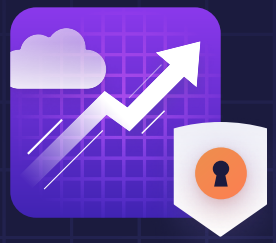
SNYK REPORT

snyk

State of Cloud Native Application Security

How cloud native adoption transforms the way organizations defend against security threats



As cloud native adoption increases, security needs to be built in as standard

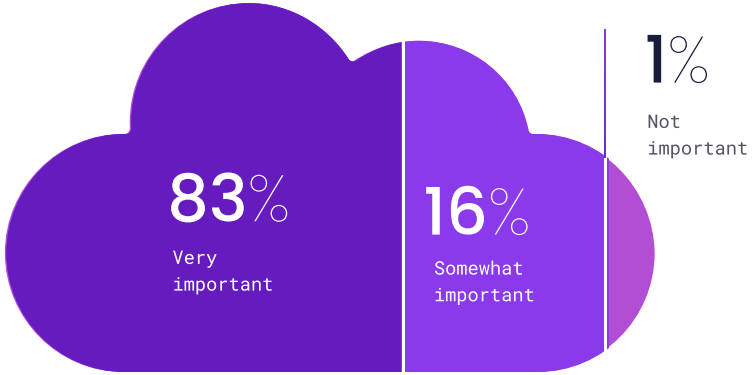
99% of companies recognized security as important to their cloud native strategy

Success in the cloud native era is defined by an organization's ability to deliver new versions of software faster and more efficiently, which is reinforced by our survey results. Being able to deploy code to production faster and more easily manage those applications were the primary reasons for moving towards containerized infrastructure. However, as companies embrace cloud native technologies as part of their digital transformation, security is seen as a key factor to building successful platforms. While only 36% of respondents stated that security was one of the main reasons for moving their production applications into containers, **99% of respondents recognized security as an important element in their cloud native strategy**. In addition, over 80% stated security is very important to them.

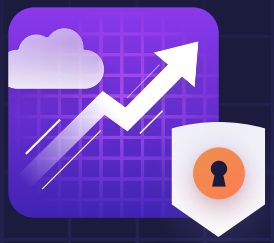
What are the main reasons for moving your applications into containers?

68%	67%	43%	36%	11%
Deployment velocity	Ease of management	Reduce costs	Improved security	Attracting talent

How important is security to your cloud native strategy?

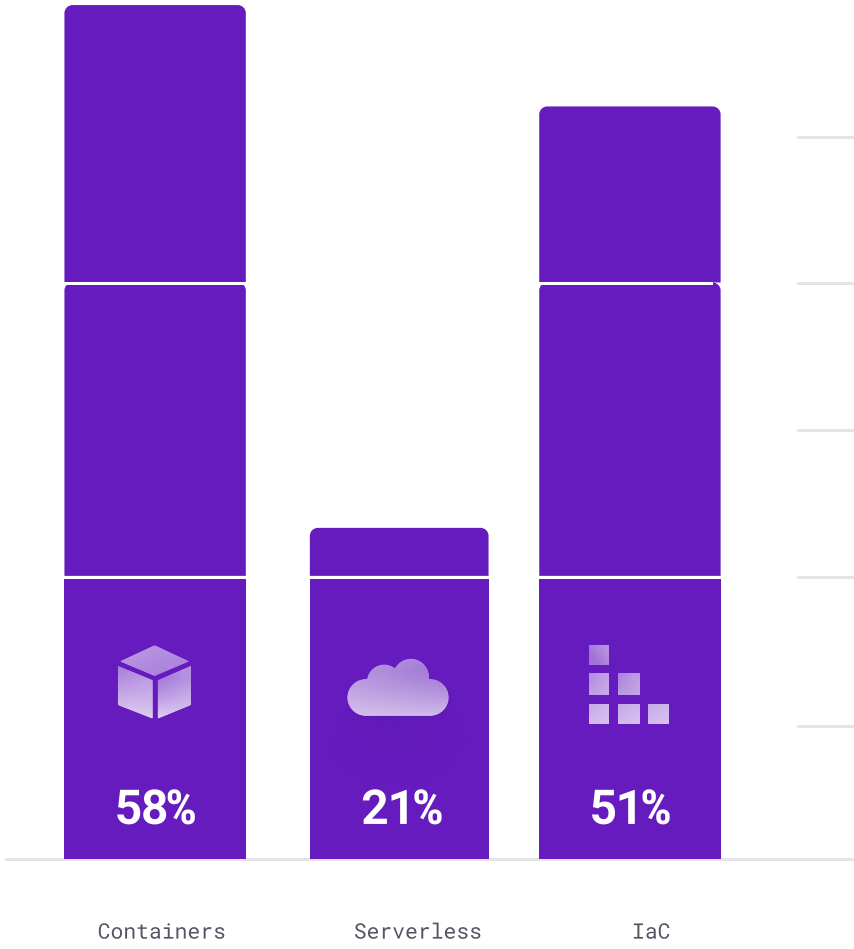


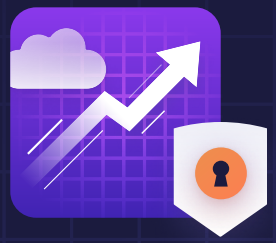
snyk



Over 78% of production workloads are deployed as containers or serverless applications

In total over 78% of production workloads are deployed as containers or serverless applications. Containers continue to be the dominant mechanism for cloud native application deployment, with nearly 60% of production workloads deployed in containers. Penetration of serverless technologies is now significant across all company sizes, and makes up more than a fifth (mean average) of all production workloads. Usage of cloud native technologies is strong across all company sizes, indicating that adoption is becoming mainstream. With over 50% of respondent's workloads also being deployed with some form of Infrastructure As Code, use of software-driven infrastructure has increased alongside the container and serverless growth trends. Usage of these core technologies is one of the key indicators of cloud native transformation in general, and so we use these metrics throughout this report as indicative of the level of adoption within an organization.





