The LIQUID SOFTWARE Company

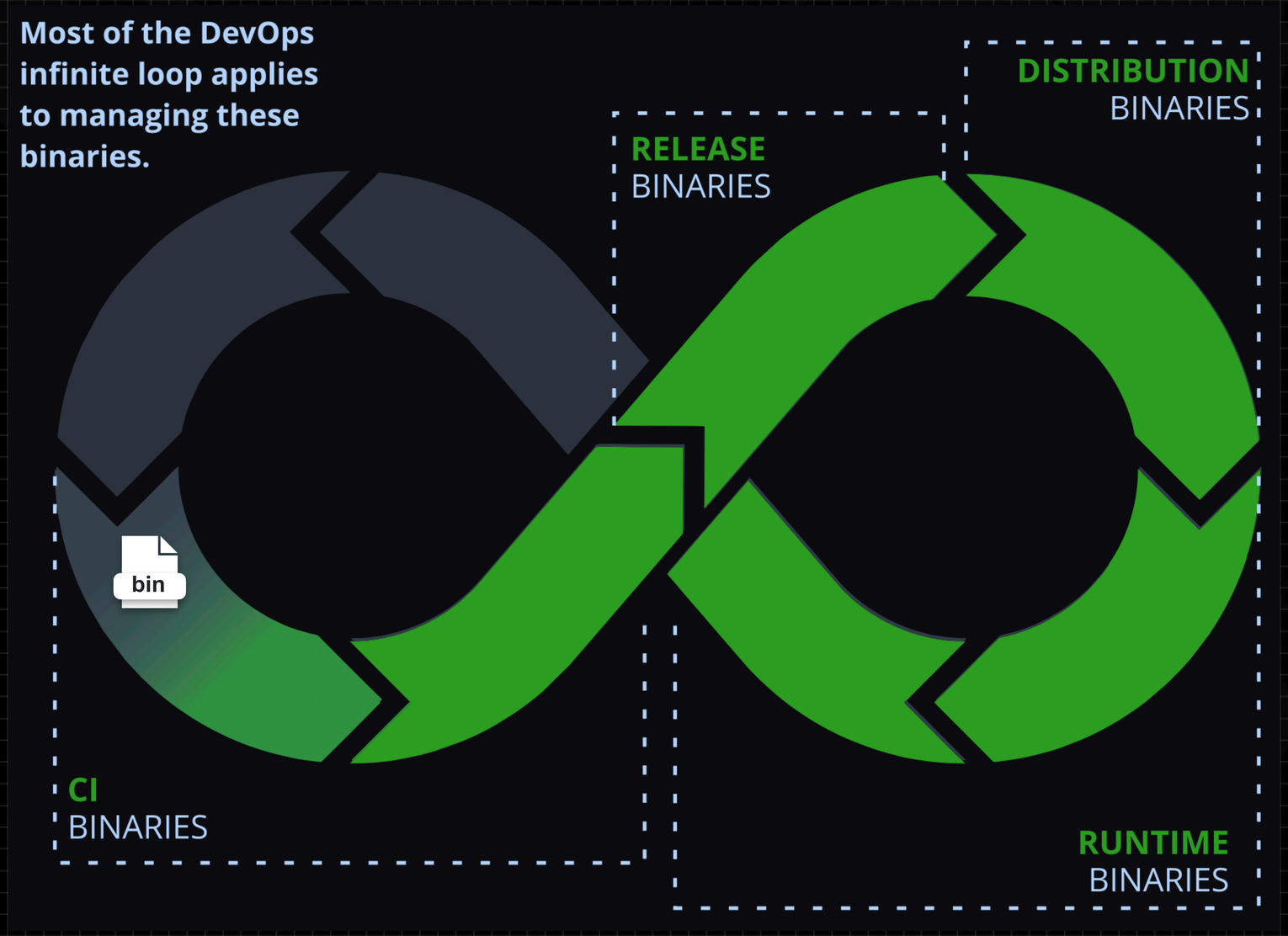
Introduction to JFrog Platform

Carlos Moya | Senior Solutions Engineer | cmoya@jfrog.com

The Liquid Software Company

A Bit Of Context

A binary-centric approach to DevOps



Overview of the JFrog Platform

BUILD & TEST → RELEASE → DEPLOY

The Liquid Software Company

Addressing common challenges with Artifactory

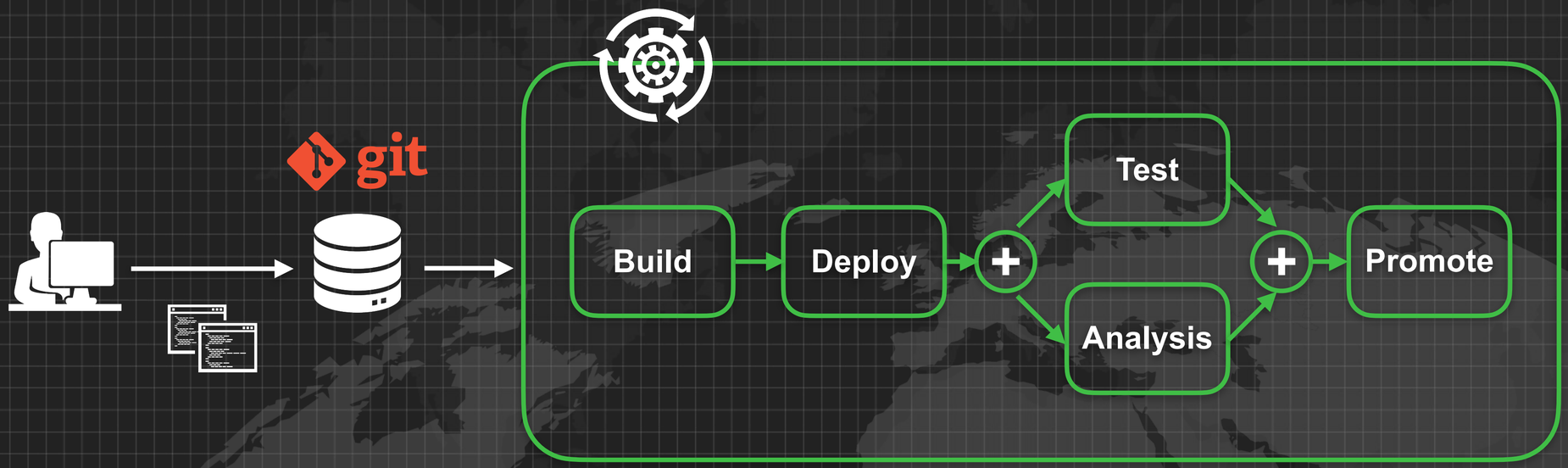
Basic

The
Liquid
Software
Company

Single Development Team, single location

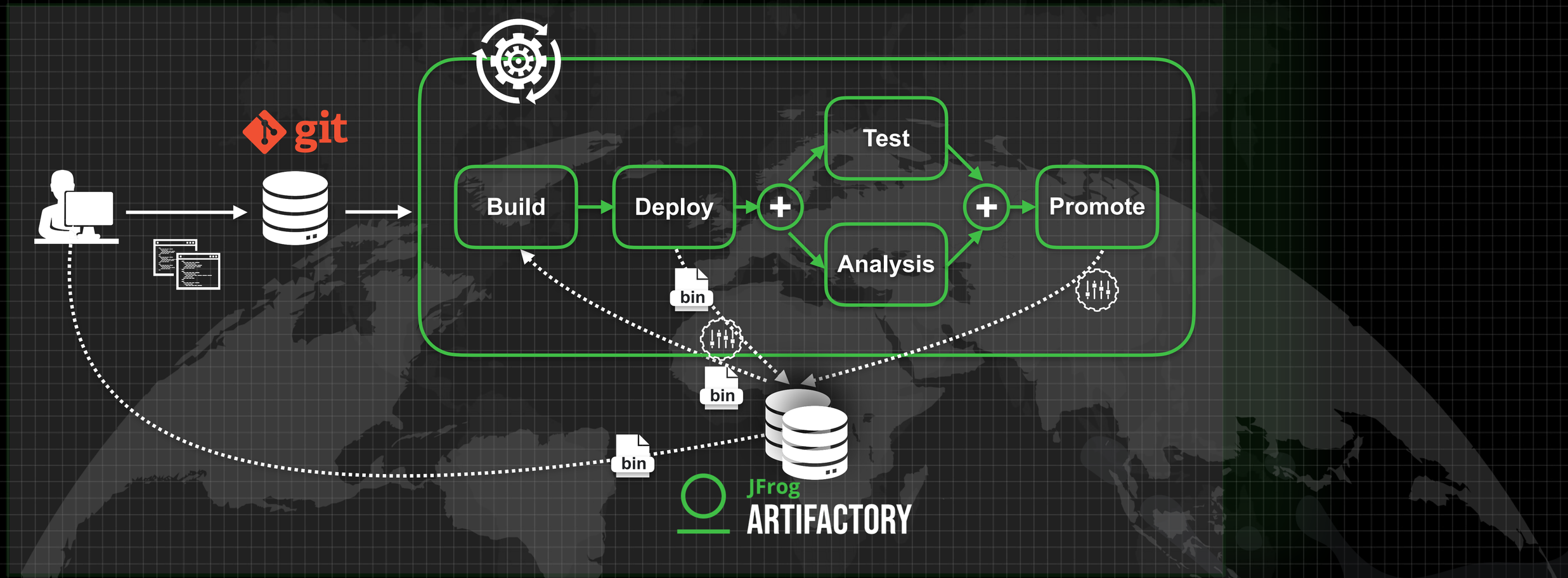
The Liquid Software Company

Single Development Team, single location



JFrog
The Liquid Software Company

Single Development Team, single location



JFrog
The Liquid Software Company

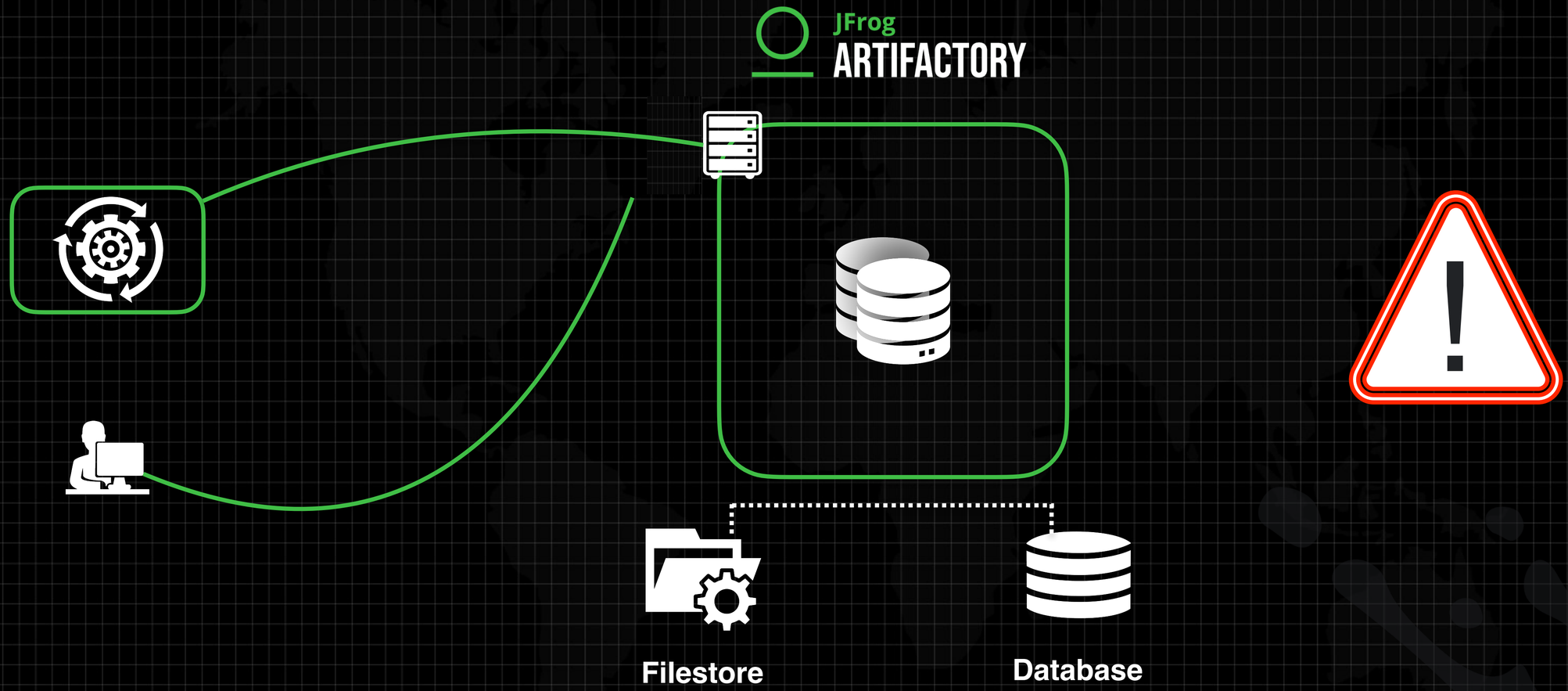
Key features

- Checksum based storage
- Integrates with 30+ package managers
- Full metadata for all supported package formats
- REST API, CLI, AQL, User Plugins
- Built in integrations with automation tools for CI/CD
- Local / Remote / Virtual repositories
- Projects

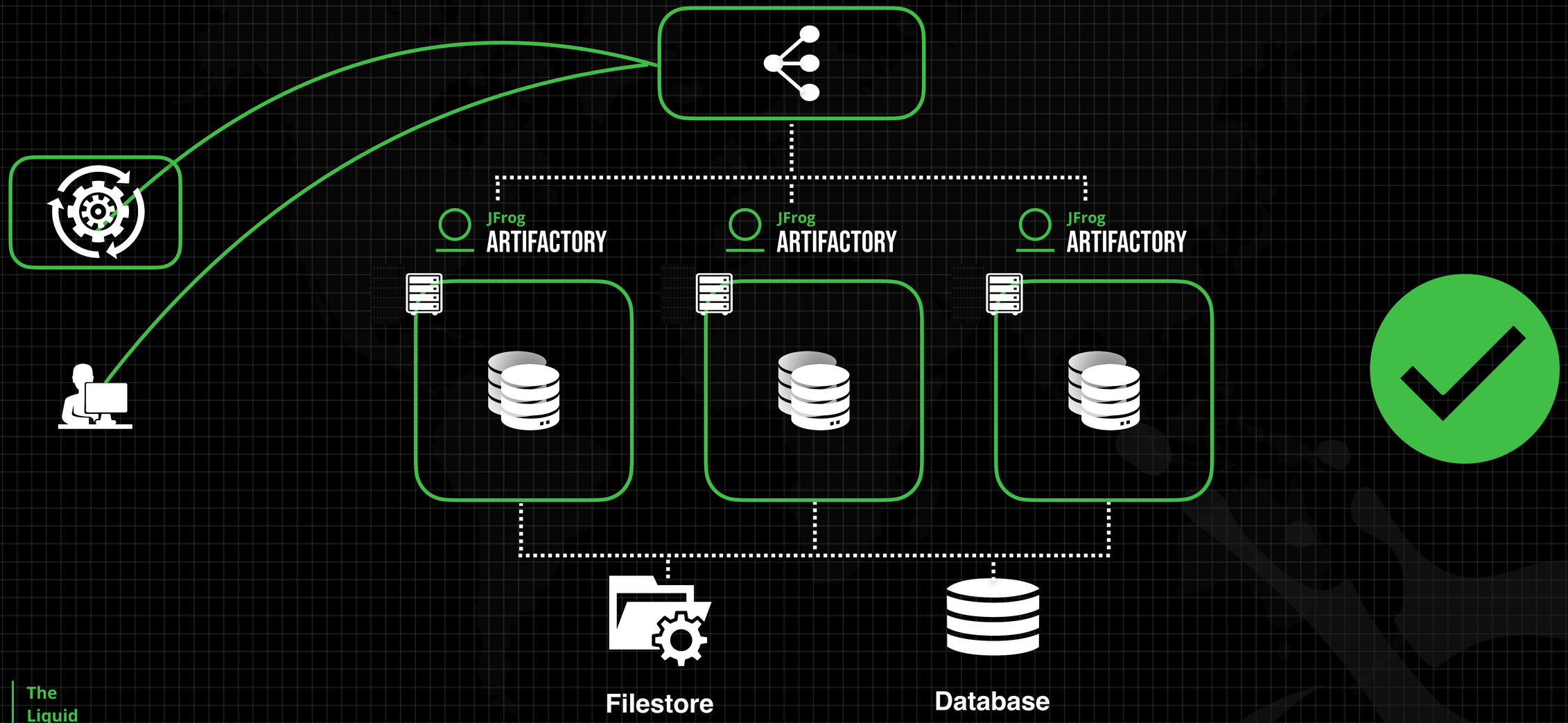
Build Info

The Liquid Software Company

Binary management as critical service



Binary management as critical service



The Liquid Software Company

Key features

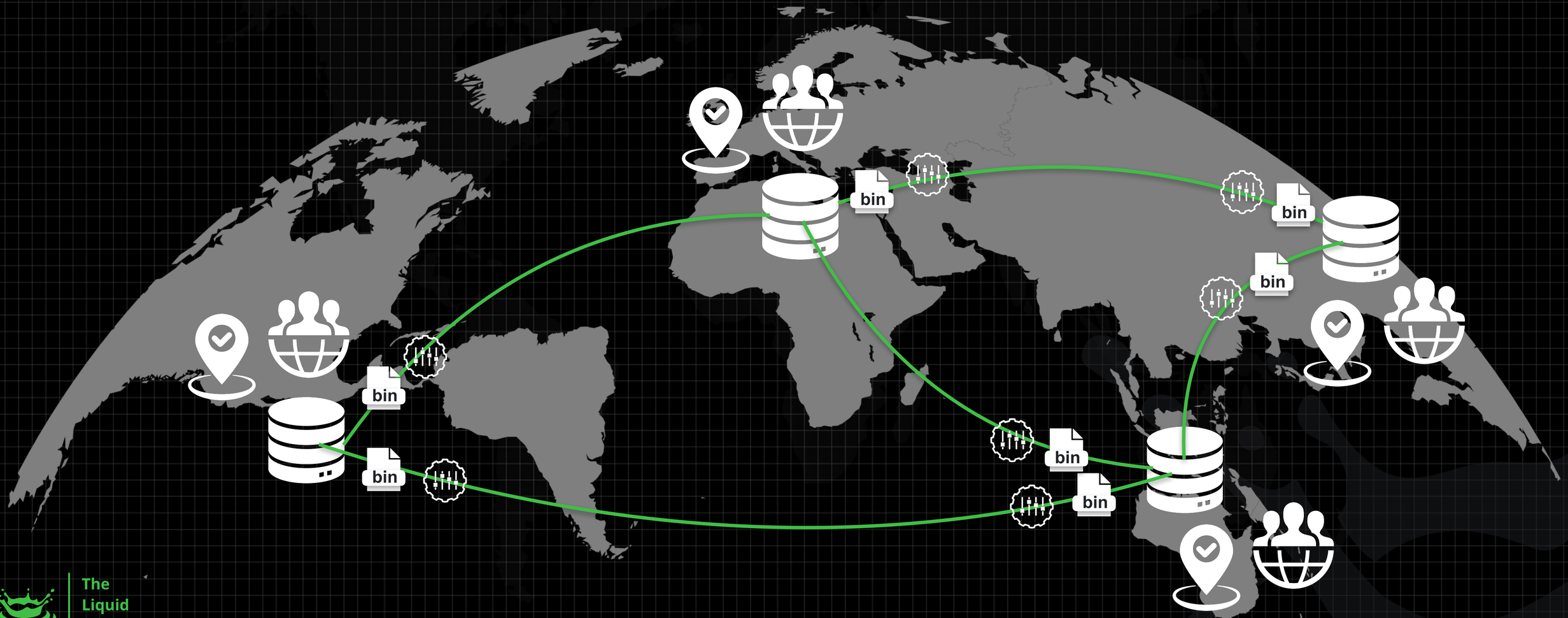
- Zero Downtime Upgrades| Resiliency | Performance
- Read and Write caches
- Filestore sharding
- Cloud storage support

