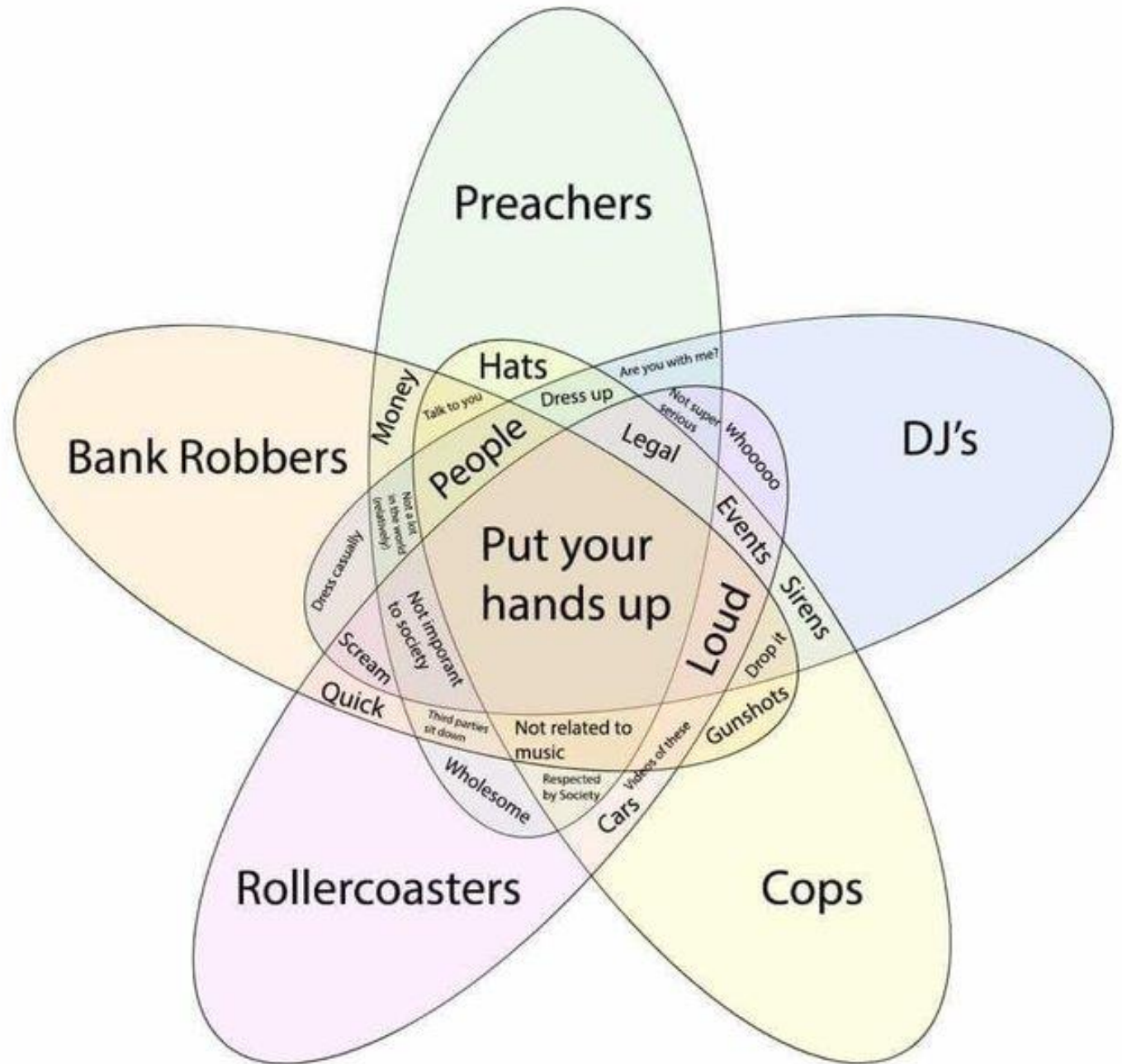
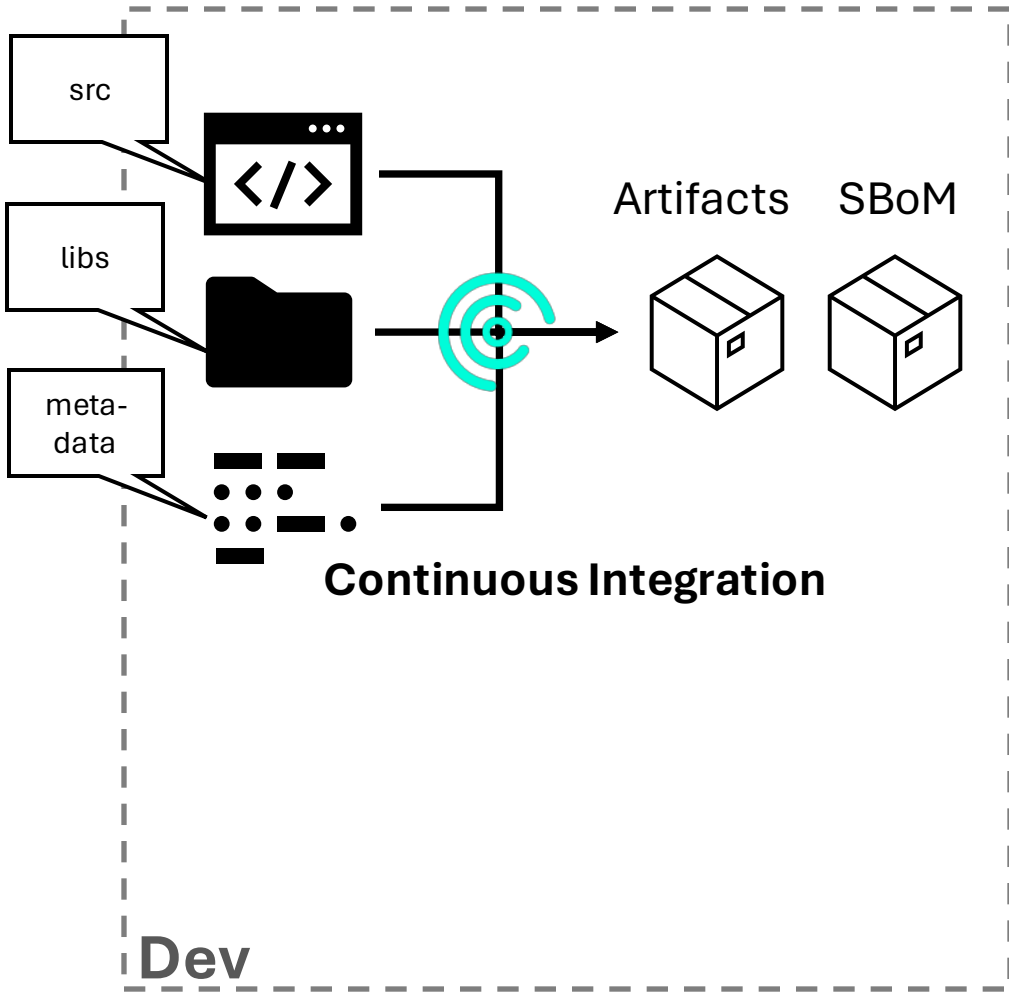


