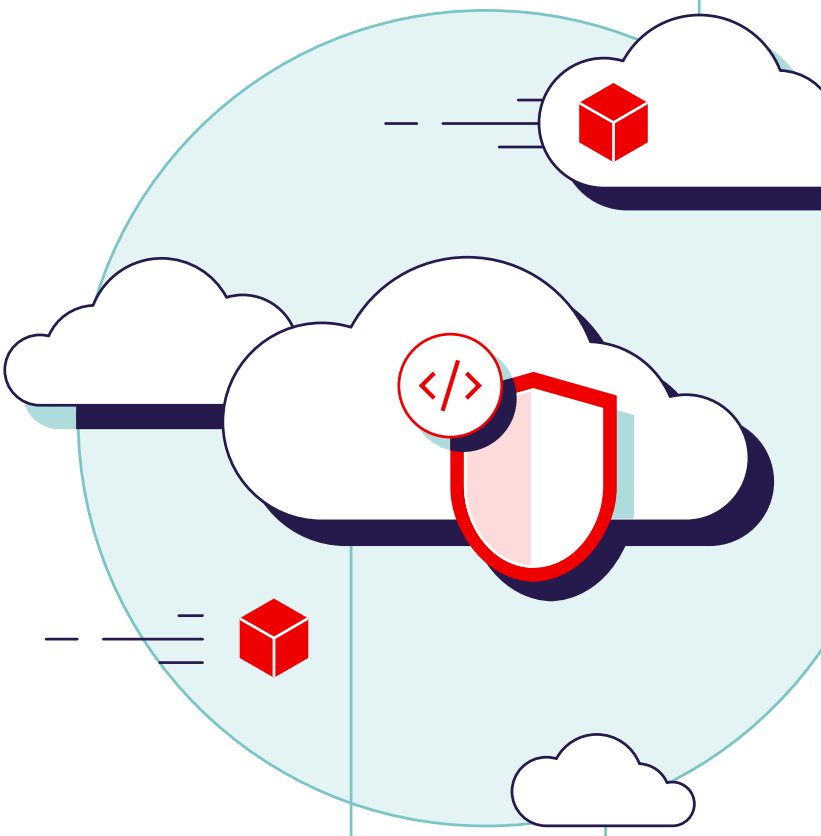
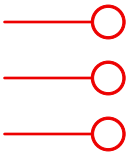
Red Hat

State of Kubernetes security report

2023





Executive summary

Our 2023 edition of the State of Kubernetes Security Report delves into the latest findings from our annual survey around cloud-native security, focusing on containerized workloads and Kubernetes.

This report is based on a survey of 600 DevOps, engineering, and security professionals from across the globe spanning large enterprises and small-to-medium sized organizations. The report uncovers some of the most common security challenges organizations face on their cloud-native adoption journey, and their impact on the business. We examine specific security risks that organizations are most worried about and the steps they take to mitigate those risks, including risks to their software supply chain and their applications at runtime.

In addition, we identify the types of security incidents and how often survey respondents experienced them in their Kubernetes environment, and provide best practices and guidance for application development and security teams that could lower their security risk.

With security as one of the biggest concerns with Kubernetes adoption, and security identified as the #1 IT funded priority for 2023,[1] it's never been more important for the Security team to collaborate with the Development and Operations team and embed security controls earlier in the developer workflows. Our report looks at how responsibility for Kubernetes security is distributed across Dev, Sec, and Ops, and reveals the latest trends in DevSecOps adoption.

As always, we encourage readers to benchmark the health of their Kubernetes security against the findings in this report to find areas of improvement and get insights into how to reduce or eliminate security gaps. Container and Kubernetes security, while challenging, offers an opportunity for organizations to confidently accelerate development velocity, but only if security isn't treated as an afterthought. Much like the presence of brakes in an automobile allows you to accelerate at high speeds with confidence, security, when done right, can embolden the organization to innovate faster and deliver value with confidence.

1. Red Hat blog. "Red Hat Global Customer Tech Outlook 2023: Security is the top priority as digital transformation continues," 15 Nov 2022.

Key findings

67% Reported delaying or slowing down deployment due to Kubernetes security concerns

37% Experienced revenue or customer loss due to a container/Kubernetes security incident

38% Cite security as a top concern with container and Kubernetes strategies

17% Reported having no DevSecOps initiatives, with DevOps and Security remaining separate

35% Said their existing container and Kubernetes security solution slows down development

30% Identified vulnerabilities as their biggest worry for their container and Kubernetes environment

Security issues continue to impact business outcomes

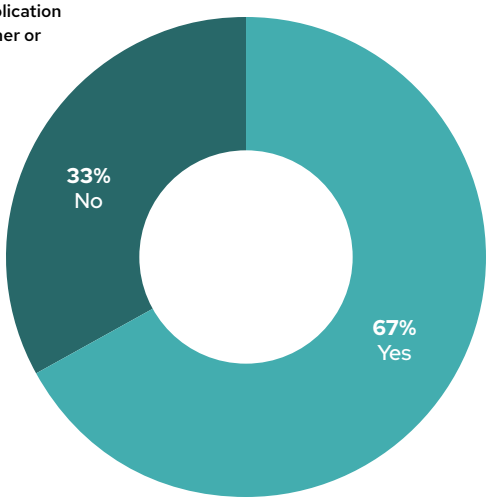
67% of companies have delayed or slowed down deployment due to a security issue

Organizations are adopting cloud native technologies like Kubernetes and microservices-based application architectures to transform how they build, run, and scale applications. While some are building all new applications as microservices, others are refactoring existing applications alongside managing monoliths. However, our survey found that 67% of respondents have had to delay or slow down application deployment due to security concerns.