Advanced

Many Development Teams, spread across the globe

The Liquid Software Company

Many Development Teams, spread across the globe



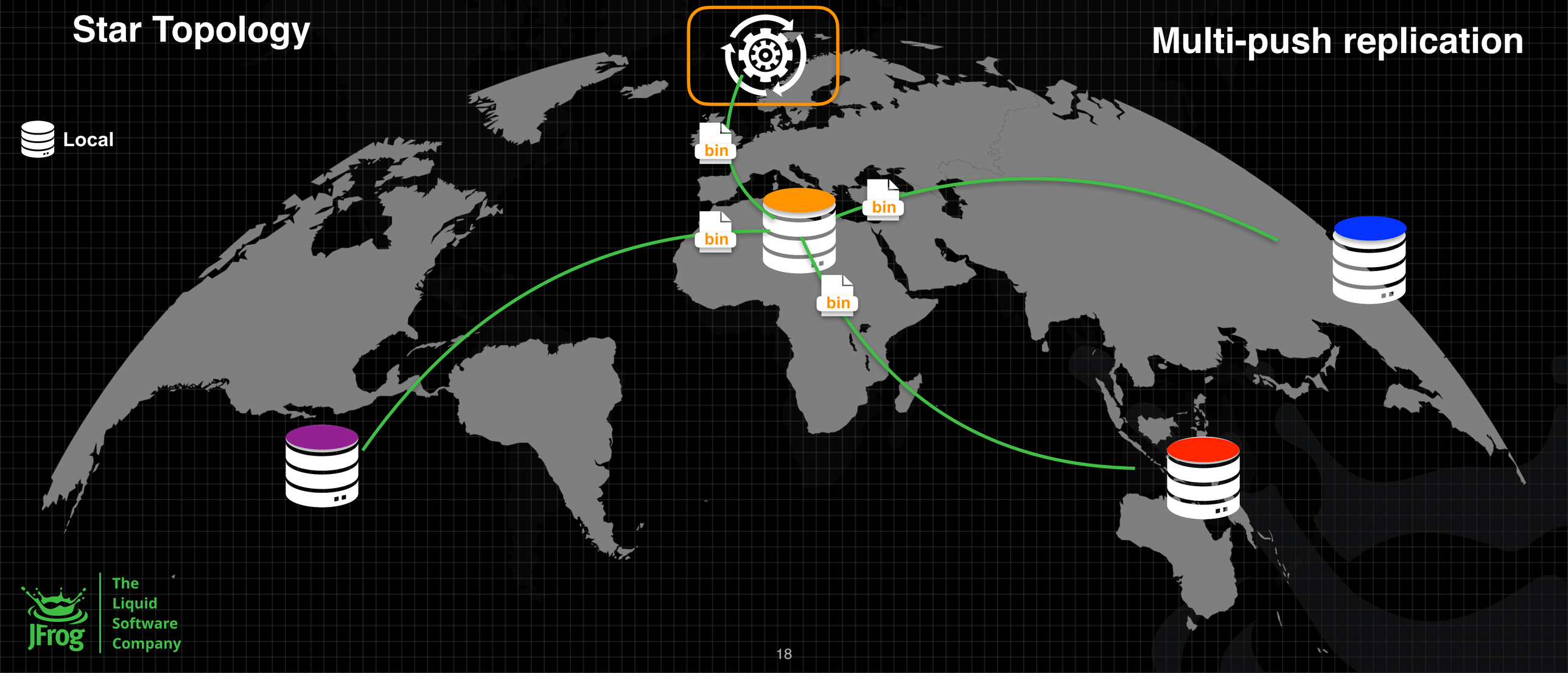
JFrog
The Liquid Software Company

Many Development Teams, spread across the globe

One central CI / CD Server

Star Topology

Multi-push replication



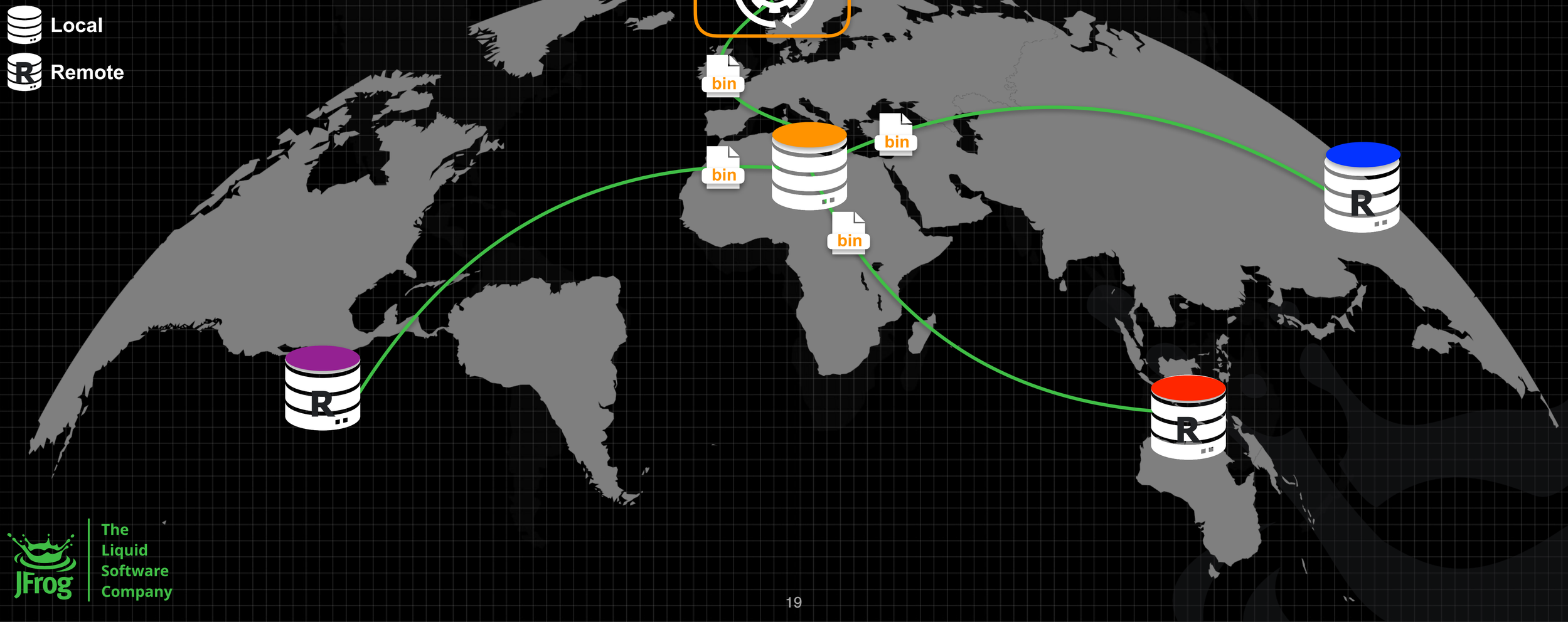
The Liquid Software Company

Many Development Teams, spread across the globe

One central CI / CD Server

Star Topology

Pull replication



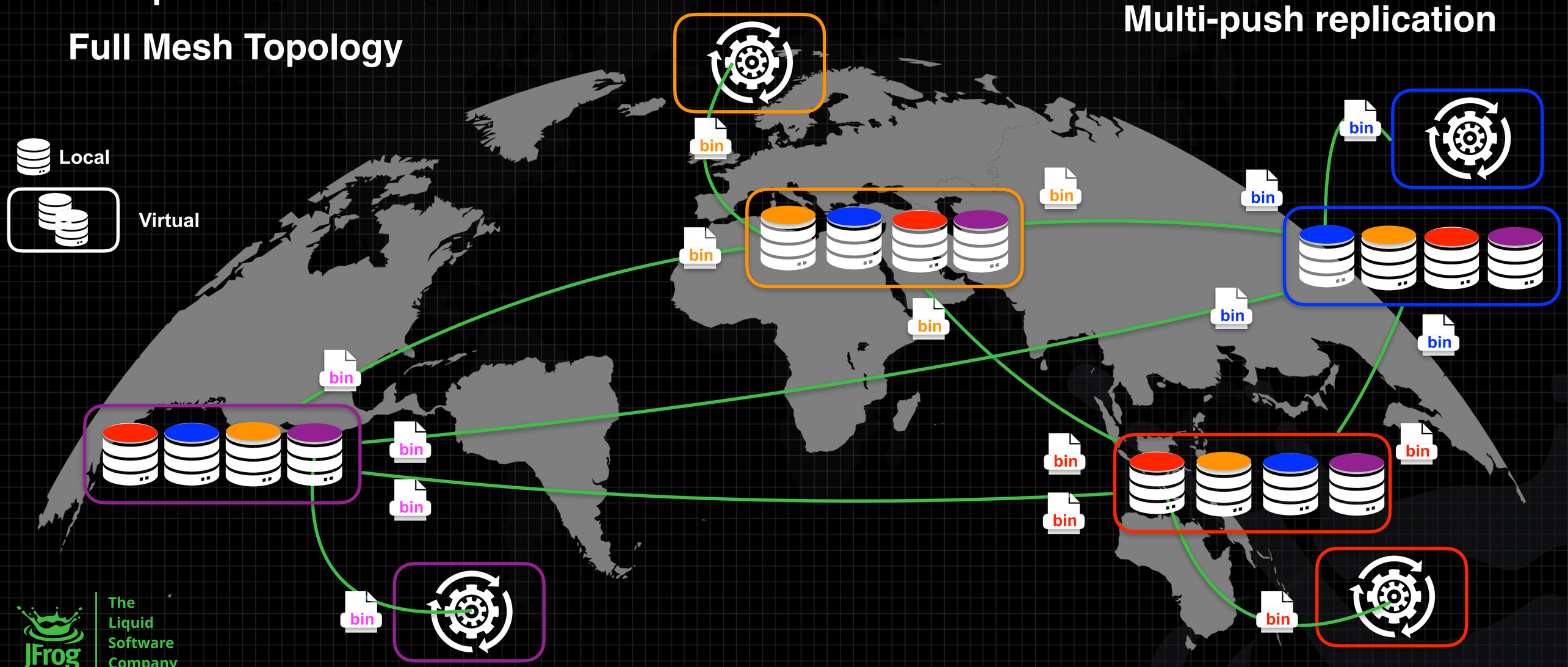
The Liquid Software Company

Many Development Teams, spread across the globe

Multiple CI servers

Full Mesh Topology

Multi-push replication



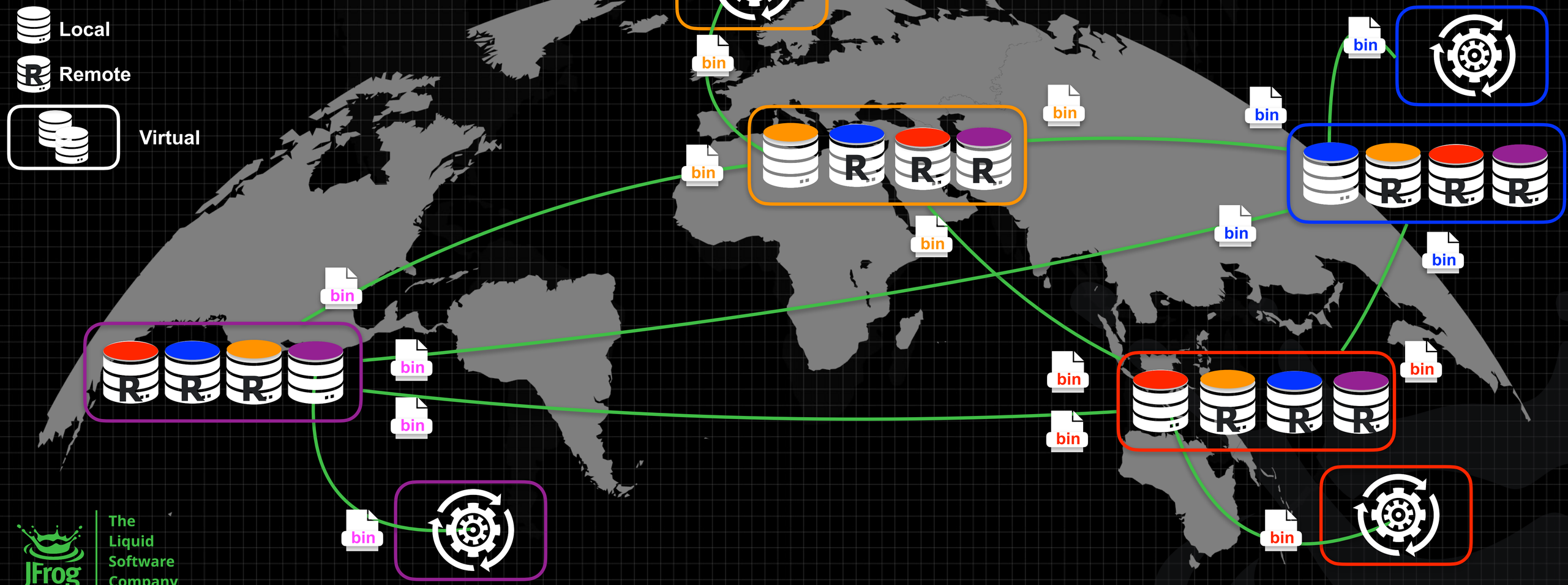
The Liquid Software Company

Many Development Teams, spread across the globe

Multiple CI servers

Full Mesh Topology

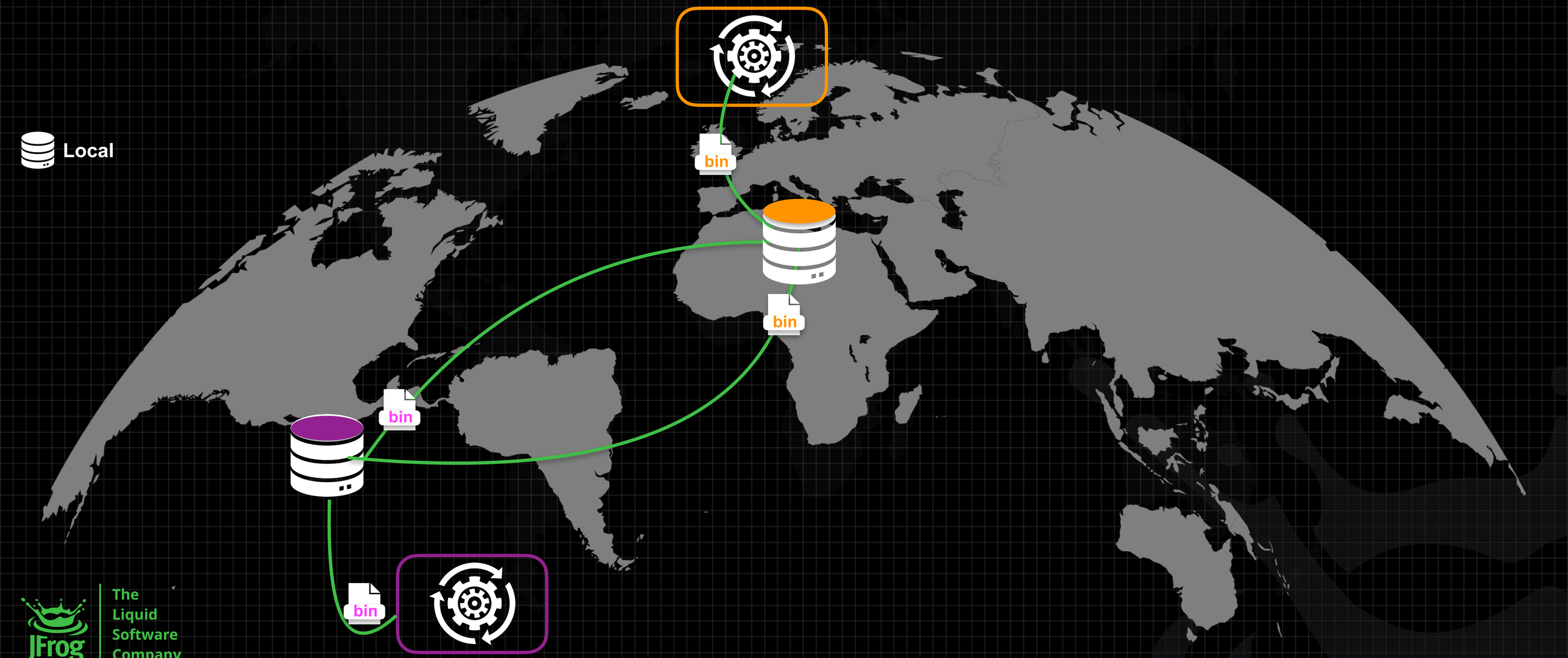
Pull replication



The Liquid Software Company

Many Development Teams, spread across the globe