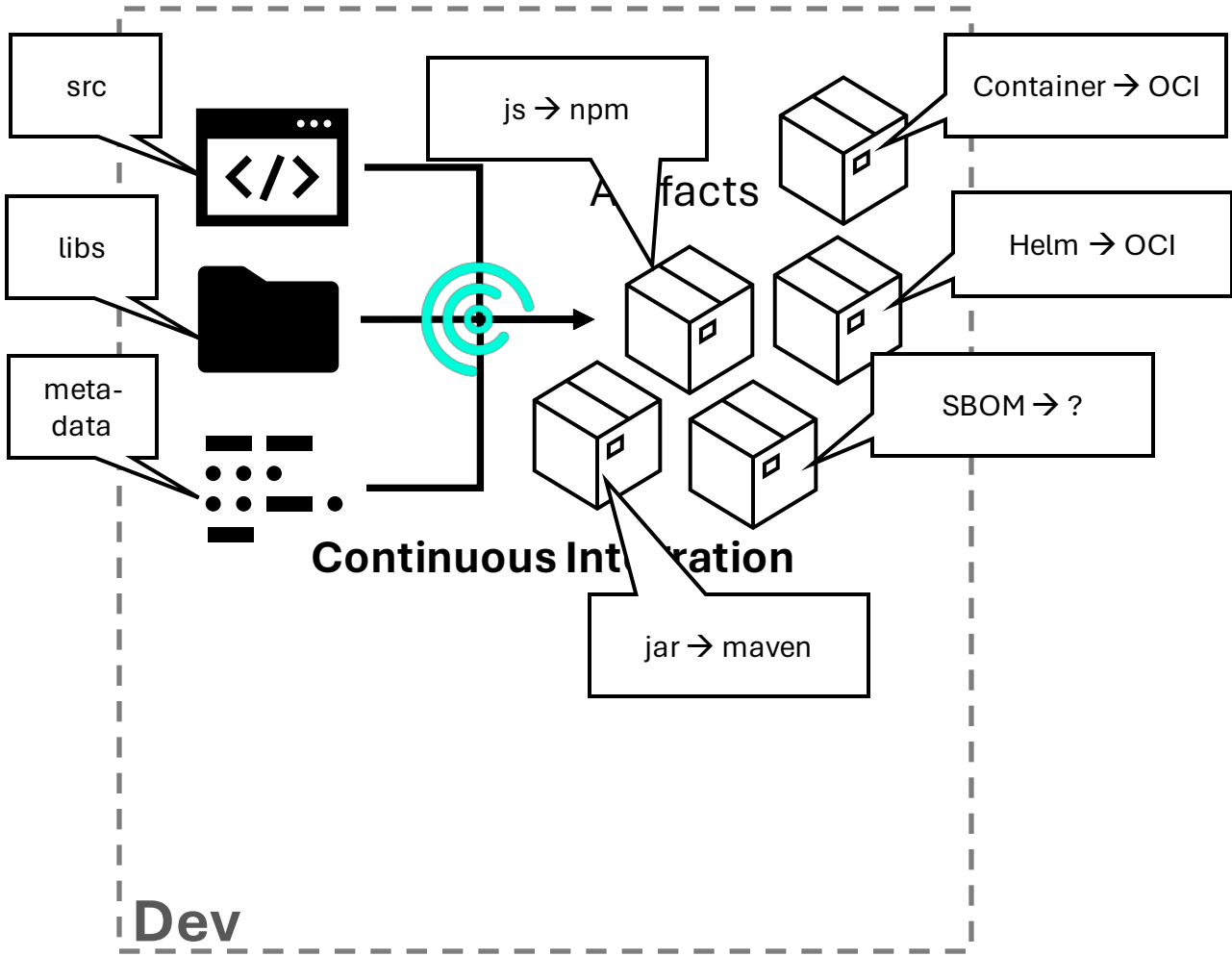
SBOM

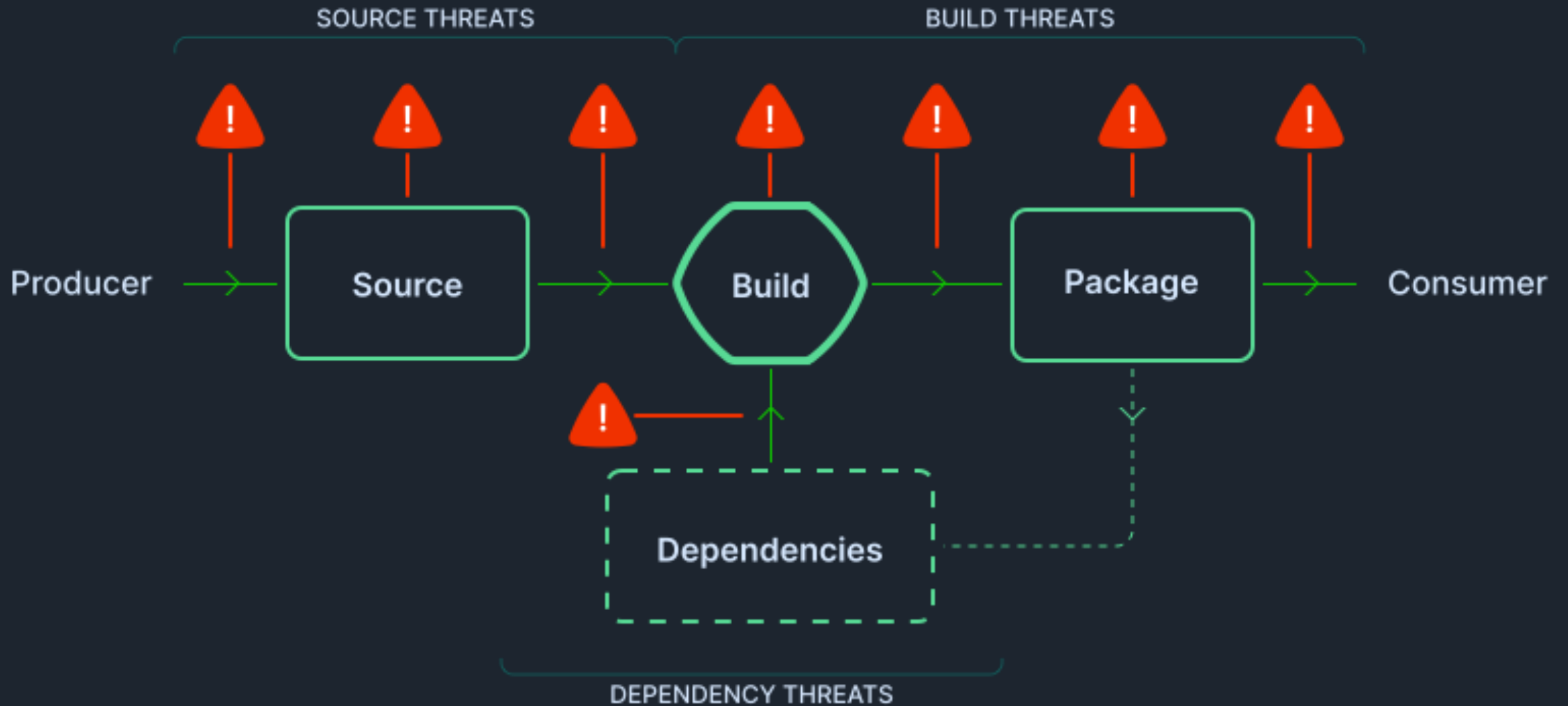


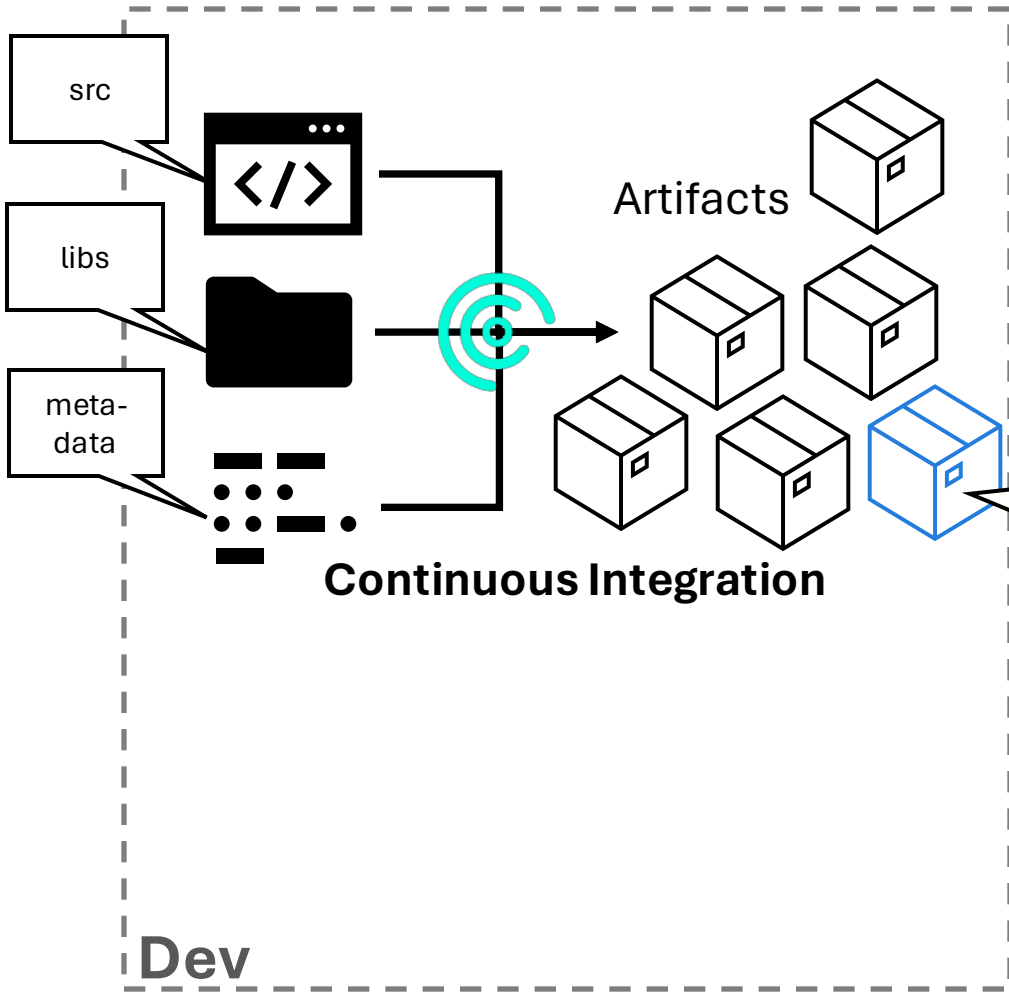
What's next