This is not surprising, as new technologies often create unforeseen security challenges. When security becomes an afterthought, the agility gained from containerization - more rapid release cycles, faster bug fixes, and greater flexibility to run and manage applications across hybrid environments - is negated. Some organizations are overwhelmed by security needs that stretch across all aspects of the application life cycle, from development through deployment and maintenance. Therefore, they need a simplified way to protect their containerized applications without slowing development or increasing operational complexity.

When security is prioritized early, organizations are making an investment in protecting their valuable business assets, such as sensitive data, intellectual property, and customer information. They are also able to better meet regulatory requirements, ensure business continuity, maintain customer trust, and reduce their long-term cost of remediating security issues later in the development life cycle or after it has been exploited.

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



Both employees and organizations as a whole pay the price for security incidents

1 in 5 respondents said a security incident led to employee termination, and more than 1 in 3 experienced revenue or customer loss

As mentioned previously, container and Kubernetes security issues often delay application rollout. Our survey found that there are other, possibly even more severe, impacts on business. 21% of respondents said that a security incident led to employee termination, and 25% said the organization was fined. This could result in a loss of valuable talent, knowledge, and experience, which could affect the business's ability to operate effectively. Furthermore, businesses that face regulatory fines due to compliance violations or data breaches face a significant financial burden, not to mention negative publicity.

Another potential negative impact of container and Kubernetes security incidents is slowing business growth. 37% of respondents identified revenue/customer loss as a result of a container and Kubernetes security incident. Security breaches could result in the delay of critical projects or product releases, as businesses must prioritize security efforts to address the vulnerabilities that were missed in the development stage. This delay could have a ripple effect on the business, resulting in lost revenue, customer dissatisfaction, or even loss of market share to competitors. Furthermore, a security incident could lead to customer loss, as customers may lose trust in the business's ability to protect their data and may seek out competitors with a stronger security track record.

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? (Select all that apply.)

Security incidents are prevalent, impacting all phases of the application development life cycle

90% of respondents experienced at least one security incident in the last 12 months

Our survey found that security incidents aren't confined to just when applications are running. Container and Kubernetes security incidents impact the full application development life cycle.

We discovered that while most of container and Kubernetes security incidents in the last 12 months occurred during the runtime phase (49%), the build/deploy phases were impacted nearly equally. Kubernetes and containers were designed for developer productivity and ease of use, not necessarily security. For example, security controls such as SELinux are critical to hardening the application yet challenging to customize and integrate into an operational environment. Therefore, some organizations may choose to disable them, which can leave the application more vulnerable to attack.

Another such example is the default behavior of pod-to-pod communication within a cluster. By default, pods within a Kubernetes cluster are allowed to communicate with each other, which creates security weak points if not properly configured. While Kubernetes does provide mechanisms for enhancing security, such as network policies and role-based access control, these features may not be enabled by default and require additional configuration.

For this reason, it's not surprising that an alarming 45% of respondents experienced a misconfiguration incident and another 42% discovered a major vulnerability to remediate. Additionally, 27% reported failing an audit. These incidents highlight the critical need for robust security measures that can keep pace with the demands of application development teams while providing the necessary protection for the full application development life cycle.

In the past 12 months, what security incidents or issues related to containers and/or Kubernetes have you experienced? (Select all that apply.)

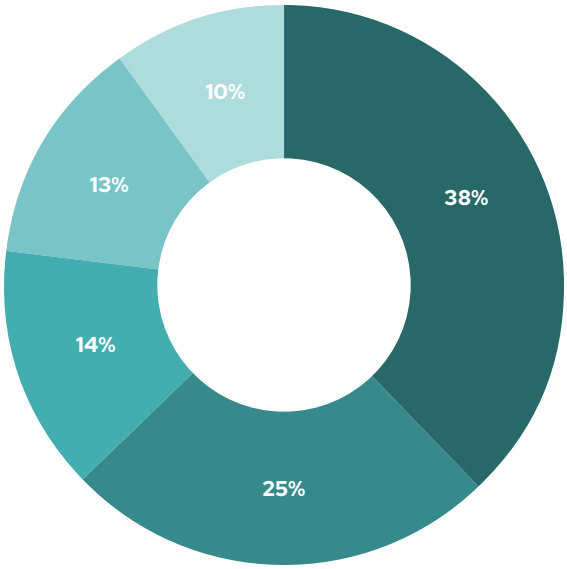
Security remains a top concern with container and Kubernetes strategies

38% of respondents either think security isn't taken seriously enough or security investment is inadequate

As the de facto container orchestrator, Kubernetes adoption continues to grow as the demand for cloud-native architectures and containerization increases. This growth hasn't always been followed by the same growth in security investments. Containers and Kubernetes introduce a new layer of complexity to the software stack, leading to additional security challenges. As mentioned previously, containers, often used in cloud-native environments, emphasize agility. Continuous delivery pipelines, for example, may not emphasize security testing and verification to the same extent as speed of deployment.

Investing in container and Kubernetes security means understanding the complexity of Kubernetes and the potential security risks associated with containerized applications, as well as implementing the necessary controls that encompass all layers of the container and Kubernetes stack. This includes the underlying infrastructure, Kubernetes control plane, the network, container images and registries, and many other components.

What is your biggest concern about your company's container strategy? (Select only one response.)



