

oak9

Product Details

February 2022



Cloud Infrastructure Security, Made Simple

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

Powering Security at the Speed of
Modern Development

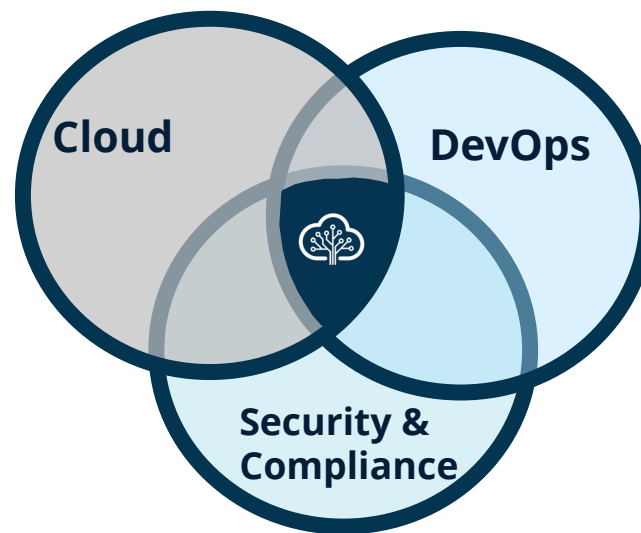
Part 1: What is oak9?

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?

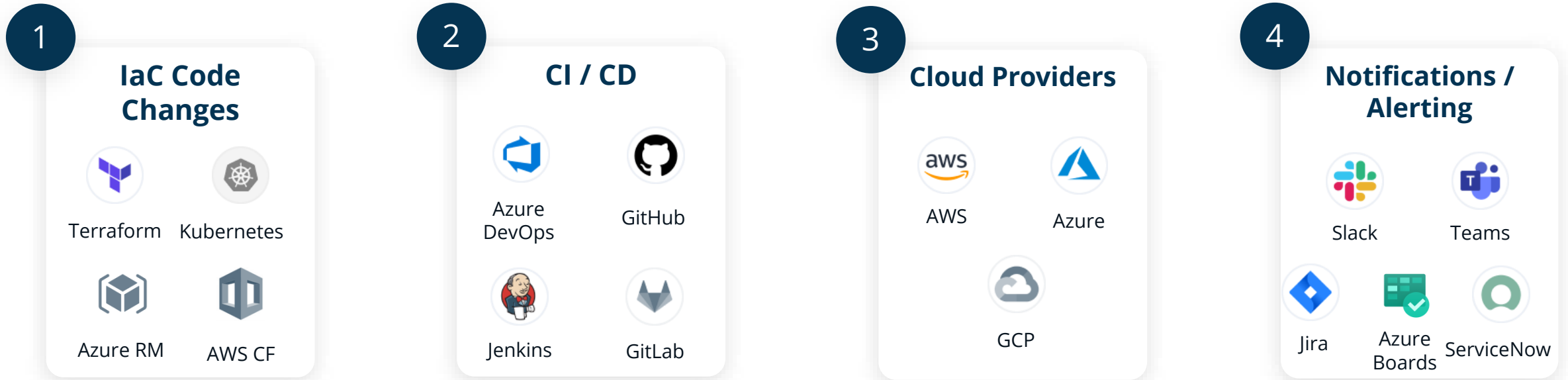
The earlier in the process the better.

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



Part 2: How oak9 Works

oak9 in action



Define a security blueprint

General Information 2 Business Context

Compliance Frameworks
Select compliance frameworks that apply to this application or your industry
If you are unsure, don't worry, oak9 will apply [best practices](#)

+ 1TAC + 201CMR17 + 23NYCRR + CSA.CCM + EU.GDPR + FCA + HIPAA
+ HITRUST.v8_0 + HITRUST.v9_4 + ISO27001 + NIST.800-53.R4 + NIST.CSF
+ NRS603A + PCI.DSS + SCIDSA

Data Sensitivity
Tell us how sensitive the data this application will store, process or communicate is

Select data sensitivity level *

Business Impact
Think about the impact to your business if this application were compromised

Select business impact level *

End Users
Think of all the possible user types that will have access to your solution

