cloudrail

Infrastructure-as-Code Security Adoption Trends

As more organizations develop their cloud environments using infrastructure-as-code, they are recognizing the importance of addressing security vulnerabilities earlier in the process.

With recent research revealing the average cost of a data breach is over $4 million, the stakes are high. Implementing proactive, continuous IaC security enables teams to catch misconfigurations or improper identity and access management permissions, and avoid inadvertently making sensitive resources publicly available.

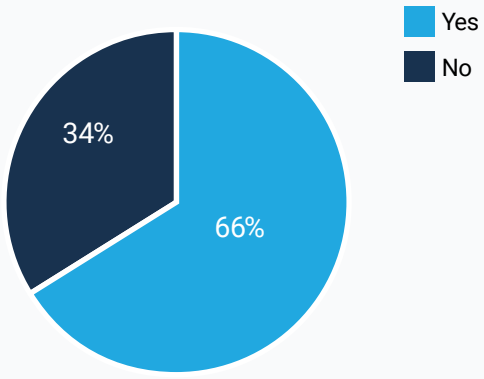
Manually reviewing infrastructure-as-code (IaC) files is time-consuming and slows down delivery times. Many organizations only have a few engineers with cloud security expertise, and they could have tens of thousands of objects running in production at one time.

These challenges will only grow as more enterprise resources move to the cloud.

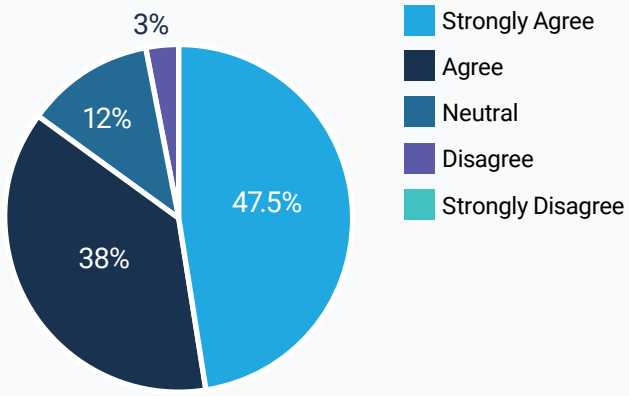
To better understand the issues today's organizations face on their cloud security journey and how they are addressing them, Indeni Cloudrail conducted a survey of over 100 security professionals, site reliability engineers, developers and others.

Here's what we found.

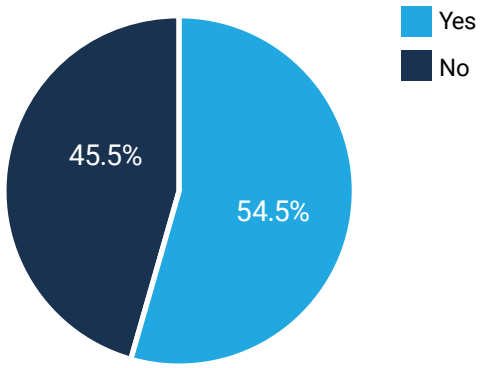
1. Are you currently using a **Cloud Security Posture Management (CSPM) tool** to scan your public cloud environment for security risks?



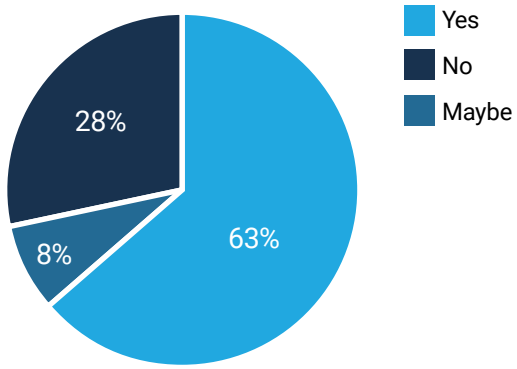
2. CSPM tools uncover issues from live resources in your cloud and remediation can be expensive. **Security scans should be part of the CI/CD so issues can be uncovered early in the development process and before deployment.** Do you agree?