38%
It isn't taking security seriously or investing in security adequately

25%
It is progressing too slowly

14%
It doesn't account for compliance needs

13%
It doesn't address skills gaps on our team

10%
It doesn't account for cultural or process changes

Kubernetes security responsibility is highly decentralized

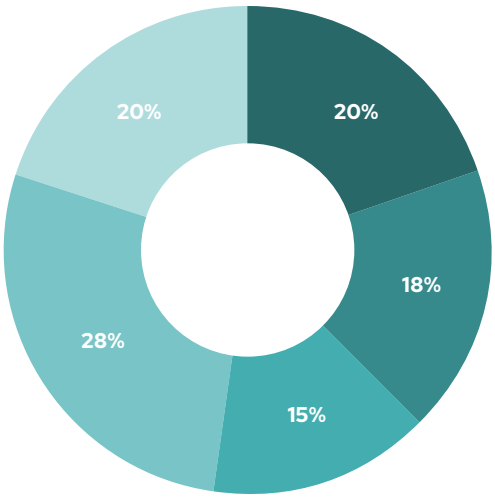
Less than a third of respondents consider the security team to be responsible for Kubernetes security

Our data once again shows that Kubernetes security responsibility isn't standardized to a single role across organizations. Only 28% of respondents consider their Security Team as the role most responsible for container and Kubernetes security. Protecting Kubernetes applications spans multiple teams because multiple teams usually contribute towards building containerized applications and Kubernetes, from building container images to setting up the cluster infrastructure, configuring the control plane, and implementing proper access controls and authorization mechanisms.

Safeguarding containerized applications requires different roles to own a piece of the system and processes used in the development life cycle, such as the DevOps team responsible for managing the cluster infrastructure, the security team responsible for implementing security policies and controls, the application developers responsible for securing their applications and the images used by them, and the operations team responsible for managing access controls and authorization mechanisms.

To bridge these gaps, container and Kubernetes security processes and tooling must facilitate close collaboration among different teams—from developers to DevOps to operations to security—instead of perpetuating team isolation that may plague organizations.

What role at your company is most responsible for container and Kubernetes security? (Select only one response.)



20%
Ops (architect, platform, infrastructure, SRE, cloud)

18%
DevOps

15%
DevSecOps

28%
Security (cloud security, security eng., InfoSec)

20%
Developer

DevSecOps isn't just a buzzword

Nearly half of respondents have a DevSecOps initiative in an advanced stage

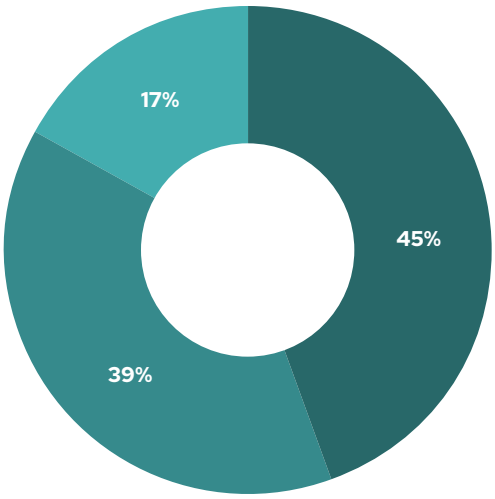
Our survey found that the majority of organizations are embracing DevSecOps—a term that encompasses the processes and tooling that allow security to be built into the application development life cycle, rather than as a separate process.

As organizations recognize the importance of integrating and automating security throughout the software development life cycle, they are likely to be more proactive and effective in identifying and mitigating security risks early in their container and Kubernetes deployments.

According to our survey, 45% of respondents have reached an advanced stage of DevSecOps integration, where security is integrated and automated throughout the software development life cycle (SDLC). This indicates that these organizations have successfully implemented DevSecOps practices and tools such as automated security testing, continuous security monitoring, and security-focused code reviews. Another 39% understand the value of DevSecOps and are in the early stage of adoption.

However, with 17% of organizations operating security separate from DevOps, lacking any DevSecOps initiatives, they may also be missing out on the benefits of integrating security into the SDLC, such as improved efficiency, speed, and quality of software delivery. This could indicate that these organizations may be more reactive in their approach to security, only addressing security issues when they arise at runtime or right before deploying applications in production rather than proactively working to prevent them. They are likely paying the price in the form of slower application rollouts.

Do you have a DecSecOps initiative in your organization? (Select only one response.)



45% Yes
It's in an **advanced stage**, where we're integrating and automating security throughout the life cycle

39% Yes
It's in an **early stage**, with DevOps and security collaborating on joint policies and workflows

17% No
DevOps and Security remain separate, with minimal collaboration

Vulnerabilities and misconfigurations are top security concerns with container and Kubernetes environments

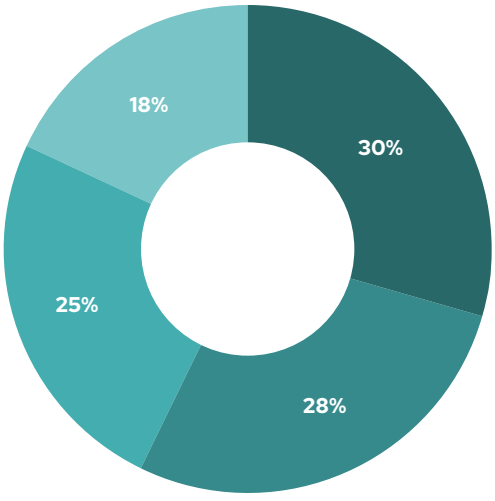
More than 50% of respondents are worried about misconfigurations and vulnerabilities, owing to the fact that containers and Kubernetes are highly customizable

Containers and Kubernetes are highly complex, with various components that need to be securely configured. The dynamic environments in which containers operate, with containers turning on and off rapidly, also makes it a challenge to maintain consistent security posture. The shared host operating system kernel and other resources also mean that a single vulnerability in one container can potentially affect other containers on the same host, while a vulnerability in the host itself can potentially affect all containers running on that host. The large number of third-party components, such as base images, libraries, dependencies, adds yet another layer for individuals to configure and ensure that they remain free of vulnerabilities.