+ Consumers + Business Partners + Workforce

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



Visualize IaC

The screenshot displays the oak9 interface for an Azure Project 101. The top navigation bar includes the oak9 logo, a 'New Project' button, and the user profile 'Eyad Ararat'. The main area shows a visual map of resources including 'demo-biz-vm', 'demo-web-vm', 'storageaccountsecrgbef0', 'kubernetes', 'demo-keyvault-oak9', 'AppGatewayforLBTest', 'cptesteam-test-hub', and 'aks-vnet-40413388'. Below the map, a section titled 'Demo-Dbserver-Pq2ydxwxfky5e: Design Gaps (14)' lists three critical issues:

- demo-dbserver-pq2ydxwxfky5e is missing or has poorly configured TLS settings**
Impact: Insecure TLS ciphers and versions could put the confidentiality of data-in-transi...
Standards: NIST.800-53.R4, HITRUST.v9_4, HITRUST.v8_0
- demo-dbserver-pq2ydxwxfky5e has missing or improperly configured data-at-rest encryption**
Impact: Sensitive data in storage is susceptible to unauthorized access
Standards: NIST.800-53.R4, HITRUST.v9_4, HITRUST.v8_0
- demo-dbserver-pq2ydxwxfky5e does not ensure firewall is being used to ingest network traffic**
Impact: Not using packet filtering to control network traffic could lead to malicious traf...
Standards: NIST.800-53.R4, HITRUST.v9_4, HITRUST.v8_0

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



Review Detailed Recommendations

openvpn-eks-dev-2a does not ensure firewall is being used to ingest network traffic Impact: Not using packet filtering to control network traffic could lead to malicious traf...		HIPAA	?	EC2 Instance	zZ	🛡️
Issues	Recommendations					
🔴 NetworkInterfaces.GroupSet does not have the security group identifier set	Set NetworkInterfaces.GroupSet to the security group identifier to ensure only the intended access is granted	📄				
*.oak9.cloud is not configured to use keys issued by Trusted Authorities Impact: This is something most compliance frameworks will look for and can make it p...		HIPAA	?	Certificate Manager	zZ	🛡️
Issues	Recommendations					
🔴 CertificateAuthorityArn is not specified to issue certificate from a private certificate authority Impact: Using public certificate authorities poses risk of issuing certificates from malicious entities	If CertificateAuthorityArn is not defined, AWS uses its public certificate authority to issue certificates. It is recommended to issue certificates from a private certificate authority controlled by your organization	📄				
TerraformParser is not appropriately isolated and segregated on the network Impact: Lack of isolation and segregation can lead to unintentional access of applicati...		HIPAA	?	Lambda	zZ	🛡️
Issues	Recommendations					
🔴 VpcConfig.SecurityGroupIds is not configured	Ensure that VpcConfig.SecurityGroupIds is defined to use narrowly scoped security groups that allow only necessary inbound and outbound traffic	📄				
🟡 VpcConfig.SubnetIds is not configured	Ensure that VpcConfig.SubnetIds is appropriately defined to isolate lambda that deals with business critical applications from other non-critical applications	📄				