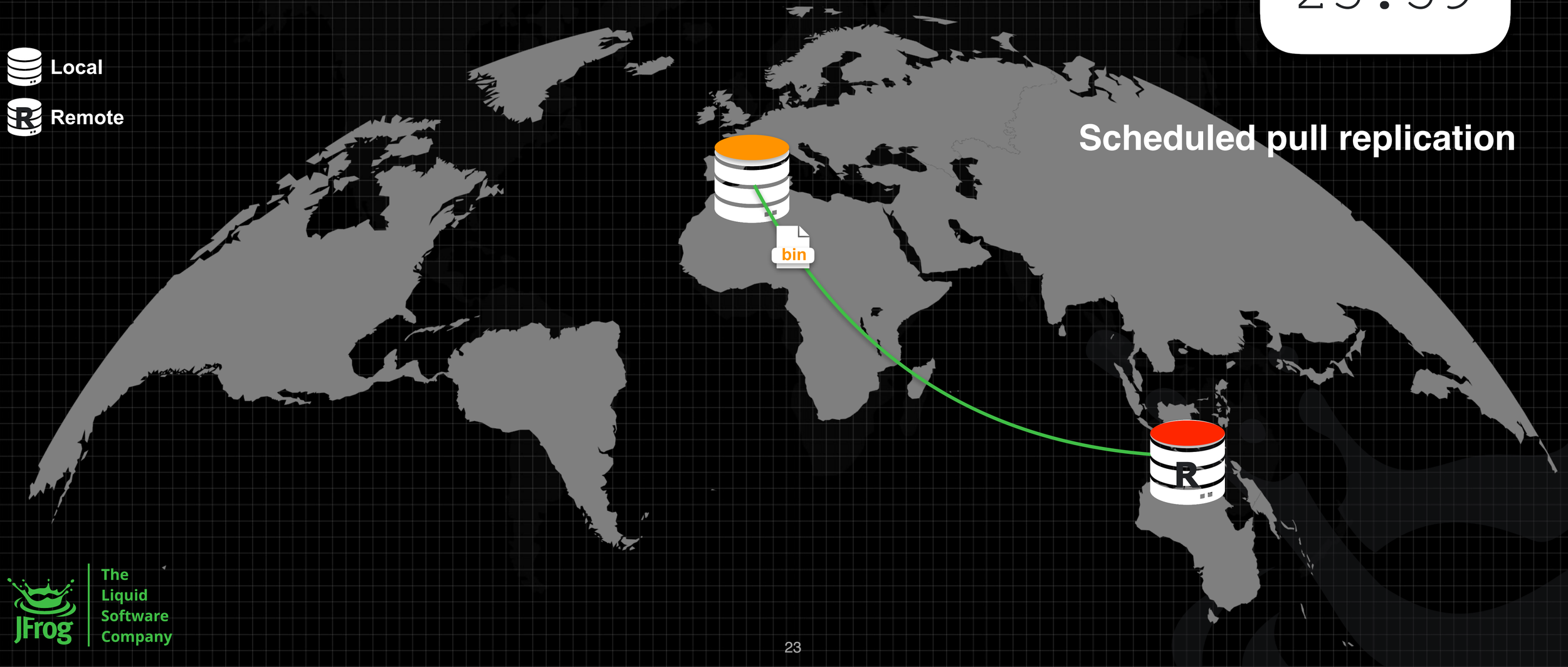
Federated repositories



The Liquid Software Company

Many Development Teams, spread across the globe

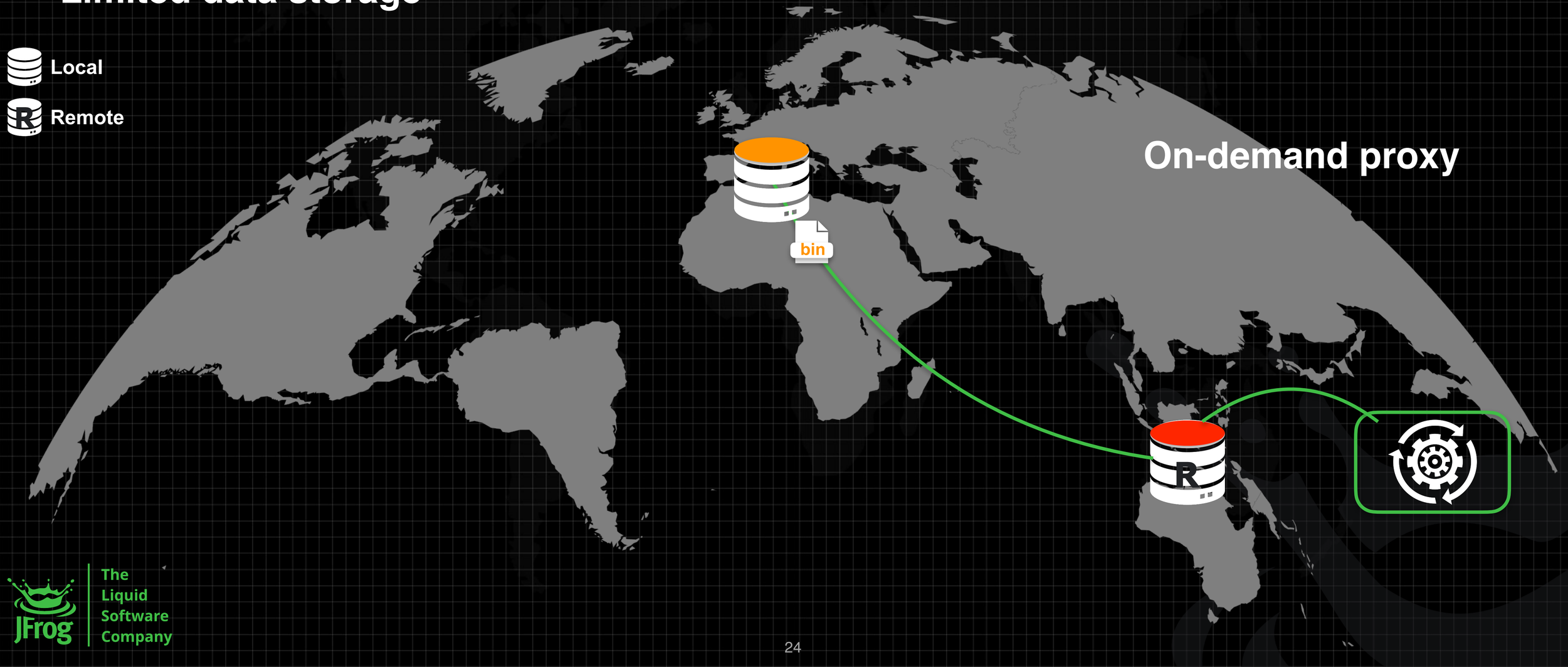
Limited bandwidth



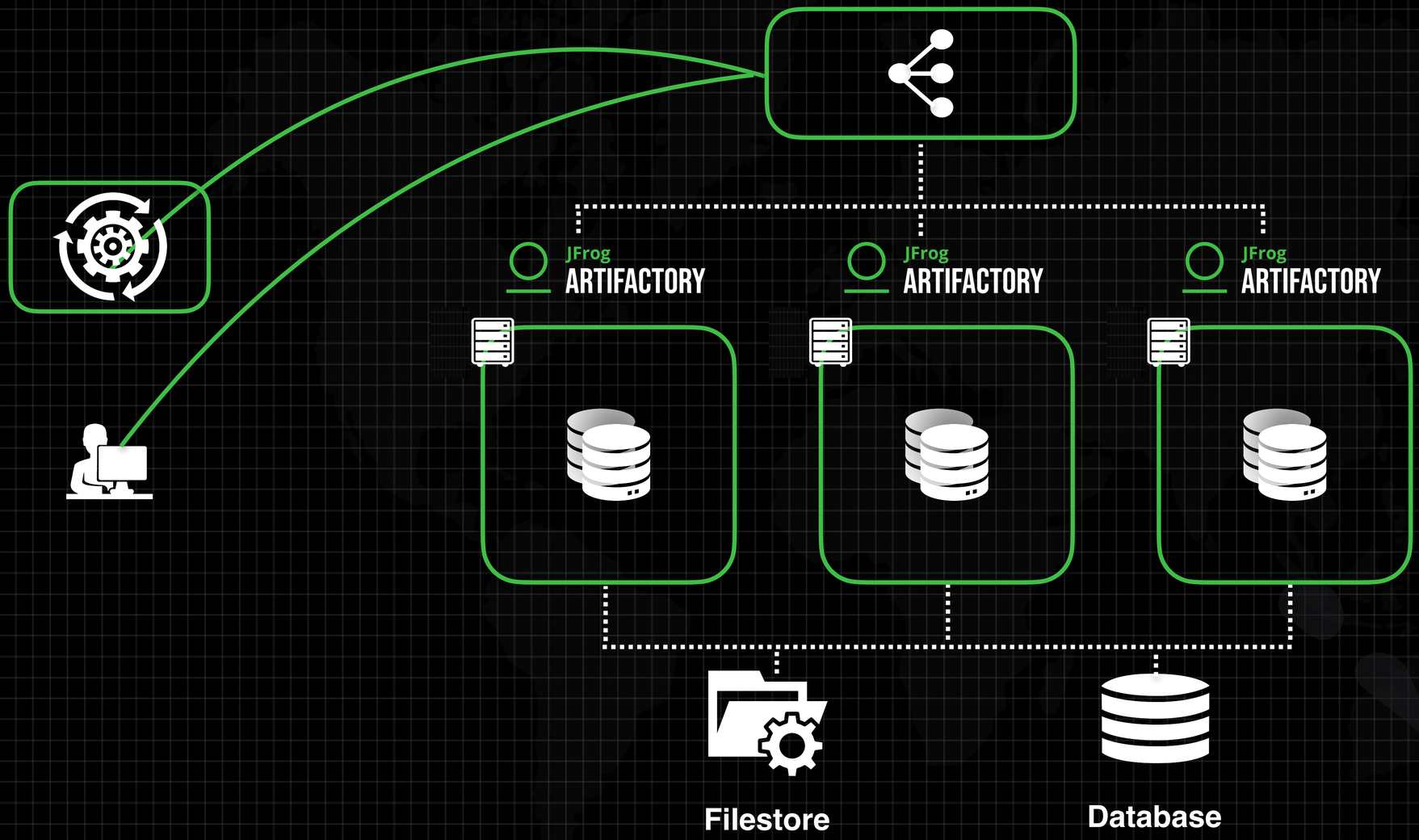
The Liquid Software Company

Many Development Teams, spread across the globe

Limited data transfer
Limited data storage



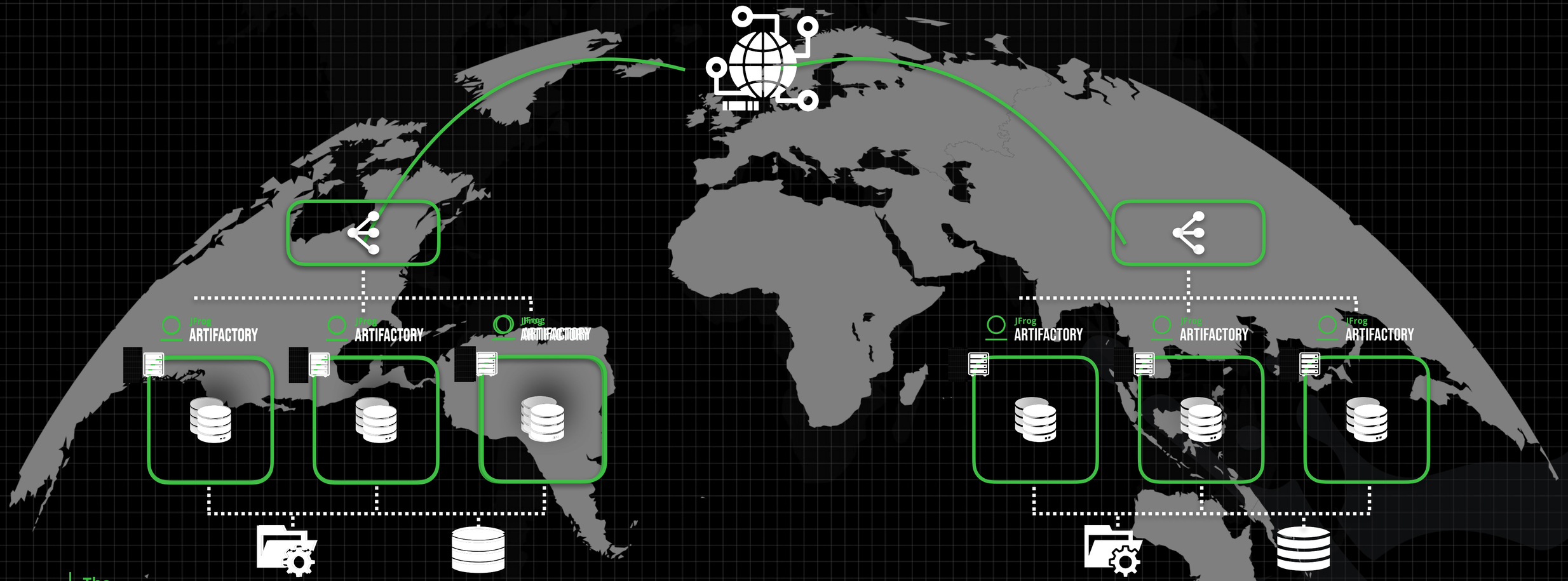
The Liquid Software Company



The Liquid Software Company

Many Development Teams, spread across the globe

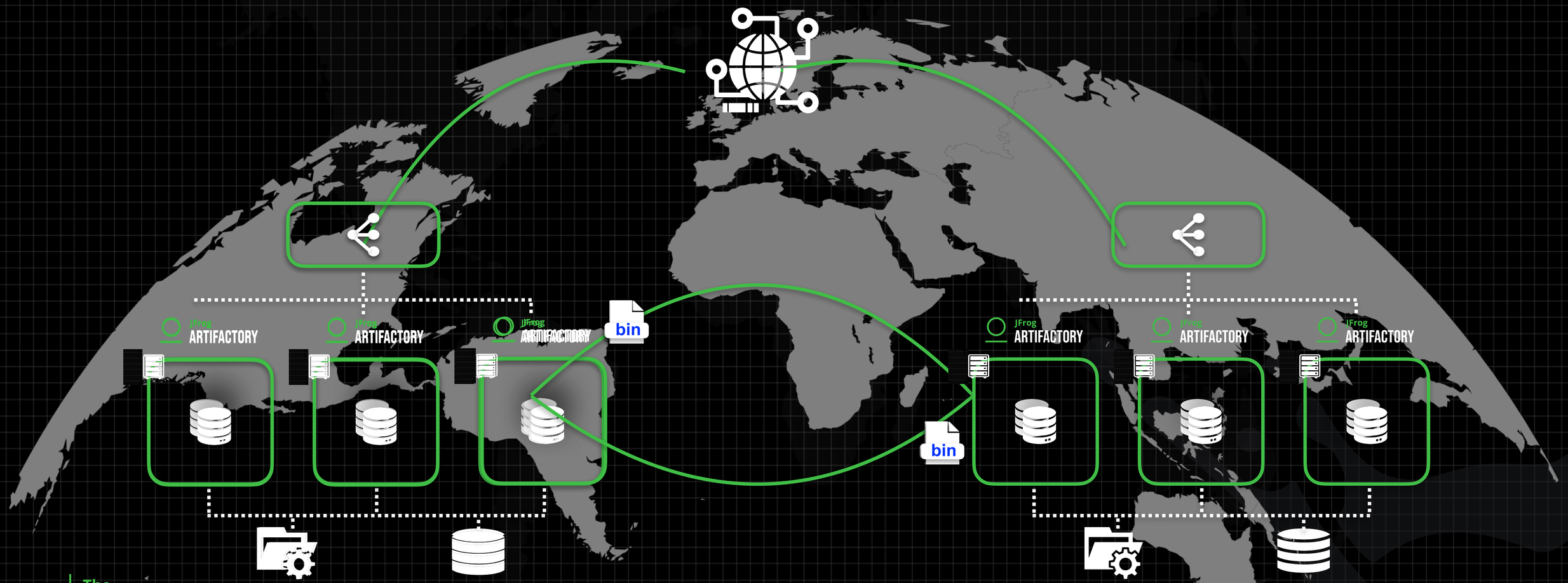
Geo DNS Architecture



The Liquid Software Company

Many Development Teams, spread across the globe

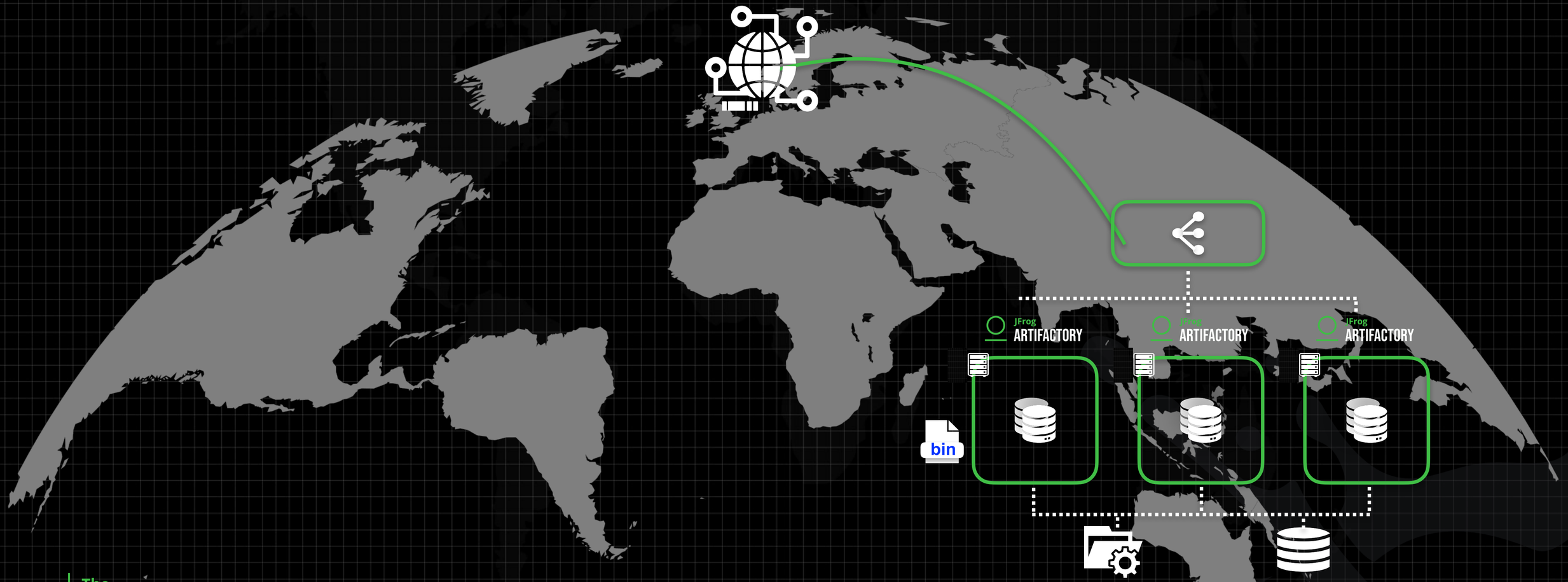
Geo DNS Architecture



The Liquid Software Company

Many Development Teams, spread across the globe

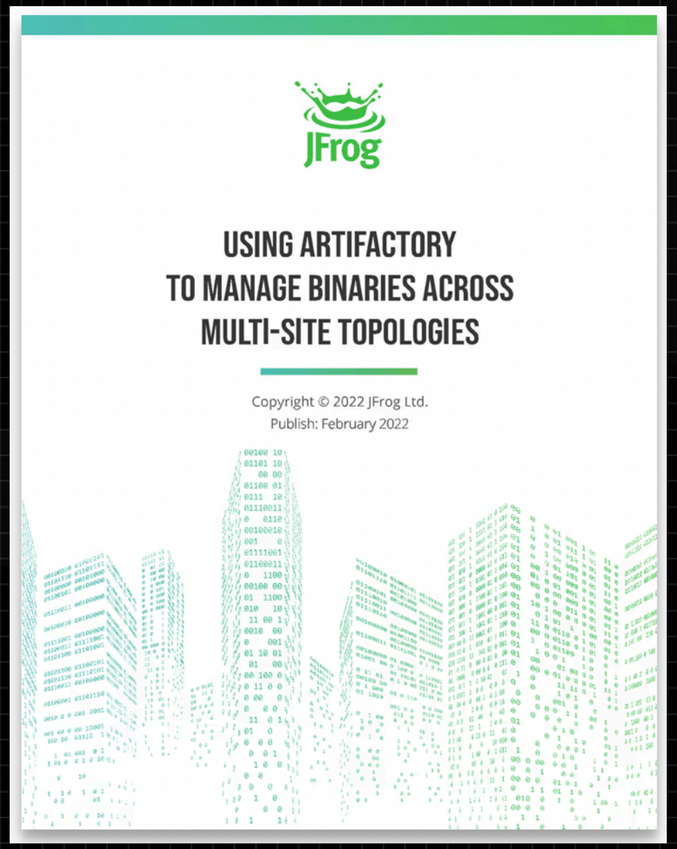
Geo DNS Architecture



The Liquid Software Company

Useful links

https://jfrog.com/whitepaper/replication-using-artifactory-to-manage-binaries-across-multi-site-topologies/