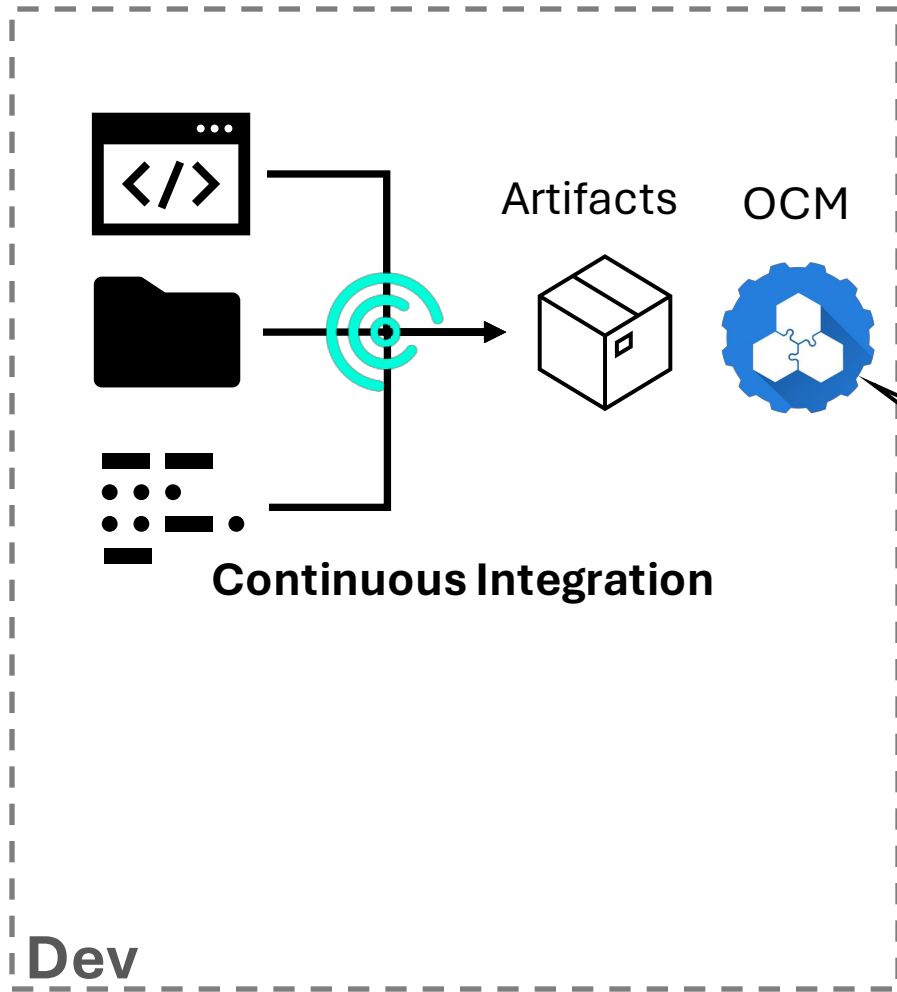
SBOM of all Product Artifacts?
Can we use it as Product Description?
Can we use it for **OPERATIONAL e2e** purposes?
Technology-agnostic?