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



Remediate Security Issues

The screenshot displays a code review interface for Terraform files. It shows three files: dynamodb/main.tf, elb/main.tf, and s3/main.tf. The dynamodb/main.tf file shows a resource 'aws_dynamodb_table' with a change from 'enabled = false' to 'enabled = true'. The elb/main.tf file shows a resource 'aws_elb' with a listener configuration where 'instance_protocol' and 'lb_protocol' are changed from 'http' to 'https', with remediation suggestions: '# Listener.instance_protocol should be set to any of SSL,HTTPS' and '# Listener.lb_protocol should be set to any of SSL,HTTPS'. The s3/main.tf file shows a resource 'aws_s3_bucket' with a rule configuration where 'sse_algorithm' is changed from 'AES128' to 'aws:kms'.

```
@@ -1,6 +1,6 @@
1 1 resource "aws_dynamodb_table" "dynamodb" {
2 2   server_side_encryption {
3 3 -   enabled = false
4 4 +   enabled = true
5 5   kms_key_arn = "arn:(redacted)"
6 6 }

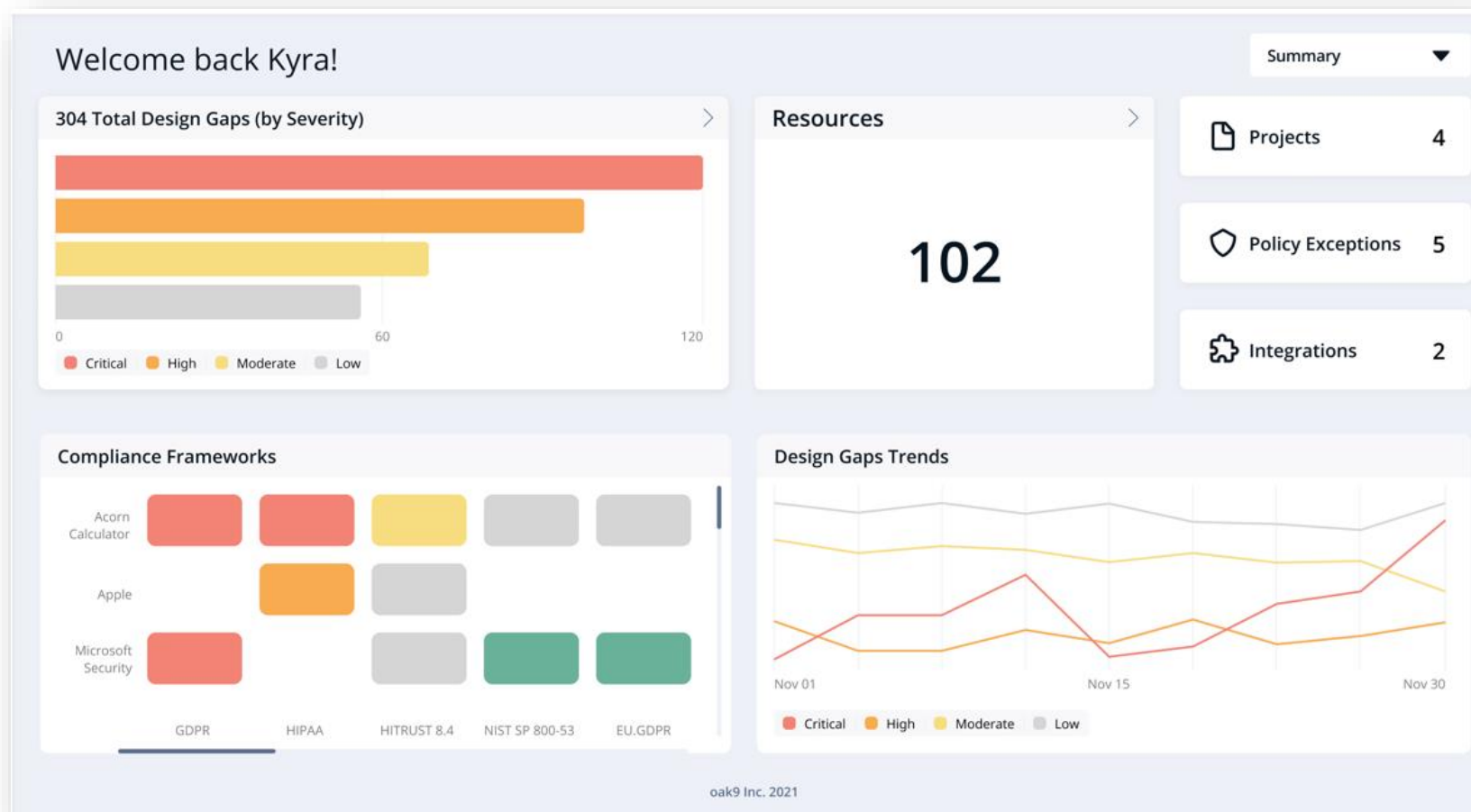
@@ -14,9 +14,9 @@ resource "aws_elb" "bar" {
14 14
15 15   listener {
16 16     instance_port = 8080
17 17 -   instance_protocol = "http"
17 17 +   instance_protocol = "https" # Listener.instance_protocol should be set to any of SSL,HTTPS
18 18     lb_port = 80
19 19 -   lb_protocol = "http"
19 19 +   lb_protocol = "https" # Listener.lb_protocol should be set to any of SSL,HTTPS
20 20   }
21 21
22 22   listener {

@@ -11,7 +11,7 @@ resource "aws_s3_bucket" "s3" {
11 11   rule {
12 12     apply_server_side_encryption_by_default {
13 13       kms_master_key_id = "arn:(redacted)"
14 14 -     sse_algorithm = "AES128"
14 14 +     sse_algorithm = "aws:kms"
15 15   }
16 16 }
17 17 }
```

