Fugue

Addressing Cloud Security with OPA

Josh Stella, Co-Founder & CTO, Fugue

Agenda

1. Overview of misconfiguration risk in the cloud era
2. Why policy-as-code is mandatory for security and compliance
3. Introduction of Open Policy Agent for policy as code
   ...and the growing OPA ecosystem of tools
4. Technical deep dives into the OPA toolbox for cloud security
5. Getting started with policy as code using OPA
6. Q&A

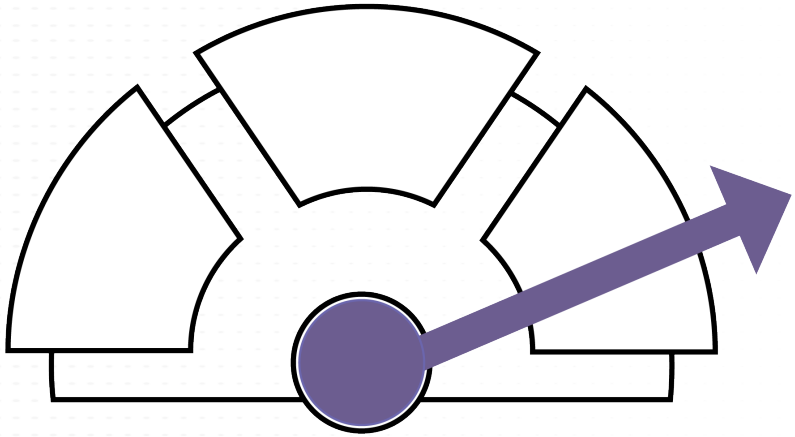
Fugue

Cloud misconfiguration is a major security risk

> *Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes.*
>
> – Neil MacDonald, Gartner

93%

CONCERNED FOR MAJOR SECURITY BREACH DUE TO MISCONFIGURATION



Fugue

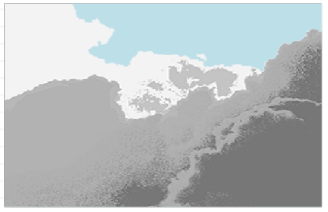
Cloud misconfiguration is a major security risk

66%
IAM

59%
SECURITY GROUP RULES

51%
OBJECT STORAGE ACCESS POLICIES

42%
ENCRYPTION IN TRANSIT DISABLED



Fugue

Cloud misconfiguration is often overlooked

Many dangerous cloud misconfigurations are:

- not recognized as misconfigurations by security teams
- not considered policy violations by compliance frameworks
- exceedingly common in enterprise cloud environments

...like needles continuously appearing in a haystack

Fugue

Hacker strategy has evolved

Before Cloud	Cloud
1. Identify your target organization	1. Identify misconfiguration vulnerabilities
2. Search for vulnerabilities to exploit	2. Prioritize your target organizations

Bad actors use automation to find and exploit cloud misconfiguration

Fugue

The cloud attack surface is complex and ever-expanding

Datacenter

- Physical infrastructure
- Generally static
- Manually deployed, configured, and maintained

Cloud

- Software-defined infrastructure
- Highly dynamic
- Deployed, configured, and maintained via APIs
  - Manually, or...
  - Automated with Infrastructure as code (Terraform; Cloudformation)

Developers now build and modify their own infrastructure environments

Fugue

Cloud complexity requires policy-as-code for security at scale

Datacenter

- Infrastructure teams deliver infrastructure to app teams
- Validations and audits are generally performed manually
- Partial and inconsistent API coverage

Cloud

- Developers create and modify their own infrastructure via complete and consistent APIs
- Validations + audits are either:
  - Manual (error-prone, slow, not scalable)
  - Automated with policy as code (accurate, fast, scalable)

Policy as code empowers engineers own the security of their cloud-based systems.
Repeatable, testable, sharable, scalable, peer-reviewed

Fugue

Policy-as-code provides developers with security feedback

Programming languages

Logical functions can be expressed as code.

Compilers and interpreters provide feedback to developers on whether their code is functionally correct.

Policy-as-Code

Your security posture can be expressed as code.

Policy-as-code evaluation provides feedback to developers on whether their code and systems are correct regarding security.

Fugue

Open Policy Agent: an open standard for policy-as-code

- Sponsored by the Cloud Native Computing Foundation (CNCF)
- Declarative policy using easy-to-learn Rego language
- Can validate any JSON data structure
- Can be adopted for a wide variety of cloud use cases
  - Cloud infrastructure (e.g. AWS; Azure; GCP)
  - Kubernetes transactions
  - API governance

  ...and many more
- Robust tooling ecosystem
  - Regula for validating Terraform
  - Fregot for working with the Rego (OPA's policy language)

  ...and many more

Fugue

Proprietary offerings vs. Open Policy Agent

Proprietary

- Single use case
- Lock-in and vendor risk
- No version control
- Often inflexible for sophisticated requirements
- No ecosystem or community
- No portability of rules
- Engineers gain limited skills
- Employers are challenged to find skilled engineers

Open Policy Agent

- Multiple use cases
- No lock-in or vendor risk
- Version control (in your repo)
- Extremely flexible for sophisticated requirements
- Robust ecosystem and community
- Rules portability
- Engineers gain valuable skills
- Employers can find skilled engineers

Fugue

Myth: infrastructure-as-code is a prerequisite for policy-as-code

"We're not ready for policy-as-code because we haven't yet adopted infrastructure-as-code."

