
KubeCon
CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022
TiKV
TiKV
HELM

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Securing the IaC Supply Chain

Jesse Sanford, Autodesk
Jason Hall, Chainguard

Introduction

- **Jesse Sanford:** Lifelong software engineer focused on site reliability and Infosec. Currently helping architect the juncture of developer enablement and security/compliance at Autodesk. Continuously delivering parent of two young daughters.

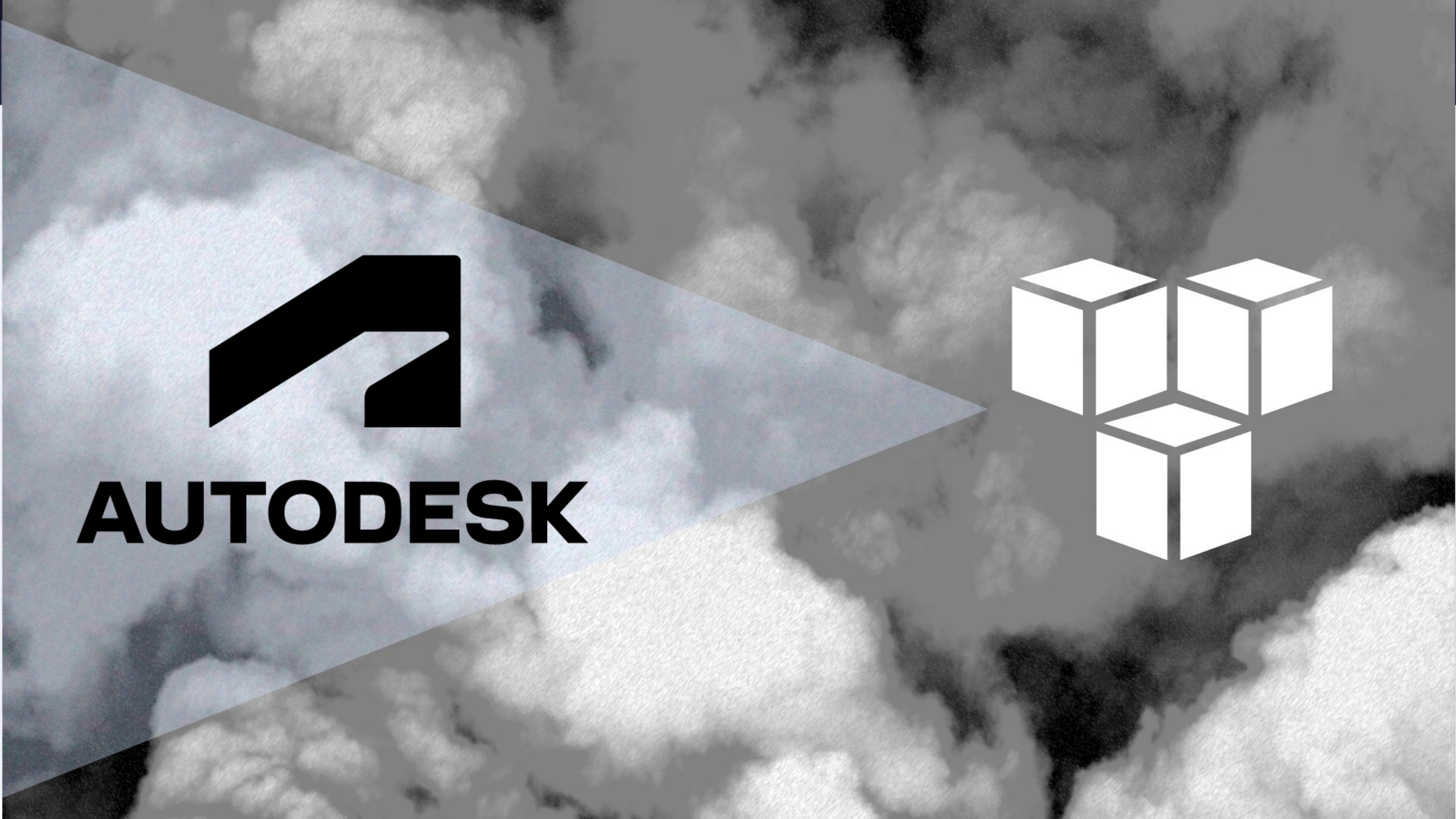
- **Jason Hall:** Troublemaker, connoisseur of fine hacks. Securing supply chains by default at Chainguard, focused on secure base images and secure software distribution.