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

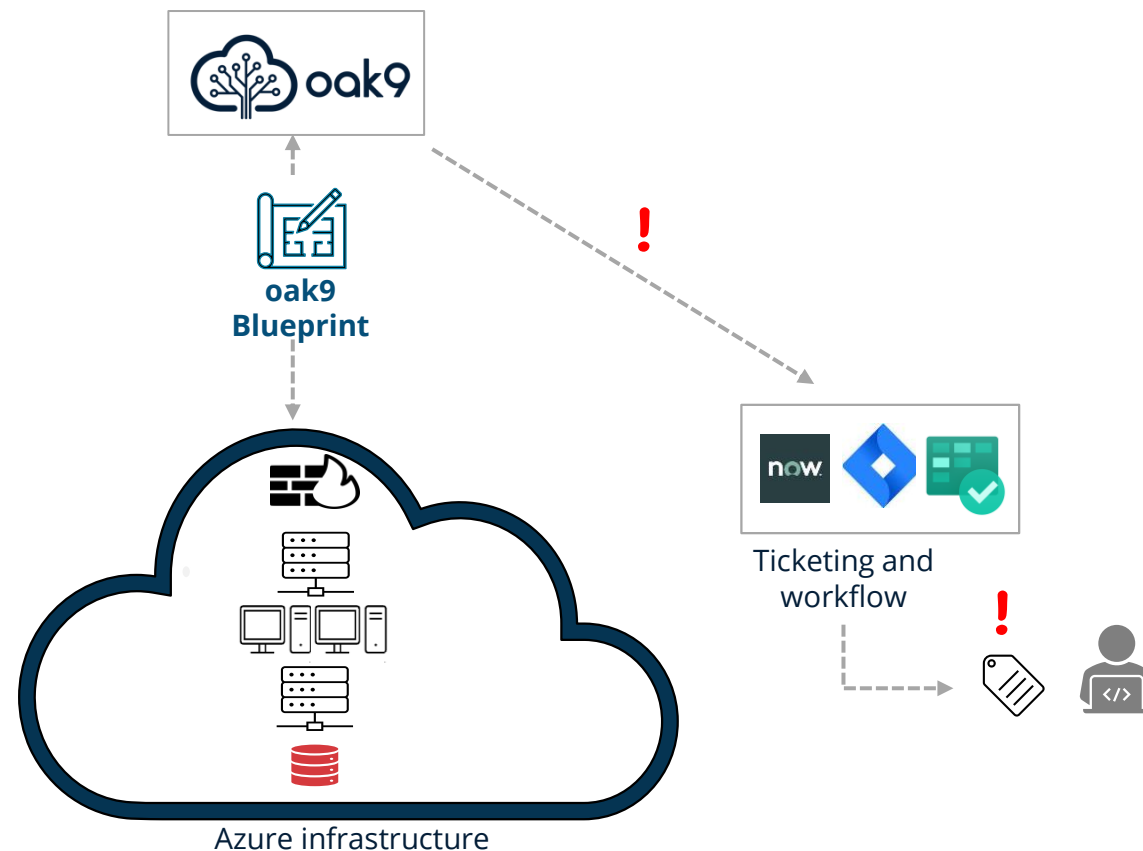


oak9's executive dashboard provides a holistic view into your environment, reporting on compliance and security across the enterprise.