Securing your binary supply chain with Xray

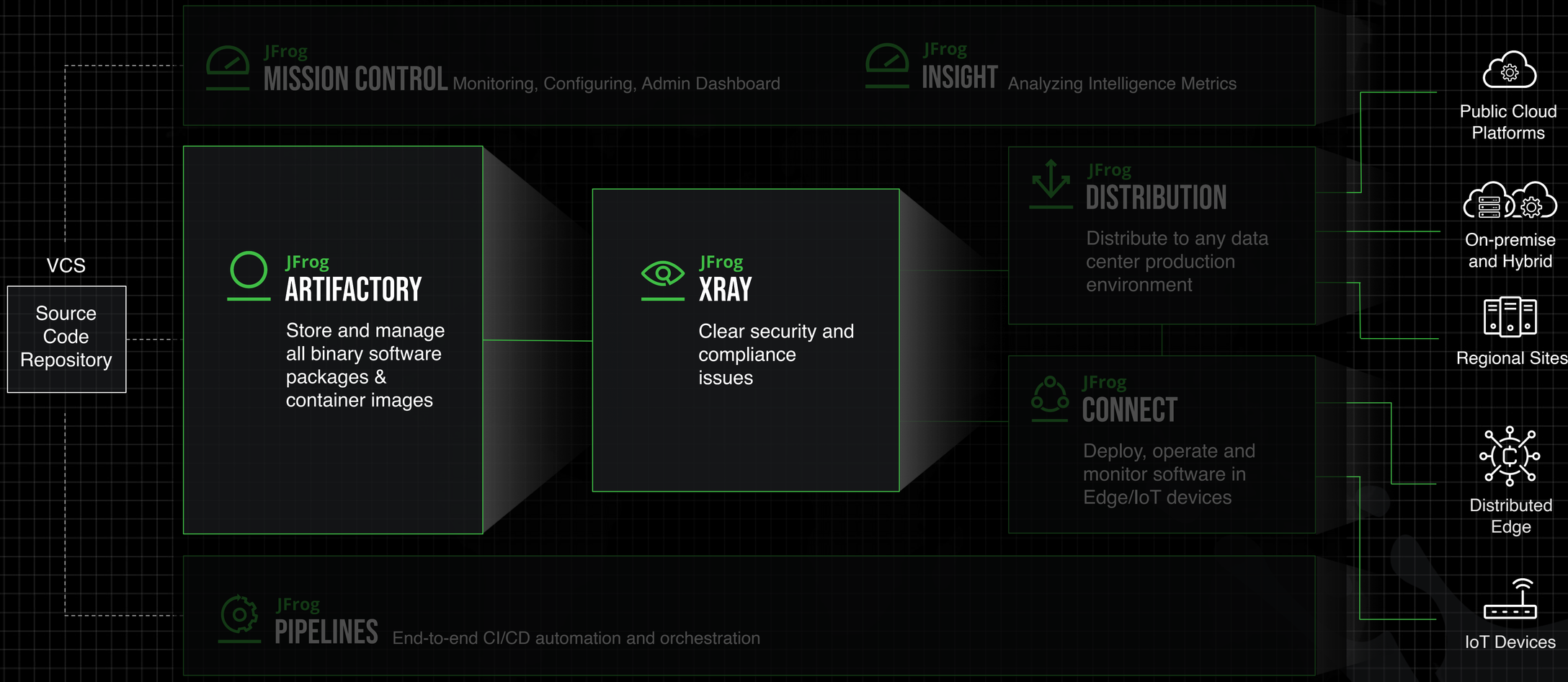
The
Liquid
Software
Company

Introduction Xray

Overview of the JFrog Platform

The Liquid Software Company

Overview of the JFrog Platform



BUILD & TEST | RELEASE | DEPLOY

The Liquid Software Company

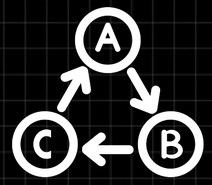
Source: Anchore report

What is the need

> In an average application, **85 -90%** of the codebase is open source

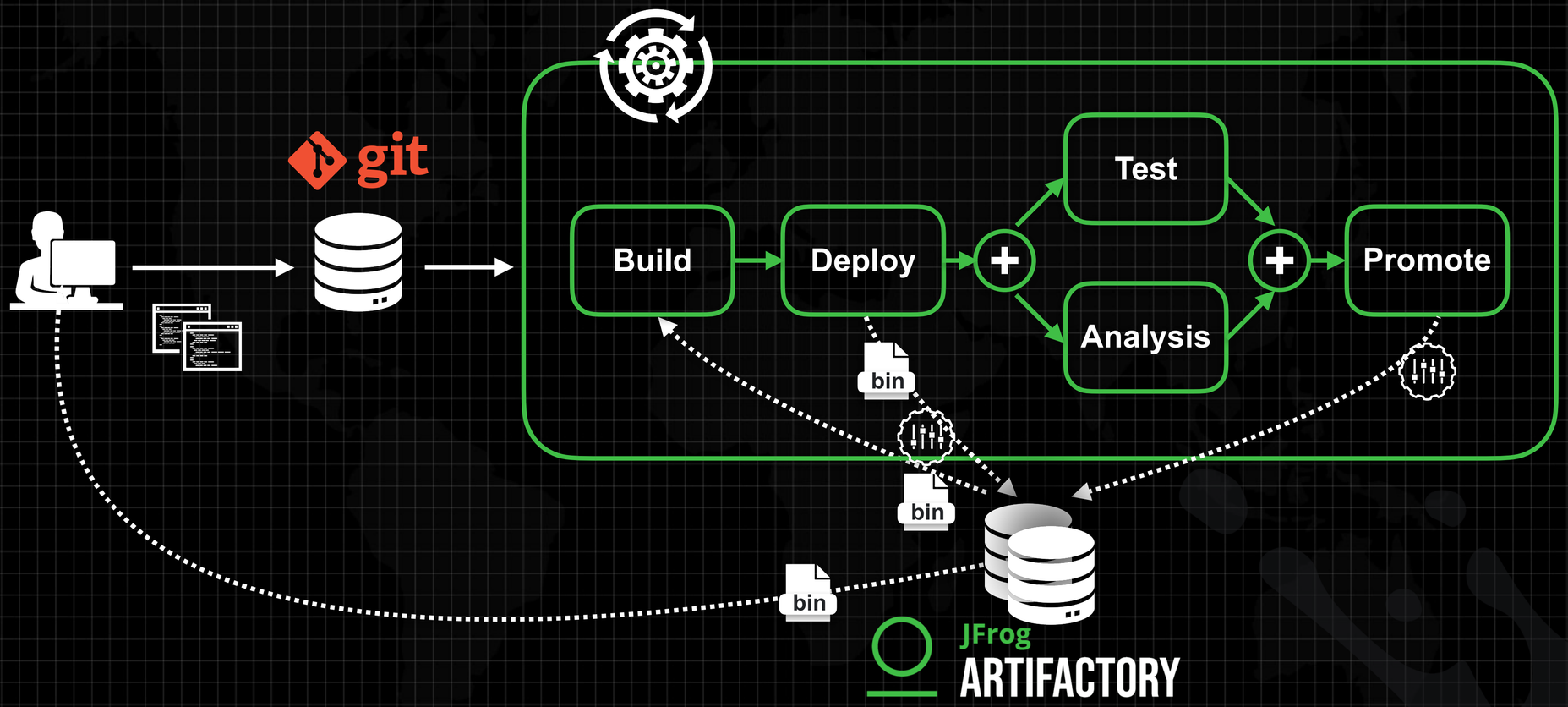
> **49%** of codebases analysed had at least one component with a high-risk vulnerability

> **90%** of applications used at least one open source component that was out-of-date by four or more years, or was abandoned



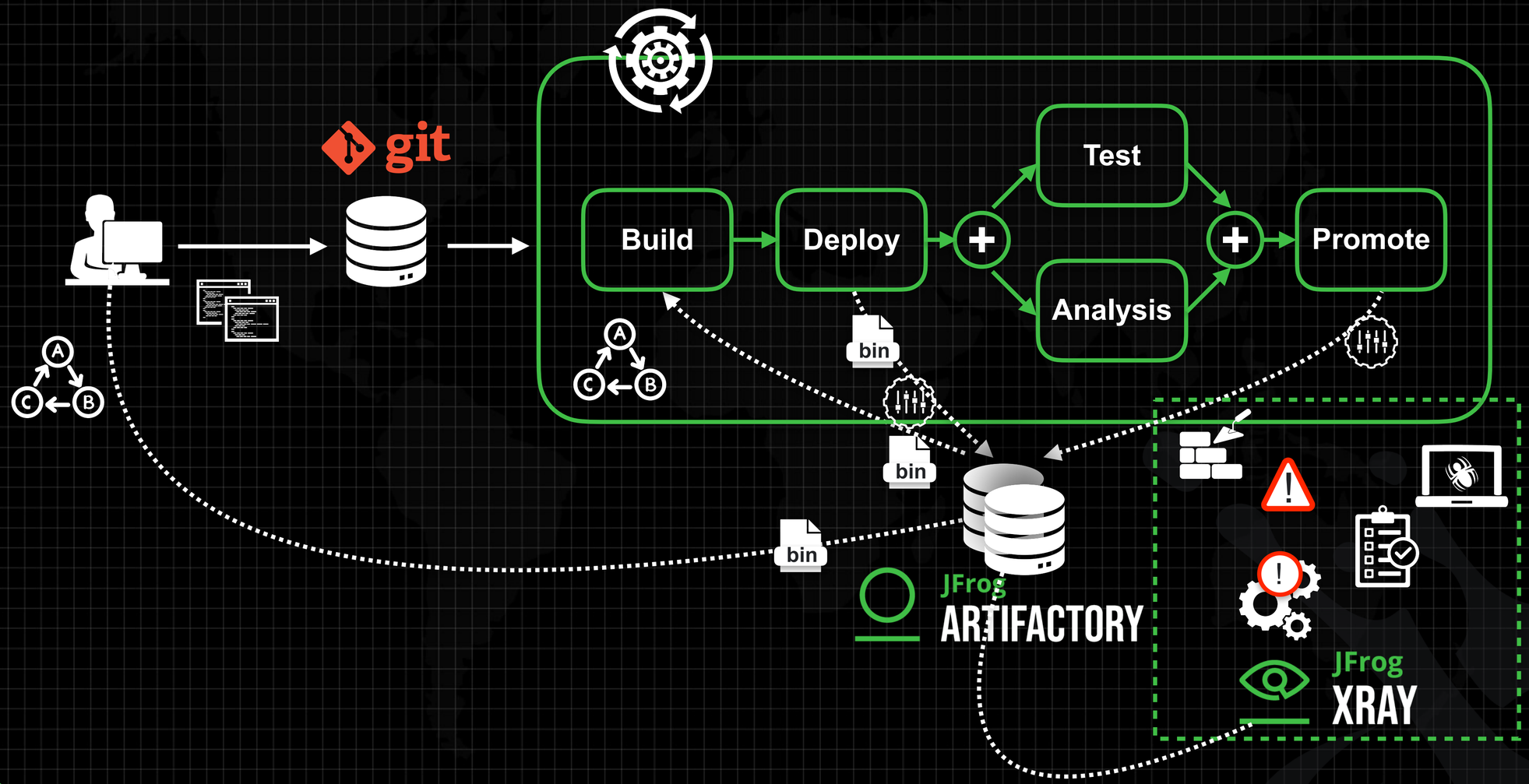
JFrog The Liquid Software Company

What is the need



The Liquid Software Company

What is the need



The Liquid Software Company

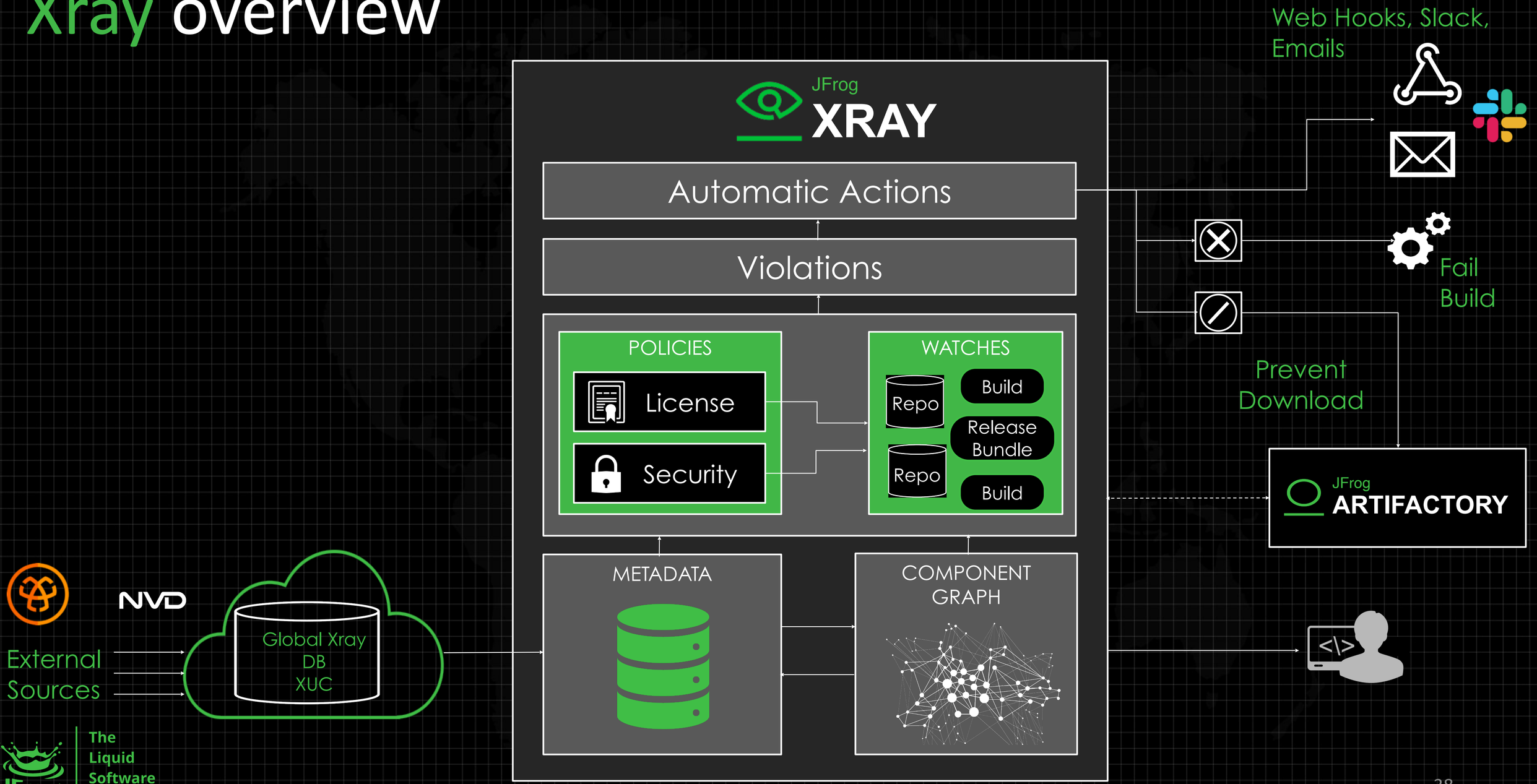
Top Notch Security Research At Your Fingertips

- Certified CNA
- In-Depth Research
- Discover and disclose new OSS vulnerabilities
- Analyze novel attack methods
- Help the community and customers with OSS Tools promptly

https://research.jfrog.com/

The Liquid Software Company

Xray overview

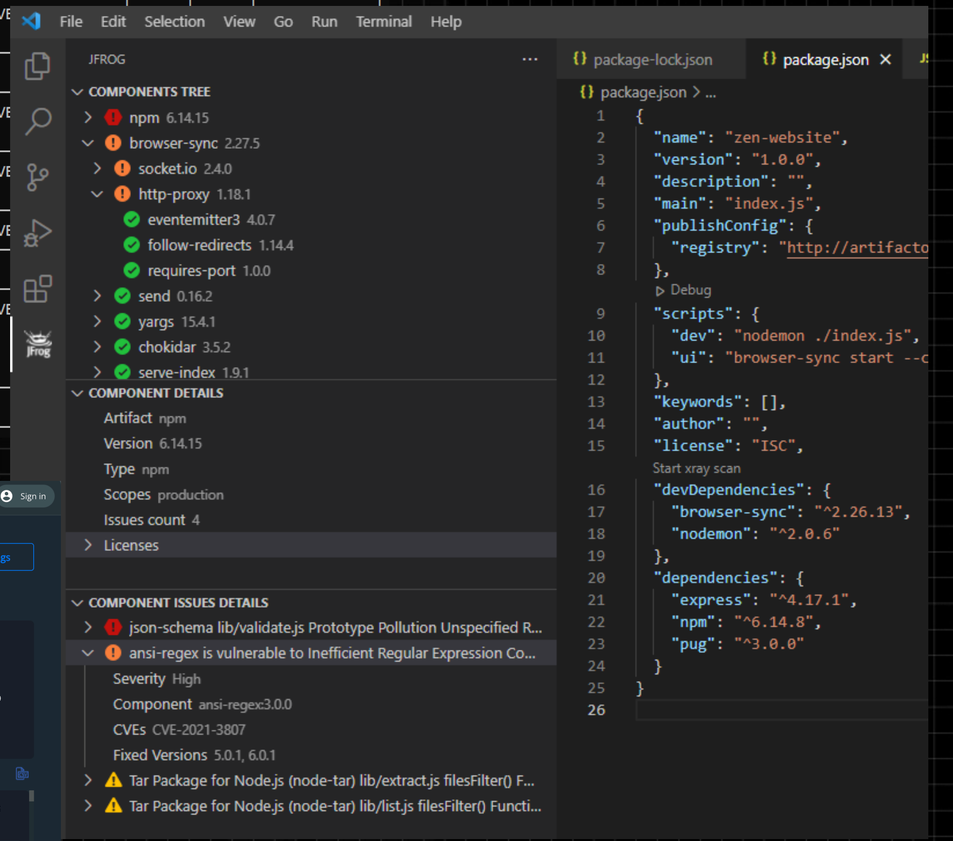


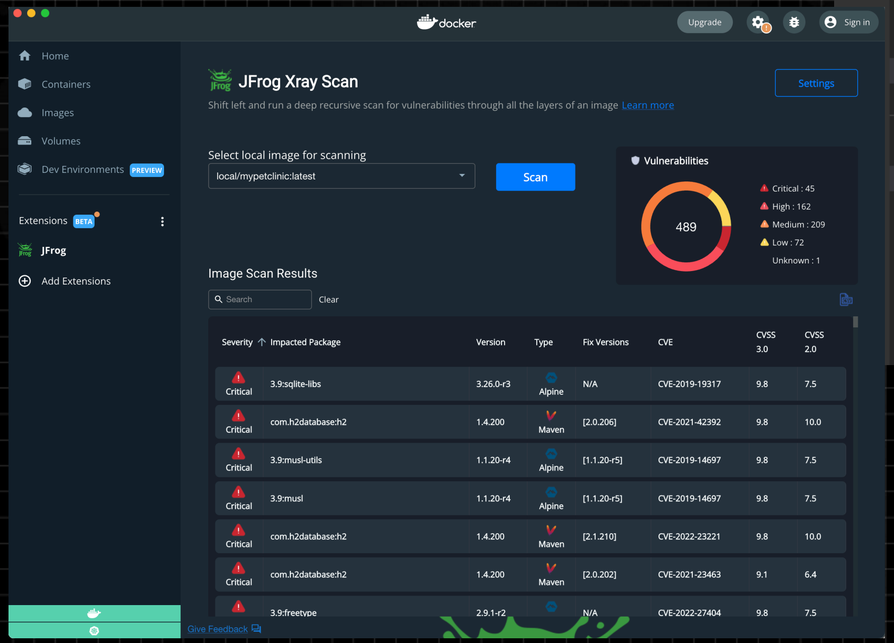
The Liquid Software Company

JFrog Xray | Shift left to empower developers

- IntelliJ Idea
- VSCode
- Eclipse
- Visual Studio
- JFrog CLI
- Docker Desktop

SEVERITY	IMPACTED PACKAGE	IMPACTED PACKAGE VERSION	TYPE	FIXED VERSIONS	COMPONENT	COMPONENT VERSION	CVE	CVSS V2	CVSS V3	ISSUE ID
Critical	json-schema	0.2.3	npm	[0.4.0]	npm	6.14.15	CVE			
High	http-proxy	1.18.1	npm	(,0.0.0)	browser-sync	2.27.5				
High	ansi-regex	3.0.0	npm	[5.0.1] [6.0.1]	npm	6.14.15	CVE			
High	ansi-regex	4.1.0	npm	[5.0.1] [6.0.1]	npm	6.14.15	CVE			
High	engine.io	3.5.0	npm	[4.0.0]	browser-sync	2.27.5	CVE			
Medium	tar	4.4.19	npm	[6.1.4]	npm	6.14.15				
Medium	debug	4.1.1	npm	[4.3.1] [3.2.7] [3.1.0] [2.6.9]	browser-sync	2.27.5	CVE			
Medium	tar	4.4.19	npm	[6.1.4]	npm	6.14.15				