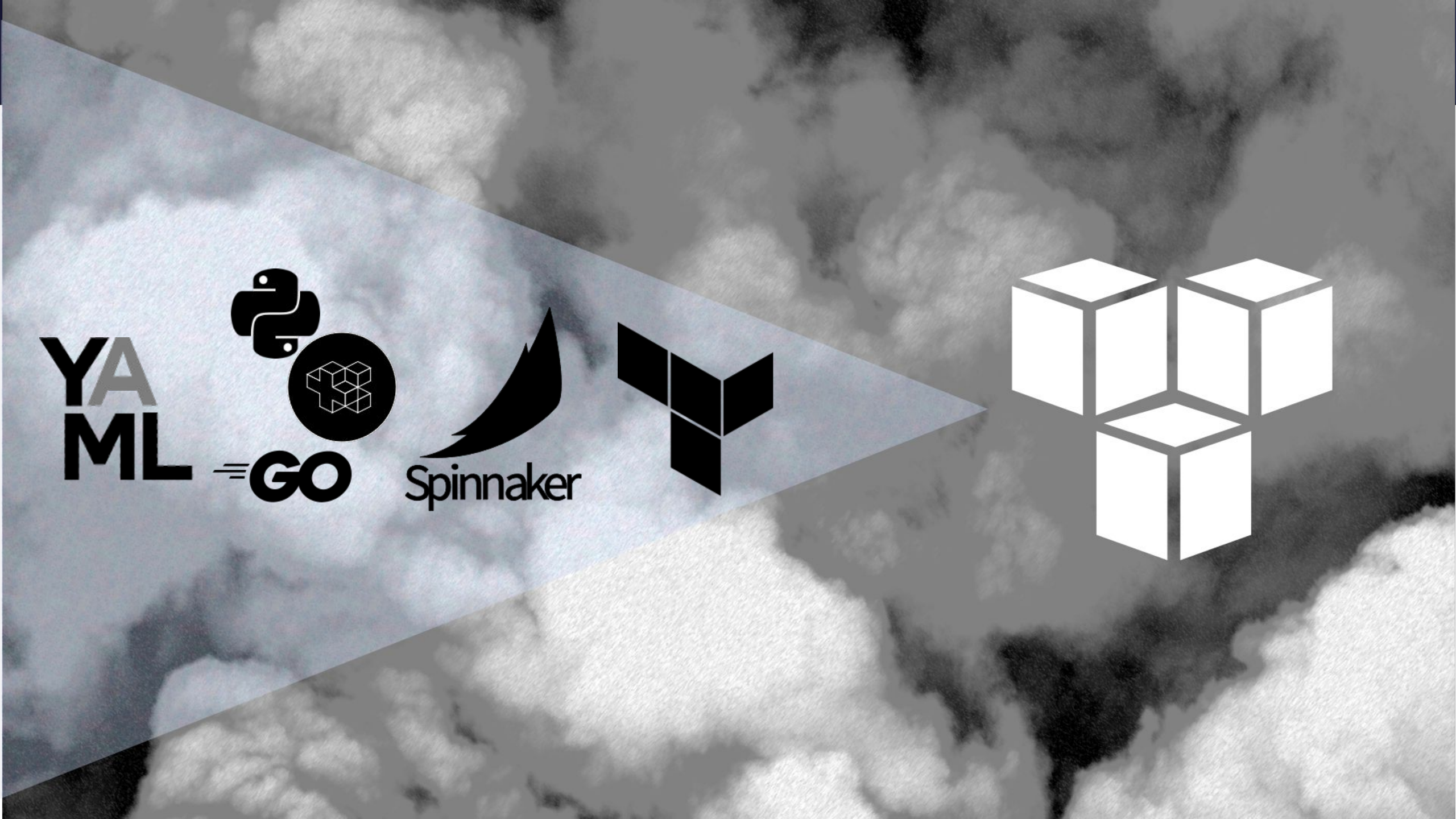
Terms

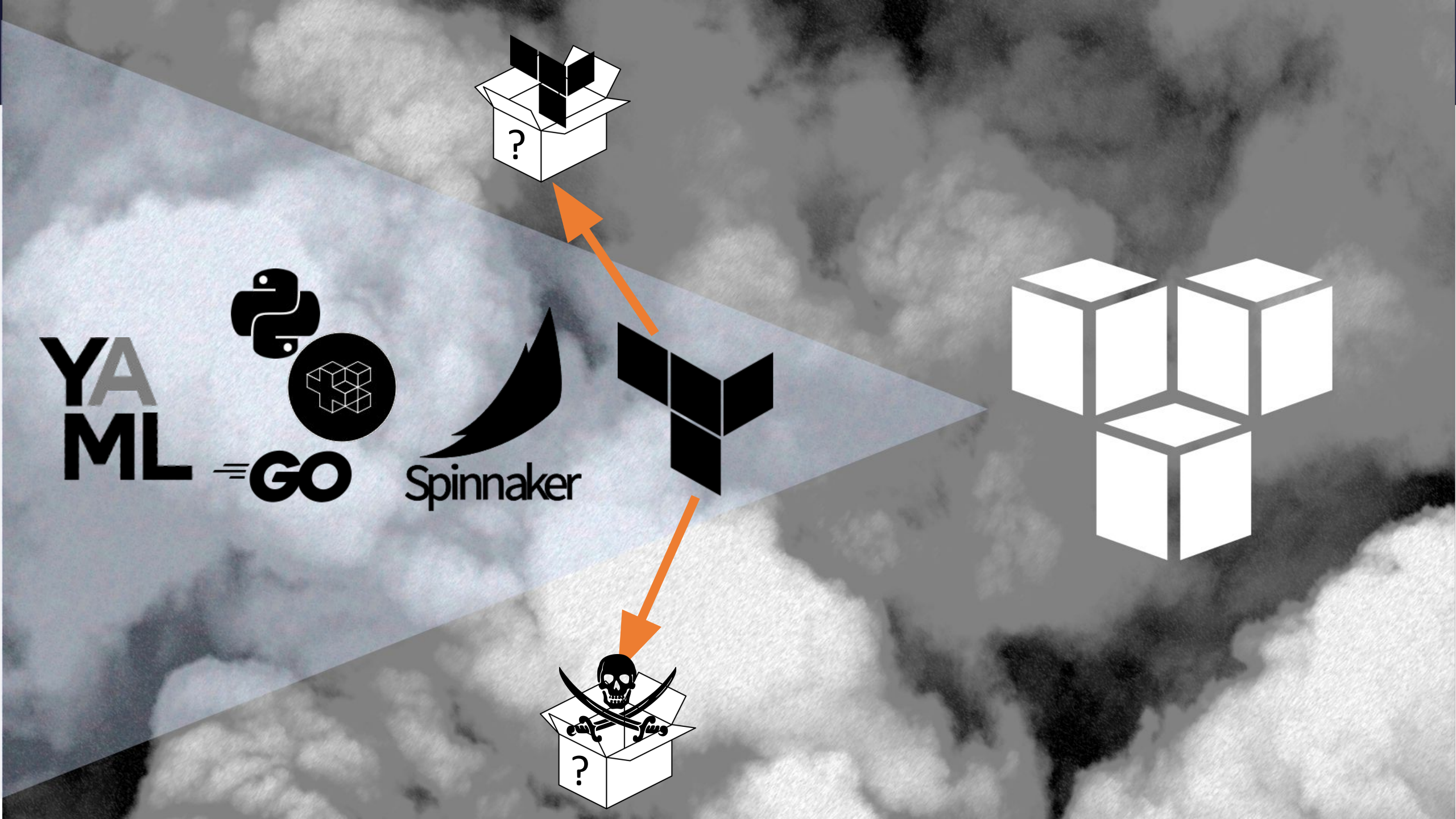
- **IaC: Infrastructure as Code**
  - Declaratively describe your infrastructure
  - VMs, networks, users, permissions, *everything*
  - IaC machine makes it so
  - **Examples:**
    - Crossplane
    - Pulumi
    - Terraform

