oak9
Product Details

February 2022

oak9

Cloud Infrastructure Security, Made Simple

Powering Security at the Speed of Modern Development

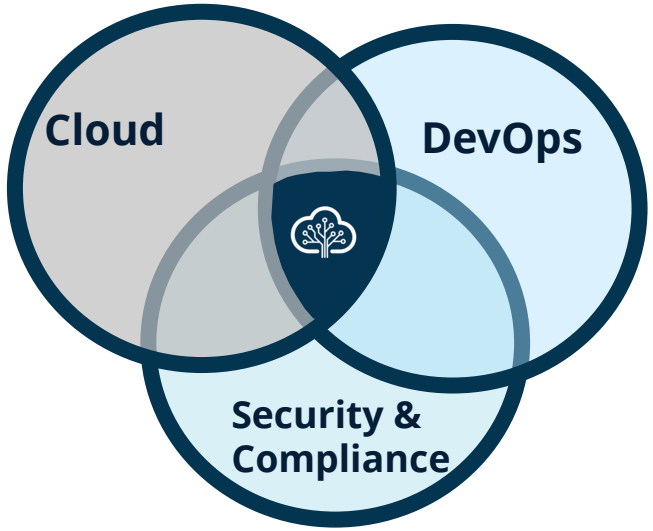
oak9: a SaaS solution for developers to mitigate security and compliance gaps PRIOR to production deployment

Part 1: What is oak9?

What we do, what problem we solve, the value prop

Product Intro

oak9 is a SaaS product that continuously scans **Infrastructure as Code** (IaC) and **cloud infrastructure**, finding and fixing **security** and **compliance** design gaps **before they go to production** in the development process**.**



Product Intro

The Problem:

IaC has increased both the **speed** and **scale** at which developers create new cloud infrastructure, but now teams are forced to choose **between making deadlines and keeping applications secure.**

The Value Prop:

oak9 reduces risk and saves time by using tailored blueprints to ensure "**always on compliance**" with PCI, ISO, NIST, and other security standards.

What Does oak9 Do?

We have already mapped standards like PCI, ISO and NIST to specific technical security requirements – these are our "***blueprints***".

We then take these blueprints and use them to validate and monitor your Azure and AWS infrastructure, via cloud APIs to ***find and fix security/compliance issues***.

We use these same blueprints to scan Terraform code, whether via CI/CD pipelines, code repos, or CLI to fix security issues ***before they go to production***

Part 2: Common Questions

Let’s get down to details…

Is oak9 a CSPM tool?

Is oak9 a CSPM – like Azure Security Center?

No. We're much more than that.

Cloud Security Posture Management (CSPM) tools are great for identifying issues with your production environment.

But wouldn't it be great to avoid those mistakes in the first place?

By scanning and remediating Infrastructure as Code in the dev cycle, **oak9 prevents bad designs from going into production**.

Is oak9 a CSPM tool?

What if I have cloud infrastructure that isn't managed with IaC?

No problem, we understand that not every environment is perfect.

In addition to scanning your **IaC**, oak9 will also scan your **deployed cloud infrastructure** and detect security design gaps in your manually-deployed cloud components.

While we aren't *really* a CSPM vendor, we eliminate your need for separate CSPM tools.

Is this a static config checker?

So, is oak9 just searching for common misconfigurations?

No! We build a model of your applications' architectures, then overlay our tailored blueprints to identify security gaps in your design.

You can apply different tailored blueprints to different applications, based on security and compliance needs.

Other competitors do static "search and replace" without considering that **one size does not fit all! Context matters.**

Is oak9 a tool kit or a complete product?

Do we have to write our own policies, or can oak9 just tell us what needs to be done?

We can tell you exactly what you need to do to be secure and compliant.

We've done the hard work of mapping common standards like NIST / HITRUST etc. and enumerating all their technical requirements, so you don't have to.

We then look at your environment and tell you which of the standard's requirements apply to your application infrastructure – and how to fix anything that's out of compliance.

We keep our database of standards and cloud components up to date, **making compliance easy for developers**.

How Does oak9 Integrate?

What entry points does oak9 use to secure a customer's environment?

The earlier in the process the better.

1. We have a **command-line tool** for developers to use as they write IaC.
2. We plug in to various **CI/CD pipelines** to scan code before it goes to prod.
3. We connect directly to **code repositories** and scan when code gets checked in.
4. We scan **production cloud environments**, scanning deployed components
5. We integrate in to existing **workflow, ticketing, and notification systems** to provide alerts.