SNYK REPORT

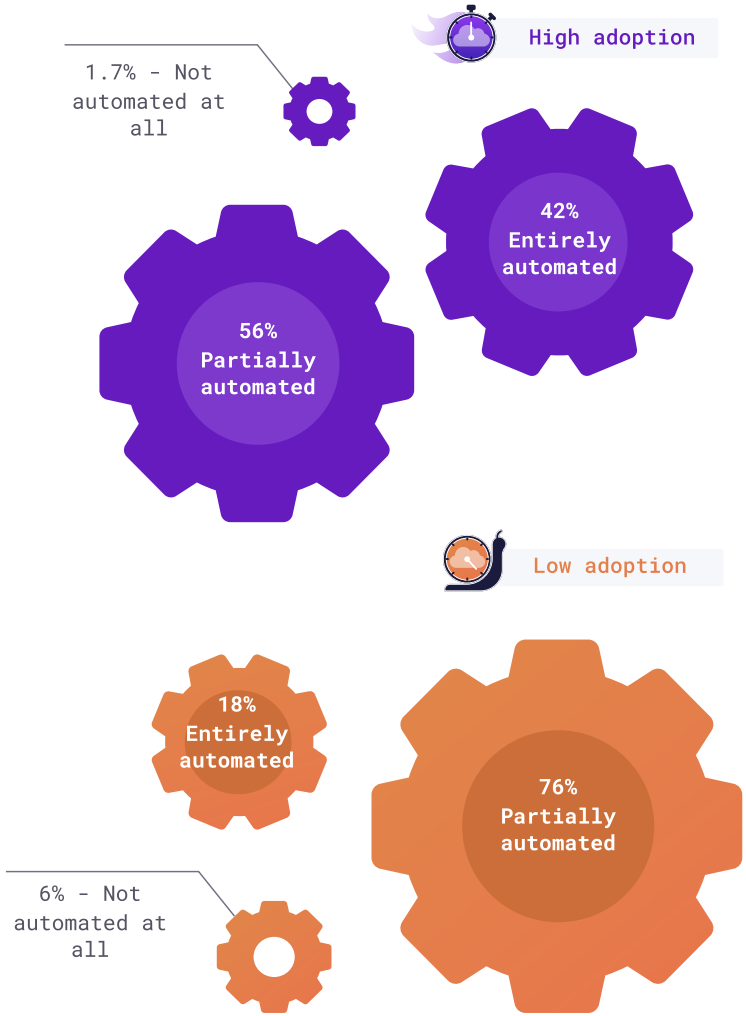
Download Snyk's Infrastructure as Code Security Insights report for the trends on how companies are using and securing IaC today and common roadblocks to it's wide spread use

DOWNLOAD NOW

While 95% of respondents use automation, only 33% fully automate their deployment pipeline

Deployment automation is one of the key tenets of cloud native practices, enabling development velocity. Our survey showed that over 95% of respondents were using some level of automation with almost a third having an entirely automated deployment pipeline. By comparing the upper and lower quartiles of cloud native production usage (high levels of adoption vs low levels of adoption), we can see that organizations that show high levels of cloud native adoption are over twice as likely to have an entirely automated deployment process than organizations with low cloud native adoption.

Are your application deployments manual or automated?

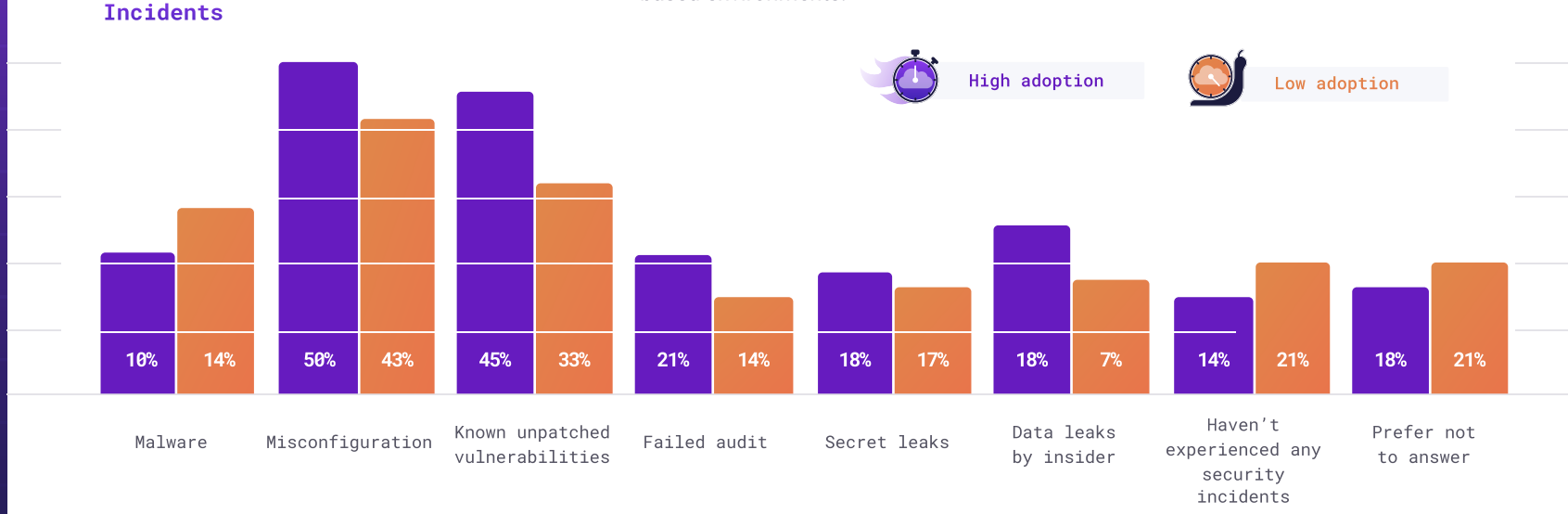


Over half of respondents suffered from a misconfiguration or known vulnerabilities incident

Misconfiguration and known unpatched vulnerabilities were responsible for the greatest number of security incidents in cloud native environments

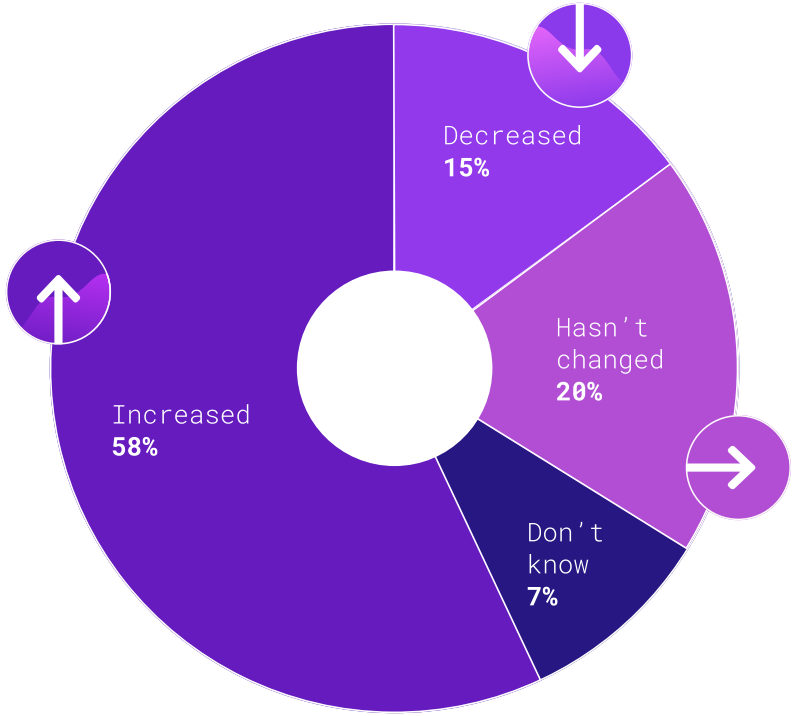
In contrast to where organizations are most concerned, we also asked about previous incidents that occured in production. The top two incident types by a distance were misconfiguration and known unpatched vulnerabilities, at 45% and 38% respectively. Over 56% experienced a misconfiguration or known unpatched vulnerability incident involving their cloud native applications.