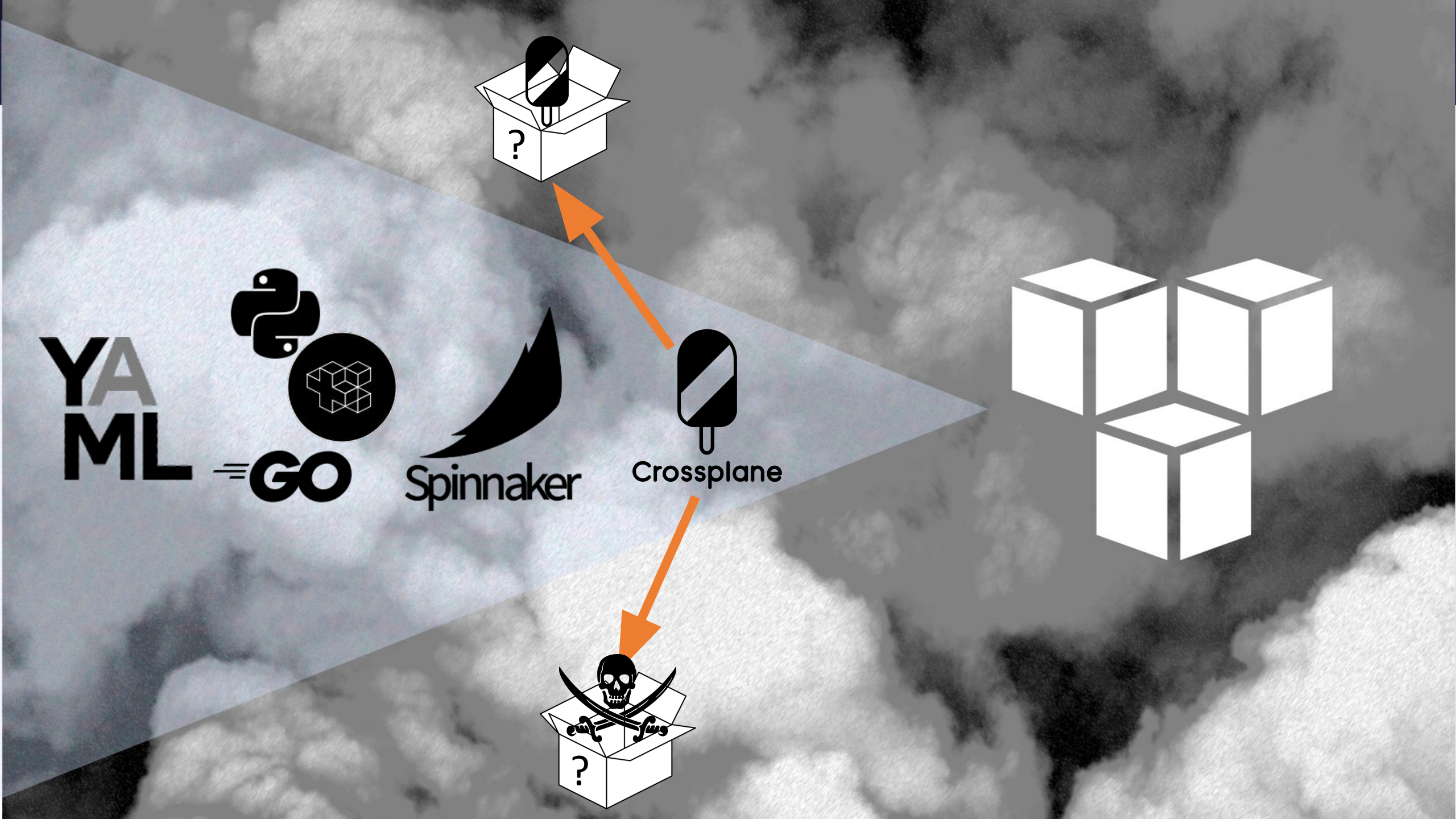
Terms

- **[Software] Supply Chain**
  - All that code you depend on that you didn't write
  - *Where* you got it from, *how* you got it from there
  - Specifically interesting problems with *open source* software dependencies