Security across the SDLC

From start to finish

Design → Code → Build & Test → Deploy → Operate

1 IaC Code Changes

- Terraform
- Kubernetes
- Azure RM
- AWS CF

2 CI / CD

- Azure DevOps
- GitHub
- Jenkins
- GitLab

3 Cloud Providers

- AWS
- Azure
- GCP

4 Notifications / Alerting

- Slack
- Teams
- Jira
- Azure Boards
- ServiceNow

Design securely
From the start

Integrate seamlessly
in your CI/CD pipeline

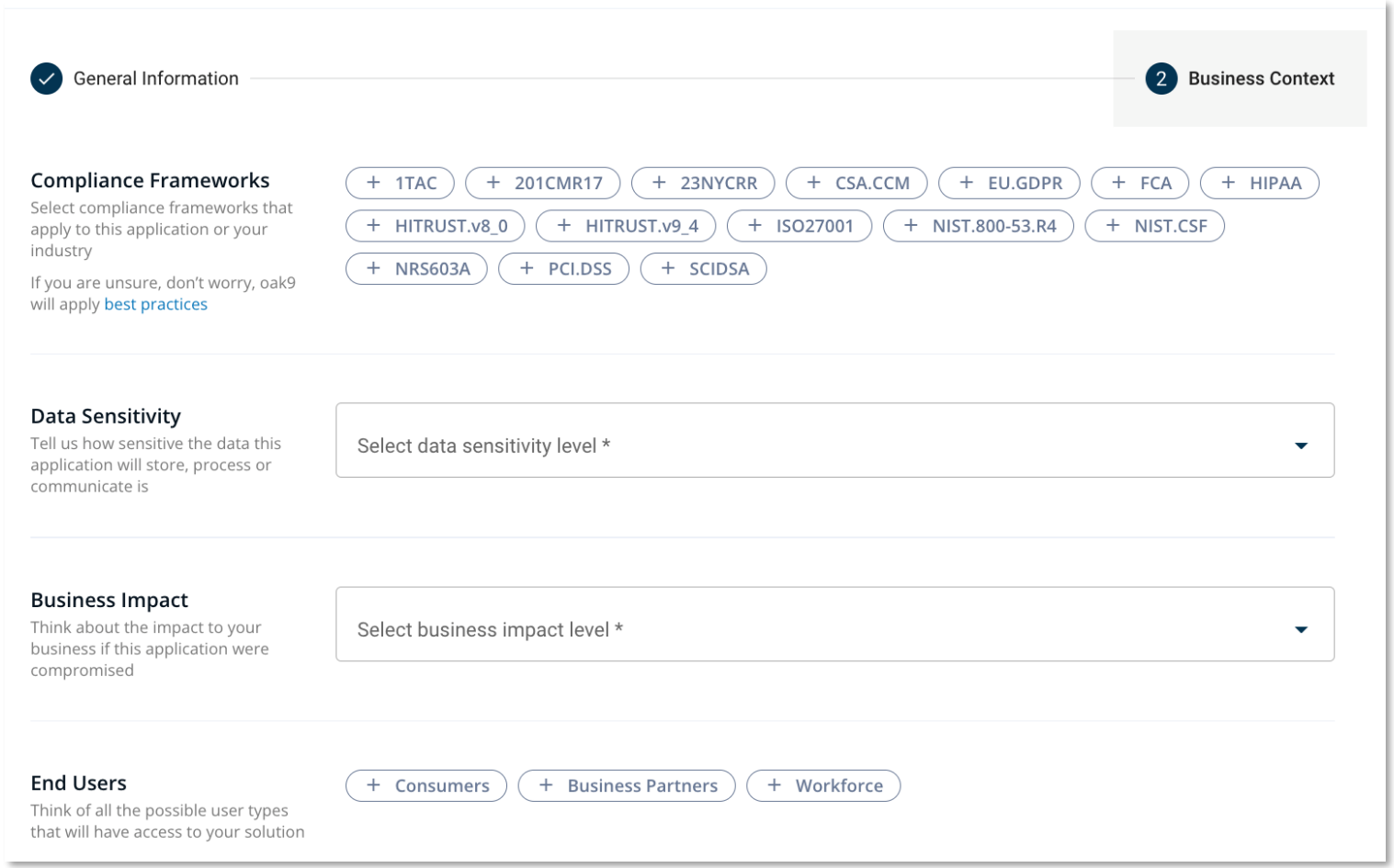
Continuous
Monitoring
Drift Detection

Notifications &
Alerting

Part 2: How oak9 Works

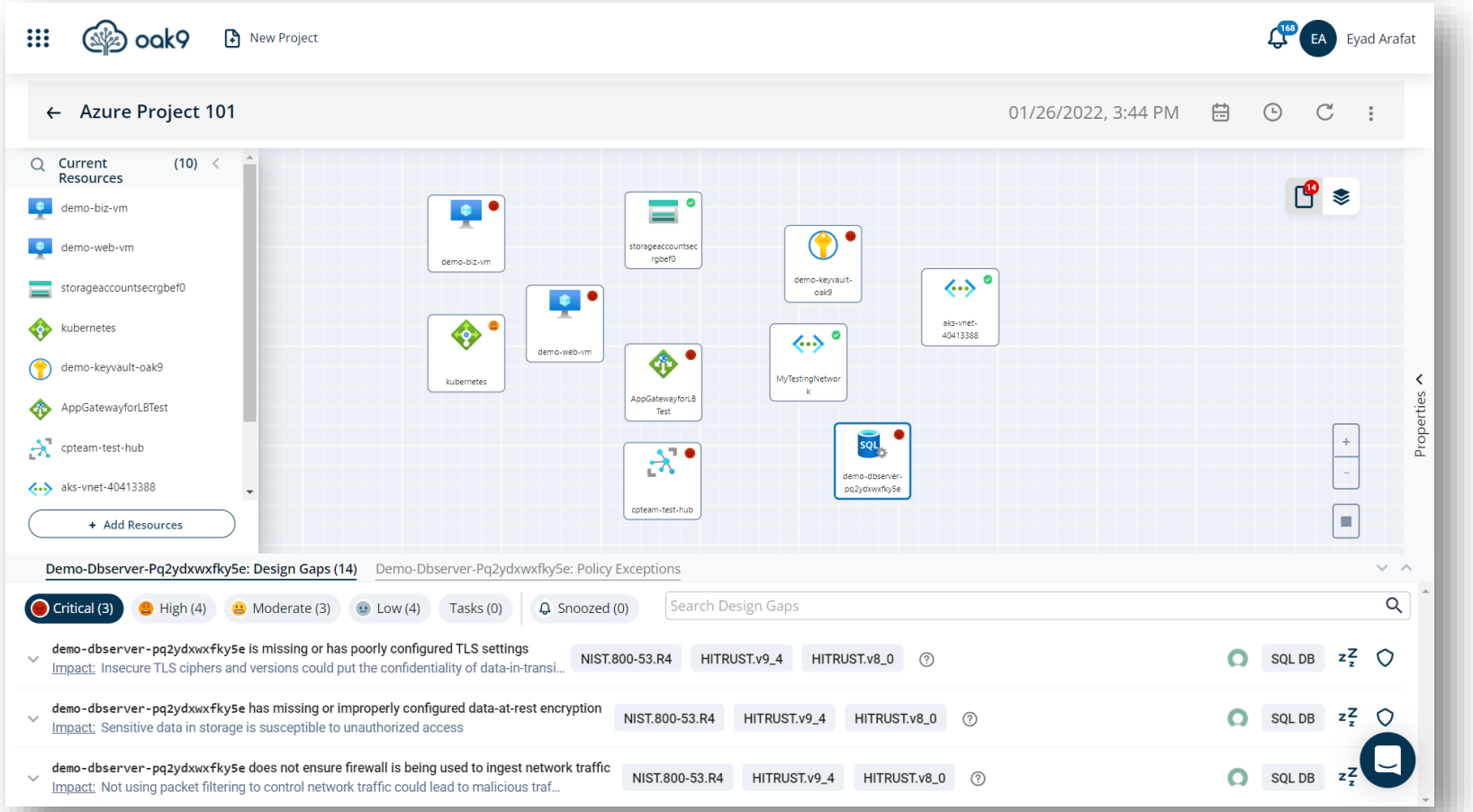
oak9 in action

Define a security blueprint