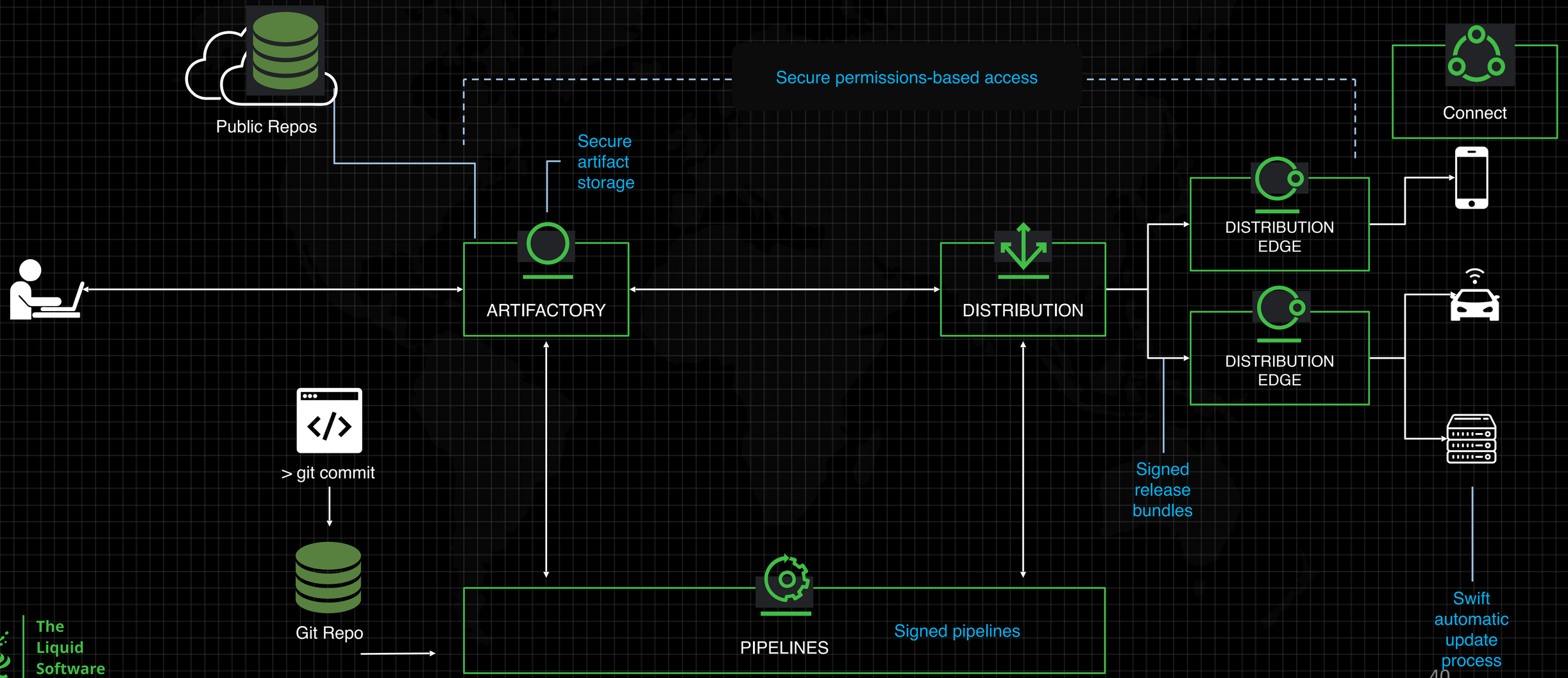




The Liquid Software Company

End-to-end security with the JFrog Platform

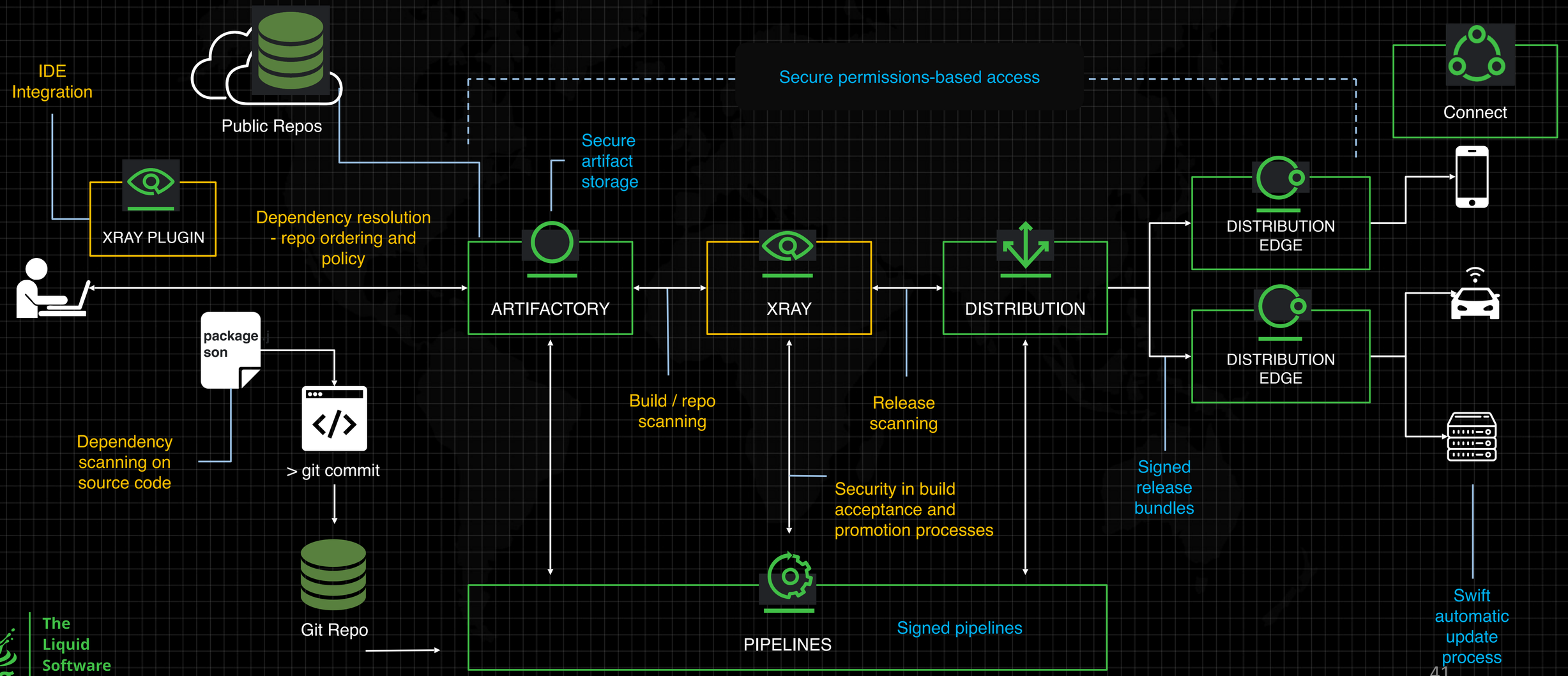
Continuously securing the software supply chain



The Liquid Software Company

End-to-end security with the JFrog Platform

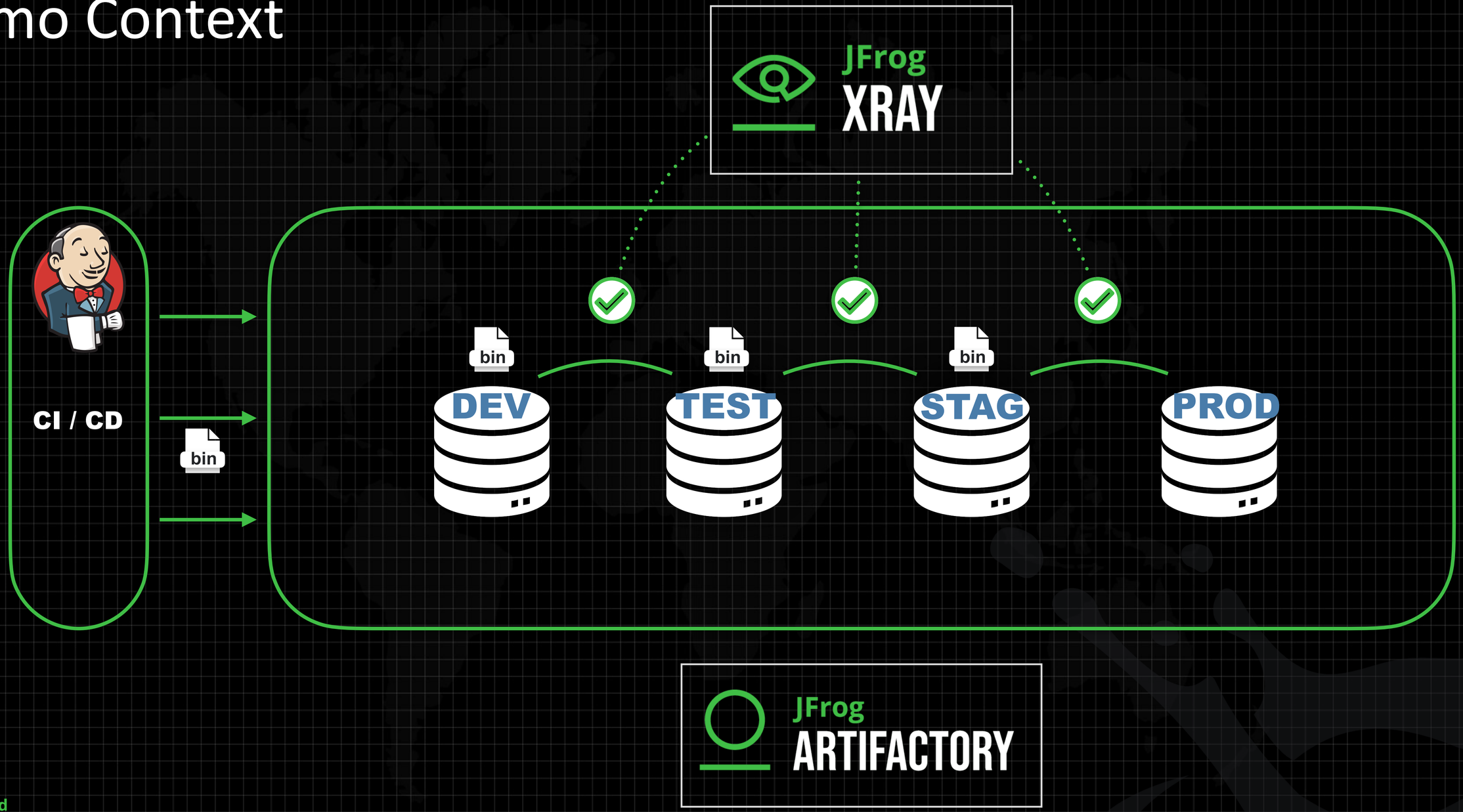
Continuously securing the software supply chain



The Liquid Software Company

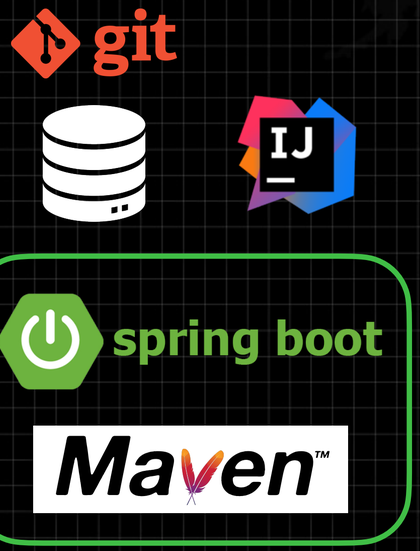
Demo Xray

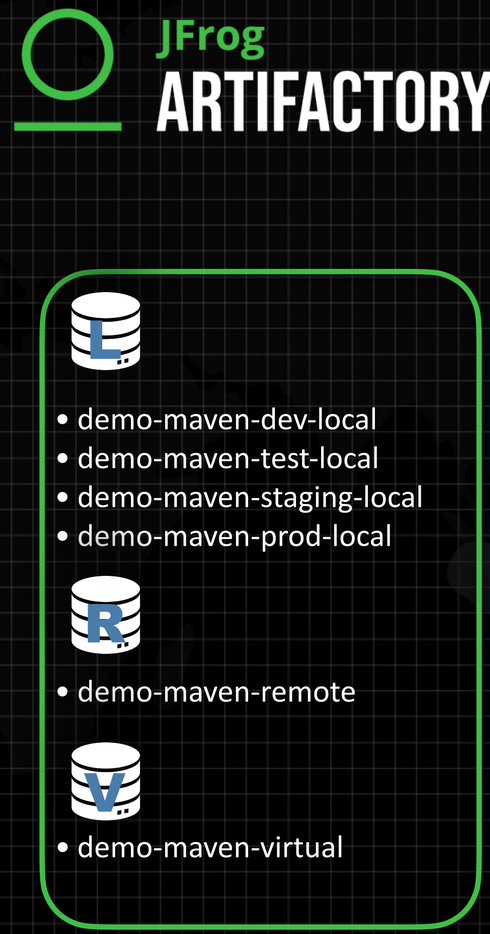
Demo Context



The Liquid Software Company

Demo Environment





JFrog XRAY

BuildWatch

GS_SPRING_BOOT_main_mvn

RepoWatch

demo-maven-prod-local

BuildPolicy

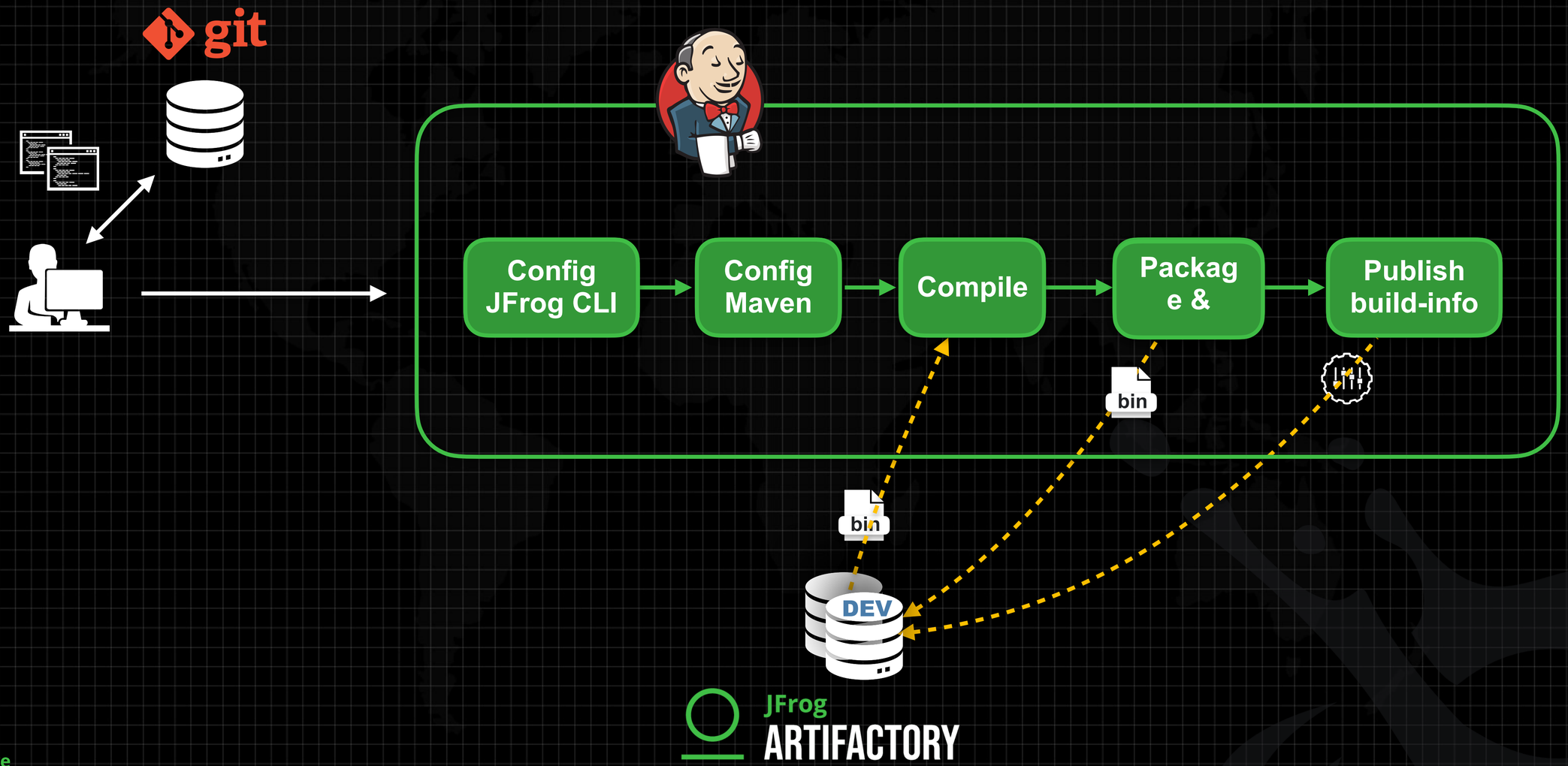
Critical 9<= CVSS <= 10
Generate violation
Fail Build
High 7 <= CVSS < 9
Generate violation

RepoPolicy

Critical 9 <= CVSS < 10
Block download

The Liquid Software Company

Development Pipeline



The Liquid Software Company

Test Promotion Pipeline

BuildWatch

GS_SPRING_BOOT_main_mvn

BuildPolicy

Critical 9<= CVSS <= 10
Generate violation
Fail Build
High 7 <= CVSS < 9
Generate violation

—fail=false

Approve?

Config JFrog CLI → Scan build → Approve / Discard → Promote build to Test

JFrog XRAY

JFrog ARTIFACTORY

The Liquid Software Company

Staging Promotion Pipeline (I)

BuildWatch

GS_SPRING_BOOT_main_mvn

BuildPolicy

Critical 9<= CVSS <= 10
Generate violation
Fail Build
High 7 <= CVSS < 9
Generate violation

JFrog XRAY

JFrog ARTIFACTORY

The Liquid Software Company

Staging Promotion Pipeline (II)

Approve?

Config JFrog CLI → Scan build → Approve / Discard → Promote build to Staging

BuildWatch

GS_SPRING_BOOT_main_mvn

BuildPolicy

Critical 9<= CVSS <= 10
Generate violation
Fail Build
High 7 <= CVSS < 9
Generate violation

Ignored Violation

Critical

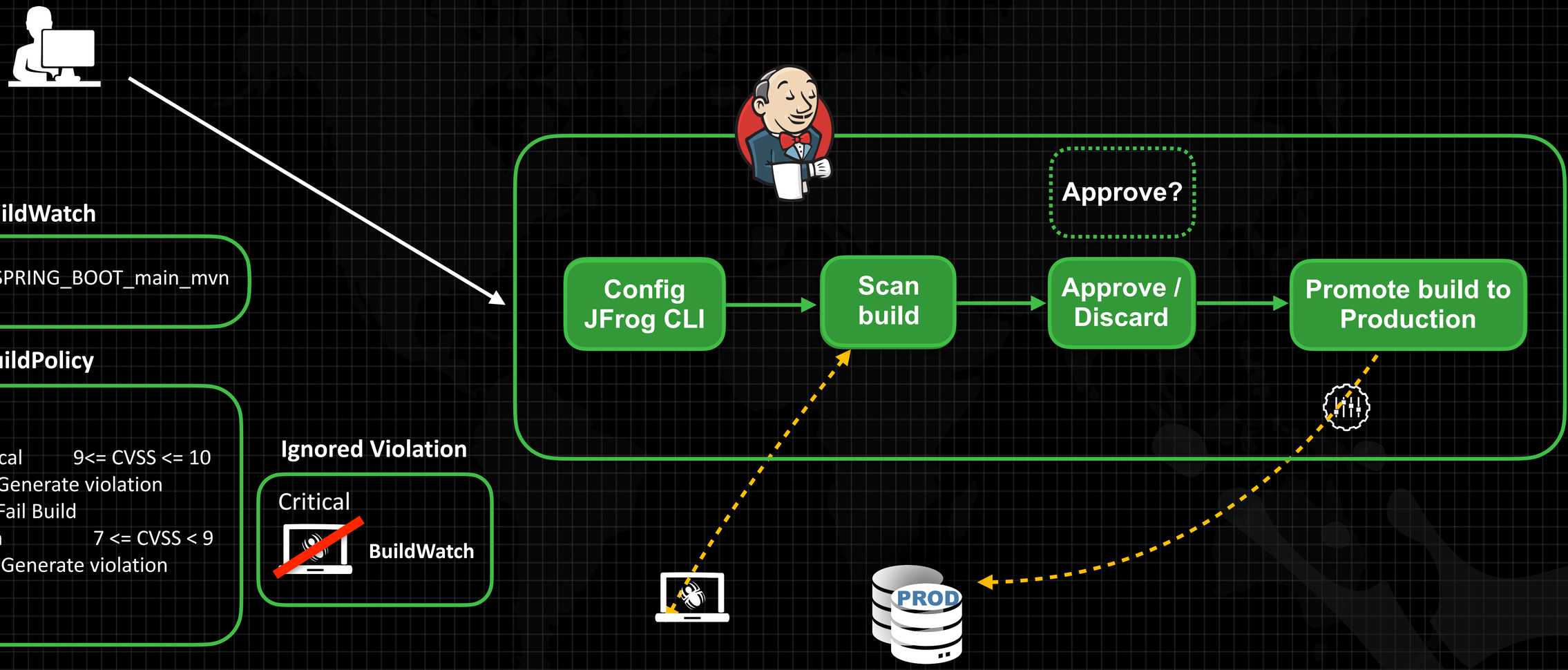
BuildWatch

JFrog XRAY

JFrog ARTIFACTORY

The Liquid Software Company

Production Promotion Pipeline



The Liquid Software Company

Deploy on Production Runtime Pipeline (I)

BuildWatch

GS_SPRING_BOOT_main_mvn

BuildPolicy

Critical 9<= CVSS <= 10
Generate violation
Fail Build
High 7 <= CVSS < 9
Generate violation

Ignored Violation

Critical
BuildWatch

Config JFrog CLI

Deploy on runtime

JFrog XRAY

JFrog ARTIFACTORY

RepoWatch

demo-maven-prod-local

RepoPolicy

Critical 9 <= CVSS < 10
Block download

The Liquid Software Company

Deploy on Production Runtime Pipeline (II)