Taken together, this makes managing security configuration and detecting and mitigating vulnerabilities a particularly challenging task, and something that our survey respondents worry about the most.

One of the ways to mitigate the risks of misconfigurations and vulnerabilities is to automate the security scanning necessary to detect the most common security issues, such as making sure containers aren't running with root privileges, fixable vulnerabilities don't end up in production environments, and you are not running with default configurations for security-sensitive components.

Of the following risks, which one are you most worried about for your container and Kubernetes environments? (Select only one response.)



30%
Vulnerabilities

28%
Misconfigurations/exposures

25%
Attacks

18%
Failing compliance (SOC2, PCI, HIPAA, etc.)

The majority of companies with security misconfiguration concerns are taking steps to address them

Exposed/unprotected sensitive data is the most worrying security misconfiguration (32%)

With security configuration as one of the leading causes for concern, we asked respondents the exact misconfigurations that worry them the most, and the responses made it clear there isn't a single misconfiguration that is significantly more worrisome than the rest. This underscores the challenge of and the need for taking a comprehensive approach to understanding all the various components of containers and Kubernetes that expose you to a security risk and implementing developer-friendly controls that bring your security risk down to an acceptable level.

The good news in our finding is that organizations aren't simply ignoring these security risks, but are actively taking steps to address them. For example, retaining default configurations has often been a pain point for many security experts across all IT functions, and 75% of our respondents who worried about retaining default configurations are also taking steps to address it.

Which of the following types of security misconfigurations are you most worried about? (Select all that apply.)		Which of the following types of security misconfigurations is your company taking steps to address? (Select all that apply. Results among those who cite each concerns.)
32%	Exposed/unprotected sensitive data	72%
29%	Unpatched flaws	70%
28%	Retaining default configurations	75%
28%	Coding errors	72%
26%	Unused components deployed increasing attack surface	67%
26%	Poor network security	76%
24%	Overprivileged containers	70%
24%	Use of insecure/untrusted image roots	59%
23%	Undetected malware	71%
23%	Stale, unscanned, or unverified images	66%
23%	Inadequate access controls (IAM, RBAC)	67%
20%	Presence of known fixable vulnerability	60%
16%	Exposed network port	52%

The consequences of a security misconfiguration can lead to serious problems for the application or business at large

Ransomware attacks due to a misconfiguration are the most often cited concern (40%)

Researchers often find that human error is behind the vast majority of security breaches.[2] What's especially concerning about breaches due to human error is that they can take longer to detect and mitigate, increasing the overall cost of the breach.[3] Security misconfigurations are often a human-driven process and therefore pose a serious threat to containers and Kubernetes, especially when there isn't an automated way to scan the systems to detect the misconfiguration.

41% of our respondents worry the most about ransomware attacks as a consequence of security misconfiguration, and a whopping 53% of those have experienced a ransomware attack in the last 12 months. In every instance where a respondent selected a particular consequence of a misconfiguration as one of their worries, a significantly larger number of the respondents had actually experienced that consequence. For example, while 34% of respondents worry about data deletion as a consequence of a security misconfiguration, 46% of respondents have actually experienced their data being deleted due to a security misconfiguration.

One explanation for this phenomenon could be that individuals are inundated with the number of security issues to worry about and some are simply not worth worrying about, despite the prevalence of security incidents tied to that worry. This could be due to lack of resources and understaffing for critical security roles. Another reason could be that container and Kubernetes security responsibility might be too decentralized (as we found out earlier), leading to a lack of strong ownership by any group across the organization, which might explain the general misalignment in how much respondents worry about consequences of misconfigurations compared to how often they experience those consequences.

Which of the following consequences of security misconfigurations are you most worried about? (Select all that response.)		Which of the following consequences of security misconfigurations has your company experienced in the past 12 months? (Select all that apply. Results among those who cite each concerns.)
40%	Ransomware	53%
38%	Exposure of sensitive data (PII)	50%
36%	Denial of service attack	57%
36%	Unauthorized lateral movement	54%
34%	Malware execution, resource hijacking, crypto mining, or other unauthorized processes execution	48%
34%	Data deletion	46%
32%	Unauthorized access to internal cloud resources	53%
29%	Compromised credentials	50%

2. "2022 Data breach investigations report." Verizon, accessed 14 March 2023

3. "Cost of a data breach 2022: A million-dollar race to detect and respond." IBM, accessed 14 March 2023.

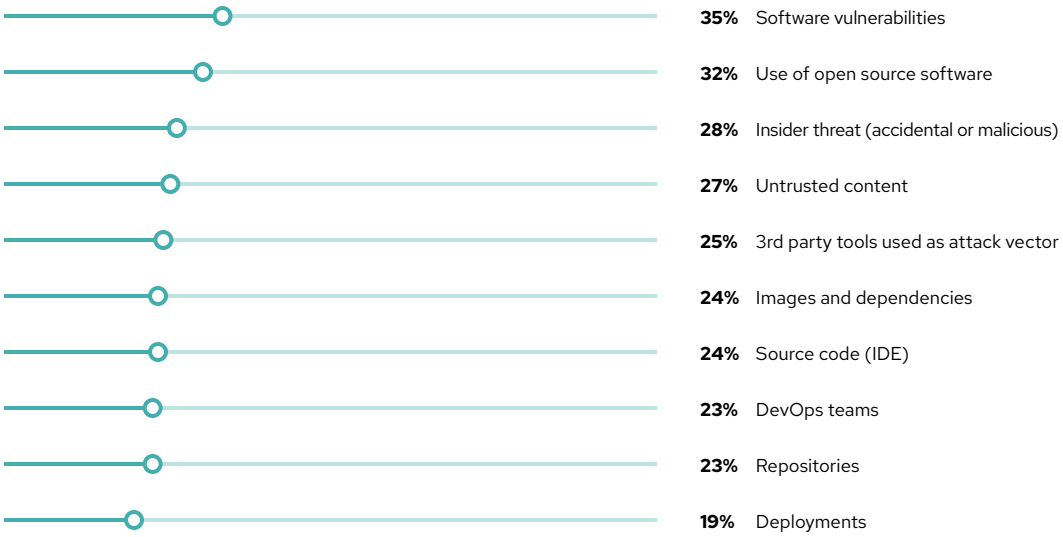
Use of open source software is a big concern for software supply chain security