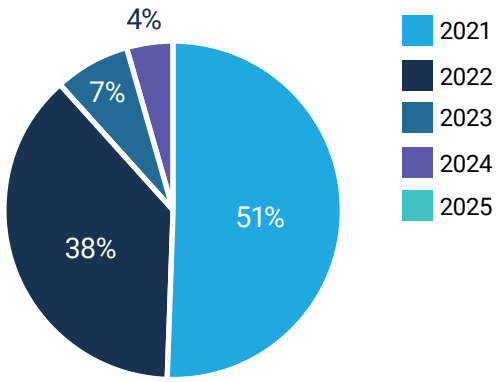
3. Are you currently using an **IaC security tool to catch security issues within the CI/CD pipeline early** in the software development life cycle?



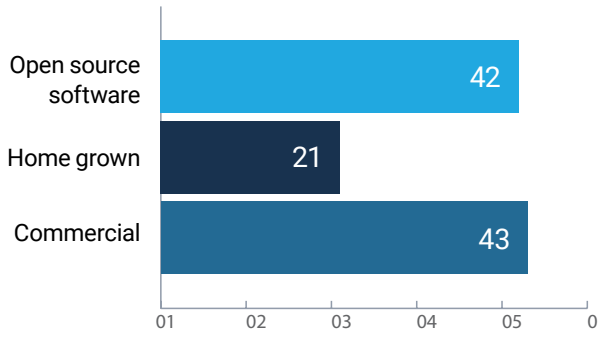
4. If your answer is "No" from the previous question, **are you planning to adopt IaC security?**



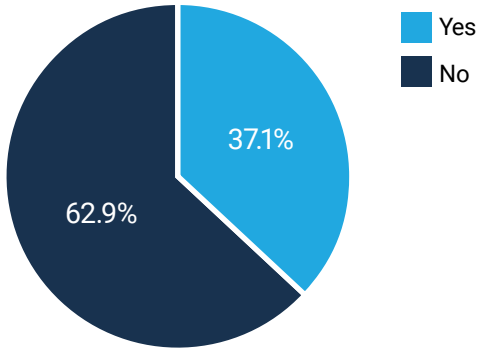
5. If your answer is "Yes" or "Maybe" from the previous question, **what year are you planning to adopt IaC security?**



6. If your answer to question 3 is "Yes", **is your IaC security tool a commercial tool, home grown, open source software?** Check all those applied.



7. If you check “Home grown” in the previous answer, **did budget impact your decision?**

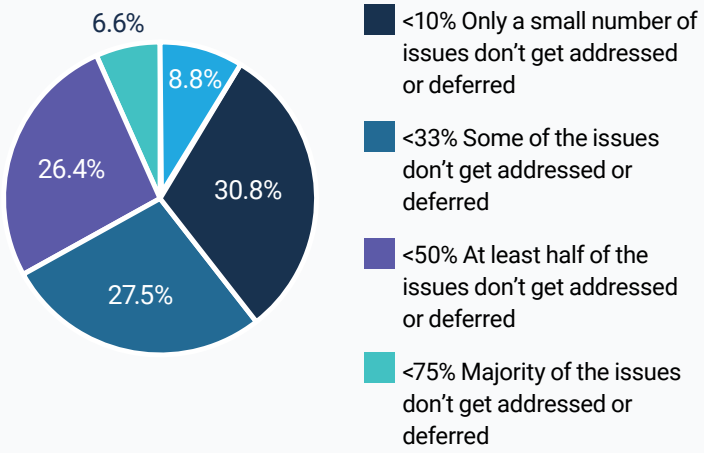


8. If your answer to question 3 is “Yes”, **what do you like about your IaC security tool? What do you dislike?**

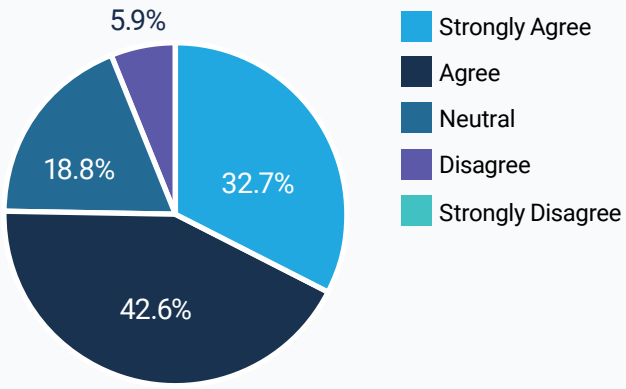
- The IaC security is fast usable and reliable, I dislike the price.
- Like: Able to catch low hanging fruit early. Dislike: no out-of-box integration with current reporting tools.
- Like: Coverage. Dislike: Complexity, lack of variable substitution.
- Integration directly into the pipeline is a positive, the API integration from the command line is poor though.
- I like that it covers both cloud environments that we deploy to (AWS, Azure). I don’t like the UI.

