kubernetes environments. Respondent organizations rely on many of these open source security tools to protect their cloud-native applications:

- 35% simplify policy management with **Open Policy Agent**, a toolset and framework for unified policies across cloud-native stacks.
- 31% check Kubernetes deployment security against the **CIS Kubernetes Benchmark** using **Kube-bench**.
- 31% ensure applications adhere to best practices with **KubeLinter**, a static analysis tool for Kubernetes YAML files and Helm charts.
- 28% identify security issues in Kubernetes clusters and cloud-native environments using **Kube-hunter**, a security testing and scanning tool.

Overall, organizations use an average of 2.1 security-related open source tools within their Kubernetes environments.

Which of the following open source tools do you use for Kubernetes security?



Q20. Which of the following open source tools do you use for Kubernetes security? Base size: Total = 600

Enhance your container and Kubernetes security

Containers and Kubernetes can speed application development and deployment across hybrid cloud environments. Integrating security-focused processes and technologies throughout their life cycles helps you protect applications without slowing development or increasing operational complexity. Safeguard sensitive data, intellectual property, and customer information. Meet corporate, industry, and government regulatory requirements. Ensure business continuity. Maintain customer trust and confidence. Reduce the costs of late remediation efforts.

Here are 3 tips for increasing the security of your cloud-native environments.

1 Use Kubernetes-native security controls

Kubernetes-native security uses declarative data and native controls to protect your container workloads.

- Analyze the declarative data available in Kubernetes to gain risk-based insights into configuration management, compliance, segmentation, and vulnerabilities.
- Simplify and speed analysis and troubleshooting using the same infrastructure and controls for development and security.
- Reduce operational conflict through security automation and scaling.

2 Extend security across application life cycles

A security focus during all application life cycle phases can help you identify and mitigate potential vulnerabilities early, reducing the risk of data breaches, cyberattacks, and compromised user trust.

- Incorporate DevSecOps best practices and internal controls into configuration checks within your security platform.
- Automate Kubernetes configuration security assessments using your container and Kubernetes platform.

3 Adopt tools that support DevSecOps practices

The right security technologies and solutions can increase collaboration between your development, security, and operations teams.

- Use your container and Kubernetes platform to perform risk assessments and provide security controls for your environments.
- Adopt tools that can identify and explain vulnerabilities in active deployments to understand and apply security-focused practices.