35% of respondents worry the most about software vulnerabilities related to their software supply chain

Software supply chain security has been a hot topic, and supply chain attacks are increasing rapidly,[4] especially after the SolarWinds attack and the discovery of Log4Shell and Spring4Shell[5] vulnerability. For this reason, we asked our survey respondents a variety of questions related to their software supply chain security in Kubernetes.

The survey findings indicate that respondents are concerned about various aspects of the software supply chain, with the top concerns being software vulnerabilities and use of open source software. Concerns about software vulnerabilities are understandable, as software vulnerabilities can lead to serious security incidents, such as data breaches, malware infections, and unauthorized access. The use of open source software poses a security challenge to software supply chains, as open source software is widely used in modern software development, and it may also introduce security risks if it contains vulnerabilities or is not properly maintained.

What aspects of the software supply chain are you worried about the most? (Select all that apply. Top responses reported.)



4. Constantin, Lucian. "Supply chain attacks increased over 600% this year and companies are falling behind." CSO news analysis, 19 Oct. 2022.

5. Kovacs, Eduard. "Vendors assessing impact of Spring4shell vulnerability." Securityweek, 4 April 2022.

Software supply chain security concerns are not misplaced

Many of those concerned have experienced supply chain security issues in the last 12 months

To better understand how organizations measure their security risk from individual components of the software supply chain, we asked respondents which specific software supply chain security issues were they most concerned with and of these, which ones have they experienced in the last 12 months.

Our findings are in line with what would be expected from sprawling software supply chains that are emblematic of a containerized environment. There are many security considerations that affect the security posture of a software supply chain, with the top three being vulnerable application components (32%), insufficient access controls (30%), and a lack of software bill of materials (SBOM) or provenance (29%).

What's also alarming is that more than half of the respondents have experienced virtually every issue that we identified in our question, with vulnerable application components and continuous integration/continuous delivery (CI/CD) pipeline weakness as the top two most cited issues that were experienced, with 69% and 68% respectively.

Which of the following software supply chain security issues is your company most concerned about? (Select all that apply.)		Which of the following software supply chain security issues has your company experienced in the past 12 months? (Select all that apply. Results among those who cite each concern.)
32%	Vulnerable application components	69%
30%	Insufficient access controls	58%
29%	Lack of Software Bill of Materials (SBOM) or provenance	62%
29%	Lack of automation	56%
28%	Lack of auditability	65%
27%	Insecure container images	66%
24%	Inconsistent policy enforcement	50%
19%	CI/CD pipeline weaknesses	68%
19%	Insecure IaC templates	58%
17%	Version control weaknesses	62%

Scanning and attestation are two of the most important security controls in software supply chains

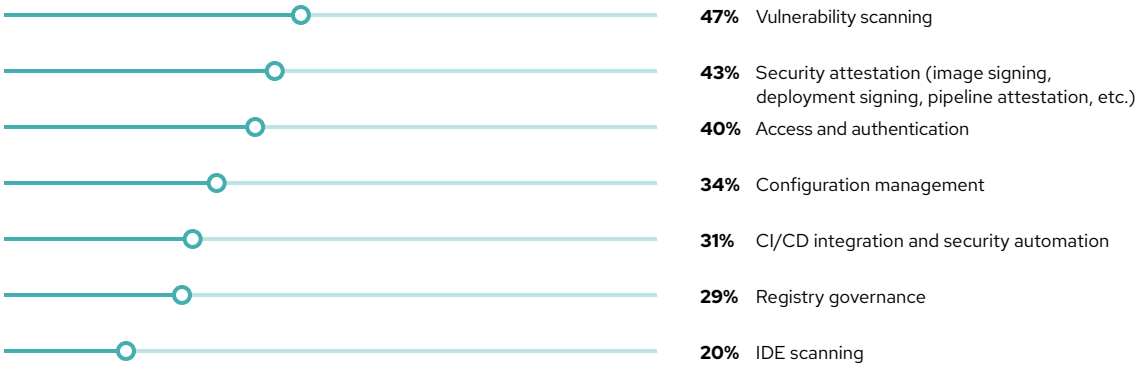
Nearly half of respondents identified artifact signing as the most important

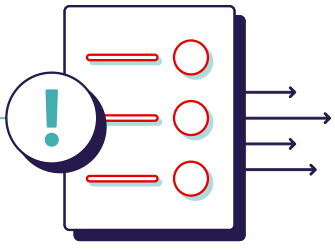
Trust is a critical component of software supply chain security. Since software is built and maintained by various parties within the supply chain, such as internal developers, third-party vendors, and open source contributors, ensuring that each party's contribution can be trusted can be challenging without the necessary mechanisms.