9. The traditional approach to security programs typically takes place towards the end of the software development life cycle. This after-the-fact technique usually results in a large number of security issues discovered past the design and build phase.

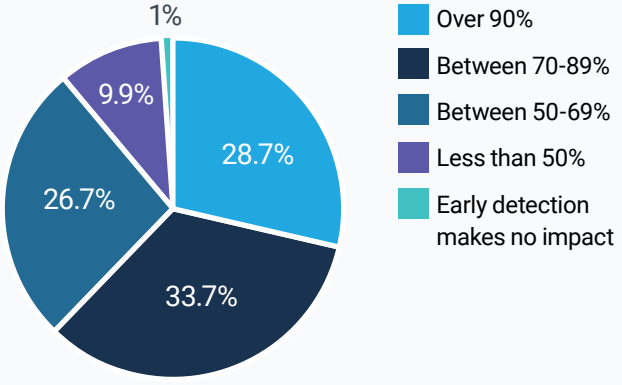
As a result, not all the security issues are being addressed because they may be too costly to fix, they are not of high risks, or for whatever business reasons. **What % of these security issues don’t get addressed in your environment?**



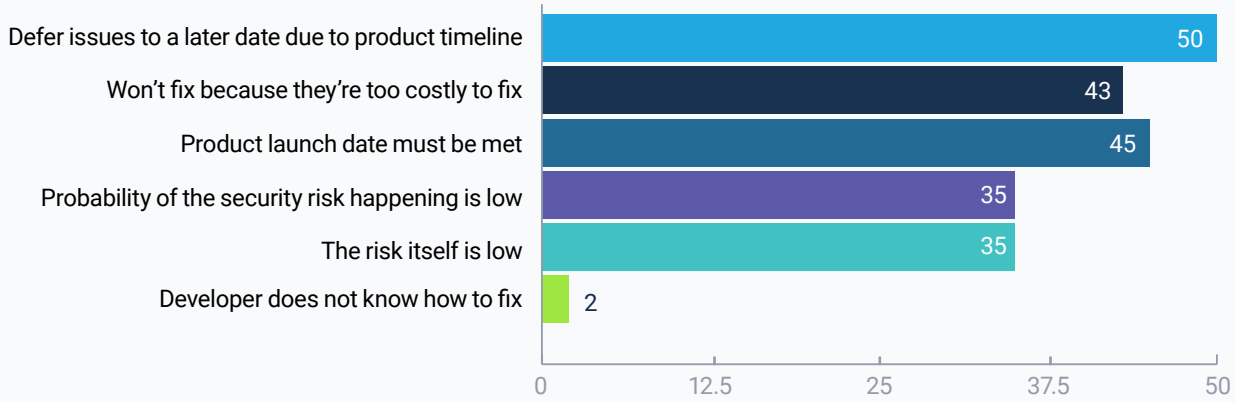
10. If these **security issues** were found in the CI/CD pipeline early in the software development life cycle before deployment, and it was close to the time you made the infrastructure change, you would likely fix it. Do you agree?



11. Out of these security issues mentioned in the previous question, **what % you think you would manage to fix?**



12. As described in question #9, **security issues found late in the software development life cycle may not get fixed.** What are the reason(s)? Check all those applied.



If your answer is "Other" from the previous question, please specify the reason(s).

- Many "findings" we see are not relevent to the threat model. Secondly we charge for our time and so clients will generally want a business case. Sometimes a clean report is good for client attentation but othertimes the findings we recieve are not relevent.
- Not using IaC to provision resources, hard to detect in those cases.
- Not all developers have been trained in cloud security fundamentals.