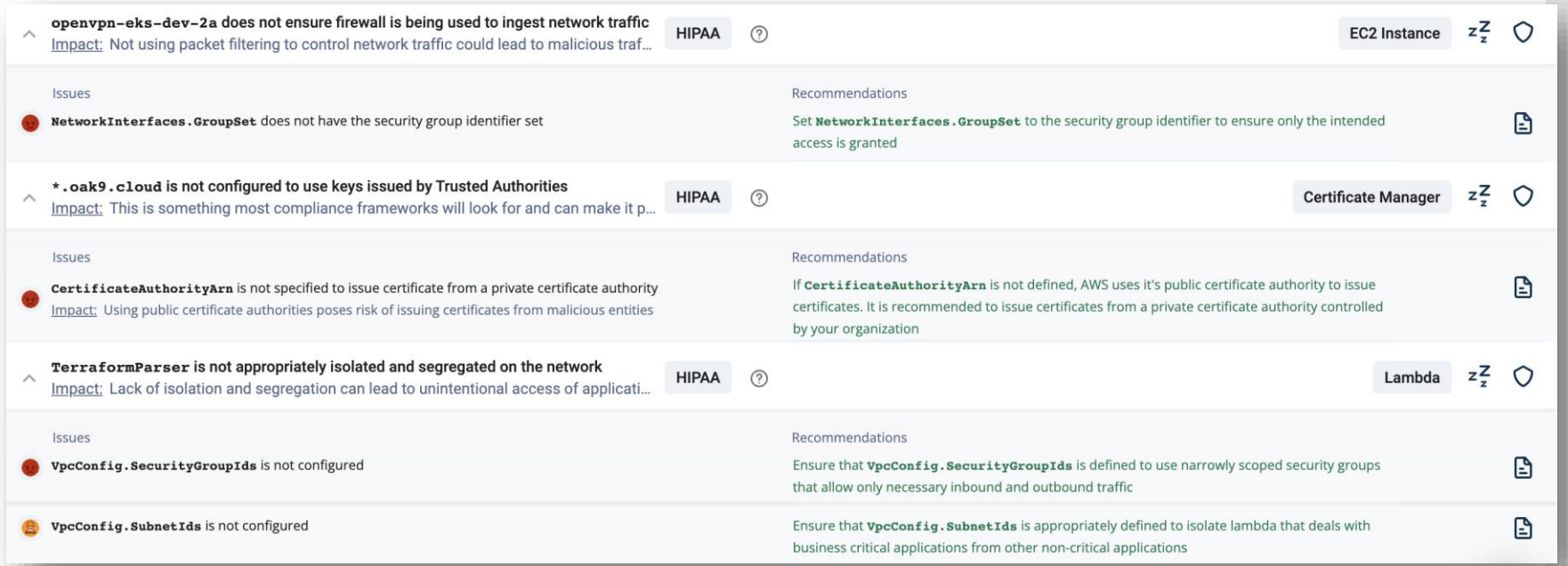
oak9 creates a blueprint based on applicable frameworks and is tailored by answering a few simple questions.

Visualize IaC



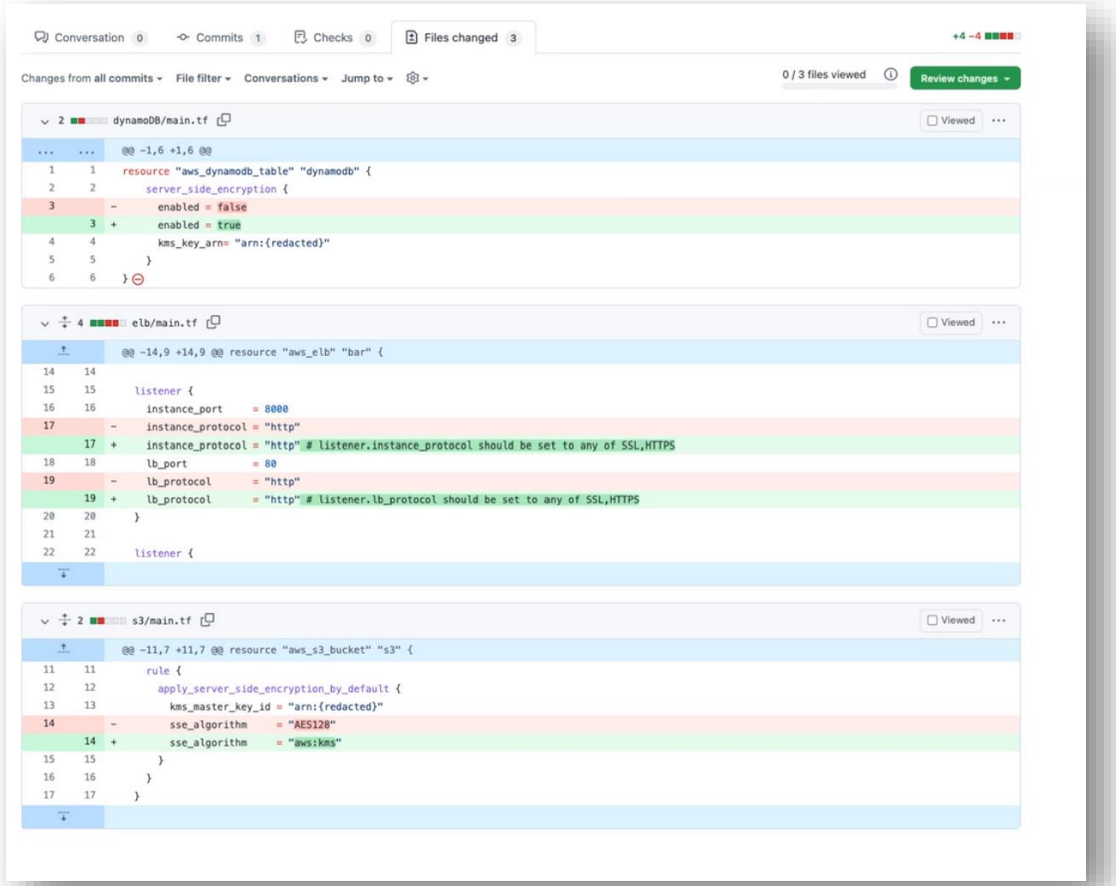
oak9 scans IaC code and cloud infrastructure, then visually maps the architecture to spotlight security design gaps.