AUTODESK


YAML
GO
Spinnaker


YAML
GO
Spinnaker


YAML
GO
Spinnaker
Crossplane


YAML
GO
Spinnaker

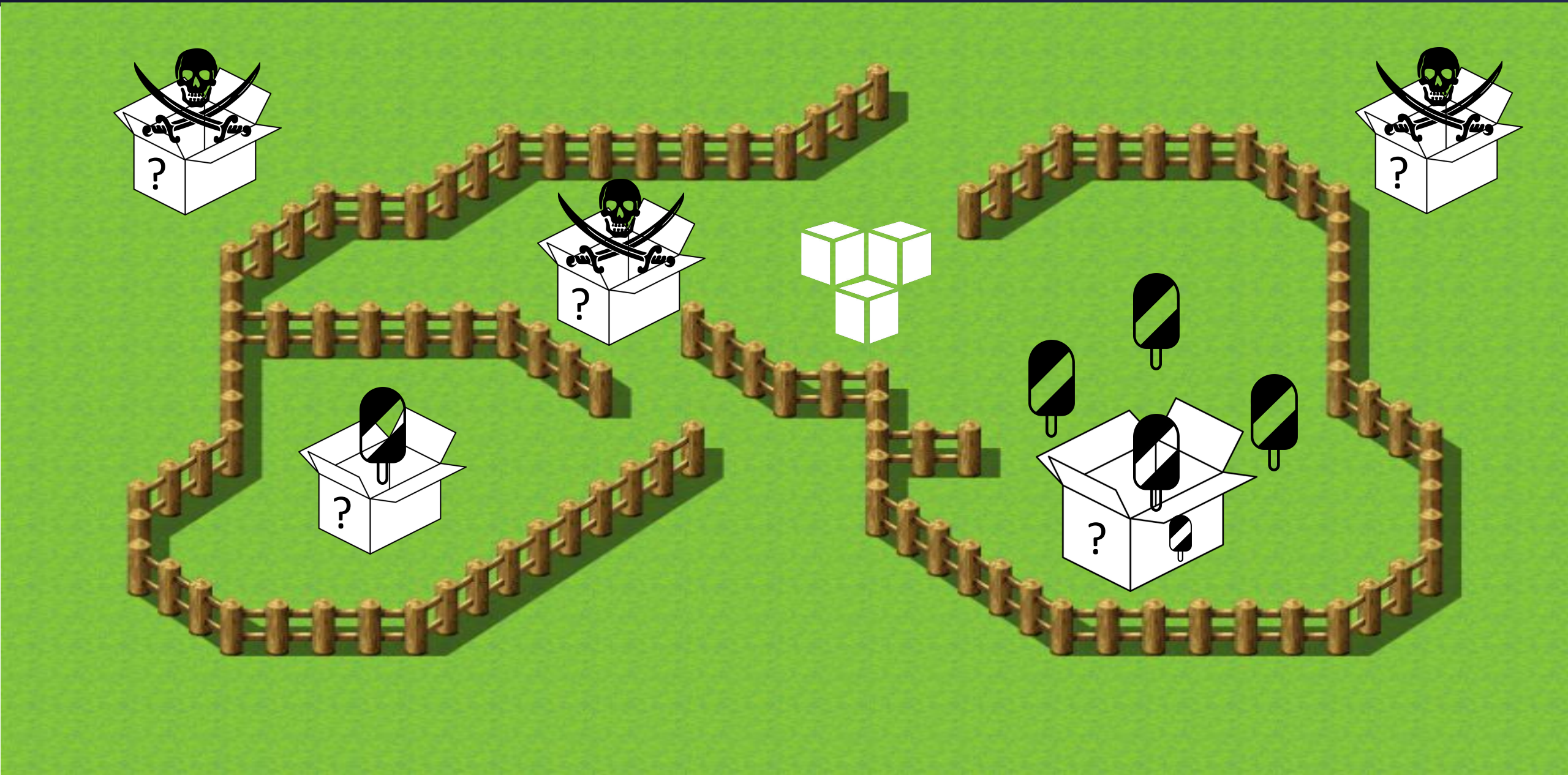
Why it matters


```
provider "registry.terraform.io/hashicorp/aws" {
  version     = "3.63.0"
  constraints = ">= 2.7.0, >= 2.42.0, >= 2.49.0, >= 3.4.0, >= 3.40.0"
  hashes = [
    "h1:lf8Qex8bhCmh8TUEAU6H4brzjy3+d4BXB6gcOYnNtNY=",
    "zh:42c6c98b294953a4e1434a331251e539f5372bf6779bd61ab5df84cac0545287",
    "zh:5493773762a470889c9a23db97582d3a82035847c8d3bd13323b4c3012abf325",
    "zh:550d22ff9fed4d817a922e7b84bd9d1f2ef8d3afa00832cf66b8cd5f0e6dc748",
    "zh:632cb5e2d9d5041875f57174236eafe5b05dbf26750c1041ab57eb08c5369fe2",
    "zh:7cfeaf5bde1b28bd010415af1f3dc494680a8374f1a26ec19db494d99938cc4e",
    "zh:99d871606b67c8aefce49007315de15736b949c09a9f8f29ad8af1e9ce383ed3",
    "zh:c4fc8539ffe90df5c7ae587fde495fac6bc0186fec2f2713a8988a619cef265f",
    "zh:d0a26493206575c99ca221d78fe64f96a8fbcebe933af92eea6b39168c1f1c1d",
    "zh:e156fdc964fdd4a7586ec15629e20d2b06295b46b4962428006e088145db07d6",
    "zh:eb04fc80f652b5c92f76822f0fec16975815438062440685 06aed69e1bb9b2af",
    "zh:f5638a533cf9444f7d02b5527446cdbc3b2eab8bcc4ec4b0ca32035fe6f479d3",
  ]
}
```