Data leaks by insiders were more than twice as likely to have occurred in organizations with high levels of cloud native adoption, reinforcing that adopting zero trust principles becomes increasingly important in fully automated cloud based environments.



Nearly 60% have increased security concerns since adopting cloud native

Adoption of cloud native technologies will undoubtedly change the security posture of your overall application. While the core security principles remain constant, as with all emerging ecosystems the best practice is still being defined, driving fresh concern as teams navigate through unfamiliar landscapes. Our survey shows organizations are nearly 4x more likely to have increased rather than decreased concerns over their security posture since adopting cloud native.

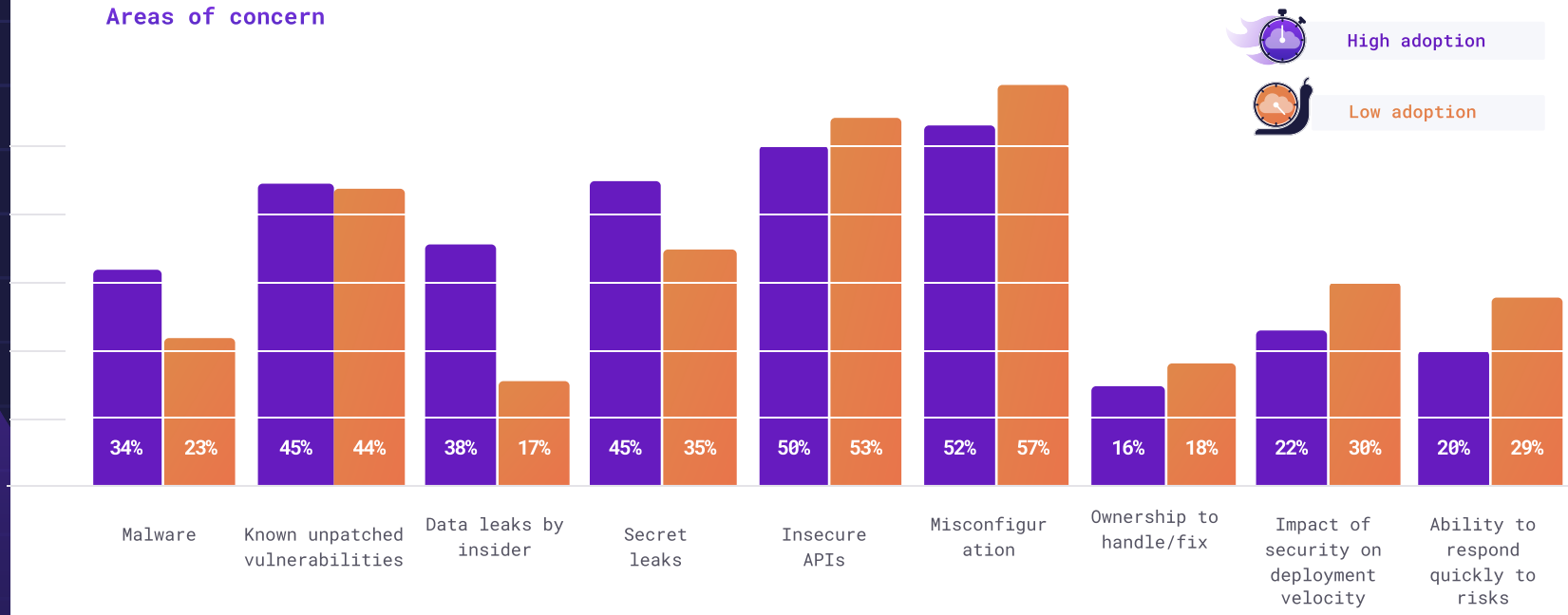


snyk

Misconfiguration is the area of most concern when moving to cloud native

Cloud native platforms utilizing automated tooling will rely on credentials such as secrets and API tokens in order to operate, and necessitates a more decentralized approach to managing such access. The need for effective management of these kinds of artifacts is a key differentiator from the more centralized pre-cloud era, and a major area of concern for operations teams transforming their infrastructure. Our survey showed that misconfigurations were the biggest area of increased concern, with over half of respondents stating it's a bigger problem for them since moving to a cloud native platform. Despite secret leaks and data leaks not showing up highly in the actual incidents data, they feature strongly as areas of increased worry particularly among high adopters of cloud native technologies.

Areas of concern



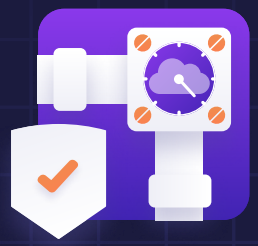
snyk

Highly automated pipelines are twice as likely to be incorporate security testing throughout their development lifecycle

