Executive Summary

Together Wiz and Tines bring mutual customers the technology to protect their cloud infrastructure at scale. Integrating the insights from Wiz's comprehensive cloud security platform with Tines's automated workflows ensures you are responding to critical security alerts from Wiz consistently and quickly. As a result, security teams can focus on the high priority security issues that they have not seen in their cloud environment before.

Market Challenge

With a limited number of engineers tasked with monitoring a rapidly growing technology stack and increasingly complex architecture across multi-cloud environments, organizations need help to take action on vulnerabilities, compliance posture, and other security issues across their entire cloud footprint.

Better Together

Tines brings No-code security operations into the Cloud Native Application Protection Platform (CNAPP) that is Wiz. Tines connects data from Wiz's industry-leading cloud security platform monitoring across your entire technology stack to automate prioritization and remediation workflows at speed and scale. Combining these tools allows you to measure your risk, focus on what matters most, and futureproof your applications against new vulnerabilities.

Use Case

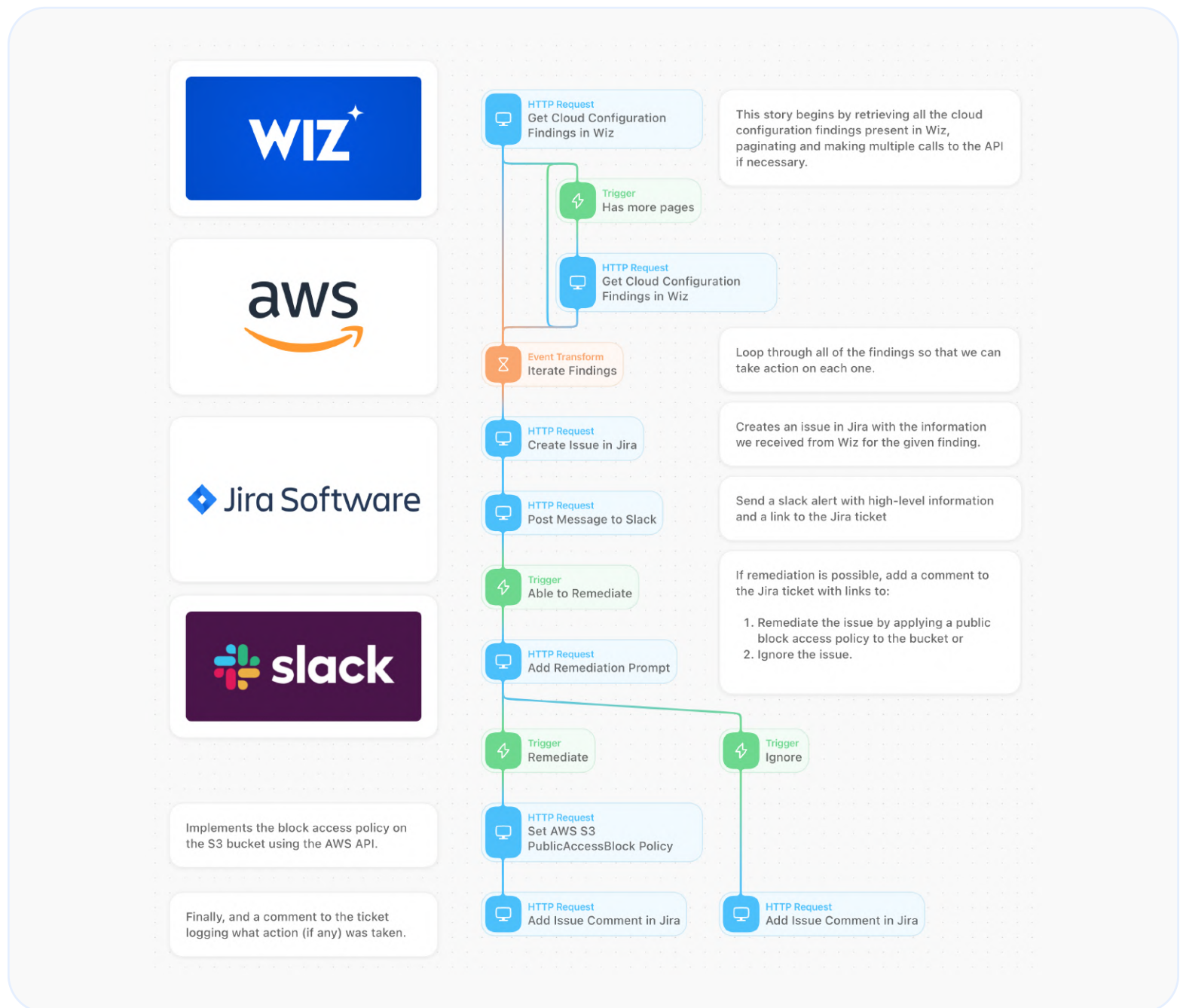Find & Remediate publicly exposed S3 buckets with Wiz.

Challenge

Exposure is identified, but remediation is manual and leaves potential critical data exposed.

Solution

Tines triggers creating a JIRA ticket, sending an alert via Slack with a remediation prompt within the Jira issue that can block access to the exposed S3 bucket identified by Wiz.

This story begins by retrieving all the cloud configuration findings present in Wiz, paginating and making multiple calls to the API if necessary.

Loop through all of the findings so that we can take action on each one.

Creates an issue in Jira with the information we received from Wiz for the given finding.

Send a slack alert with high-level information and a link to the Jira ticket

If remediation is possible, add a comment to the Jira ticket with links to:

1. Remediate the issue by applying a public block access policy to the bucket or
2. Ignore the issue.

Implements the block access policy on the S3 bucket using the AWS API.

Finally, and a comment to the ticket logging what action (if any) was taken.

About Tines

Tines offers a smart, secure workflow platform for practitioners across technical teams. It's the only platform that bypasses the need for programming skills, delivering powerful workflows straight into the hands of every team within an organization. Tines brings an impact-first approach, securely building thousands of mission-critical workflows per day across a diverse range of customers, including Canva, Databricks, Elastic, Kayak, Mars, McKesson, and Oak Ridge National Laboratory. The company was co-founded in 2018 in Dublin, Ireland, by former security practitioners Eoin Hinchy and Thomas Kinsella, and has raised $96.2M in funding to date from investors including, Felicis, Addition, Accel, Blossom Capital and Lux Capital.

About Wiz

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.