BuildWatch

GS_SPRING_BOOT_main_mvn

BuildPolicy

Critical 9<= CVSS <= 10
Generate violation
Fail Build
High 7 <= CVSS < 9
Generate violation

Config JFrog CLI

Deploy on runtime

Ignored Violation

Critical
BuildWatch

Ignored Violation

Critical
RepoWatch

PROD

bin

JFrog XRAY

JFrog ARTIFACTORY

RepoWatch

demo-maven-prod-local

RepoPolicy

Critical 9 <= CVSS < 10
Block download

JFrog The Liquid Software Company

Shift Left

JFrog CLI

JFrog XRAY

Dependencies Scan **Supported: Npm | Maven | Gradle | Pip | Go**

```
[gs-spring-boot/complete] $ jf audit --mvn
```

On-demand Scan *(Stored under Xray / On-demand Scanning)*

```
[gs-spring-boot/complete] $ jf s target/*.jar --watches="BuildWatch"
```

Docker scan *(Existing image in local registry)*

```
$ jf docker scan [repo]/[image]:[tag]
```

BuildWatch

GS_SPRING_BOOT_main_mvn

RepoWatch

demo-maven-prod-local

BuildPolicy

Critical 9<= CVSS <= 10
Generate violation
Fail Build

High 7 <= CVSS < 9
Generate violation

RepoPolicy

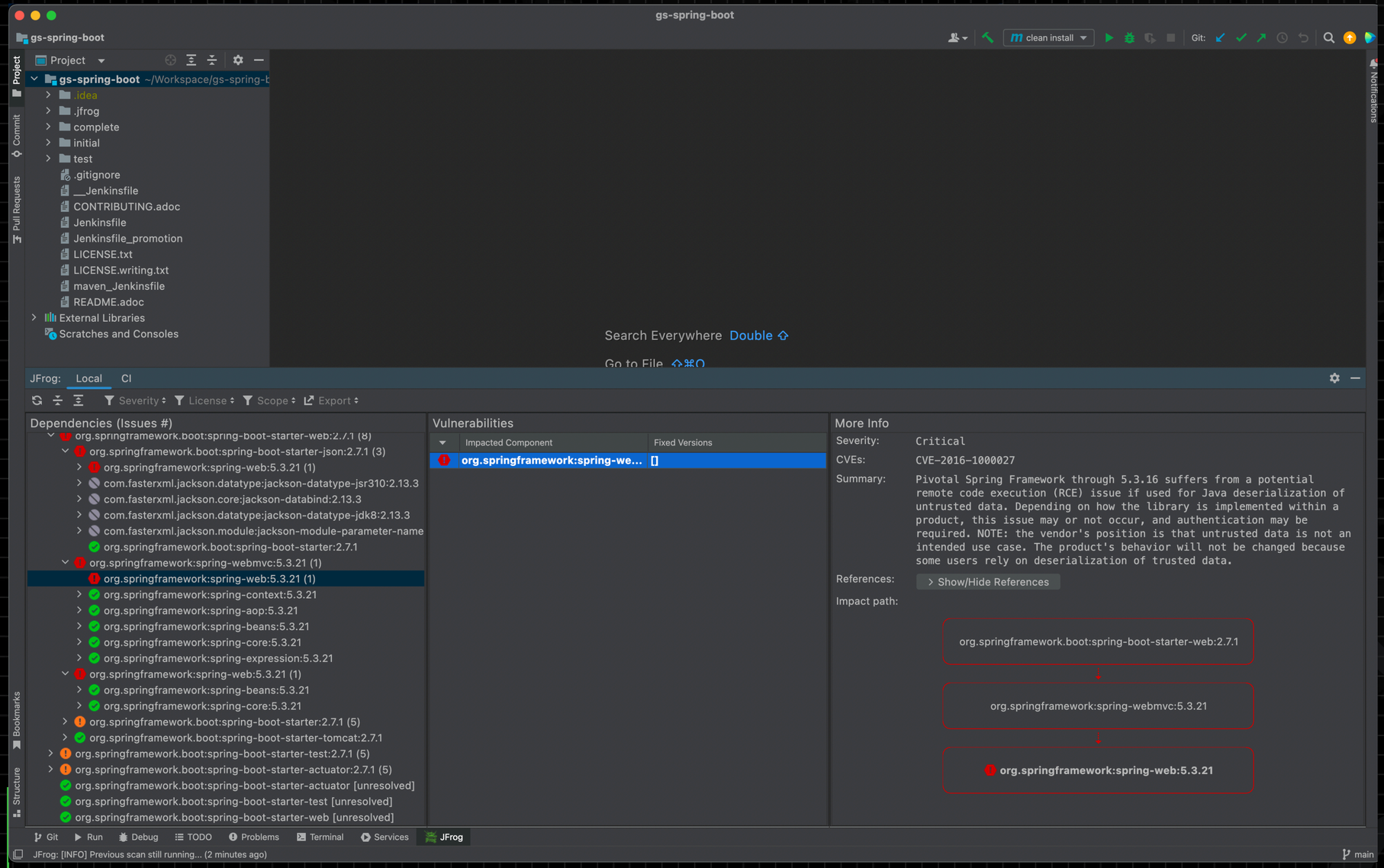
Critical 9 <= CVSS < 10
Block download

JFrog The Liquid Software Company

Shift Left (cont.)

IDE Plugin

JFrog XRAY



BuildWatch

GS_SPRING_BOOT_main_mvn

RepoWatch

demo-maven-prod-local

BuildPolicy

Critical 9<= CVSS <= 10
Generate violation
Fail Build

High 7 <= CVSS < 9
Generate violation

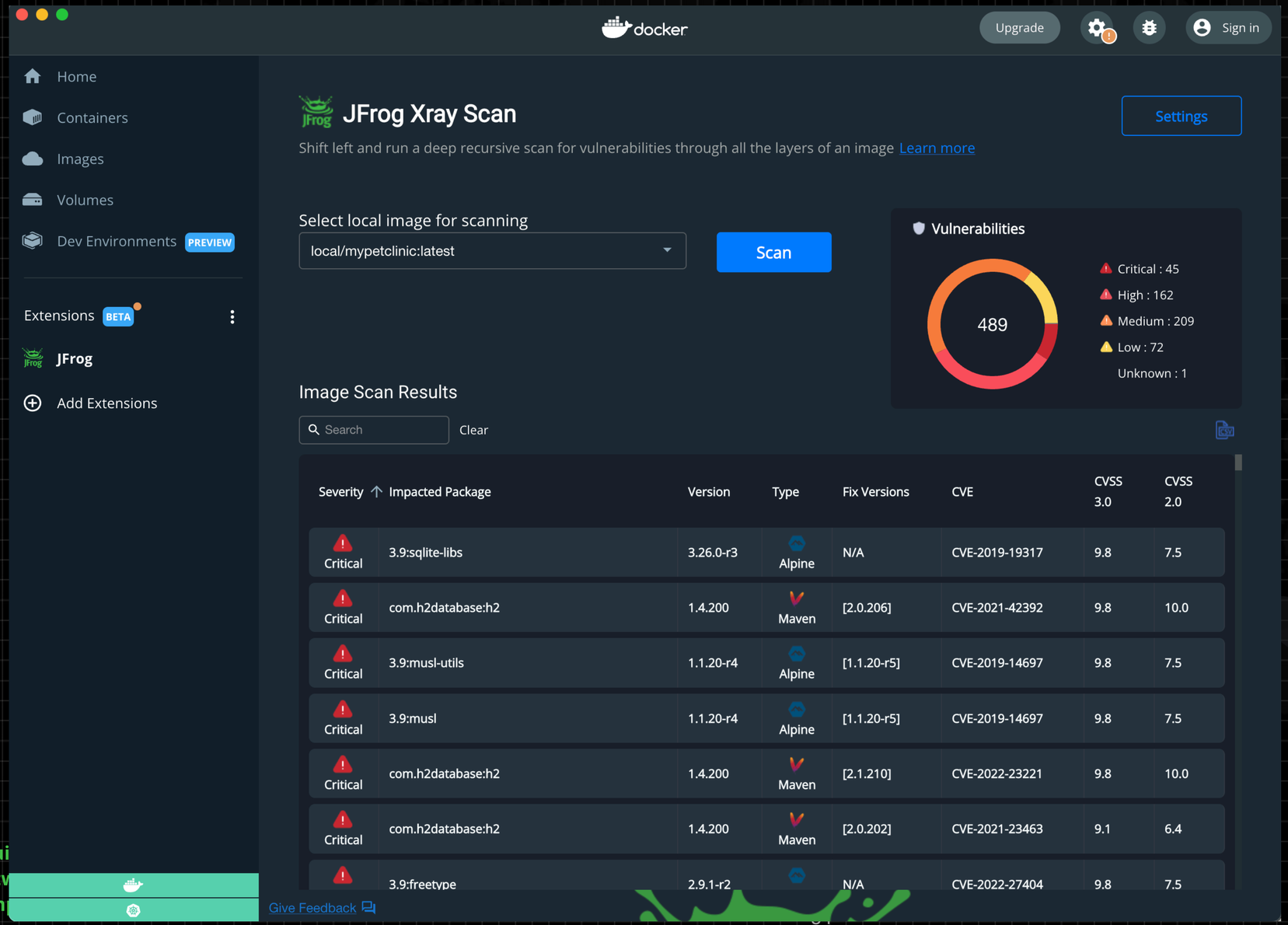
RepoPolicy

Critical 9 <= CVSS < 10
Block download

Shift Left (cont.)

Docker Desktop

JFrog XRAY



BuildWatch

GS_SPRING_BOOT_main_mvn

RepoWatch

demo-maven-prod-local

BuildPolicy

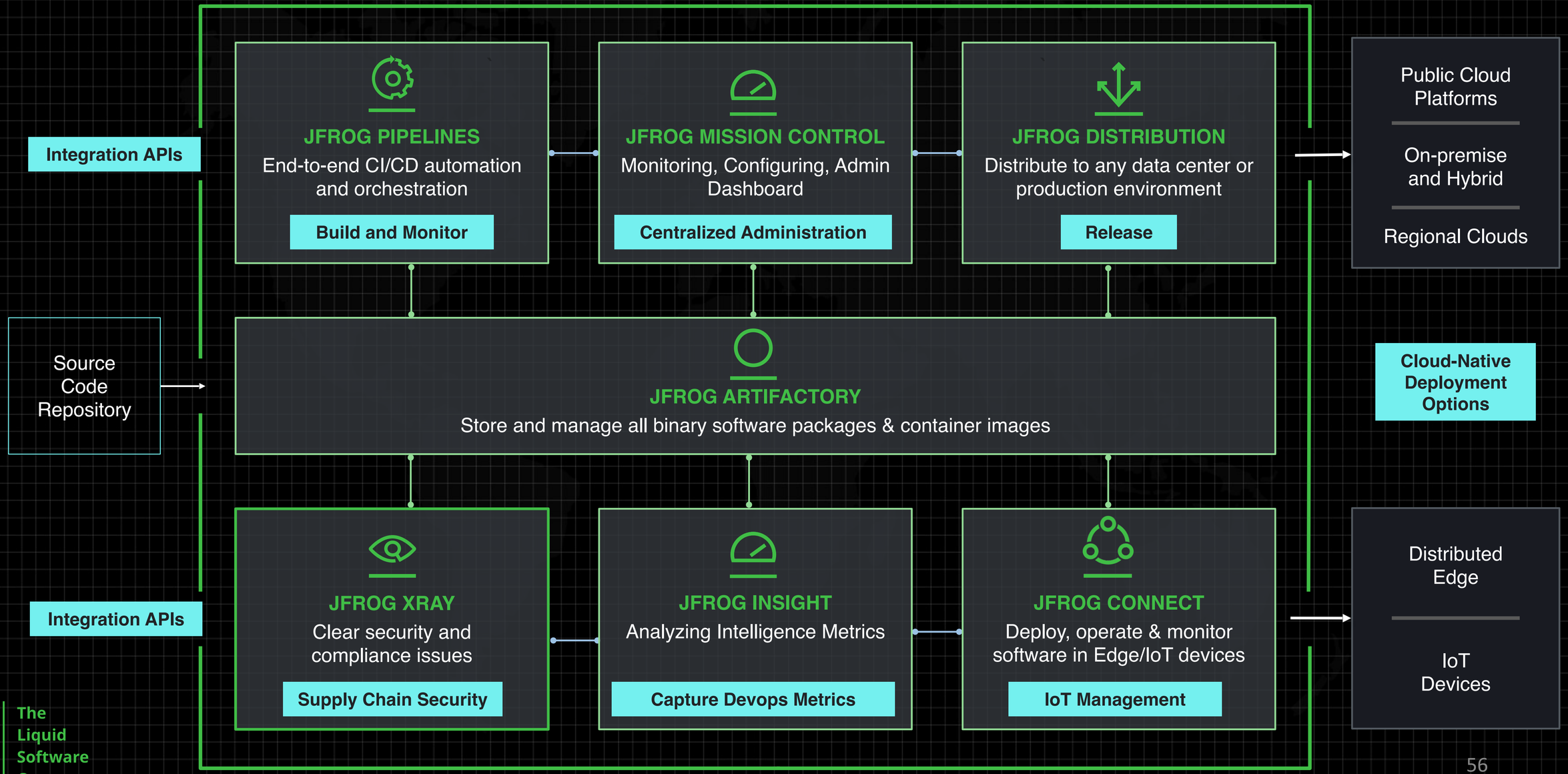
Critical 9<= CVSS <= 10
Generate violation
Fail Build
High 7 <= CVSS < 9
Generate violation

RepoPolicy

Critical 9 <= CVSS < 10
Block download

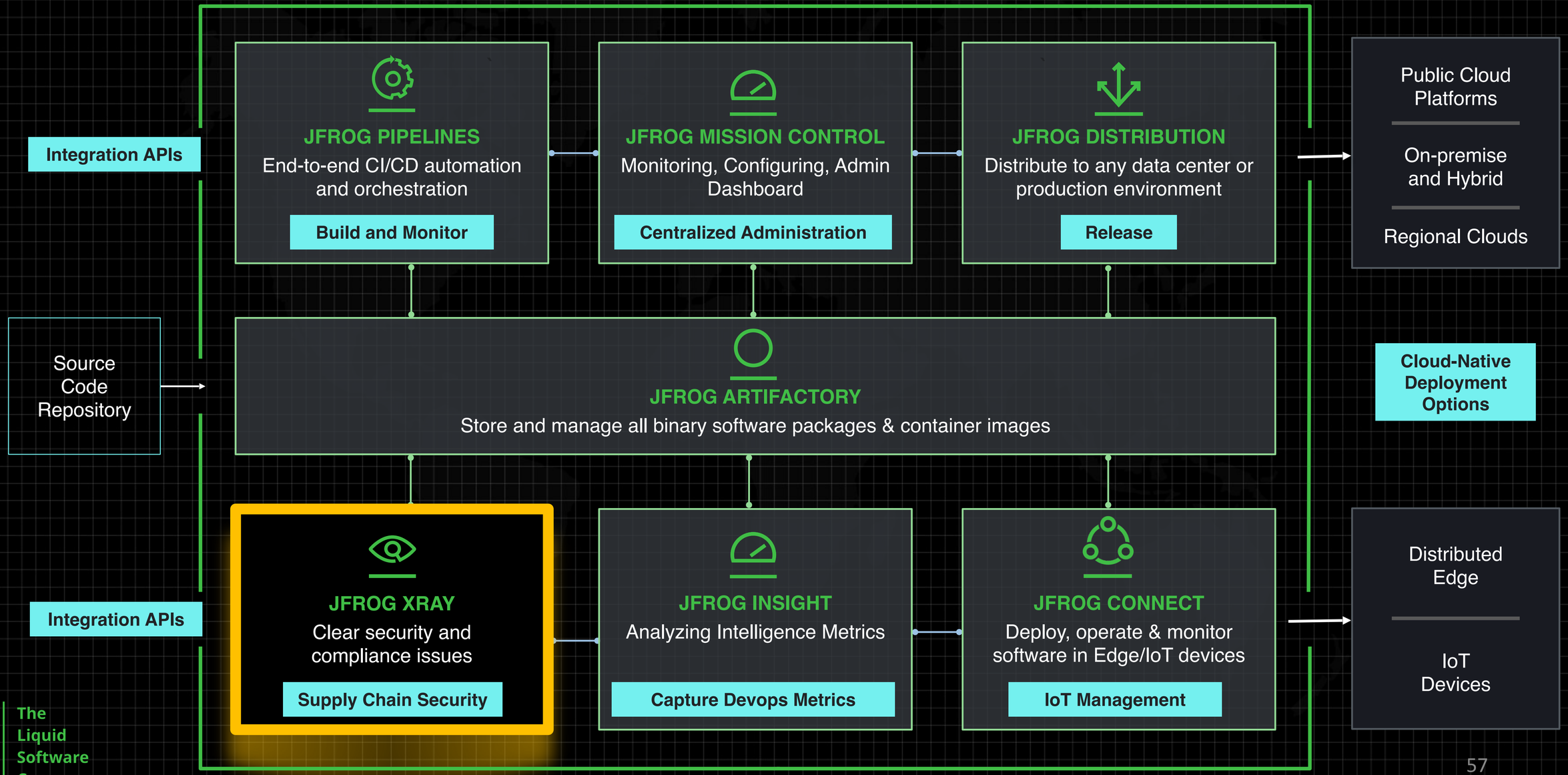
JFrog Advanced Security

THE JFROG DEVOPS PLATFORM



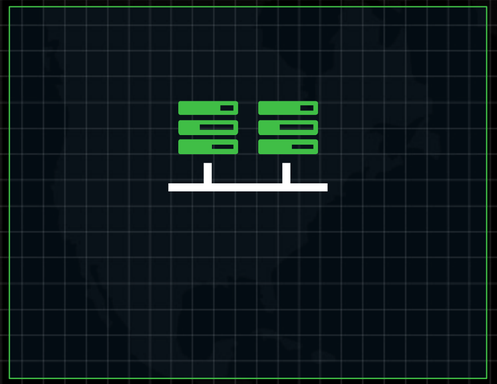
The Liquid Software Company

THE JFROG DEVOPS PLATFORM



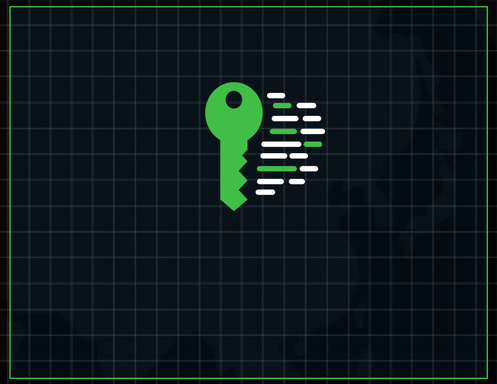
The Liquid Software Company

Software Supply Chain Attack Trends

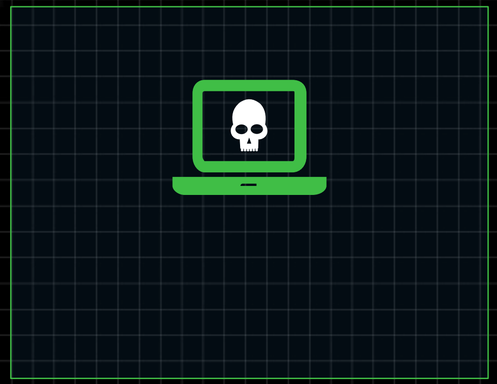


Known vulnerabilities in 3rd Party software (“CVEs”), OSS or Commercial

Unknown vulnerabilities in 1st and 3rd party code (“Zero-days”)



Non-code issues: misconfigurations, IaC, Malpractice, encryption, Secrets: private keys, passwords, services issues



Malicious code pre-injected intentionally via supply chain

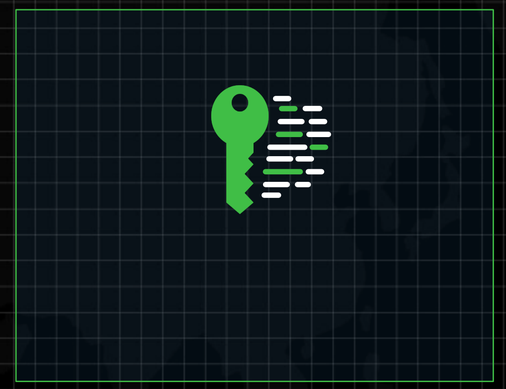
JFrog The Liquid Software Company

Software Supply Chain Attack Trends

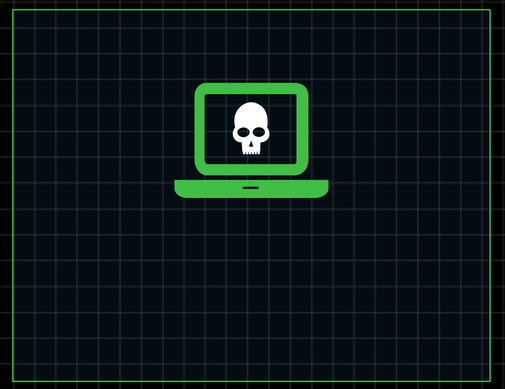
JFROG XRAY SCA

<u>Known</u> vulnerabilities in 3rd Party software (“CVEs”), OSS or Commercial

<u>Unknown</u> vulnerabilities in 1st and 3rd party code (“Zero-days”)



<u>Non-code issues:</u> misconfigurations, IaC, Malpractice, encryption, Secrets: private keys, passwords, services issues



<u>Malicious code</u> pre-injected intentionally via supply chain

The Liquid Software Company

Software Supply Chain Attack Trends

JFROG XRAY SCA

Known vulnerabilities in 3rd Party software (“CVEs”), OSS or Commercial, Contextual Analysis of CVEs

Unknown vulnerabilities in 1st and 3rd party code (“Zero-days”)

JFROG ADVANCED SECURITY

Non-code issues: misconfigurations, IaC, Malpractice, encryption, Secrets: private keys, passwords, services issues

Malicious code pre-injected intentionally via supply chain

The Liquid Software Company

Software Supply Chain Attack Trends

JFROG XRAY SCA

Known vulnerabilities in 3rd Party software (“CVEs”), OSS or Commercial, Contextual Analysis of CVEs

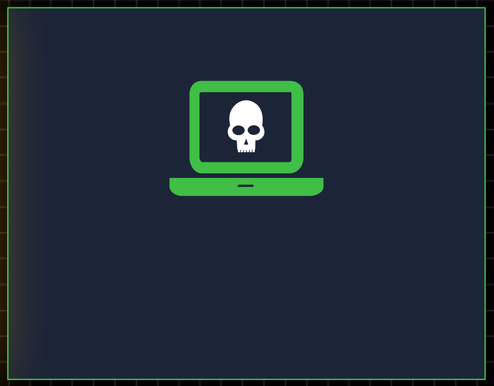
ROADMAP

Unknown vulnerabilities in 1st and 3rd party code (“Zero-days”)

JFROG ADVANCED SECURITY

Non-code issues: misconfigurations, IaC, Malpractice, encryption, Secrets: private keys, passwords, services issues

ROADMAP



Malicious code pre-injected intentionally via supply chain

The Liquid Software Company

Reinforcing Xray's Supply Chain Security Capabilities

SBOM

MALICIOUS PACKAGES

New !