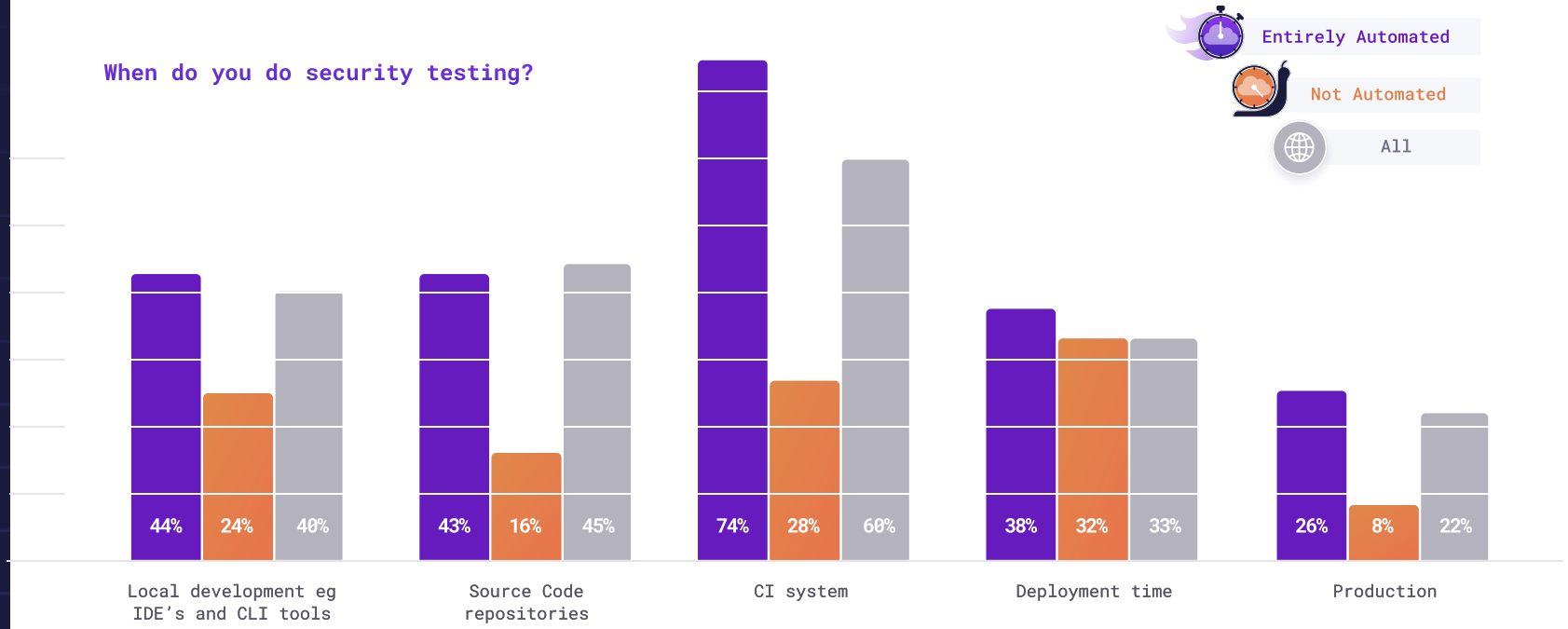
Deployment automation unlocks scalable security controls

While building fully automated deployment pipelines can be challenging, once automation and processes are in place, they can create a virtuous cycle providing multiple integration points to enable further automation This is a key enabler for security testing. Companies with high levels of deployment automation were more than twice as likely to have adopted security testing at all points throughout the software development lifecycle, when compared to organizations with no automation. While companies of all sizes showed a clear preference to test in CI and earlier, enterprises were more likely to also be testing during later deployment and production stages. Despite testing in local development environments, such as an IDE, being a developer driven task, more automated organizations were nearly twice as likely to see their development teams adopt security early on in their workflows.

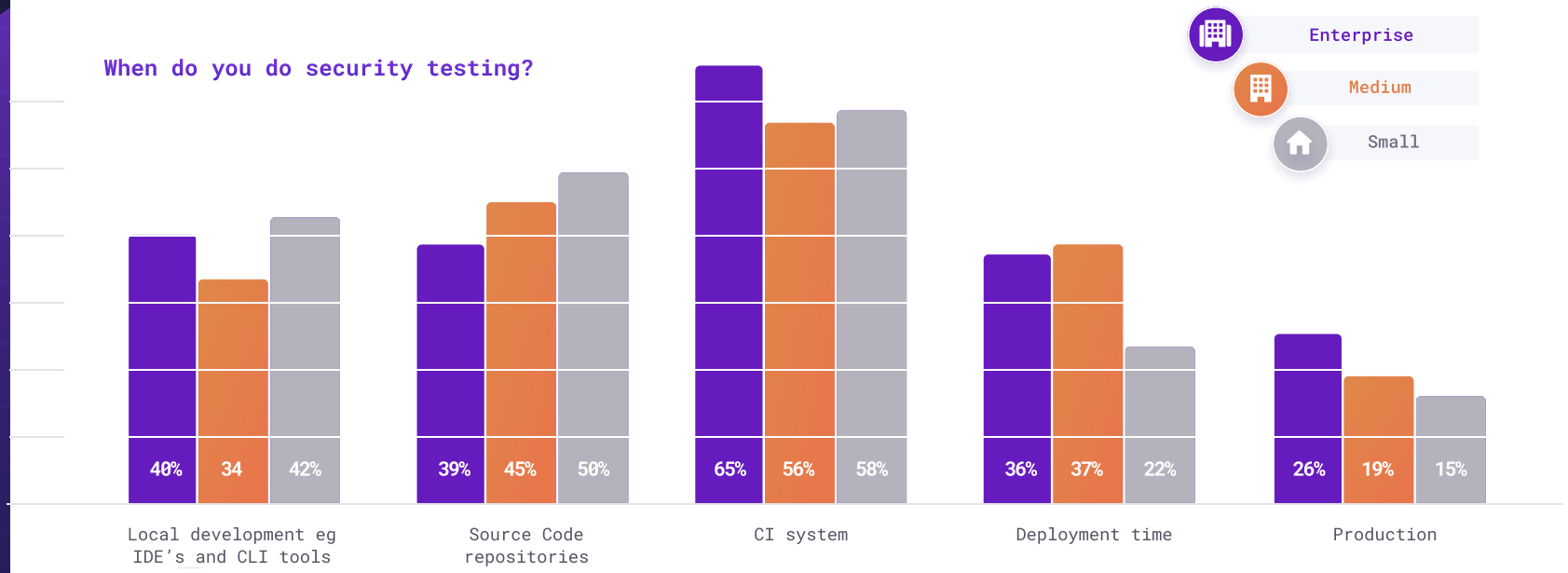
snyk



When do you do security testing?



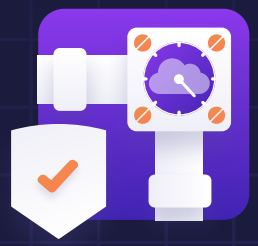
When do you do security testing?