Security attestation provides a way to ensure that the software in use meets minimum security standards and hasn't been tampered with. This builds trust while reducing the risk of security incidents or vulnerabilities being introduced in the software supply chain.

As software supply chain attacks continue to increase and awareness around the tools and processes that mitigate the attacks increases, in our future surveys, we hope to see more than 43% of respondents identify security attestation as important to their software supply chain security.

Which of the following are most important when it comes to software supply chain security? (Select up to three most important aspects. Top responses reported.)





KubeLinter and Kube-hunter are the top open source tools in use for Kubernetes security

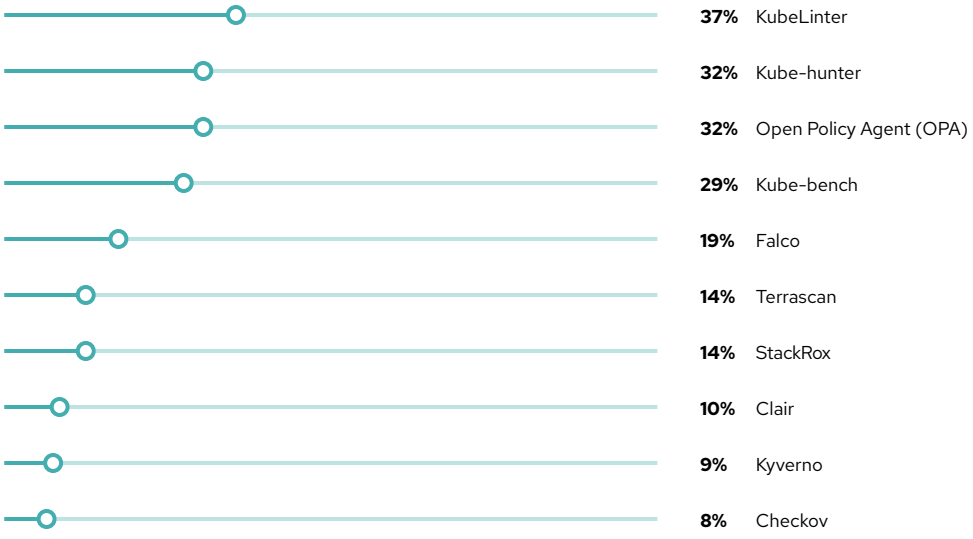
Open Policy Agent is tied with Kube-hunter as the second most used open source security tool.

Kubernetes, as one of the fastest growing open source projects ever, is supported by a rich ecosystem of open source tools and dedicated contributors who have closed many of the security gaps in containers and Kubernetes.

Alongside commercial Kubernetes security products, our respondents rely on these open source security tools to protect their cloud-native applications.

KubeLinter, an open source YAML and HELM linter for Kubernetes, is used by 37% of respondents, while 32% say they use Kube-hunter, a security testing and scanning tool used to identify security issues in Kubernetes clusters and other cloud-native environments. Another 32% use Open Policy Agent (OPA), an open source policy engine that offers a unified policy framework for not just Kubernetes but also Istio, Envoy, Prometheus, and more.

Which of the following open source tools do you use for Kubernetes security? (Select all that apply.)



3 tips for achieving better security

When security becomes an afterthought, organizations put at risk the core benefit of faster application development and release by not ensuring that their cloud-native environments are built, deployed, and managed securely.

Our findings show that what happens in the build and deploy stages has a significant impact on security, which was underscored by the prevalence of misconfigurations and vulnerabilities across organizations. Security, therefore, must shift left, imperceptibly embedding into DevOps workflows instead of being "bolted on" when the application is about to be deployed into production.

1 Use Kubernetes-native security architectures and controls

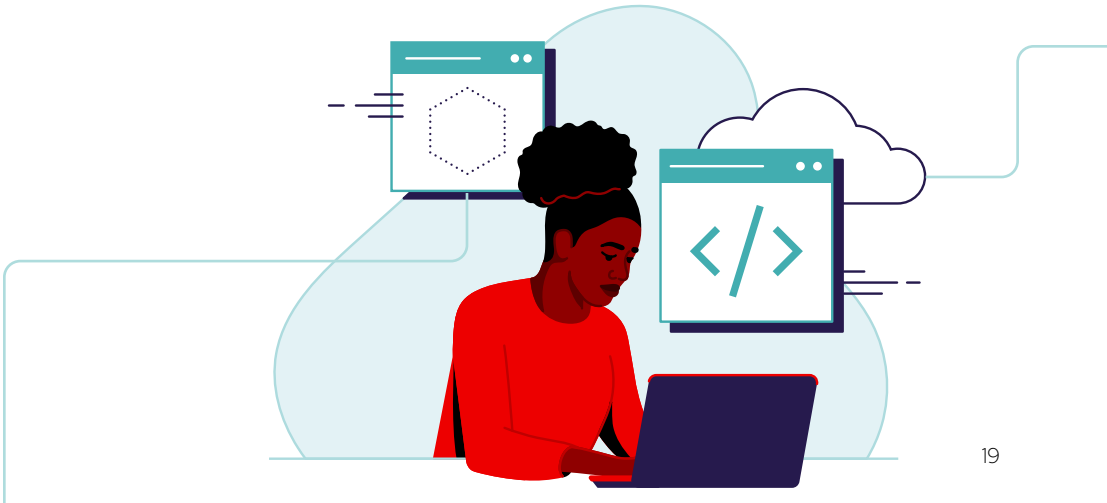
Kubernetes-native security uses the rich declarative data and native controls in Kubernetes to deliver several key security benefits. Analyzing the declarative data available in Kubernetes yields better security, with risk-based insights into configuration management, compliance, segmentation, and Kubernetes specific vulnerabilities. Using the same infrastructure and its controls for application development and security reduces the learning curve and supports faster analysis and troubleshooting. It also eliminates operational conflict by ensuring security gains the same automation and scalability advantages that Kubernetes extends to infrastructure.