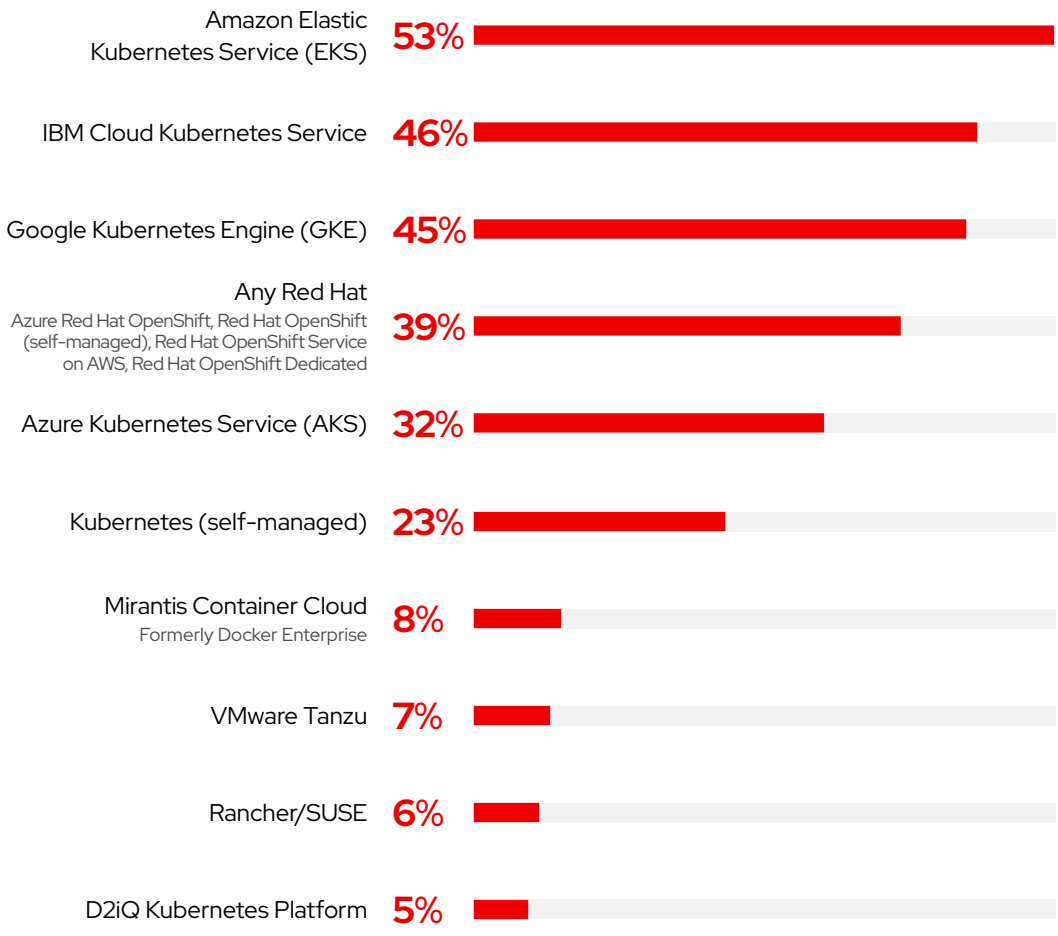
About our respondents

This section provides more details about our respondents and their organizations.

Kubernetes adoption

Most respondents use Kubernetes in production, with cloud-based Kubernetes solutions as the most popular platforms.

What Kubernetes platform do you use to orchestrate your containers?

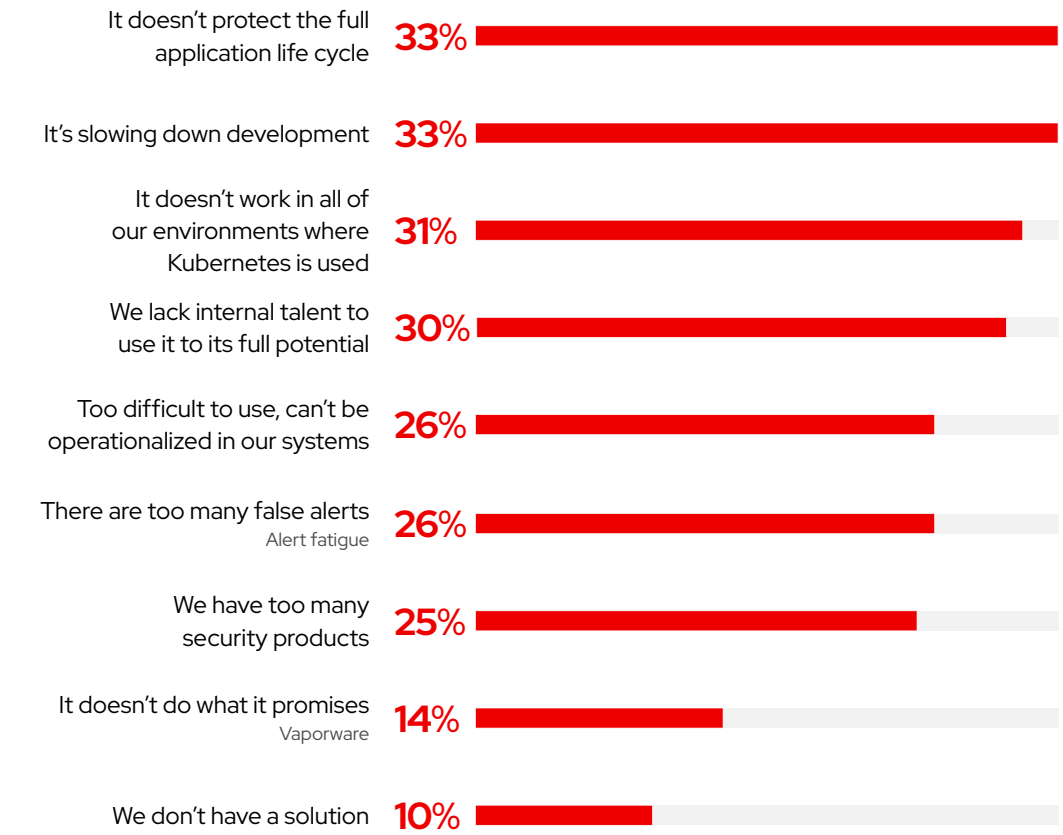


Q3. What Kubernetes platform do you use to orchestrate your containers? Base size: Those using Kubernetes = 390

Common pain points

Lack of full life cycle security and slow deployments are the 2 most common complaints about current Kubernetes security solutions.