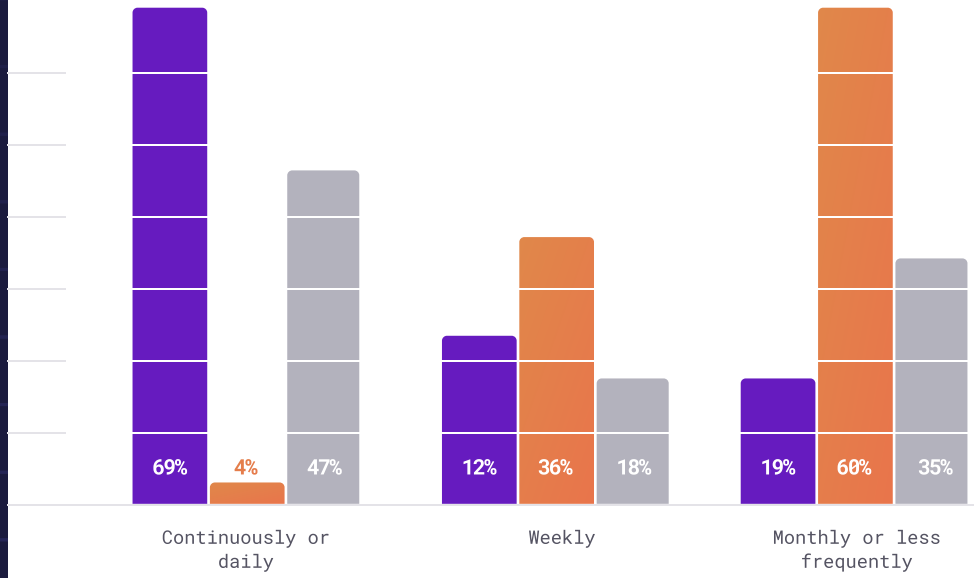
snyk

Continuous deployment empowers continuous testing

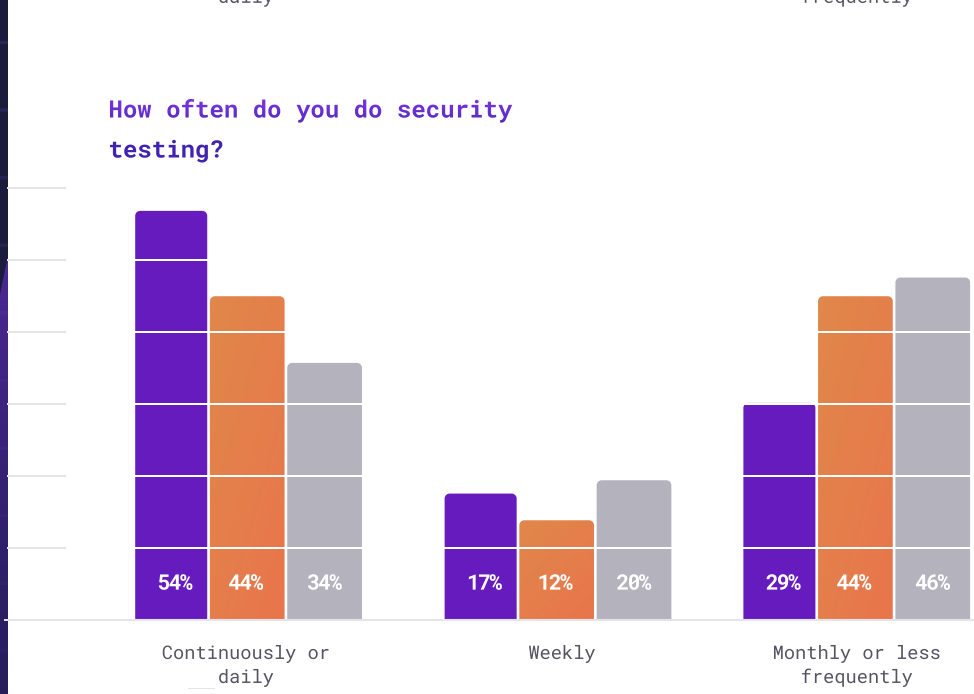
Once the use of security tooling is integrated throughout the software development lifecycle, this dramatically expands the possibilities for more regular security testing. Nearly 70% of respondents with high levels of deployment automation were able to test their security daily or more frequently. This was 17x more than respondents who had no deployment automation, and 60% of those only tested their security monthly or less frequently. This was 3x more than respondents who had full deployment automation.



How often do you do security testing?



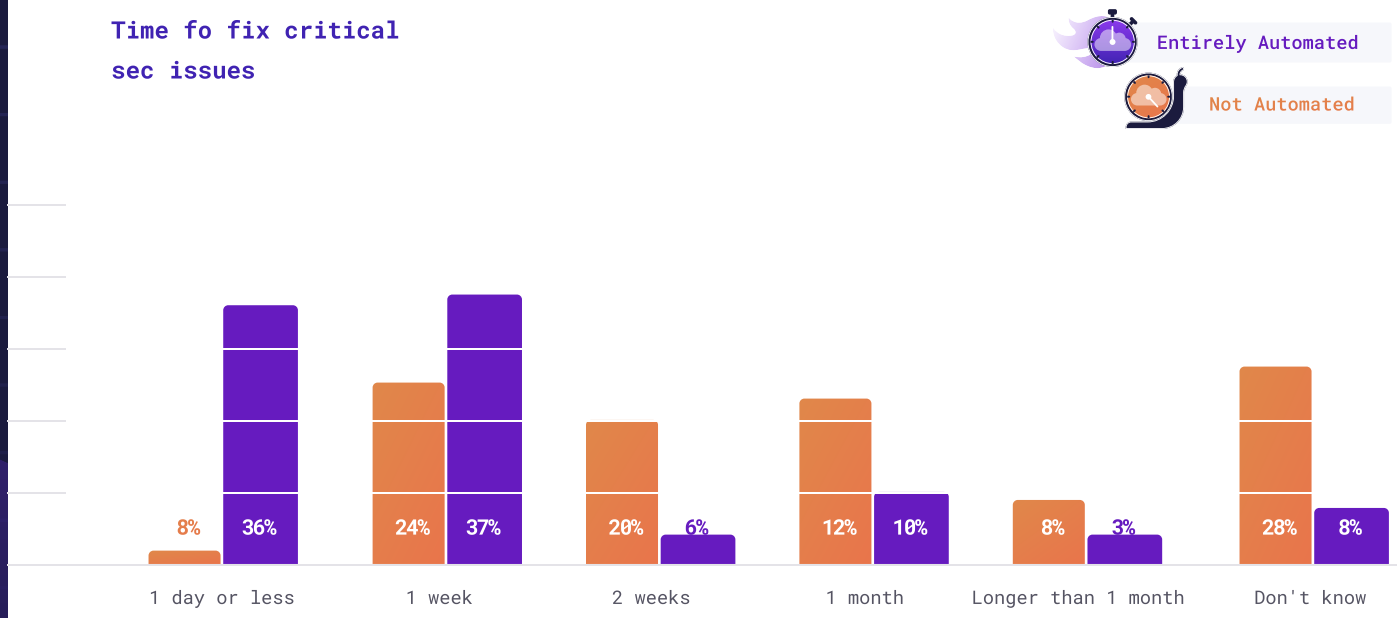
How often do you do security testing?