Revie Detailed Recommendations



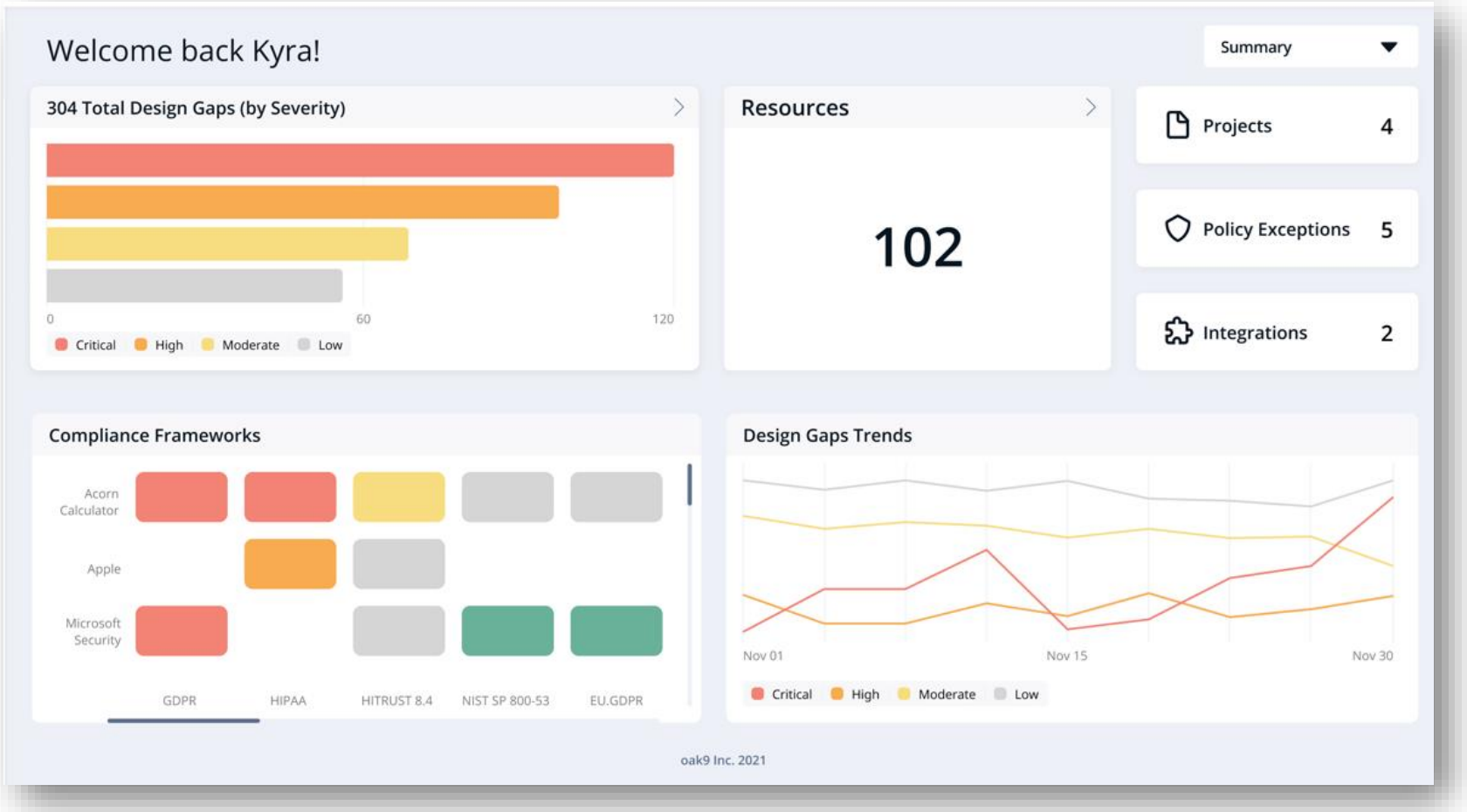
oak9 provides detailed descriptions of any issues, explains the impact and provides the specific recommendation to address problem.