Appendix: oak9 Integration Diagrams



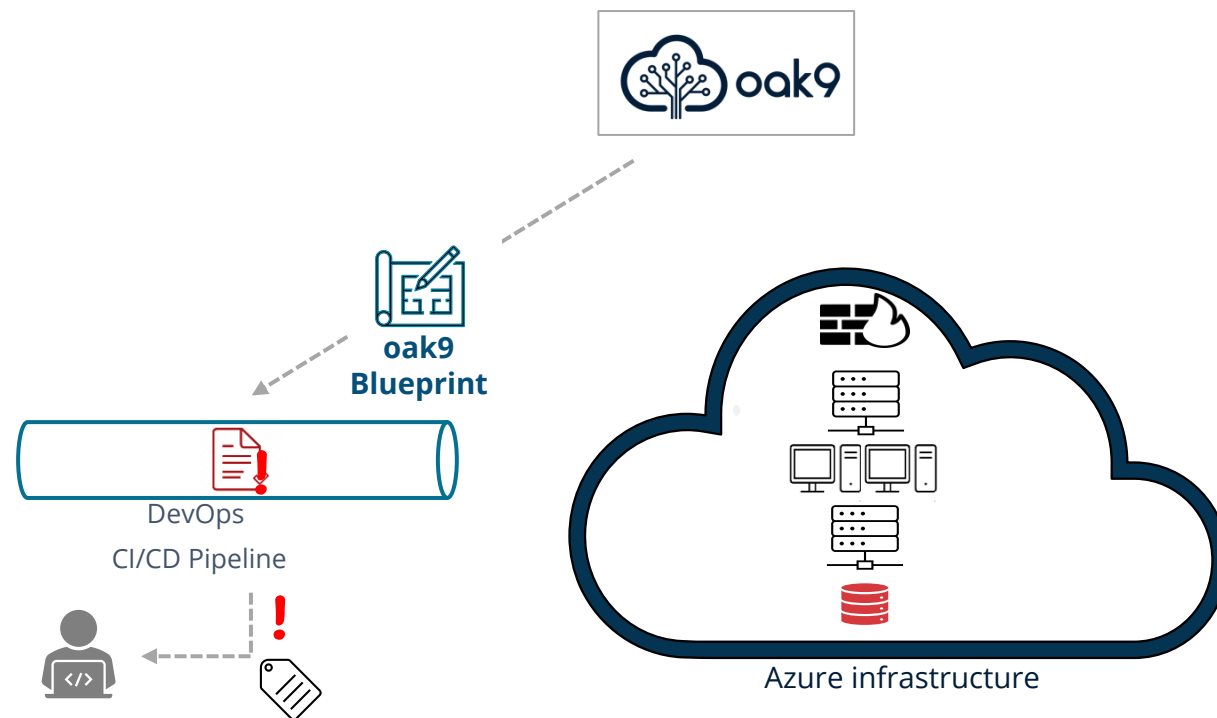
Cloud API integration



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



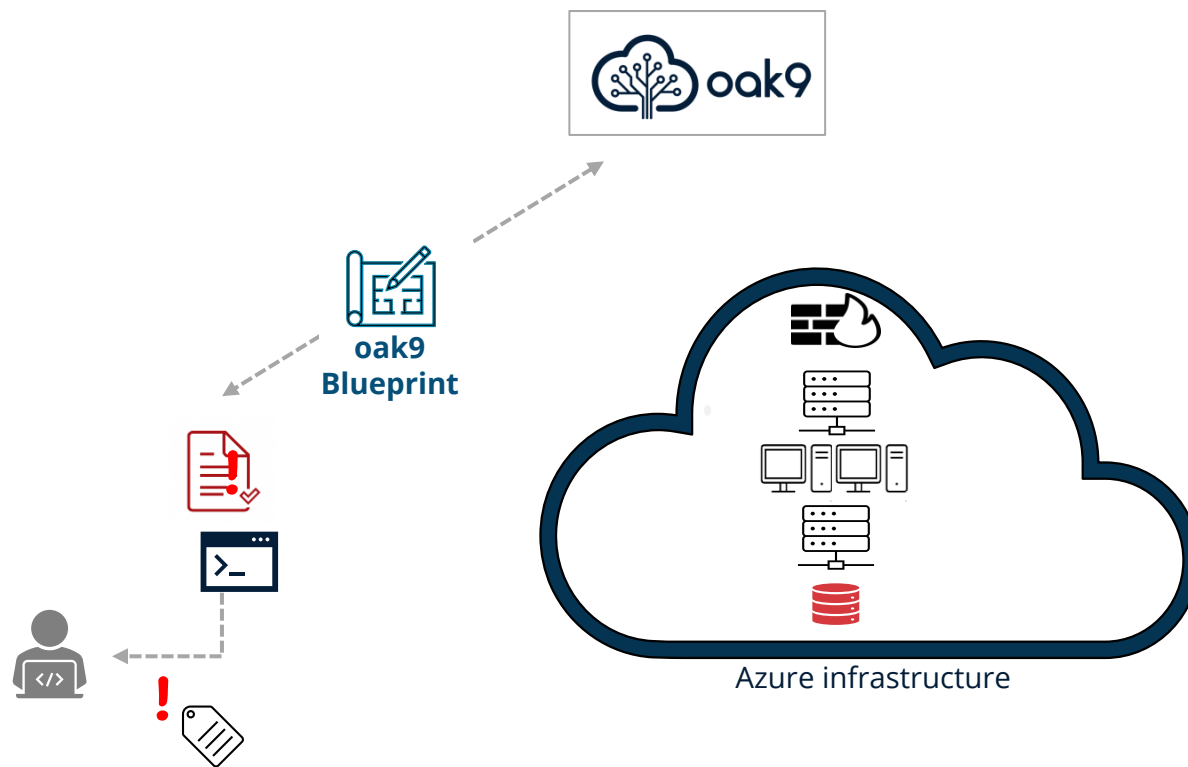