SCA +

VULNERABILITIES

LICENSES

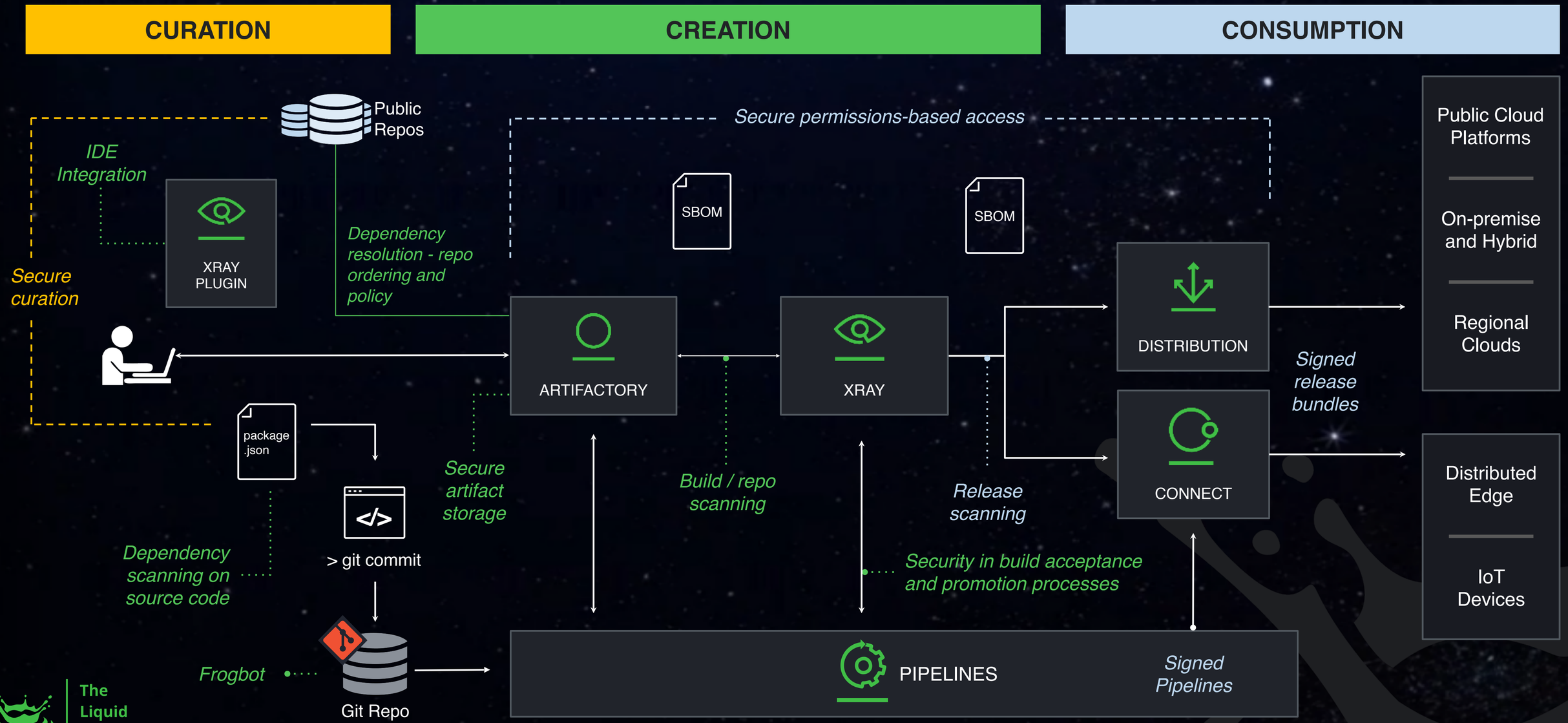
OPERATIONAL RISK

ADVANCED SUPPLY CHAIN-WIDE SECURITY CAPABILITIES

- SERVICES EXPOSURE
- SECRETS DETECTION
- IAC SECURITY ANALYSIS
- CONTEXTUAL ANALYSIS
- APPLICATION EXPOSURE

The Liquid Software Company

Security & Compliance: Infused Throughout The SSC



The Liquid Software Company

JFrog Advanced Security Capabilities

CONTEXTUAL ANALYSIS

Scan containers to identify and prioritise whether OSS vulnerabilities are actually exploitable.

SECRETS DETECTION

Detects any secrets left exposed in any containers stored in Artifactory to stop any accidental leak of internal tokens or credentials.

APPLICATION EXPOSURE

Find configuration issues, security malpractices, and insecure usage of popular OSS libraries related to your application framework

SERVICES EXPOSURE

Detect configuration issues and security malpractices for specific services and daemons included in your artifacts

IAC SECURITY ANALYSIS

Infrastructure-as-Code (IaC) Security Analysis
Scans IaC files stored in Artifactory for early detection of cloud and infrastructure misconfigurations to prevent attacks and data leak.

The Liquid Software Company

Contextual Analysis Coverage

JFrog Research Extended CVE Information

1100+ CVEs

JAS Contextual Analysis Scanner

400+ CVEs

40

Contextual Scanners Monthly

JFrog

IMAGINE

Distribute your software with JFrog Distribution

The
Liquid
Software
Company

Who is consuming the distributed software

Customer's deployment infr. / devices

External ecosystem / customers / partners

Customer's own Developers

RUNTIME DISTRIBUTION

EXTERNAL DISTRIBUTION

INTERNAL DISTRIBUTION

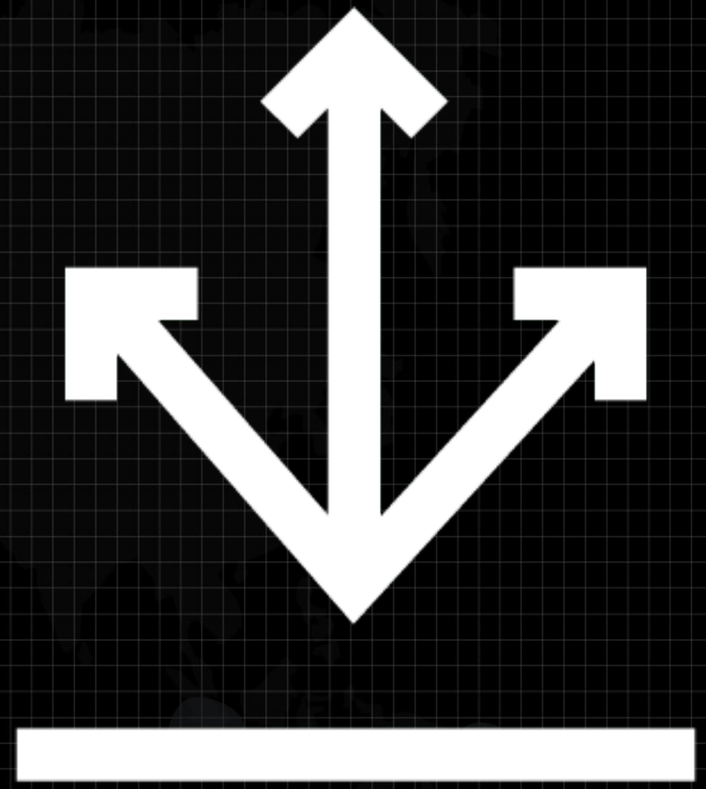
JFrog The Liquid Software Company

Possible Solutions

- Cloud Storage Hosted Solution
- CDN
- Download Centers
- Replication
- Federated Repositories
- JFrog Distribution

Possible Solutions

- Cloud Storage Hosted Solution
- CDN
- Download Centers
- Replication
- Federated Repositories
- JFrog Distribution