Remediate Security Issues



oak9's IaC analysis and remediation tells you *exactly* what you need to do to address security design gaps by providing code snippets with the fixes.

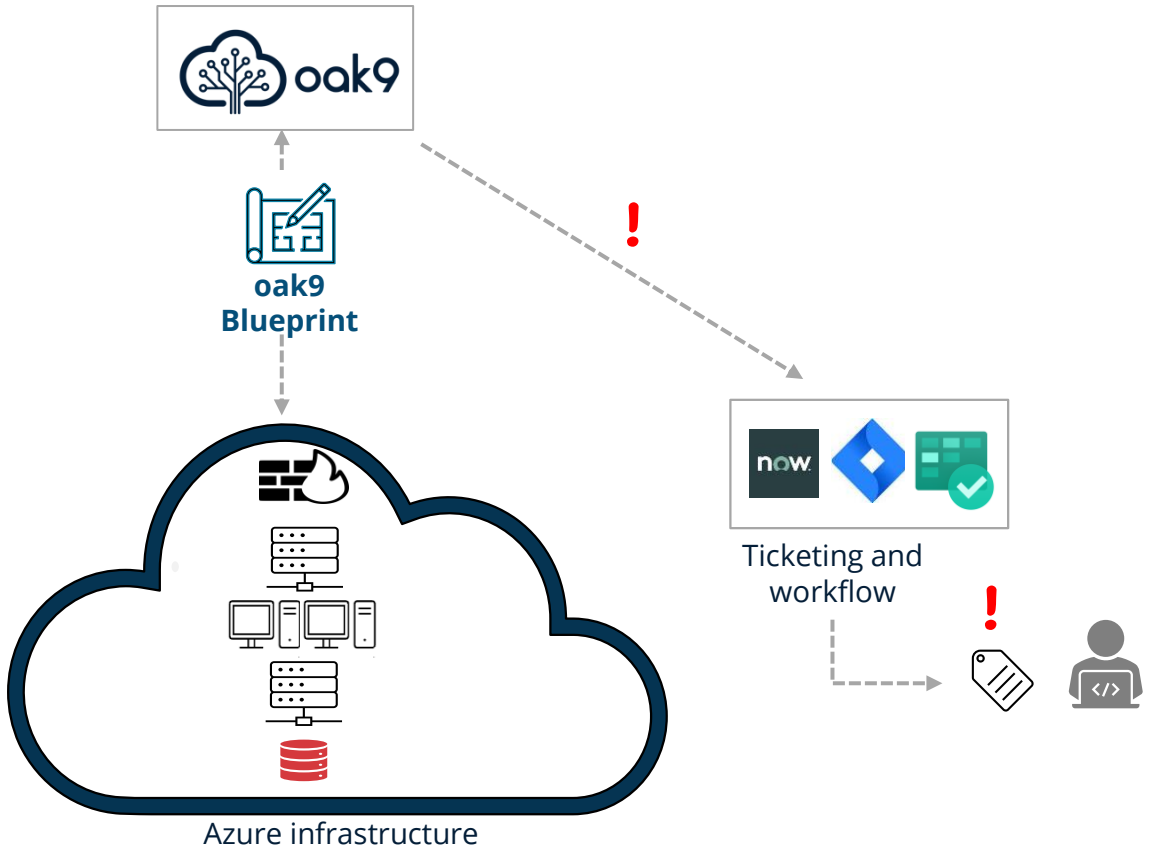
Executive Dashboard



oak9's executive dashboard provides a holistic view into your environment, reporting on compliance and security across the enterprise.