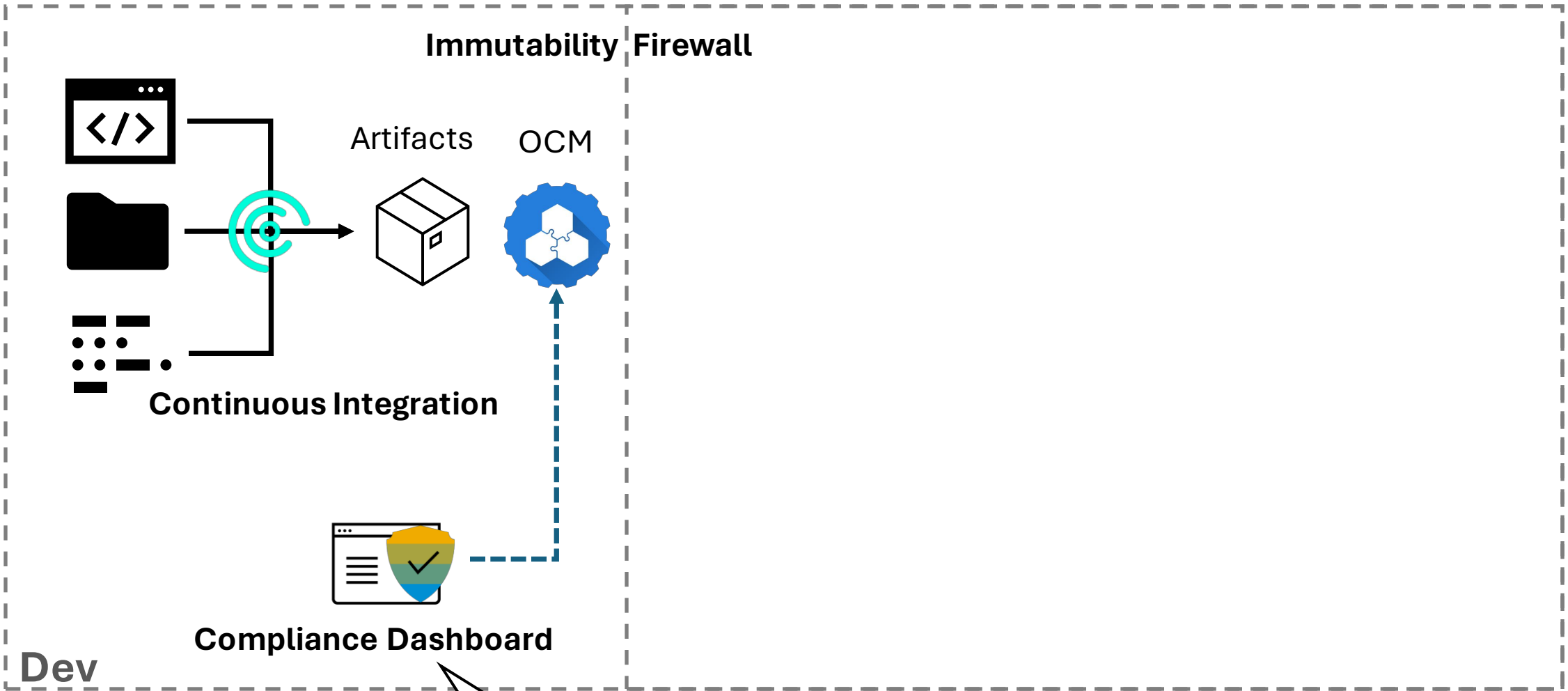
OPEN COMPONENT MODEL

An open standard to describe
software artifact delivery.

A Software Bill of Delivery (SBOD)