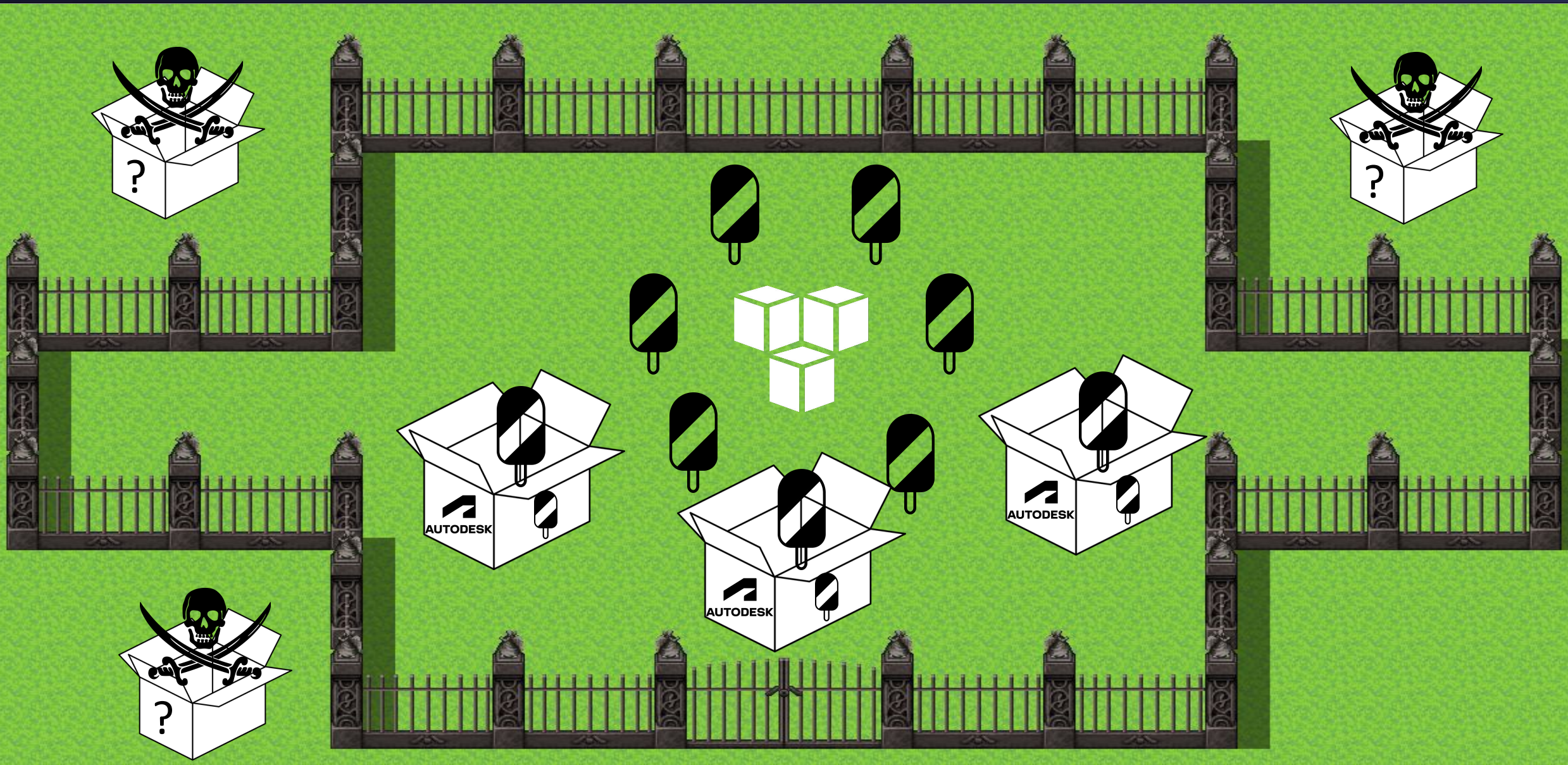
Current Mitigations

- Mandates on repo usage
- Library reference hygiene:
  - Version pinning
  - Typo checking
- Static analysis tools
  - Blacklists = Arms race
- Dynamic analysis tools
  - After the fact?
  - Who’s heuristics?

Walled Garden?



Walled Garden!

