April 2025

monzo

Dependency-Track at Monzo

Michael Macnair
Staff Engineer

April 2025

monzo

Agenda

1 Context

2 Detection performance comparison

3 Operating Dependency-Track

4 SBOM generation

5 Enriching findings

6 Questions

April 2025

monzo

1. Context

Assets

Libraries

- ~6 main git repos
- ~Homogenous tech within each
- Go, Python, Javascript, Kotlin, Swift

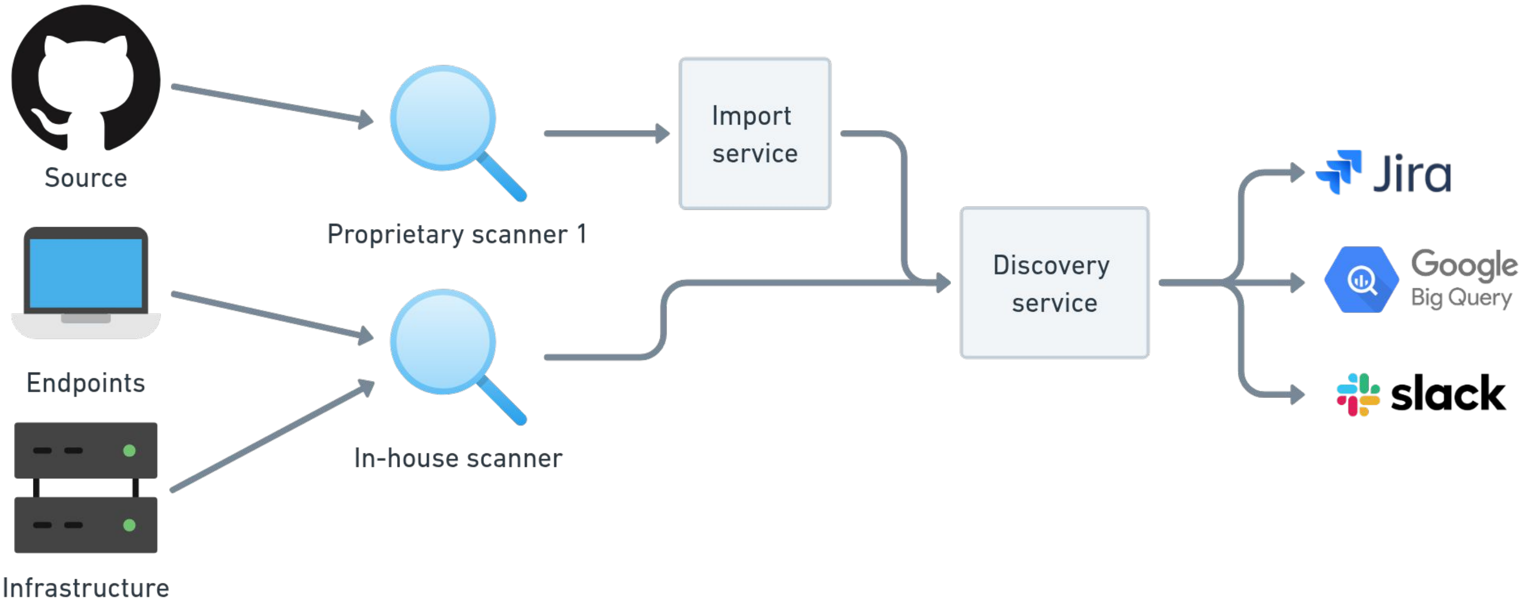
Infrastructure

- Containers
- Virtual machines
- Data centers

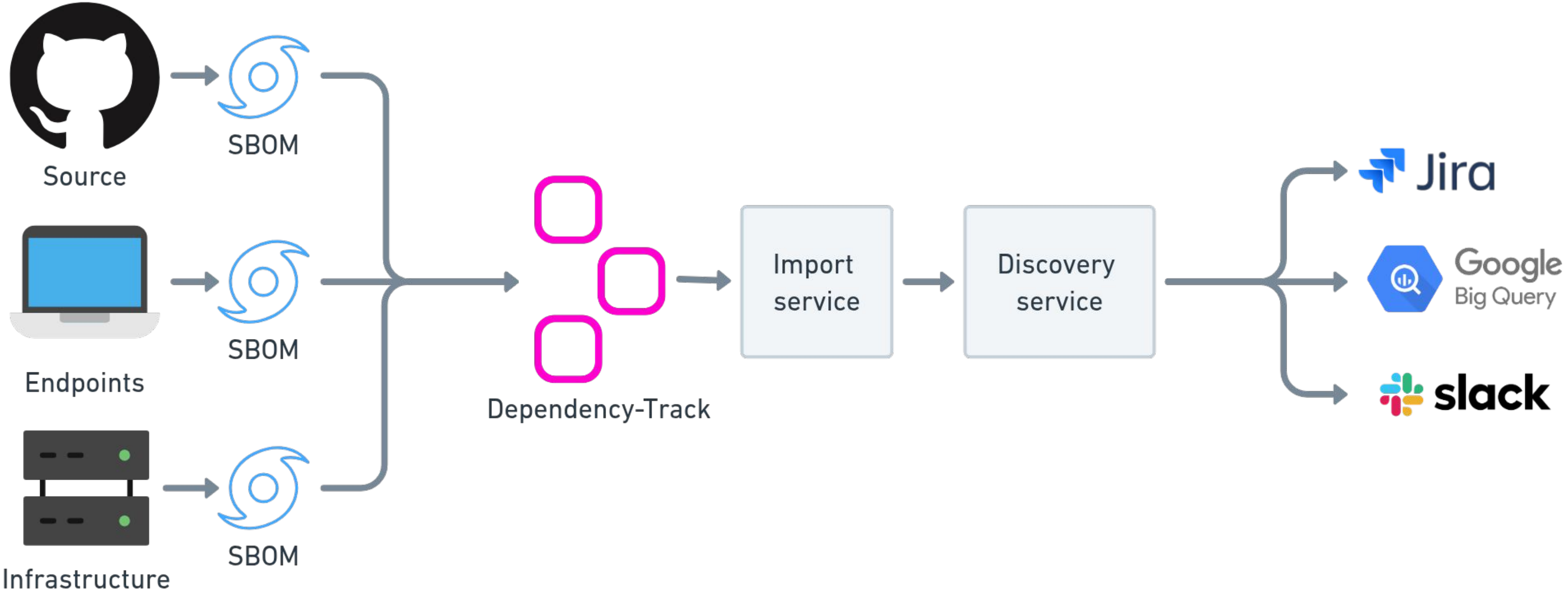
Laptops

- Primarily macOS

Old architecture

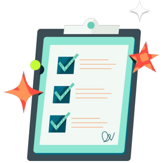


New architecture



2. Performance Comparison

Detection performance



Methodology

Ran multiple scanners across a subset of our repositories.

Manually validated any discrepancies.

We don't learn absolute performance, just relative.

False positives and negatives

Every approach missed real findings, and reported some findings that didn't apply.

Verdict

The differences weren't substantial.

Our proprietary solution could be safely replaced with an SBOM-based approach from an accuracy perspective.

3. Operating Dependency-Track

Overall experience