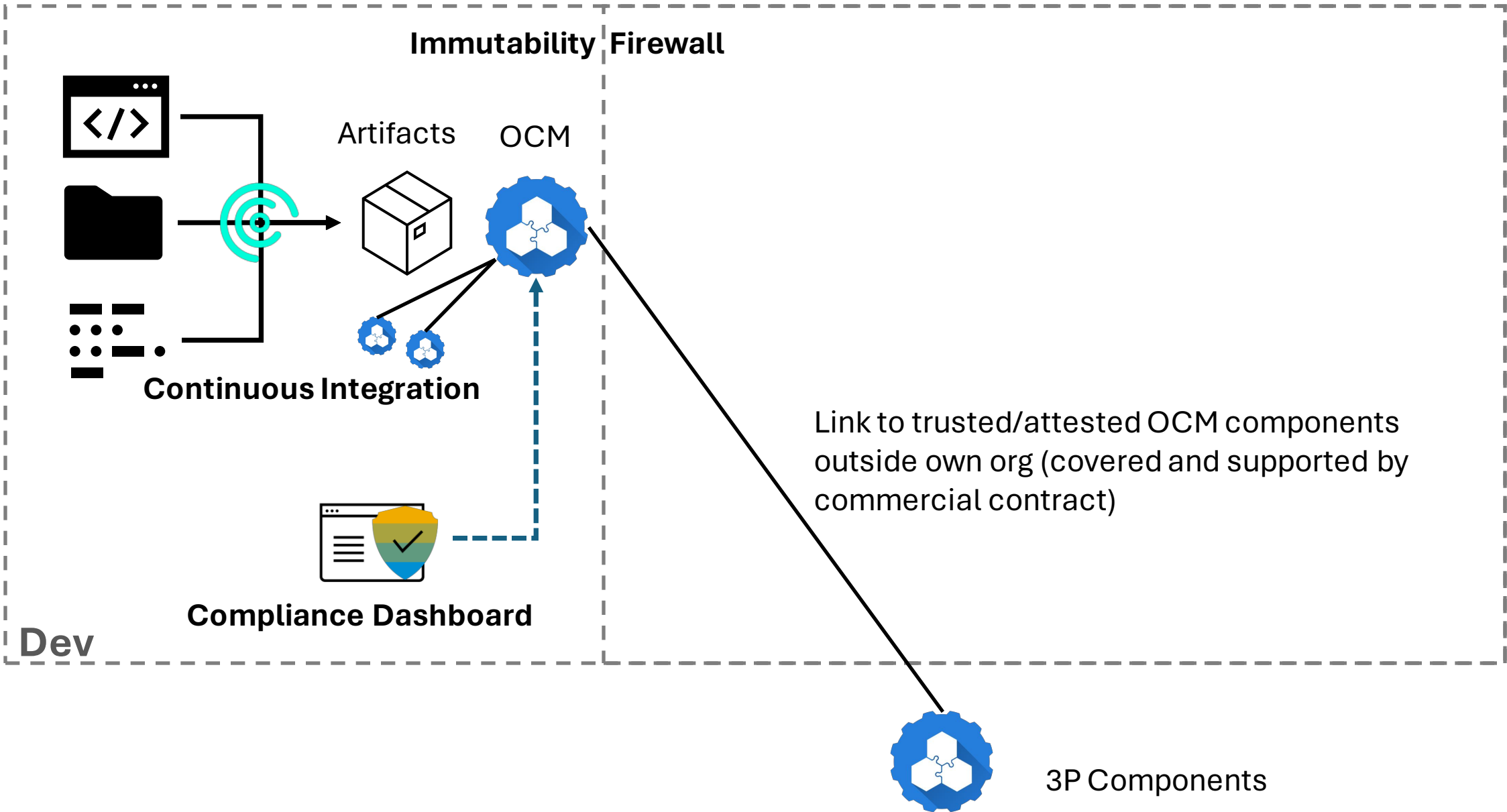


Open Component Model



Connect Findings to Product and their Components

Compliance Data Lake Graph Database



Immutability Firewall

Artifacts OCM

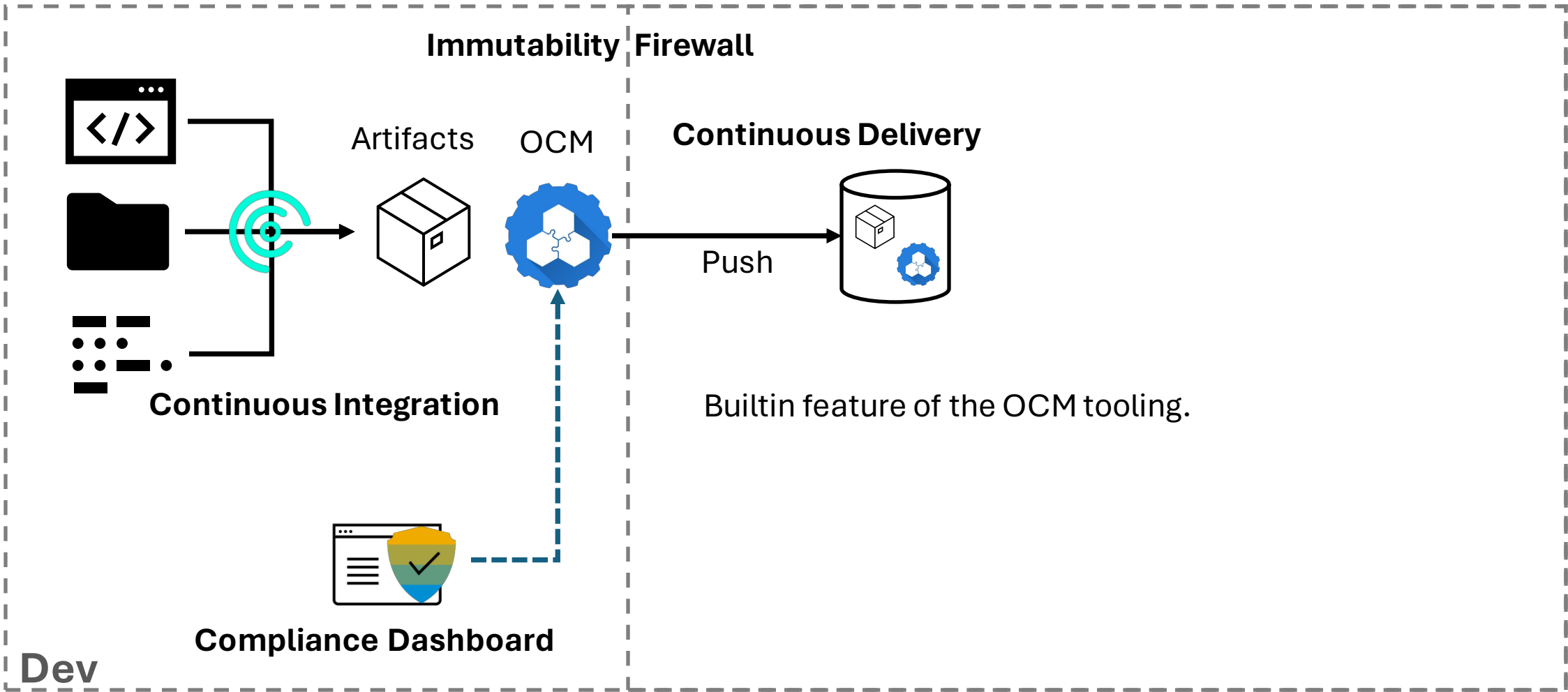