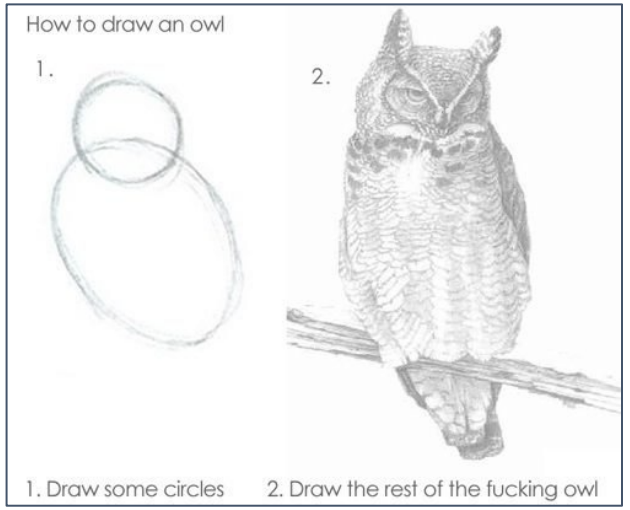


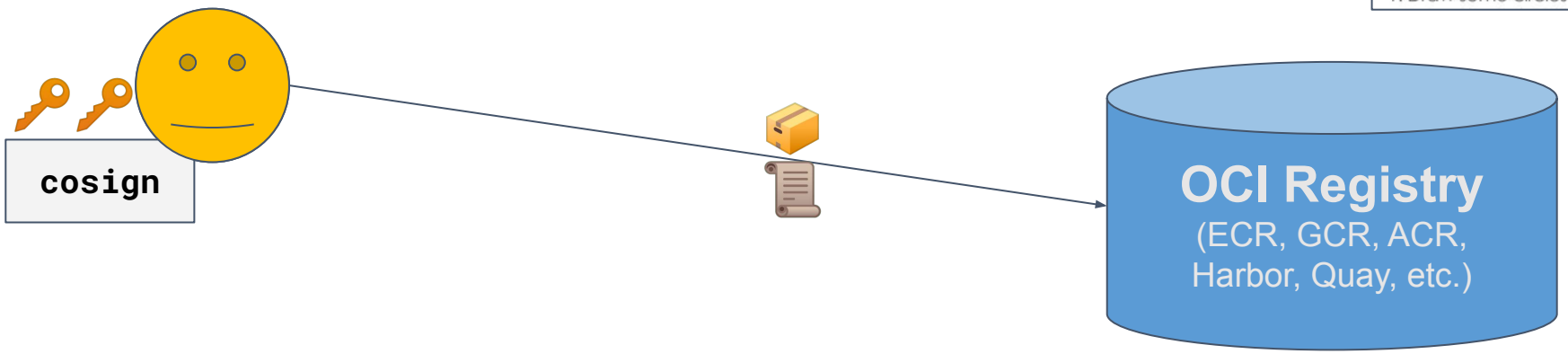
Sigstore in one slide

- **Signature, transParency and Identity Framework For Everyone**
  - …but that was already taken 🙄
- **`cosign`**
  - CLI to sign OCI images, store signatures in any old OCI registry
  - Also attach + download other non-signature things (SBOMs, attestations)
  - Also sign + verify non-container things
- **Rekor transparency log**
  - Public, verifiable, append-only log of what's been signed
- **Fulcio identity + certificate service**
  - Issues short-lived signing certificates, usually in exchange for OIDC credentials
  - "I've authed as jason@chainguard.dev with google.com, pls give me a cert to that effect"
- **Public Good infrastructure** for the above: GA soon, oncall support, defined SLAs
  - You can also run these yourself

Sigstore in one slide (cont.)