Fugue

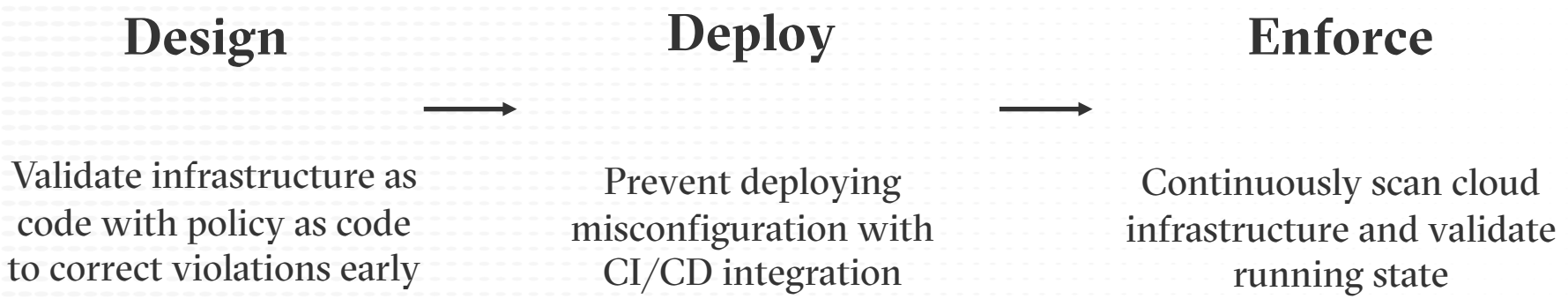
Reality: policy-as-code takes priority over infrastructure-as-code

"You need policy-as-code because the disparate methods used to create and modify cloud-based systems impact your security posture."

manual (consoles; GUIs)
CI/CD
infrastructure-as-code
multiple services configurating and automating via APIs

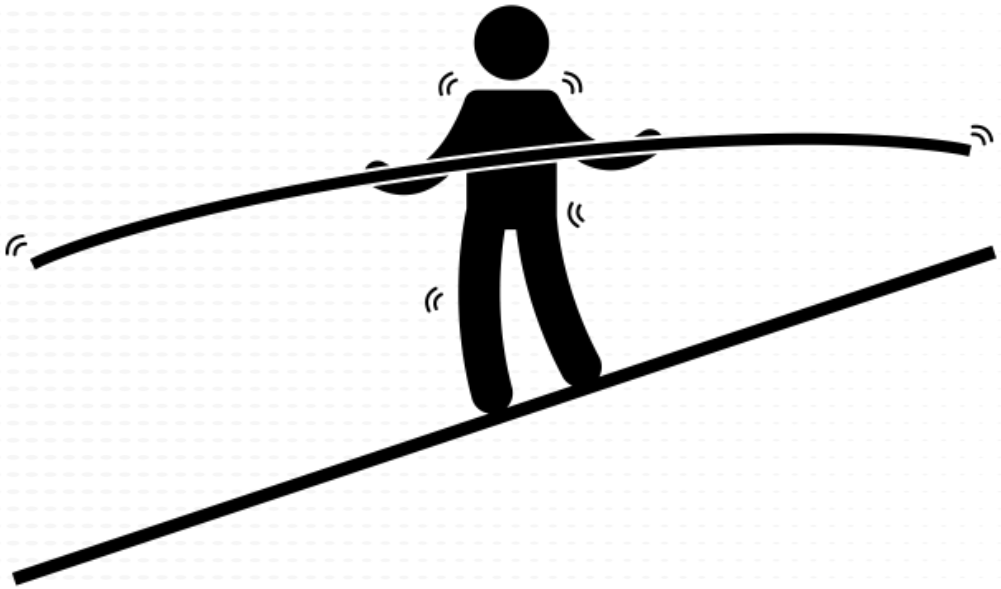
Fugue

Automating cloud security with policy as code across the SDLC



Fugue

Digging into OPA and OPA-based tools



Fugue

Questions?

Getting Started Resources

Open Policy Agent: https://www.openpolicyagent.org/

Fugue Developer for cloud environments (free): www.fugue.co/go

Validate Terraform with Regula: https://github.com/fugue/regula

Fregot (for working with Rego): https://github.com/fugue/fregot

Automated Infrastructure Compliance Framework: aicf.nltgis.com

Fugue