Continuous Integration

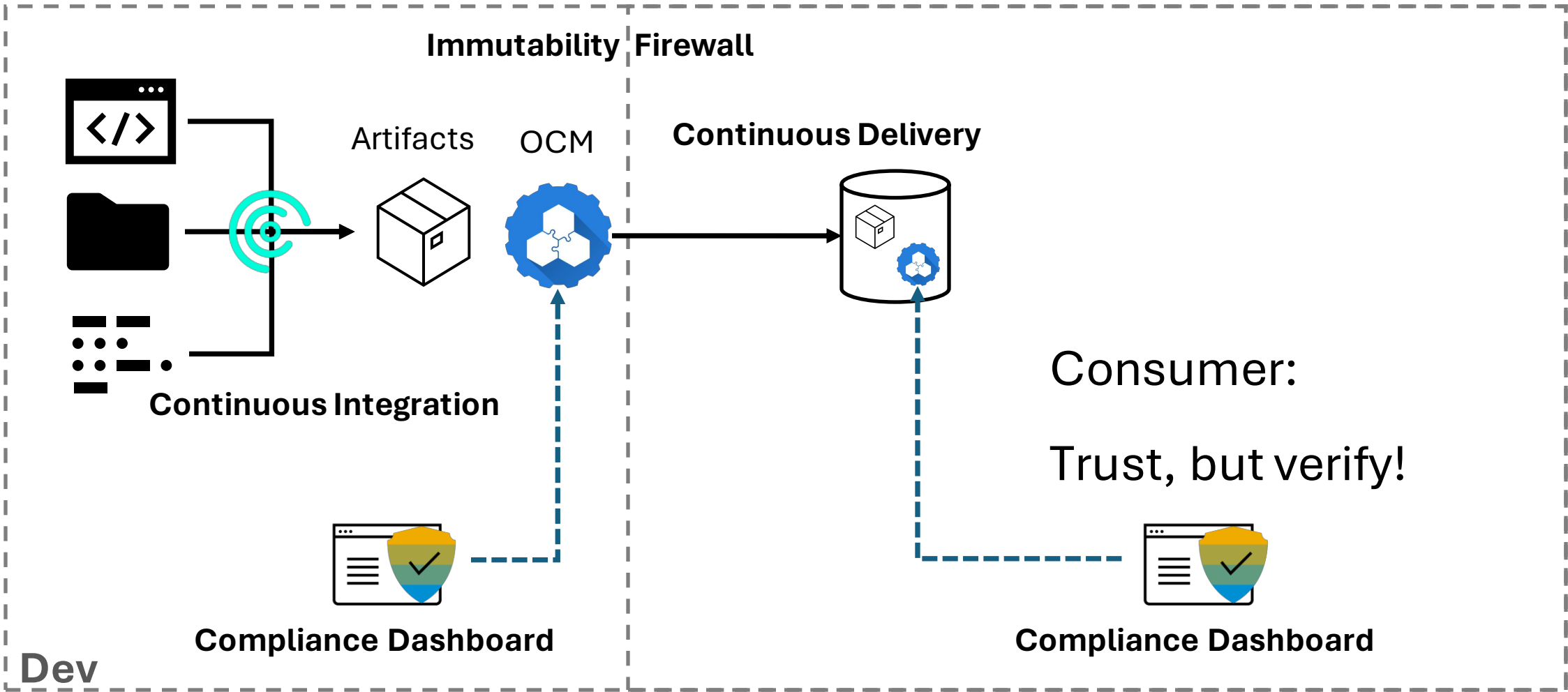
Compliance Dashboard

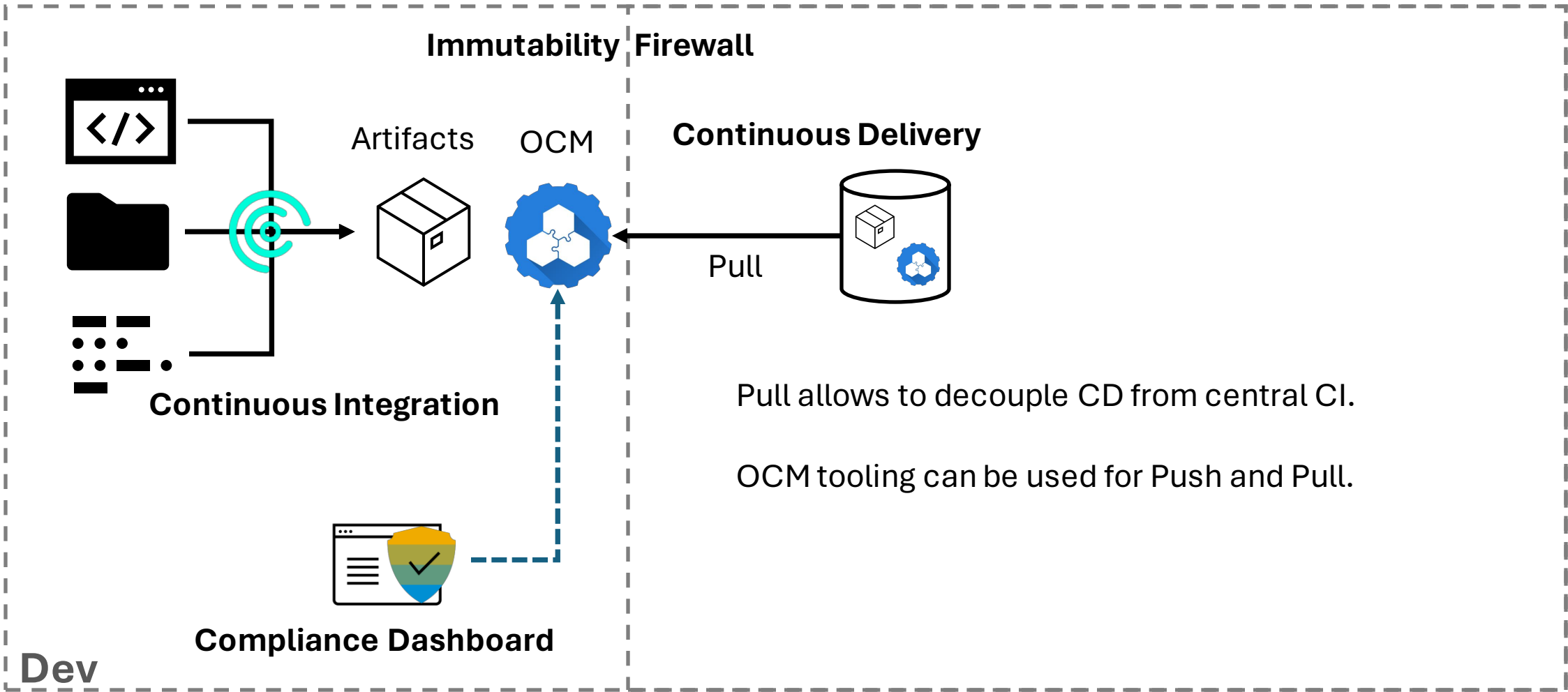
Link to trusted/attested OCM components outside own org (covered and supported by commercial contract)