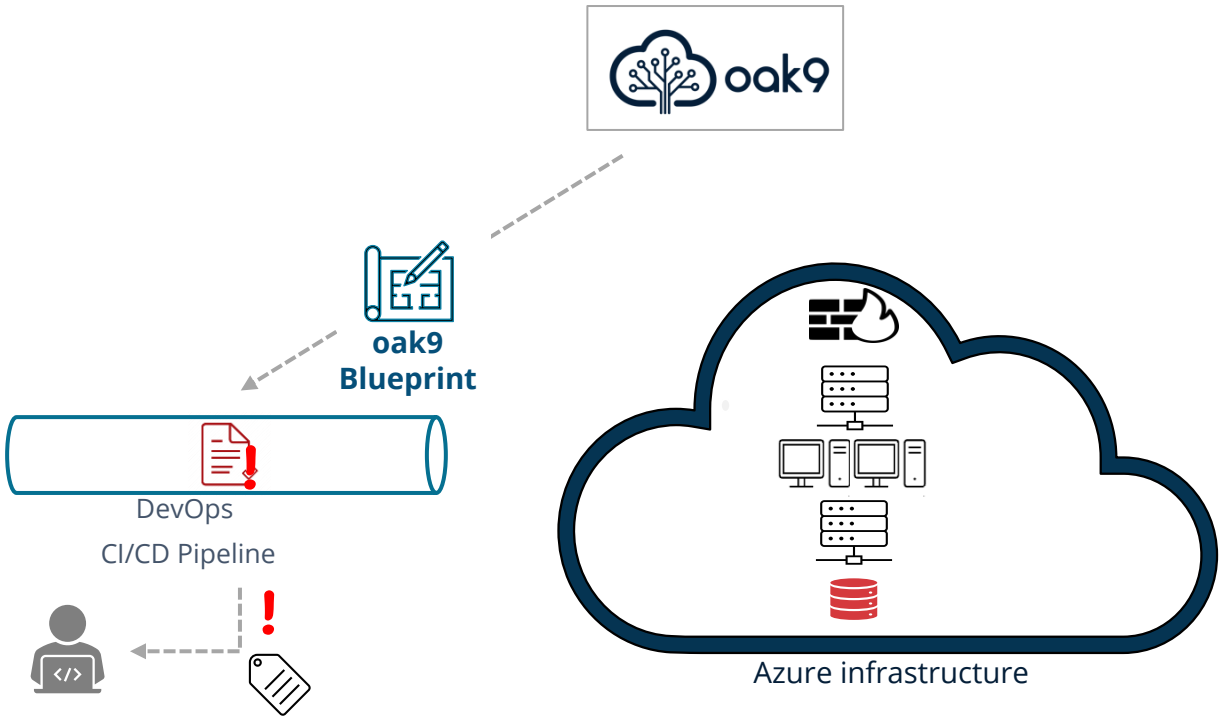
Appendix: oak9 Integration Diagrams

Cloud API integration



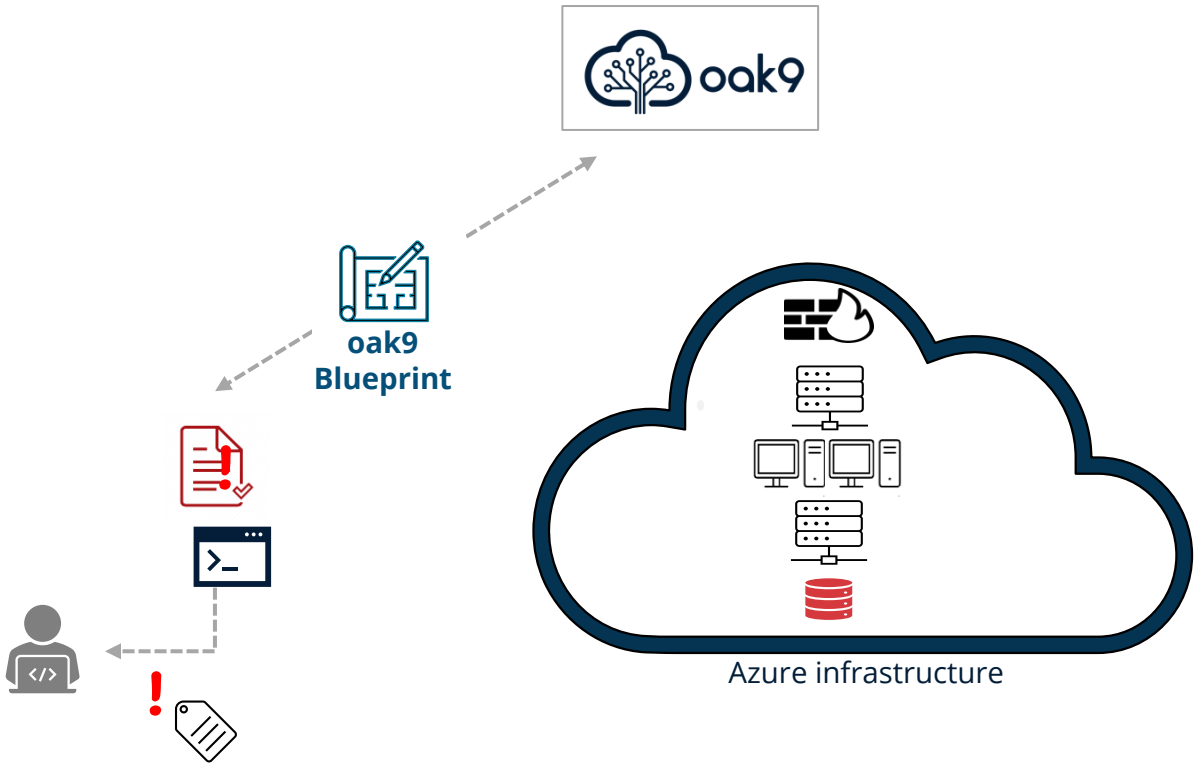
Oak9 scans customers' cloud environments with tailored security blueprints, identifying security design gaps.