snyk

Over 72% of fully automated teams find and fix critical vulnerabilities in under 1 week

Testing faster leads to fixing faster. Over 72% of respondents with high levels of automation had an average time to fix vulnerabilities of less than one week, with 36% having an average of one day or less. Those with full automation were over 4x more likely to fix security issues in a day and over twice as likely to fix within a week. Automated testing is also a key enabler of visibility - you can't fix what you can't see. This was reinforced by the 28% of organizations with low levels of automation who responded that they didn't know how long it takes them to fix issues.



snyk

Automation empowers shift left security

Companies who automate are twice as likely to implement security testing

Adopting a broad and deep approach to security practices throughout the software development life cycle is key to a successful Cloud Native Application Security program. Our survey shows that companies with higher levels of cloud native automation have a greater adoption of security testing techniques. They tend to focus more on Static Application Security Testing (SAST), scanning for vulnerabilities in application dependencies with Software Composition Analysis (SCA), container image testing, and scanning infrastructure as code which are all techniques which fit well into the paradigm of automation. Organizations with fully automated deployment pipelines are twice as likely to adopt SAST and SCA tooling into their SDLC, and almost 3x as likely to add Dynamic Application Security Testing (DAST), although in general, dynamic testing isn't as well adopted when compared with static testing. Policy compliance testing is still an emerging field, with only 23% of respondents having adopted it.

Enterprises are more likely to adopt security practices, yet smaller companies with less established security practices are keeping up

Larger companies and enterprises are, of course, more likely to have the resources to run dedicated security teams so it shouldn't come as a surprise to see enterprises having the support to adopt formal Cloud Native Application Security Practices. While in smaller organizations the security function may be wholly owned by another org, such as the engineering teams, our survey shows that they are still able to keep up, particularly in the static testing space with over half of small organizations adopting SAST, SCA and container image scanning.