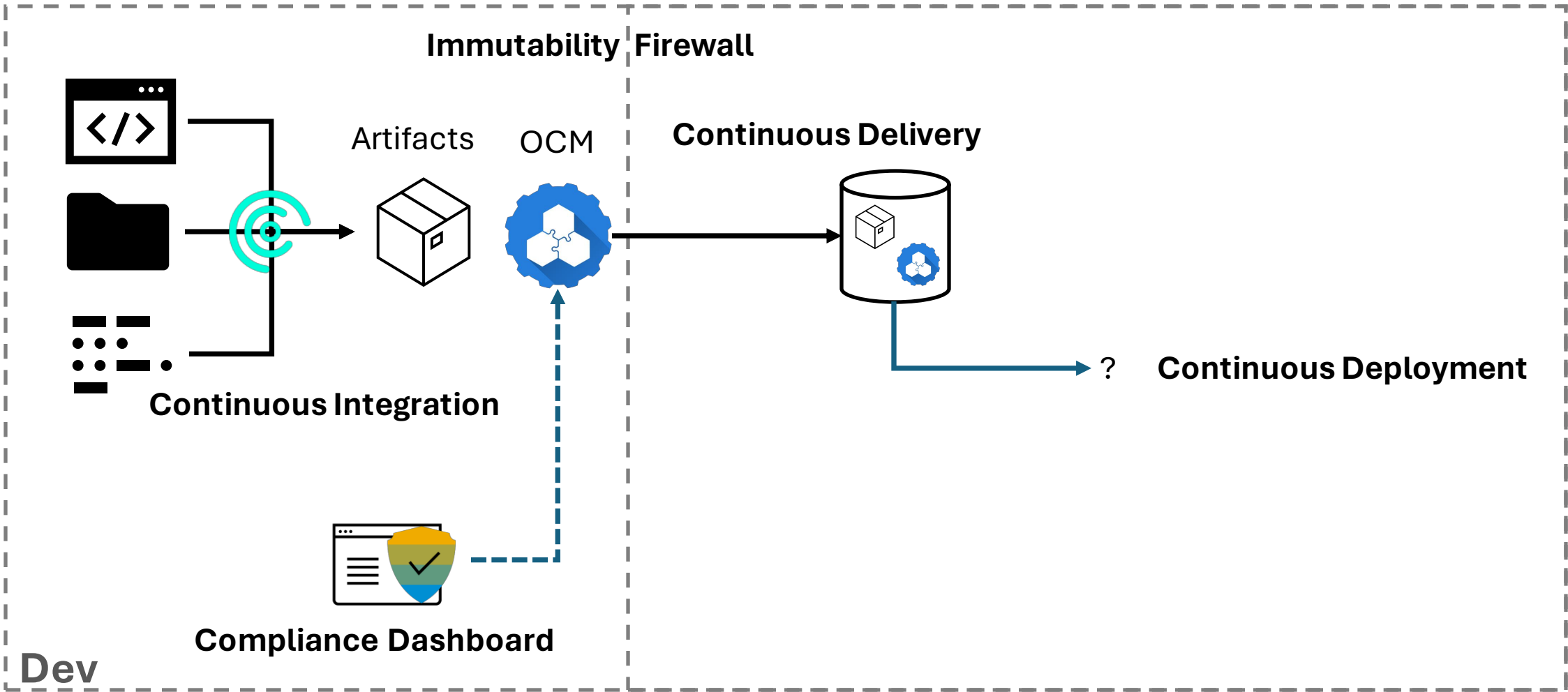
3P Components

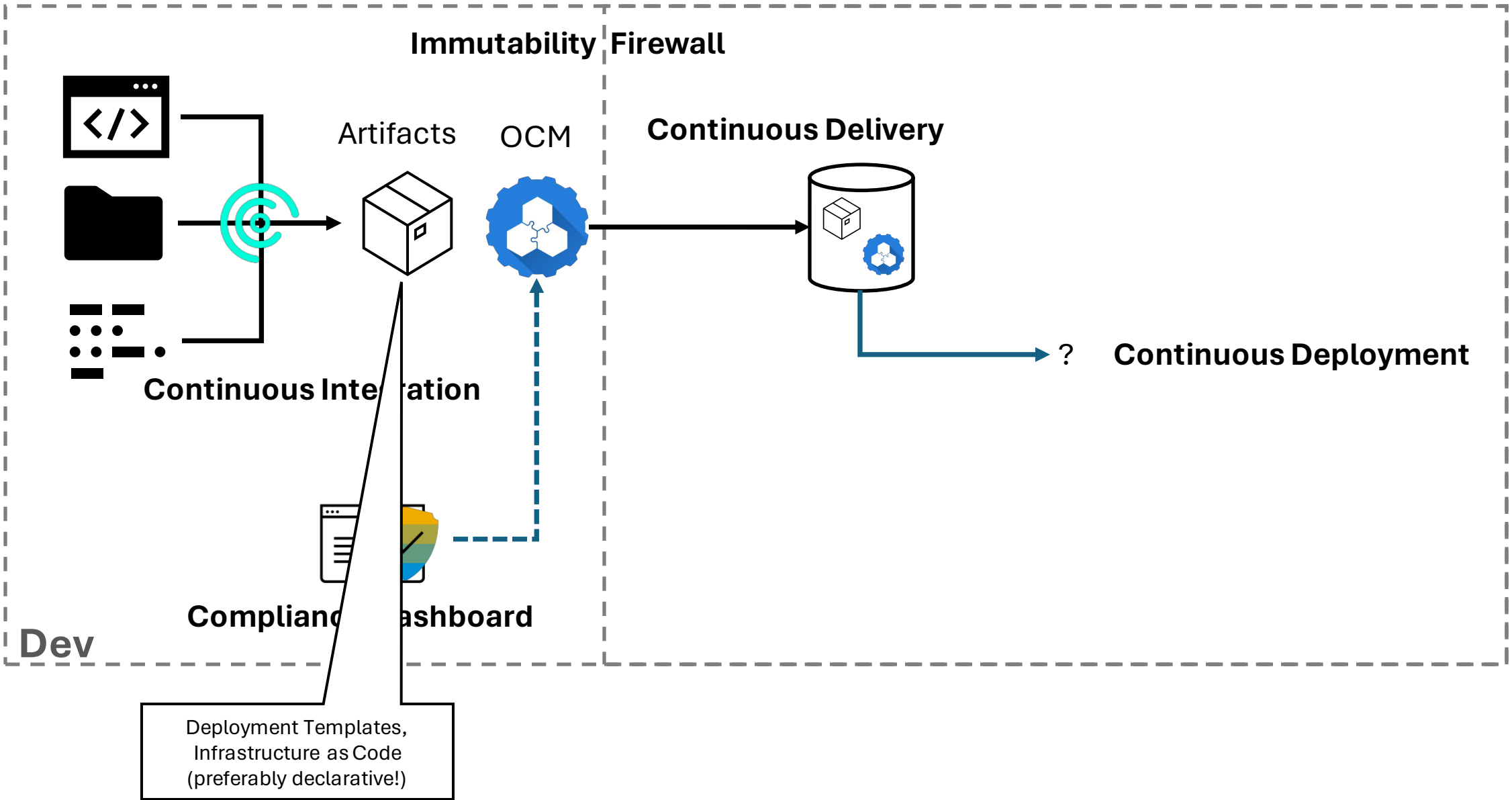
Dev

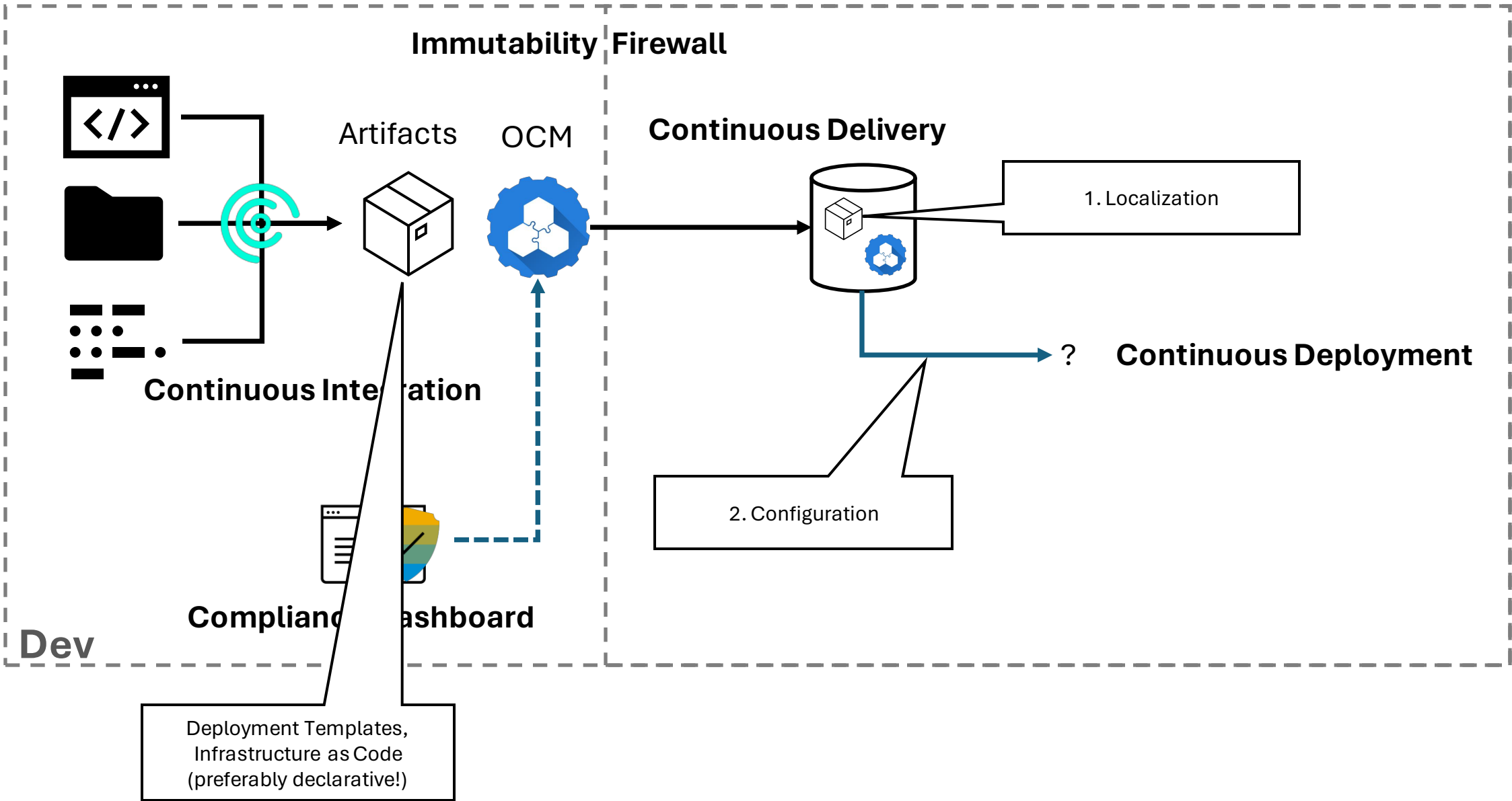


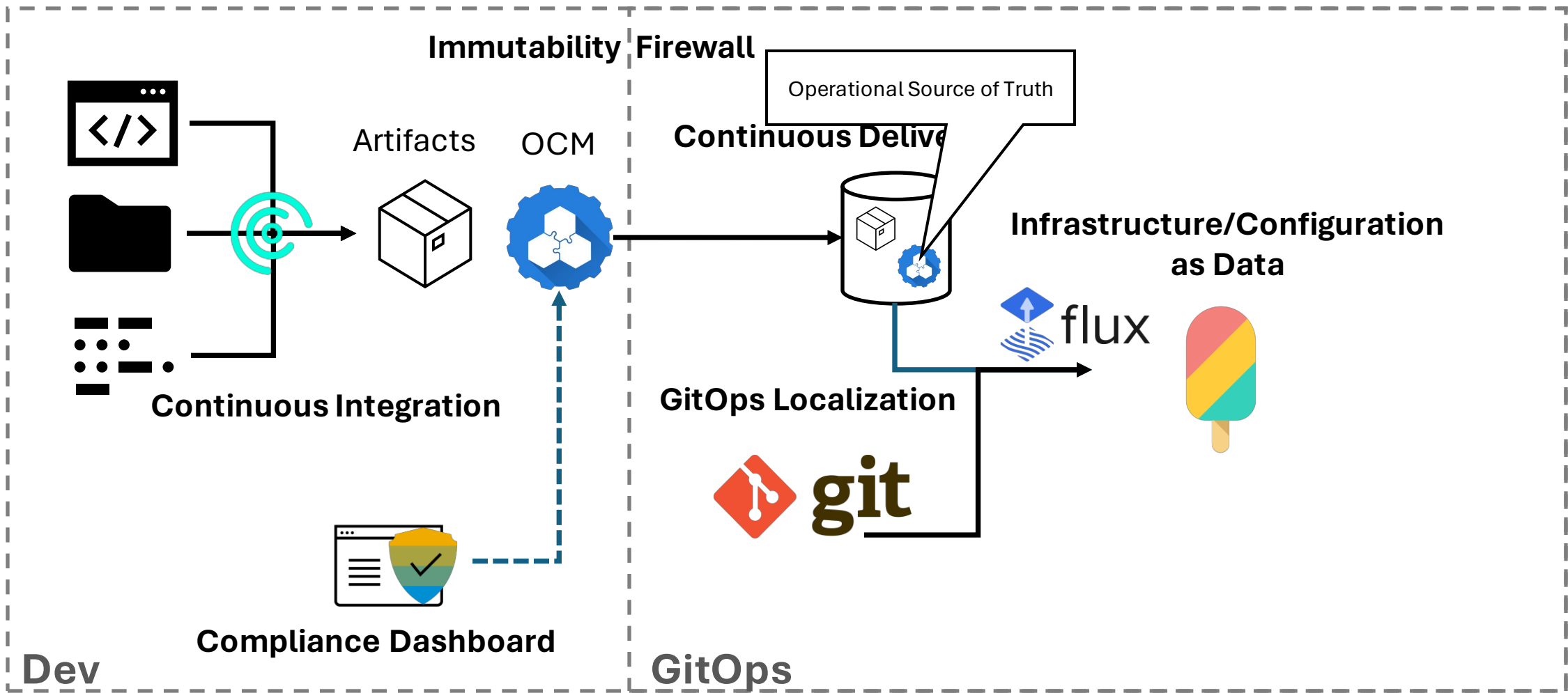


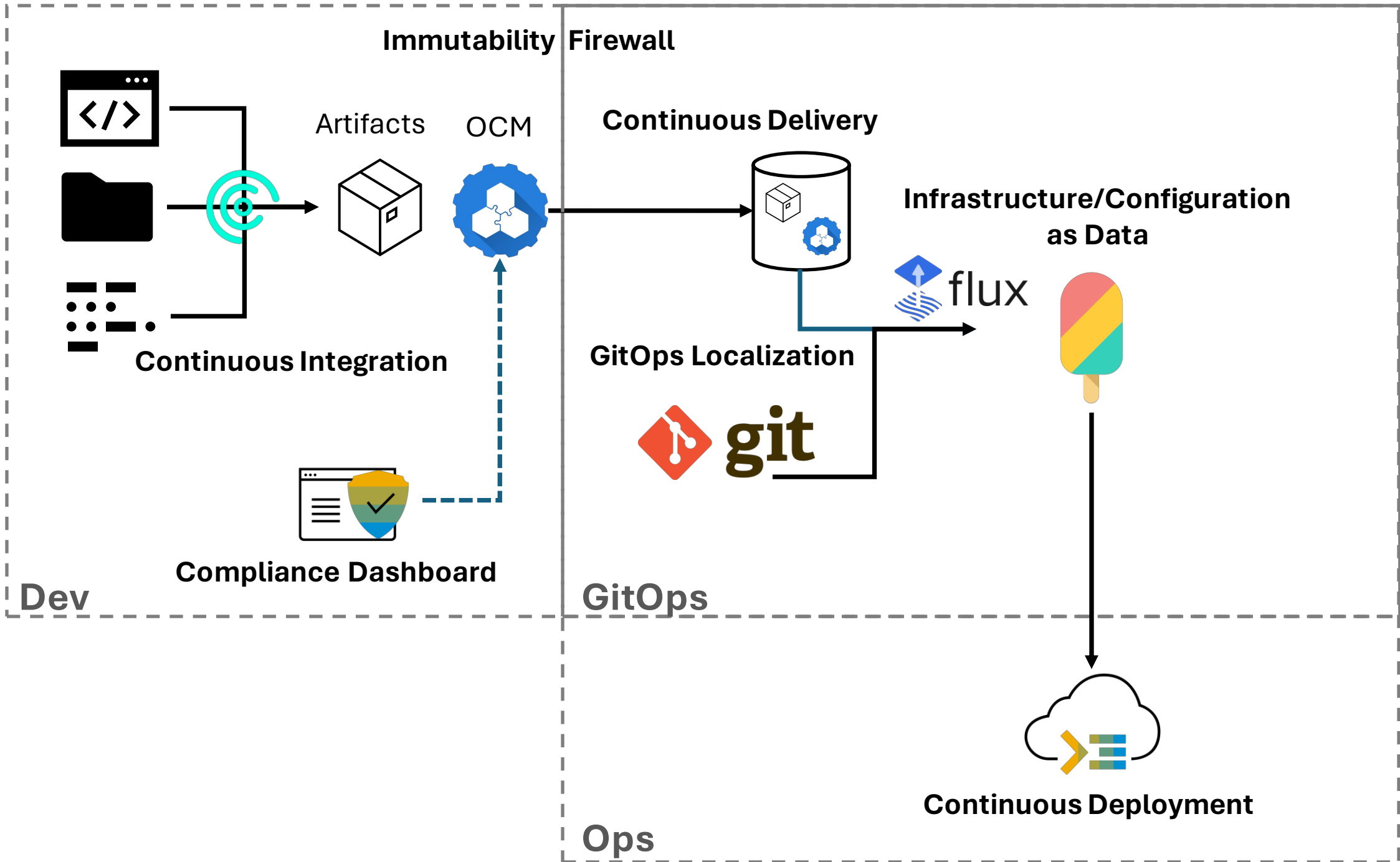














Operational SBoMs!



OCM

Arti
fact

SBOM

VEX

Meta
data

Arti
fact

Meta
data

Arti
fact

Attes-
tation

Unique OCM Characteristics

- Artifacts can be referenced at their origin location or **bundled together with the OCM component**, becoming part of the OCM component
- **Update access location of artifacts** inside OCM components **on transport** between registries, without violating signatures and without breaking deploy processes
- **Tooling** to transport OCM components and their artifacts into any environment, public, private or restricted and even air-gapped
- Integration with GitOps tools like FluxCD to enable applications using OCM to fully automate secure product deployment

Wrap-up



- OCM is a **technology-agnostic** and **machine-readable** format for the secure delivery of software artifacts
- OCM describes the parts necessary for delivery and deployment. Therefore we call it “**Software Bill of Delivery (SBOD)**”
- OCM **does not replace** any existing standard or format, but acts as a **wrapper around** existing metadata in any format and the software artifacts



OPEN COMPONENT MODEL

An open standard to describe software artifact delivery.

Open-source Apache-2.0 Licensed. [GitHub v0.6.0](#)

Get Started

<https://ocm.software>

Links and Sources



- OCM project page:
<https://ocm.software>
- OCM specification:
<https://github.com/open-component-model/ocm-spec>
- OCM project on GitHub:
<https://github.com/open-component-model>
- Demo: Deploying to Airgap with Flux & OCM
<https://github.com/open-component-model/demo-secure-delivery>
- OCM Slack channel (in Kubernetes workspace):
<https://kubernetes.slack.com/archives/C05UWBE8R1D>
- IPCEI-CIS (IPCEI Next Generation Cloud Infrastructure and Services):
<https://www.bmwk.de/Redaktion/EN/Artikel/Industry/ipcei-cis.html>