2 Security should start early but extend across the full life cycle, from build/deploy to runtime

Security has long been viewed as a business inhibitor, especially by developers and DevOps teams whose core mandates are to deliver code fast. With containers and Kubernetes, security should become a business accelerator by helping developers build strong security into their assets right from the start. Look for a container and Kubernetes security platform that incorporates DevOps best practices and internal controls as part of its configuration checks. It should also assess the configuration of Kubernetes itself for its security posture, so developers can focus on feature delivery.

3 Transform the developer and DevOps user into a security user by building a bridge between DevOps and SecOps

Given most organizations don't have a clear role or team solely responsible for container and Kubernetes security, your security tooling must help bridge the various teams, from Security and Ops to DevOps and Development. To be effective, the platform must have security controls that make sense in a containerized, Kubernetes-based environment. It should also assess risk appropriately. Telling a developer to fix all 39 discovered vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of seven or higher is inefficient. Identifying for that developer the three deployments that are exposed to that vulnerability, and showing why they are risky, will significantly improve your security posture.

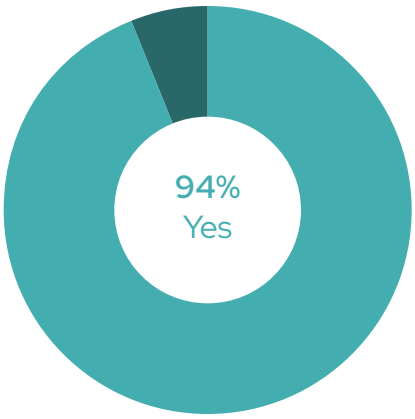


About our respondents

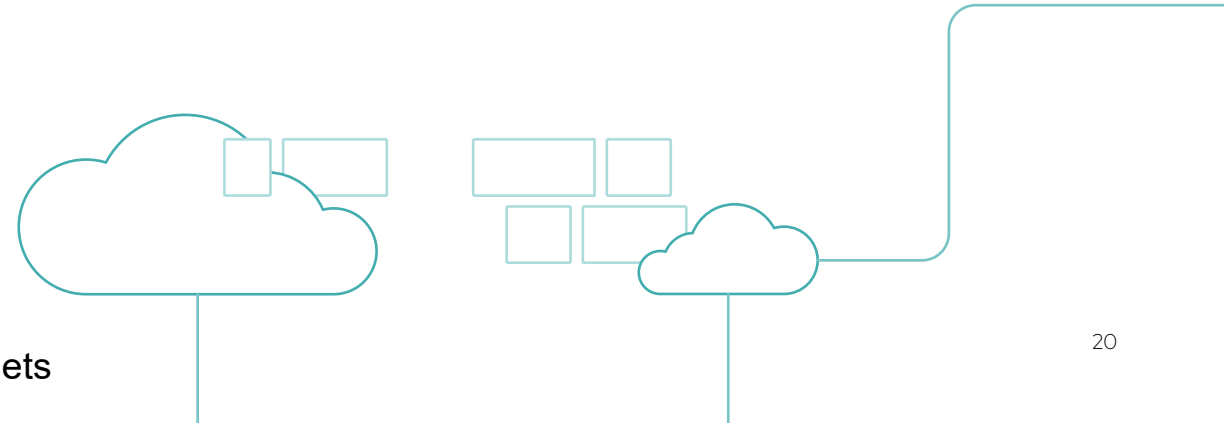
Kubernetes adoption

Most of our respondents use Kubernetes in production, with Amazon EKS, Red Hat® OpenShift®, and self-managed Kubernetes, as the three most popular Kubernetes services.

Are you running any production workloads on Kubernetes?



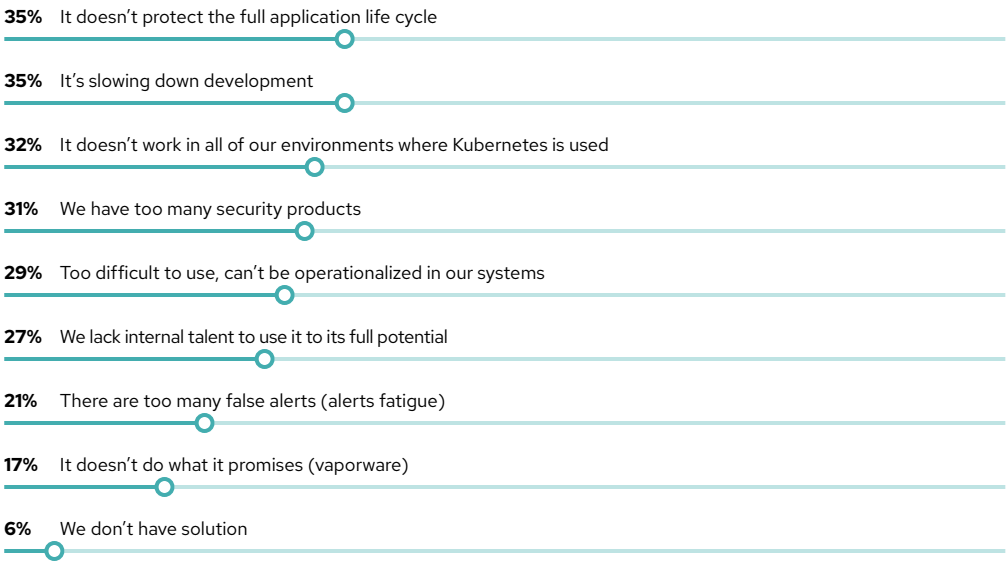
What Kubernetes platform do you use to orchestrate your containers? (Select all that apply.)