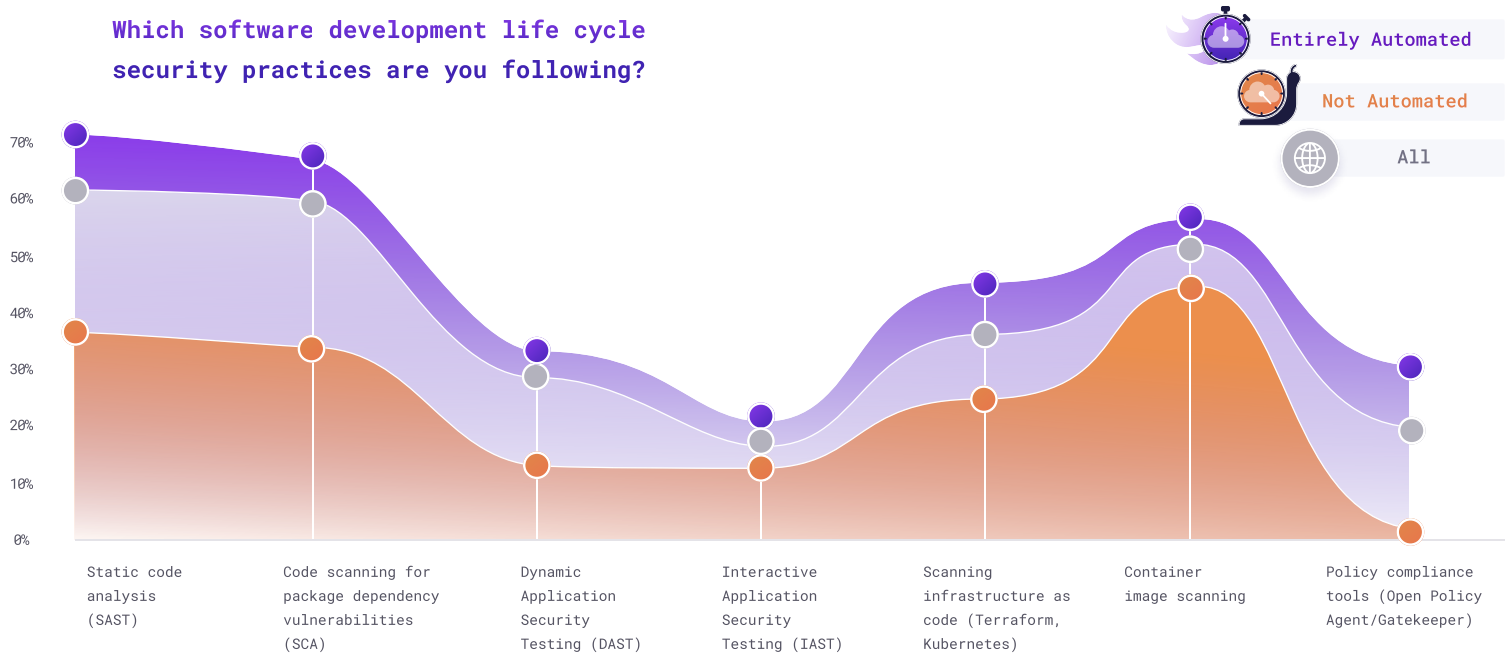
snyk

WEBINAR

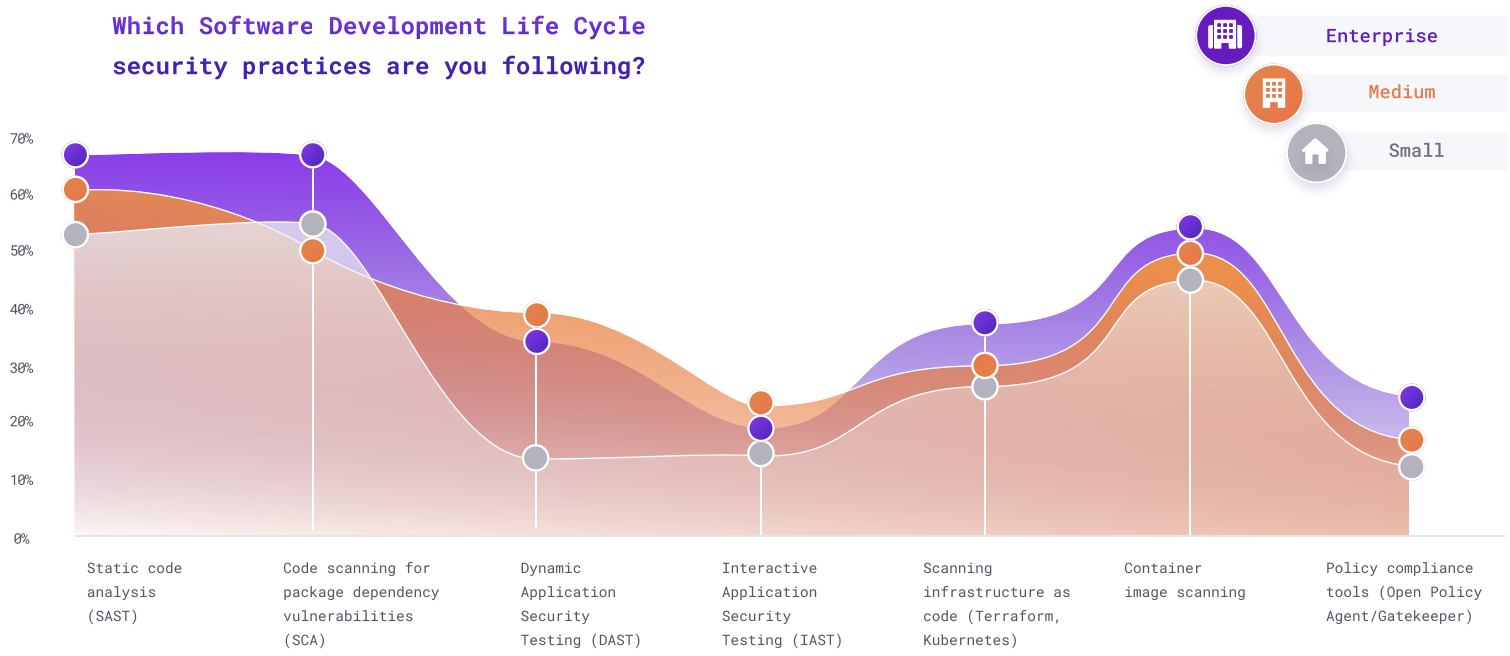
Watch this on-demand webinar to learn tips for implementing security automation into modern development environments

WATCH NOW

Which software development life cycle security practices are you following?



Which Software Development Life Cycle security practices are you following?



Security isn't just for the security team

Developers are adding security to their stack of hats

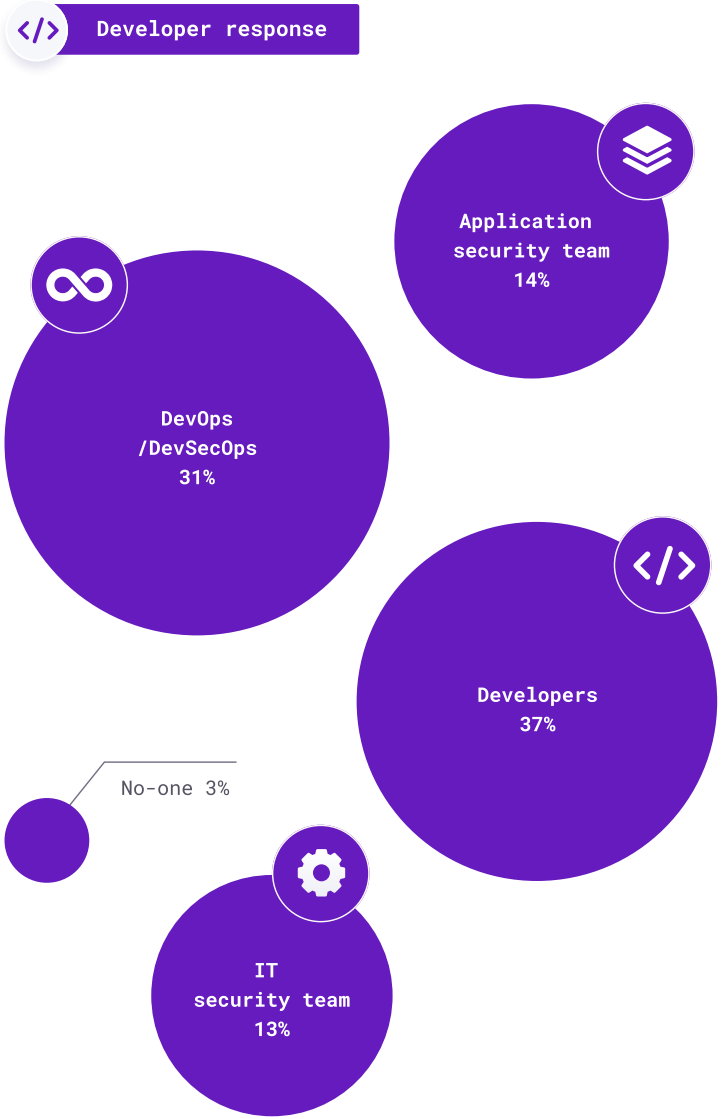
The move towards the concept of DevSecOps has accelerated in conjunction with adoption of cloud native technologies, as security shifts left in the software development lifecycle. Developers now have a pivotal role in ensuring that cloud native applications and infrastructure are secure since they increasingly contribute to the application, the infrastructure code, and workload deployment technologies. With this in mind, perception of security ownership provided interesting results in our survey set. While less than 10% of respondents in security roles believed developers were responsible for the security of their cloud native environment and applications, over 36% of developers stated that they were responsible.