CI/CD Integration



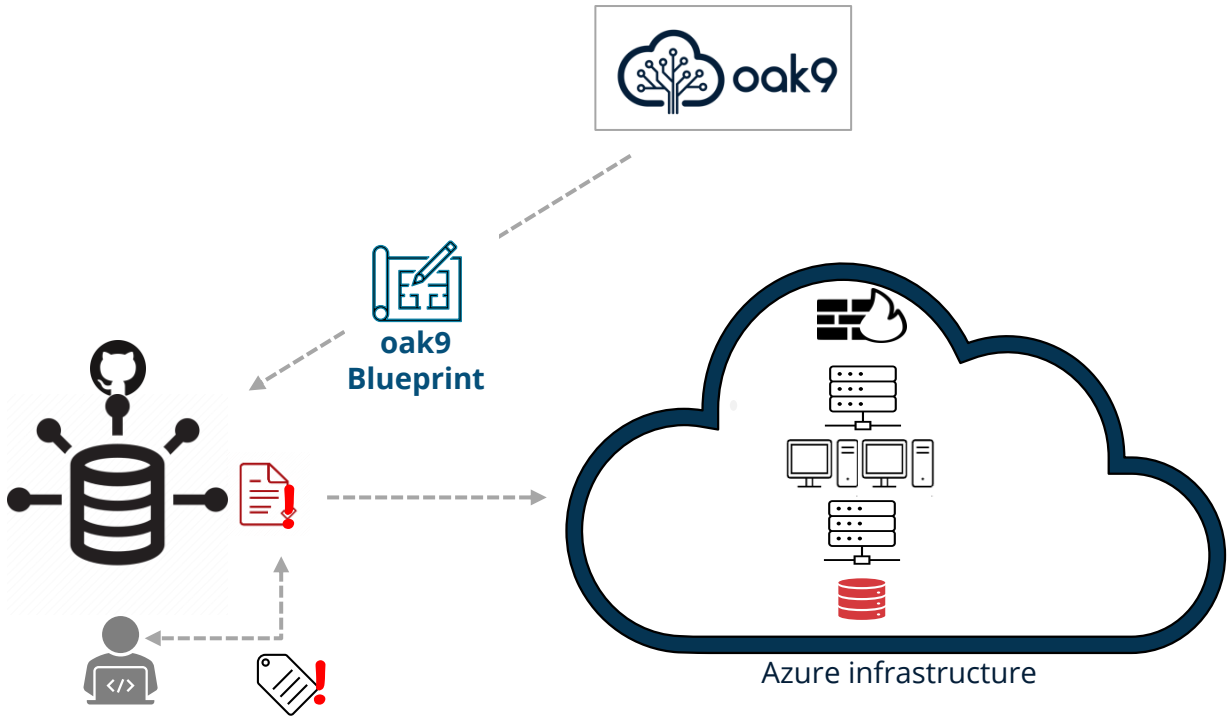
oak9 scans IaC as it passes through **CI/CD pipelines** to identify security issues before code goes to production.

Command Line Checking



oak9 scans code during development, analyzing IaC from **the command line**, before code gets checked in.

Code Repo Integration



oak9 scans IaC when it is **checked in to a repository** to identify security issues before code goes to production.

Questions?

info@oak9.io