Common pain points with Kubernetes security solutions

Lack of full life cycle security and slowing down deployment are the 2 most common complaints with respondent's current Kubernetes security solutions

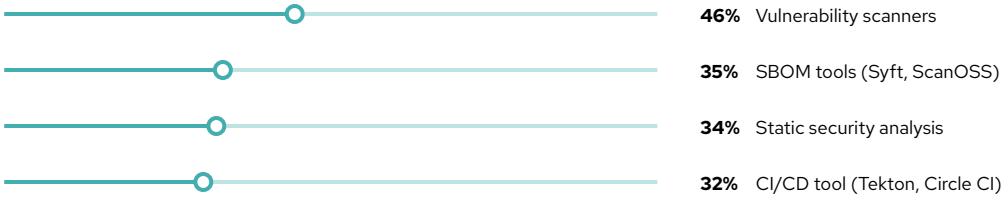
Which of the following are the biggest pain points you experience with your current Kubernetes security solution? (Select up to three top pain points.)



Security tools used for supply chain security

Vulnerability scanners are the most used security tool, followed by SBOM, static security analysis, and CI/CD tools.

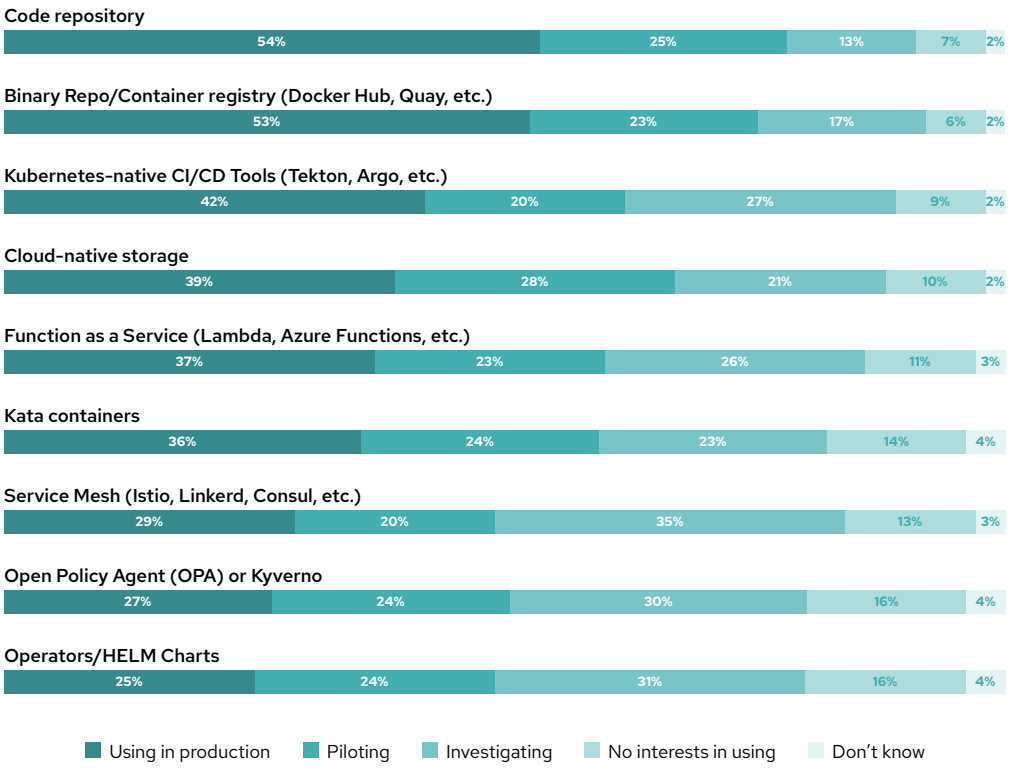
Which of the following types of security tools do you use for your software supply chain? (Select all that apply. Top responses reported.)



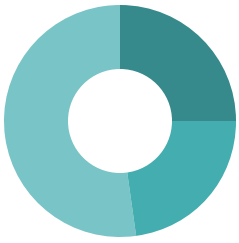
Other cloud-native technology adoption

Kubernetes-native CI/CD tools are among the top 3 types of cloud-native technologies in use.

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

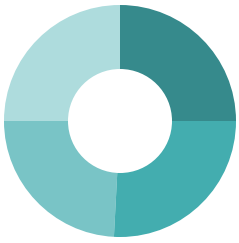


Core demographics



Company size

25% 100 to 499 employees
23% 500 to 999 employees
52% 1,000+ employees



Industry

25% Technology
26% Finserv
24% Telco/media/entertainment
25% Other industries

Learn more about Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes is a Kubernetes-native container security platform that protects your application across build, deploy, and runtime as you progress on your container journey.

As your environment grows more complex and you depend on more automation, our platform will let you operationalize security in those more sophisticated environments and keep pace with the speed of DevOps.

Kubernetes-native security provides the following crucial benefits.

- **Minimize operational risk:** Align security with DevOps by using Kubernetes-native controls to mitigate threats and enforce security policies that minimize operational risk to your applications.
- **Reduce operational cost:** Reduce the overall investment in time, effort, and personnel, and streamline security analysis, investigation, and remediation by using a common source of truth.
- **Accelerate DevOps productivity:** Accelerate the pace of innovation by providing developers actionable and context-rich guardrails embedded into existing workflows and tooling that supports developer velocity.

Ready to see Red Hat Advanced Cluster Security for Kubernetes in action? Get a personalized demo tailored for your business and needs.

Request demo