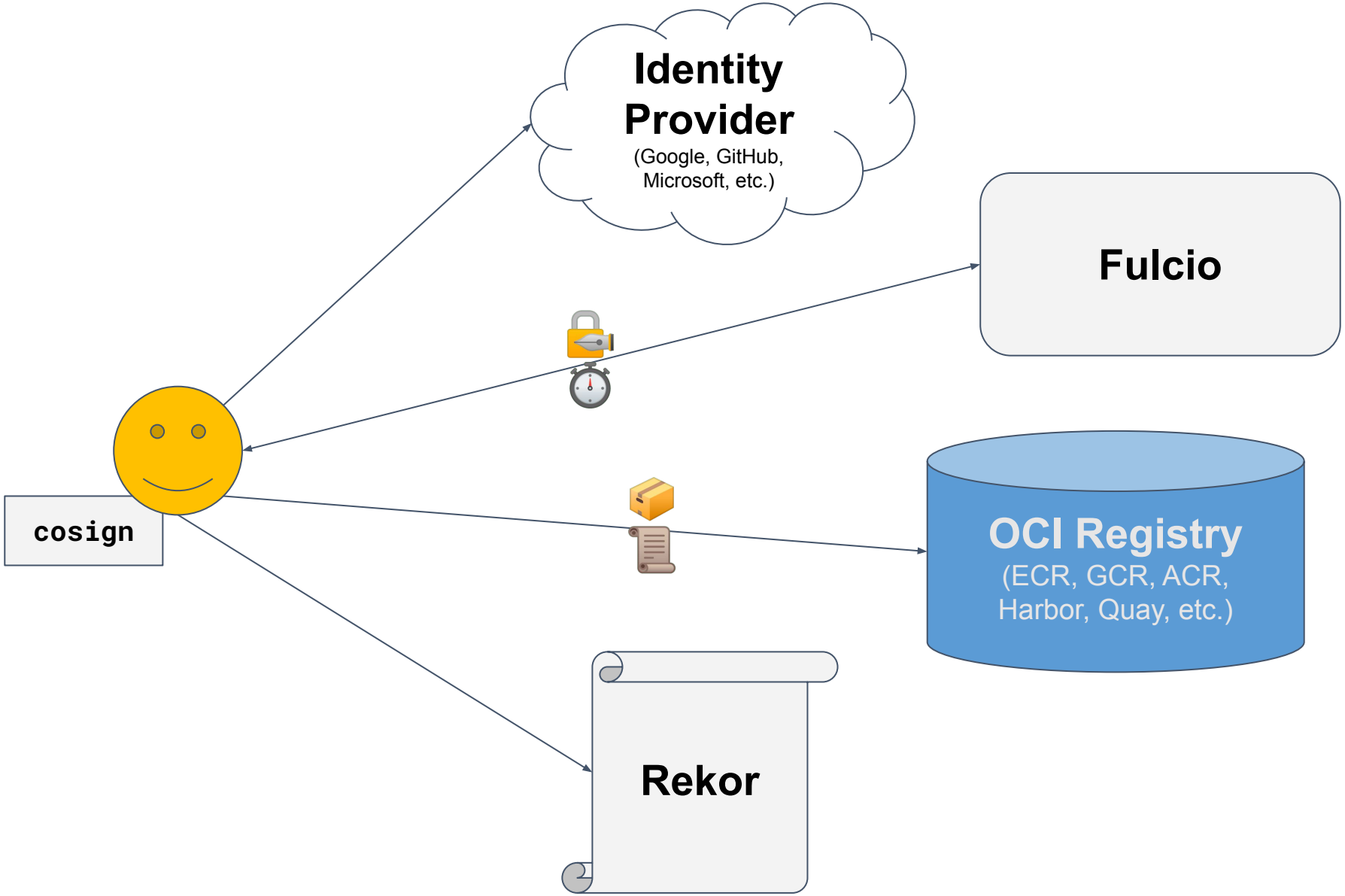
Keyful signing





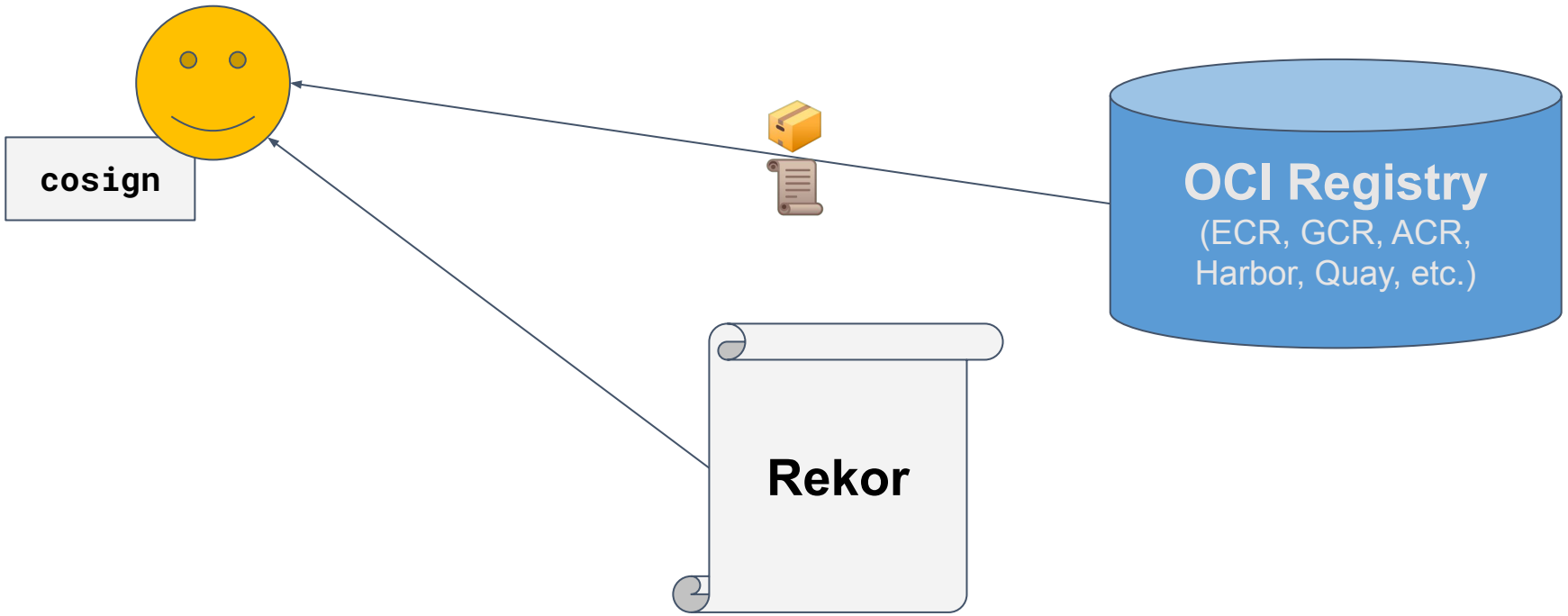
Sigstore in one slide (cont.)

Keyless signing



Sigstore in one slide (lol jk)

Keyless verification



Sigstore for Crossplane

- **Crossplane Packages are already stored in OCI registries!**
  - Can already be signed using `cosign`!
- Just need to implement verification
  - Using the ~same code as `cosign verify`

- **Keyful verification:**
  - "Was it signed by someone holding the private key
  - …that corresponds to the public key I'm holding?"
- **Keyless verification:**
  - "Was it signed by someone [in this team]
  - …according to my trusted Identity Provider
  - …verifiably, publicly, transparently?"

Demo 🎉

Call to Action

- Centralize the execution of your IaC
- Know your IaC sources
- Sign and validate them
- Scan IaC with [stat|dynam]ic analysis tools
- Run with least privilege credentials

Questions?


KubeCon
CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022
TiKV
TiKV
HELM