Dependency-Track is generally well behaved and doesn't have problems that need investigating or fixing.

Issues we encounter

Pod churn

The API server is a single instance.

When kubernetes pods rotate, the server dies.

Anything interacting with it times out.

Timeouts

Deleting projects. Occasionally permanent and need manual cleanup.

Occasional mystery timeouts.

Log noise

Too noisy to easily surface all errors for investigation.

We rely on upstream signals instead like scan or import failed.

Historic, now fixed

BOM processing bugs.

Policy violation bugs.

Ever-growing comments 🤦

Infra costs

$250

$100

$900

(monthly USD, sum of staging + prod)

Monzo services

API server & frontend

AWS Aurora

5. Generating SBOMs

The good

Monorepos

Software uniformity

Open source tools

The bad

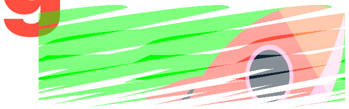
Licenses

Python licenses, in particular

Setup effort per asset/repo

4. Enriching findings

Enriching findings



1 Merge aliased vulnerabilities

2 Annotate ownership

3 Annotate how a component was included

4 Merge findings that affect multiple components

We're hiring

monzo.com/careers

monzo

SILVER

Thank you

@mykter@infosec.exchange

#proj-dependency-track on OWASP Slack