Which of the following are the biggest pain points you experience with your current Kubernetes security solution?

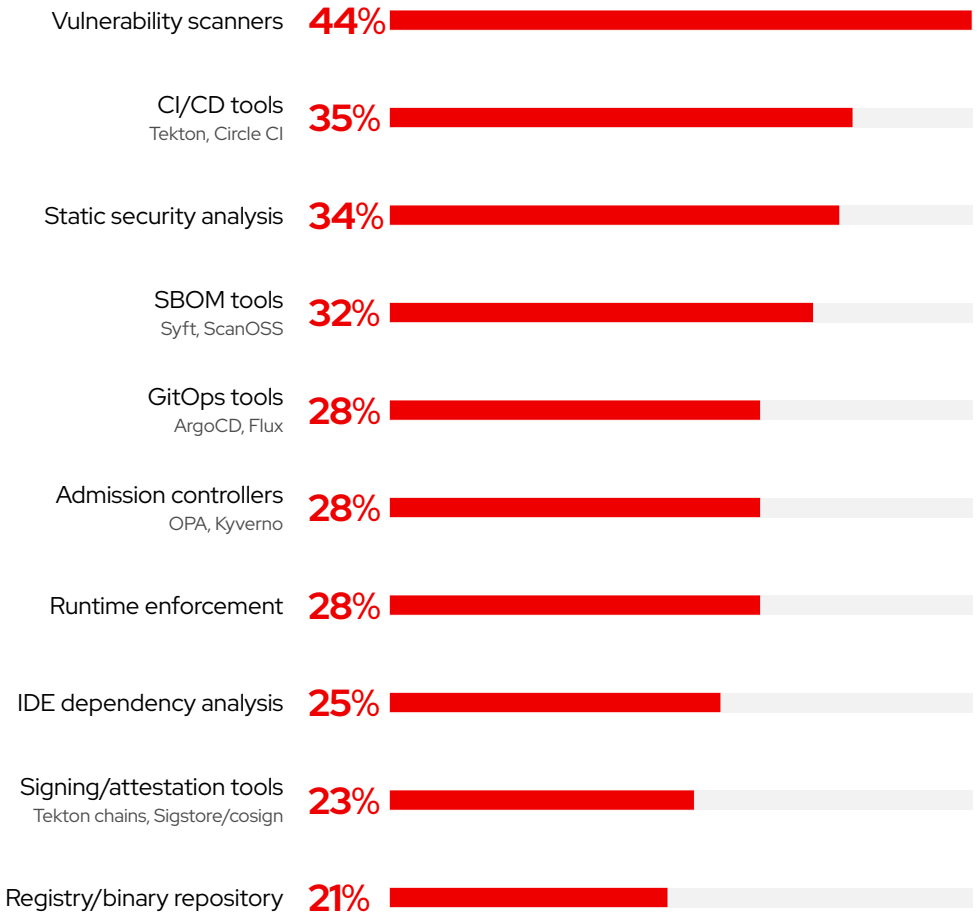


Q26. Which of the following are the biggest pain points you experience with your current Kubernetes security solution? (Please select up to 3 top pain points.) Base size: Total = 600

Supply chain security tools

Vulnerability scanners are the most used security tools, followed by CI/CD, static security analysis, and SBOM tools. Organizations use an average of 3 security tools for their software supply chains.

Which of the following types of security tools do you use for your software supply chain?