CI/CD Integration



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



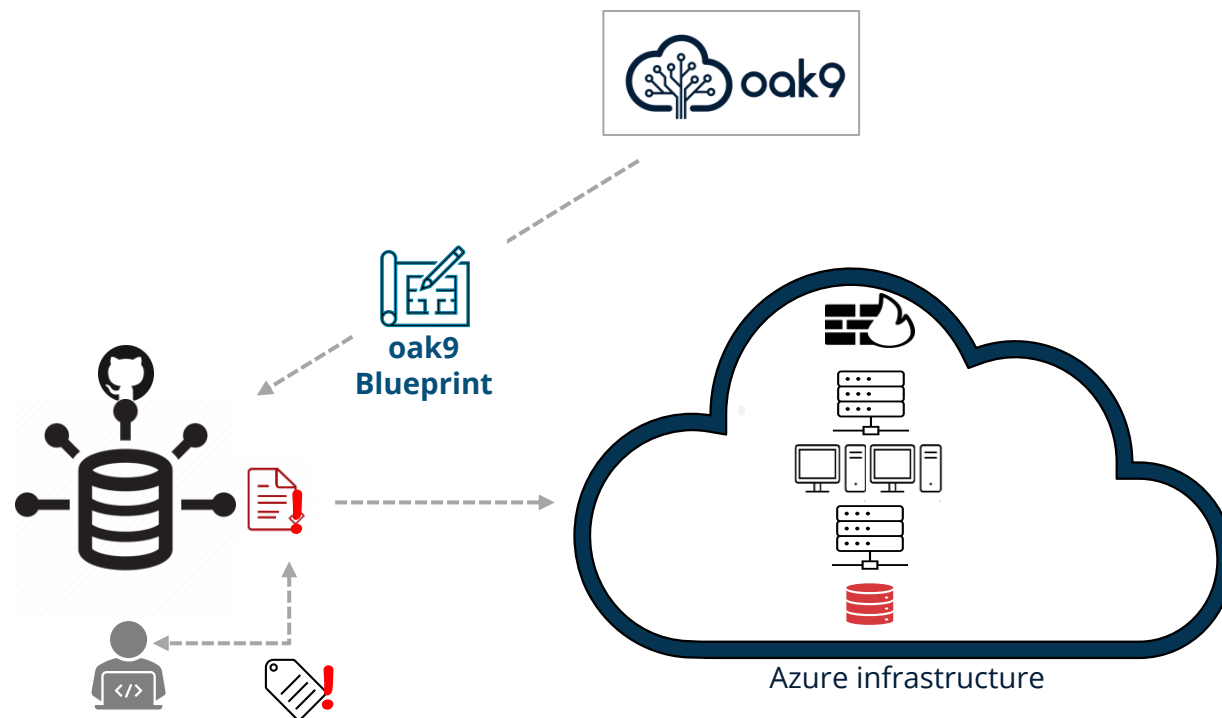
Command Line Checking



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