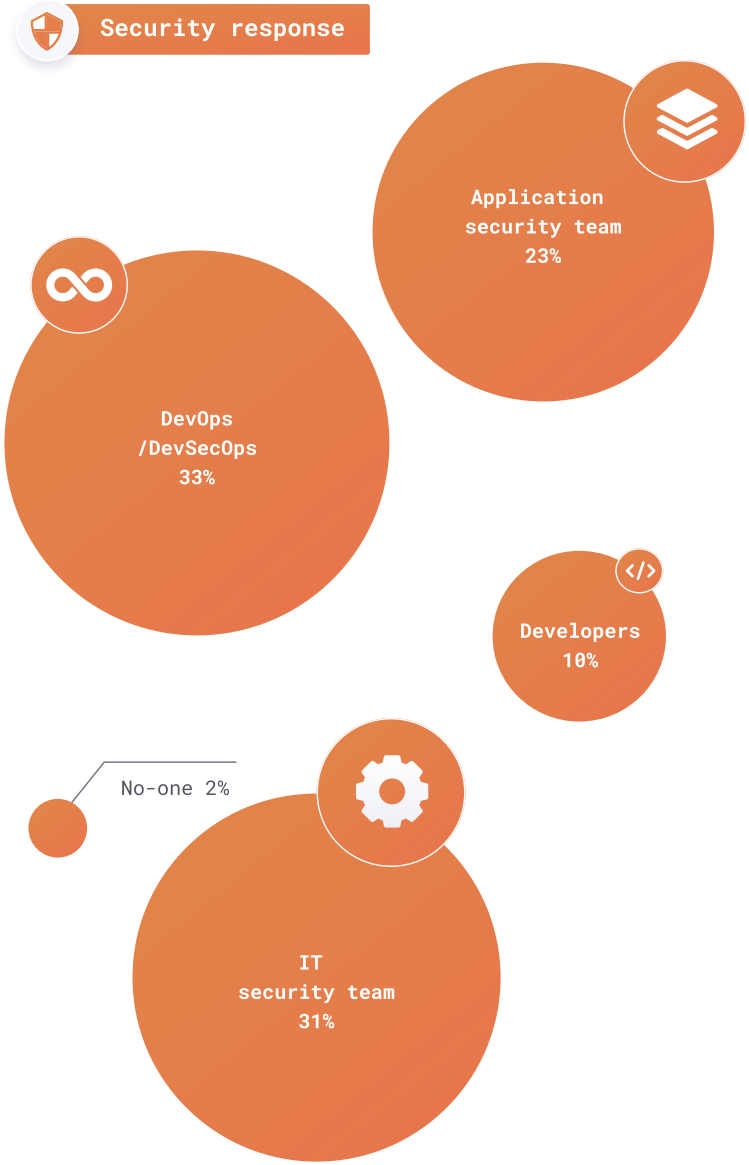
Traditionally, in a more siloed organization, the ownership of security would have sat firmly with the security team. Respondents in security roles are almost 3x more likely to attribute security ownership to the IT security team than respondents in development teams are. These indicators suggest that this ownership is being accepted by the development teams faster than the security teams are willing to let go of it. Security teams are still adjusting to the shifting responsibilities which transitioning to cloud native brings, and development teams are increasingly aware of their growing role in Cloud Native Application Security.

snyk

snyk

Who is primarily responsible for the security of your cloud native environment and applications?





VIDEO

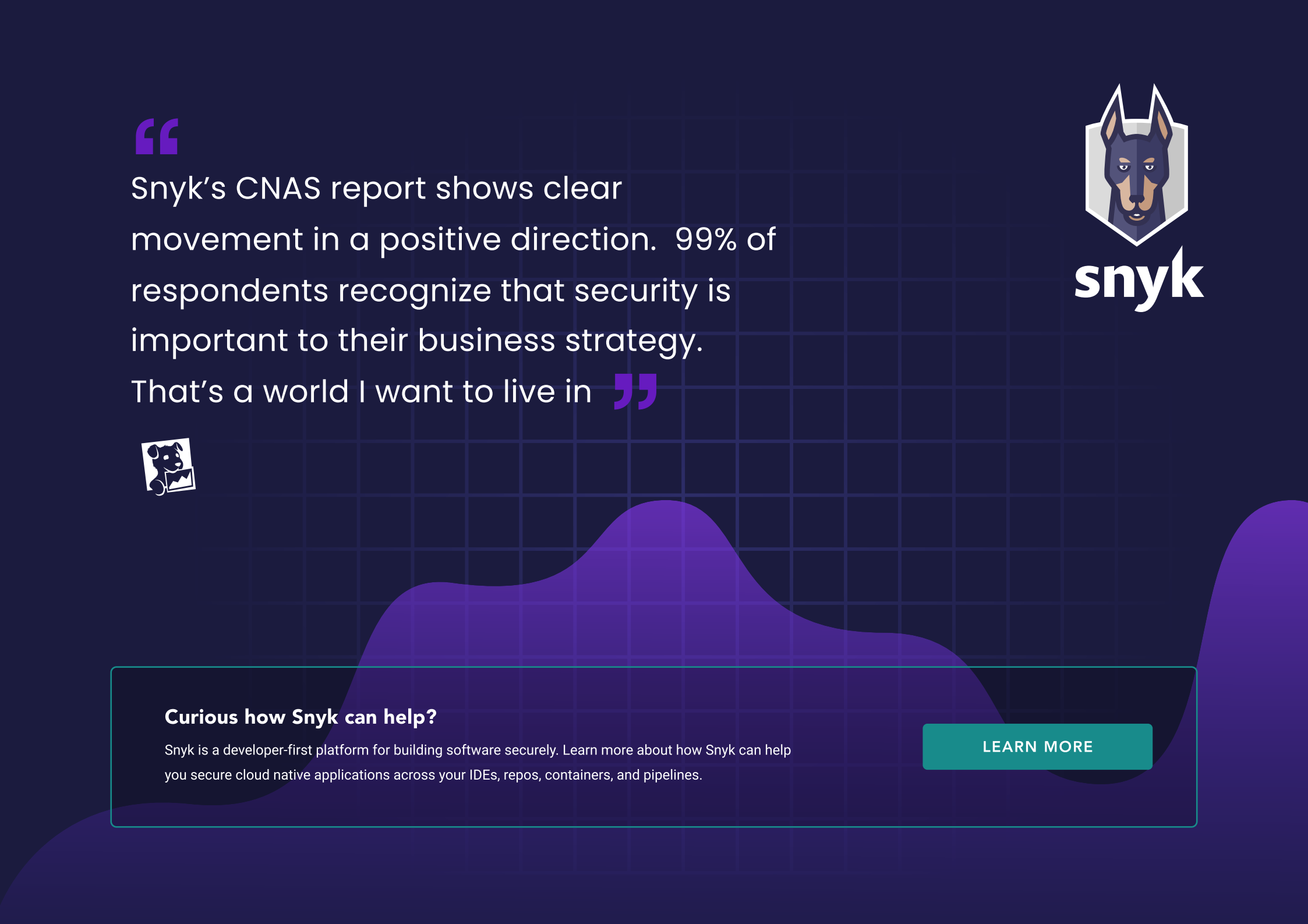
Learn how Twilio's Head of Product Security scaled through dev-first security and devsecops in a cloud native environment

WATCH NOW

Developers and security both understand the importance of Cloud Native Application Security

The increased awareness of security in development teams was also reinforced by the survey results around security exposure concerns. Both developers and security professionals alike shared that switching to cloud native technologies had increased their security concerns. Developers were just as likely to be invested in good security outcomes as the security team - good news for the adoption of DevSecOps principles which relies on shared security goals across the organization.

Has switching to Cloud Native technologies increased or decreased your security exposure concerns?


“
Snyk’s CNAS report shows clear movement in a positive direction. 99% of respondents recognize that security is important to their business strategy. That’s a world I want to live in
”
snyk
Curious how Snyk can help?
Snyk is a developer-first platform for building software securely. Learn more about how Snyk can help you secure cloud native applications across your IDEs, repos, containers, and pipelines.
LEARN MORE