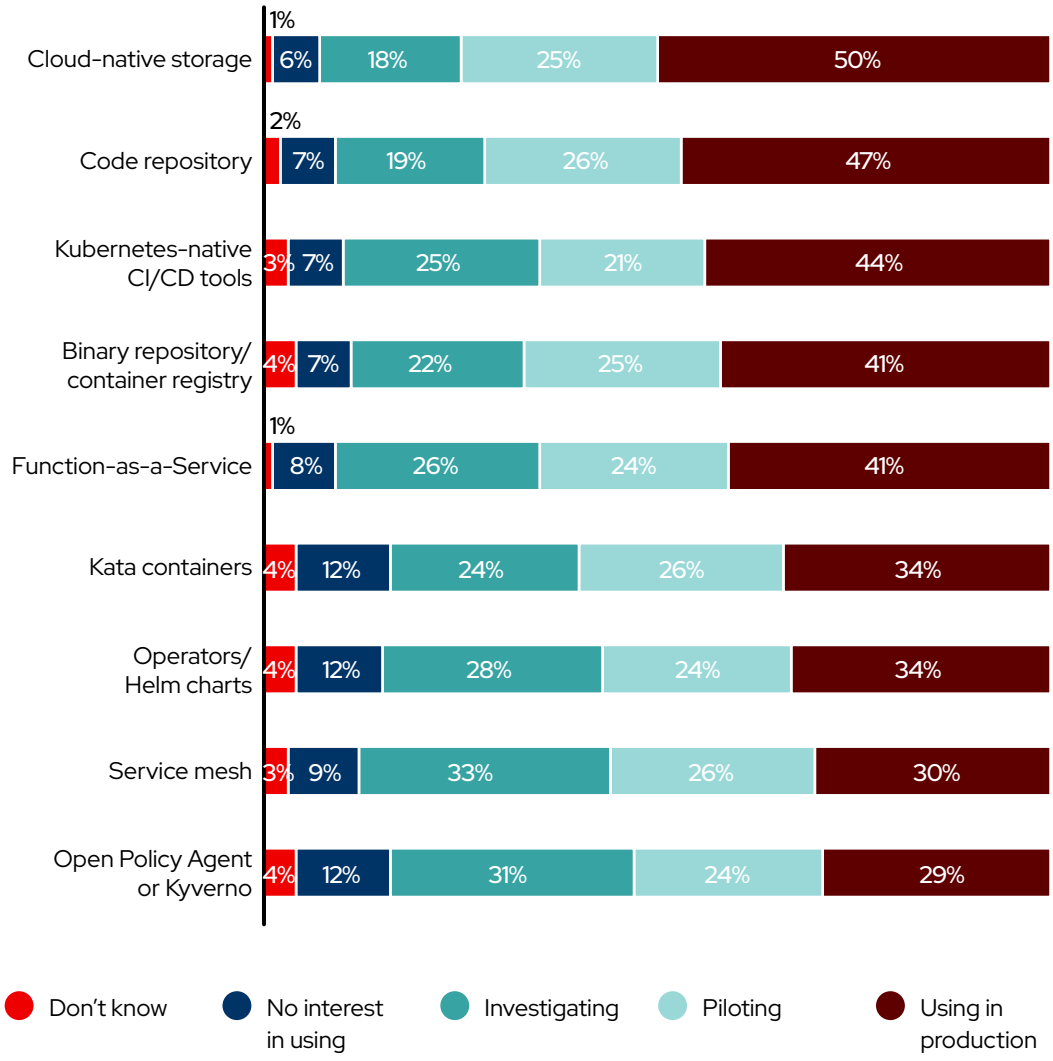


Q22. Which of the following types of security tools do you use for your software supply chain? Base size: Total = 600

Other cloud-native technologies

Kubernetes-native CI/CD tools are among the top cloud-native technologies in use.

What other cloud-native technologies are you considering or using currently?



Q6. What other cloud-native technologies are you considering or using currently? Base size: Total = 600

Percentages may not add to 100% due to rounding.

Get started with Red Hat Advanced Cluster Security for Kubernetes

Red Hat® Advanced Cluster Security for Kubernetes is a Kubernetes-native security platform that helps you build, deploy, and run cloud-native applications with more security. With Red Hat Advanced Cluster Security, you can protect containerized Kubernetes workloads in major public cloud environments and hybrid cloud platforms—including Red Hat OpenShift, Amazon Elastic Kubernetes Service (EKS), Microsoft Azure Kubernetes Service (AKS), and Google Kubernetes Engine (GKE).

Minimize operational risk

Monitor, collect, and evaluate system-level events—like process execution, network connections and flows, and privilege escalation—to detect malicious activities from active malware and unauthorized access to intrusions and lateral movement.

Increase DevSecOps productivity

Integrate Red Hat Advanced Cluster Security with your CI/CD pipelines and image registries to quickly remediate vulnerable and misconfigured images—directly in developer environments—with real-time feedback and alerts.

Protect Kubernetes infrastructure

Ensure your Kubernetes infrastructure remains hardened and protected with continuous scans against CIS benchmarks and other security best practices.

Schedule a personalized demo of Red Hat Advanced Cluster Security for Kubernetes tailored for your business and needs.

Red Hat