The Liquid Software Company

Overview of the JFrog Platform

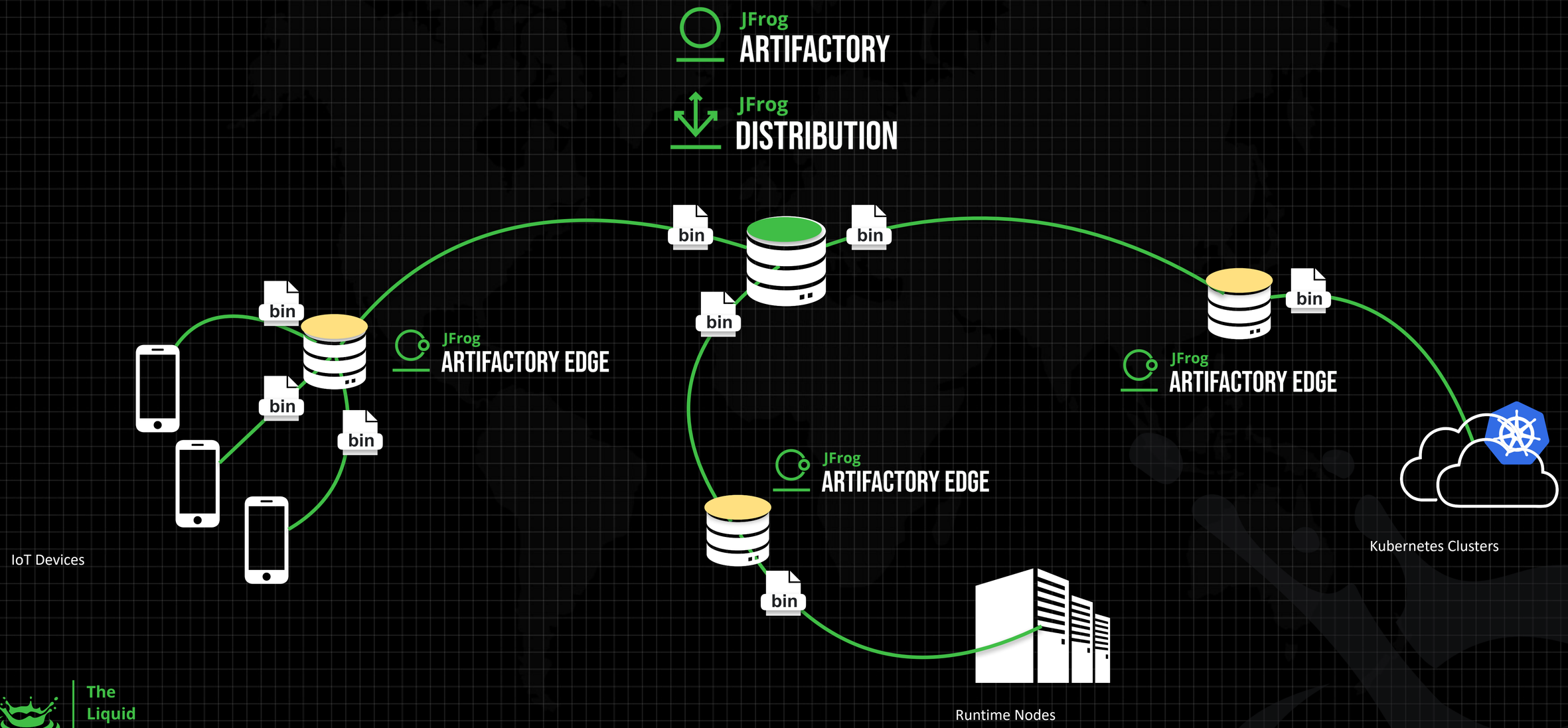
The Liquid Software Company

Overview of the JFrog Platform

BUILD & TEST → RELEASE → DEPLOY

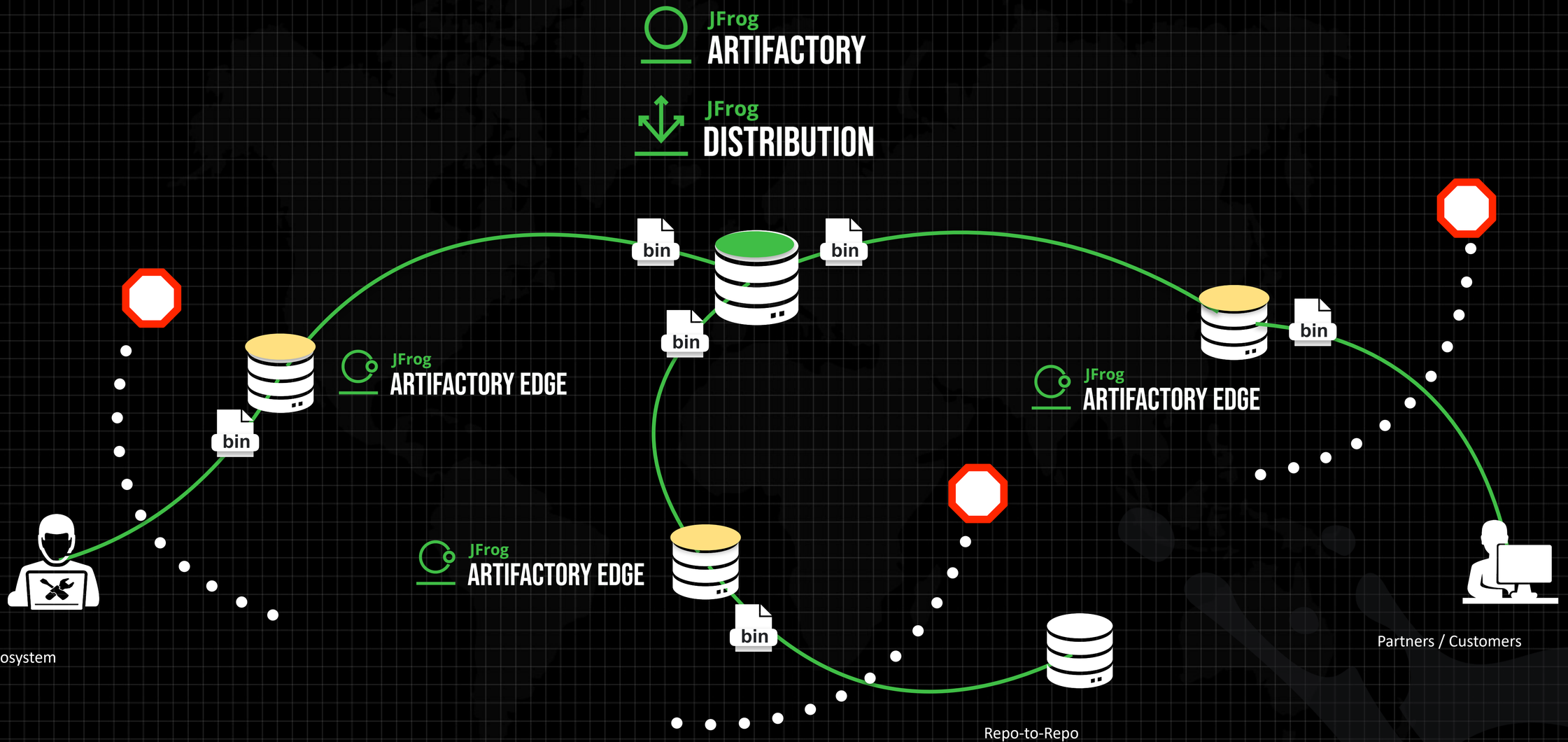
The Liquid Software Company

Runtime & Infrastructure EDGE Distribution



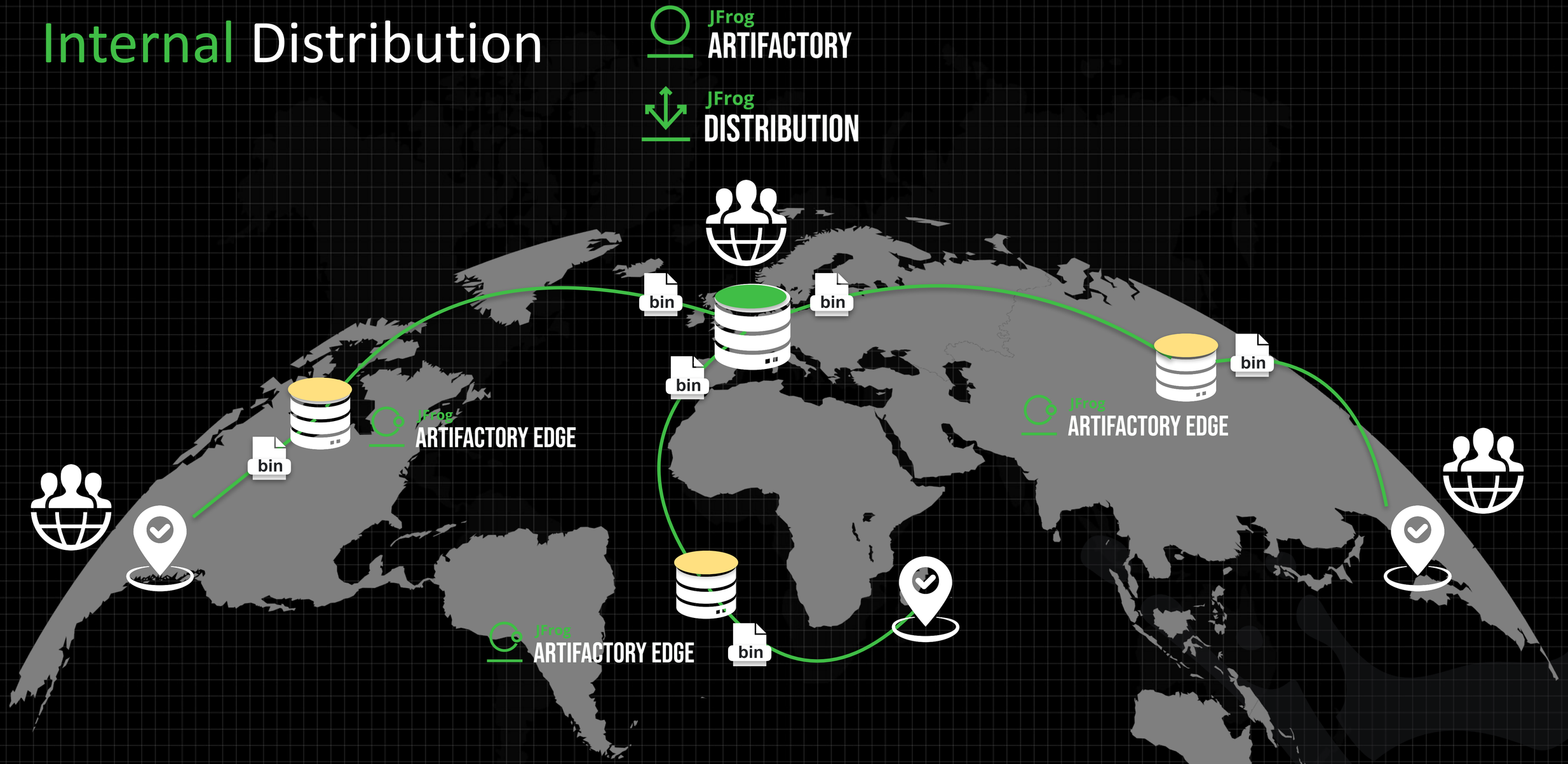
The Liquid Software Company

External Distribution



The Liquid Software Company

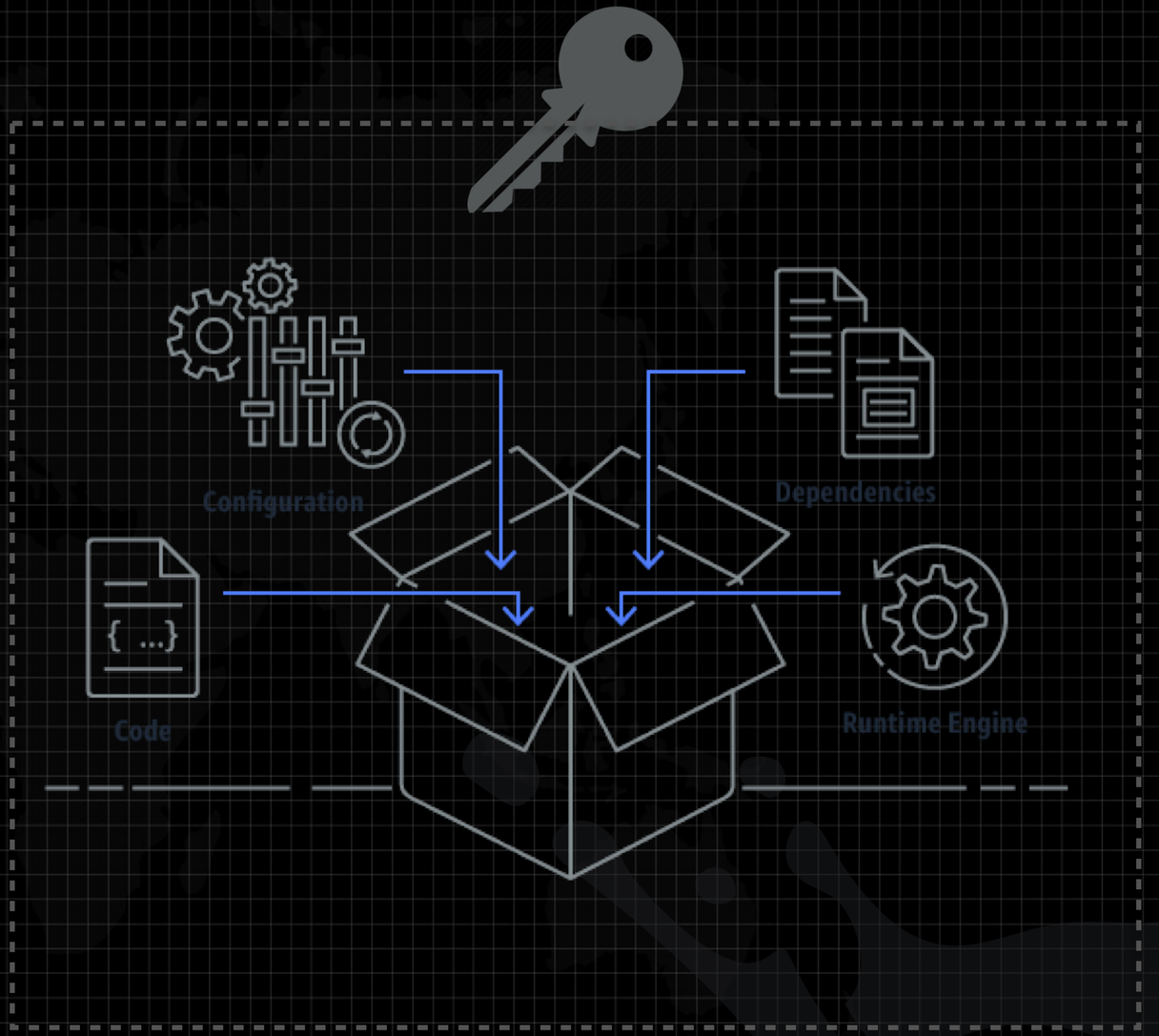
Internal Distribution



The Liquid Software Company

Release Bundle

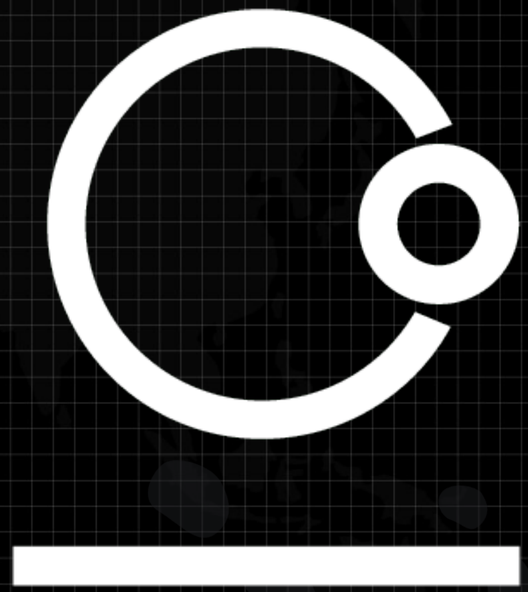
- A Release Bundle is a collection of artifacts grouped together
- This can be for example a Docker image together with a Helm chart
- Release Bundles can be created using REST API, CLI or through the Distribution UI
- Creating a Release Bundle requires Release Bundle writing permissions
- Secured and immutable



The Liquid Software Company

Edge Node

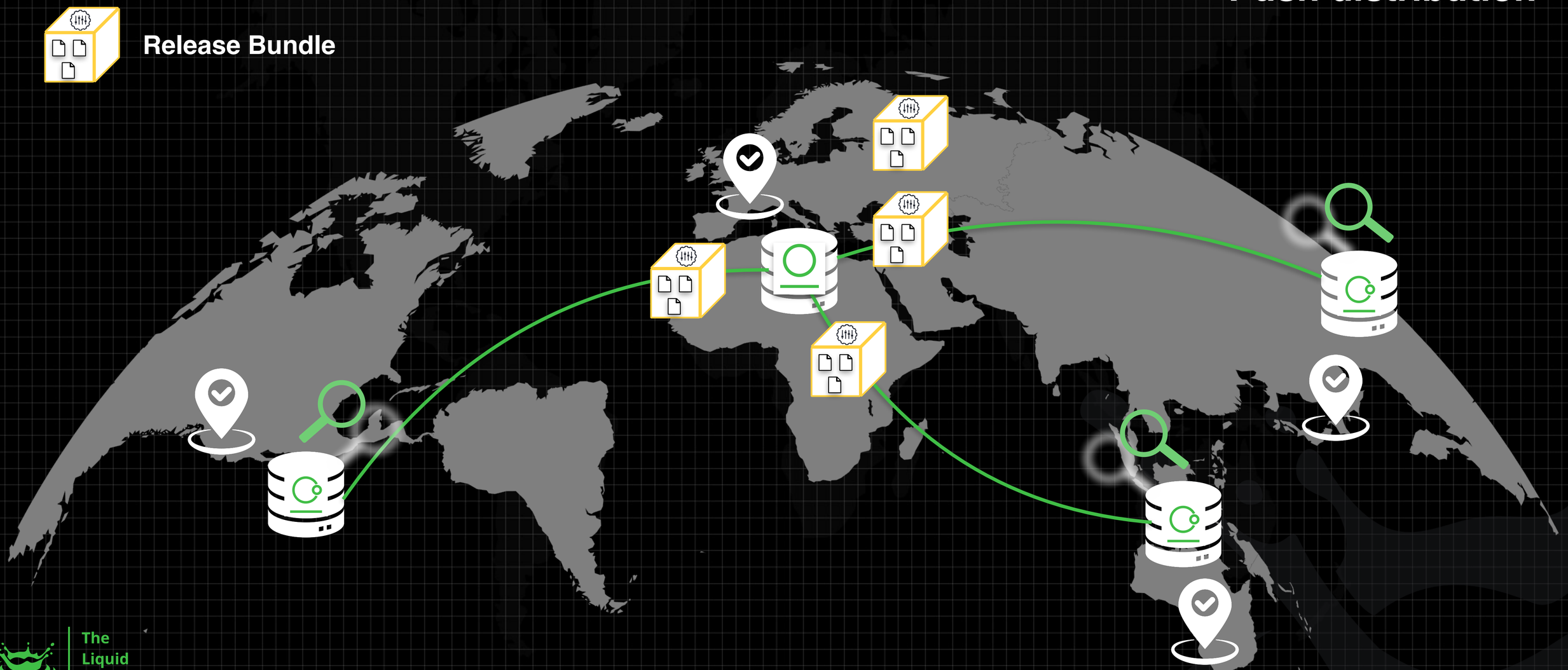
- “Read-only” artifactory
- Deployed physically close to the final destination of the artifact
- Direct upload of artifacts to an Edge node is not possible (except for a designated generic repository)
- No Remote repos (only smart remote repositories)
- No Build Integration
- No Xray scans allowed



The Liquid Software Company

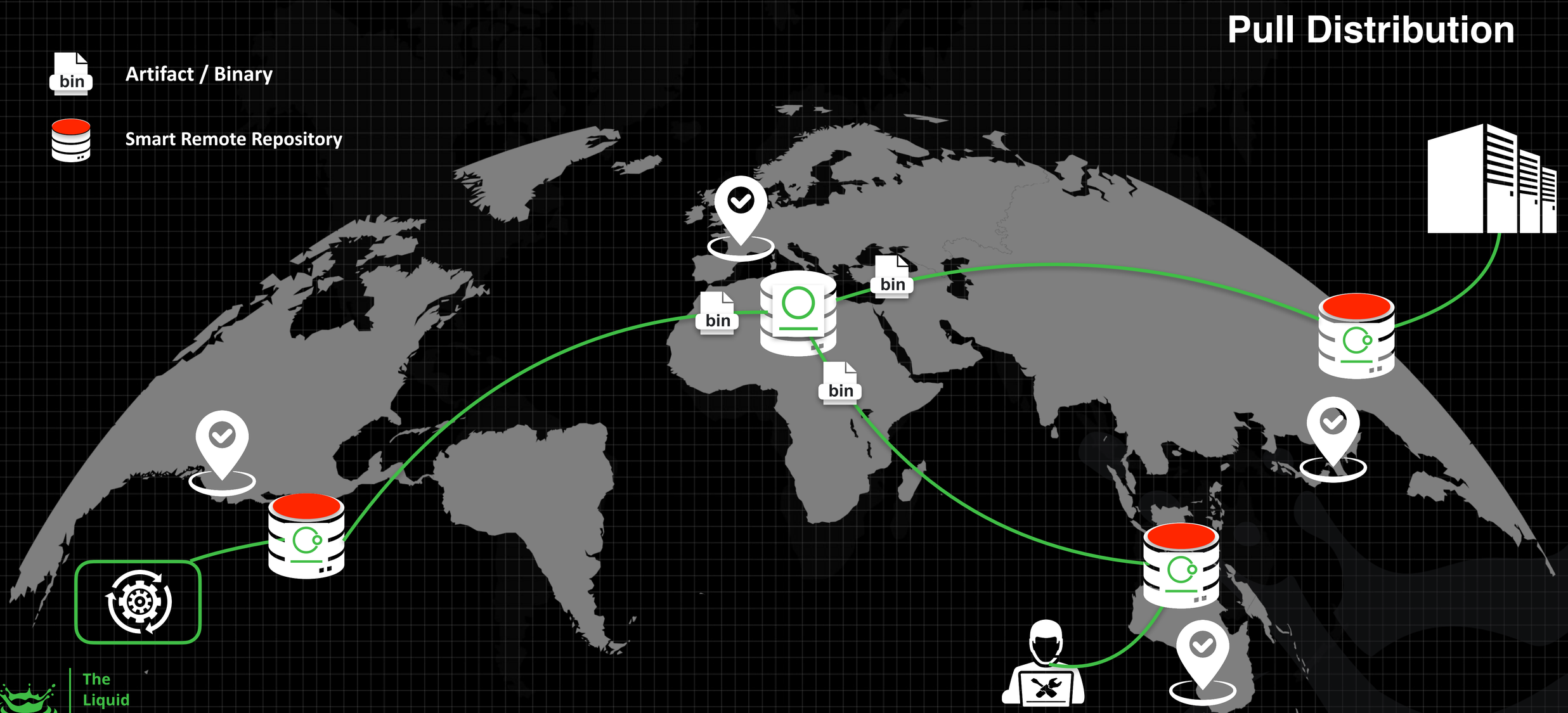
Distributing software across the globe

Push distribution



The Liquid Software Company

Distributing software across the globe



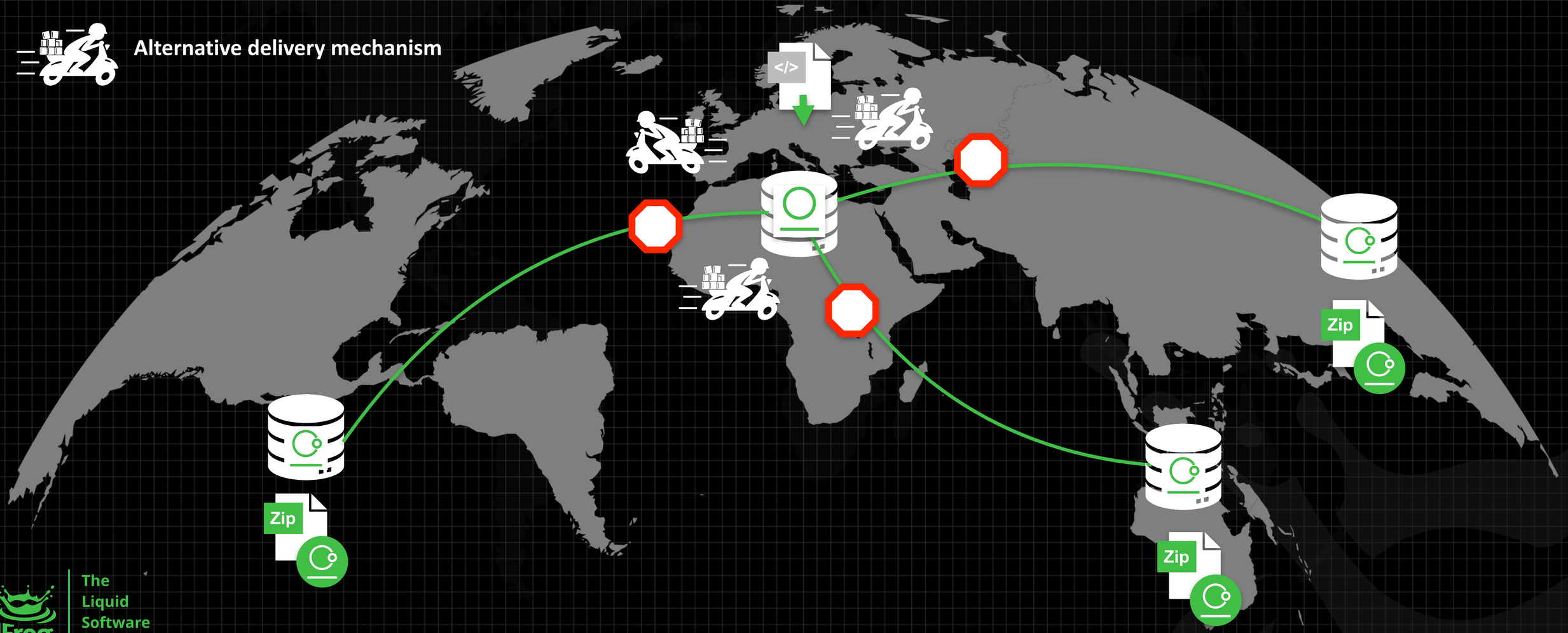
The Liquid Software Company

Distributing software across the globe

Air Gap Distribution

Firewall rules

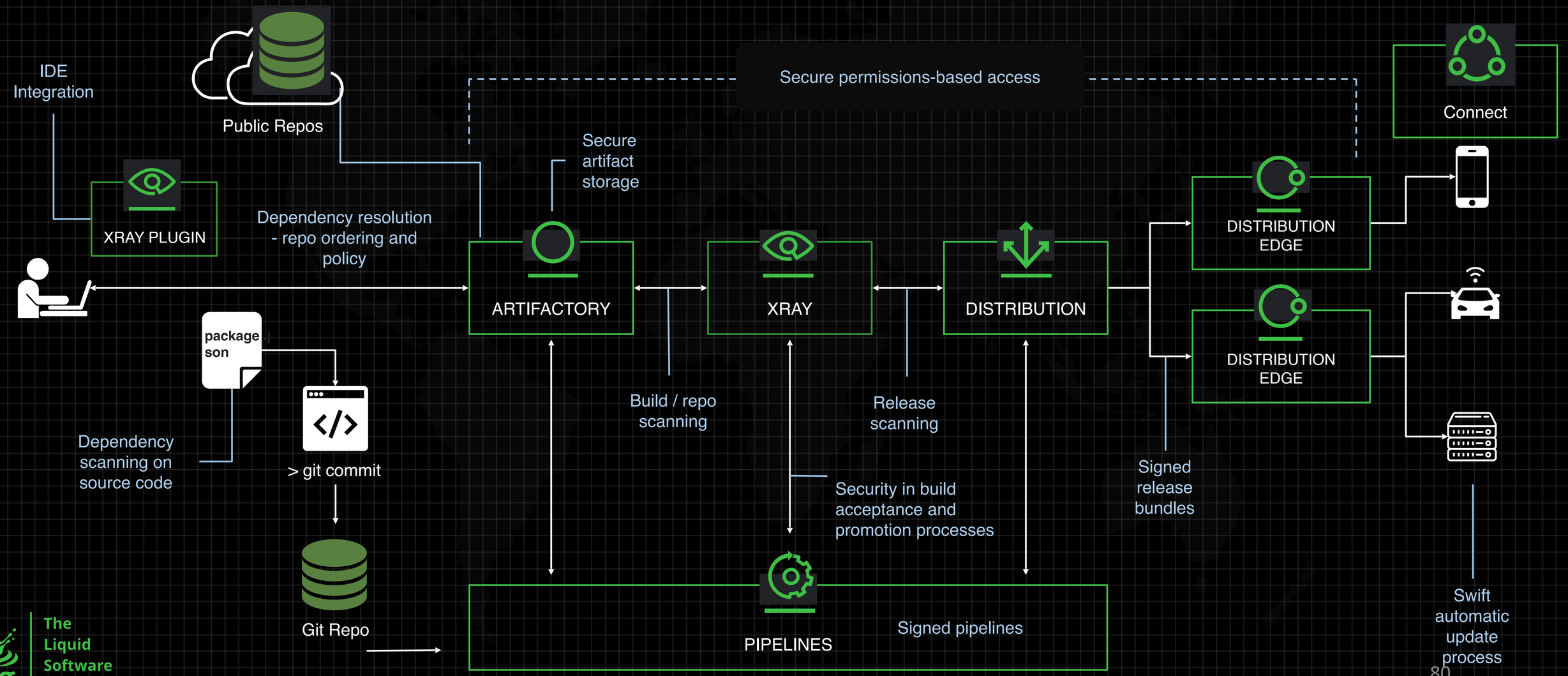
Alternative delivery mechanism



JFrog
The Liquid Software Company

End-to-end security with the JFrog Platform

Continuously securing the software supply chain



The Liquid Software Company