



KubeCon



CloudNativeCon

Europe 2020

Save Your Services From Sneaky Snoops With SPIFFE

Virtual

*Daniel Feldman
SPIFFE & SPIRE Projects*

About Me



KubeCon



CloudNativeCon

Europe 2020

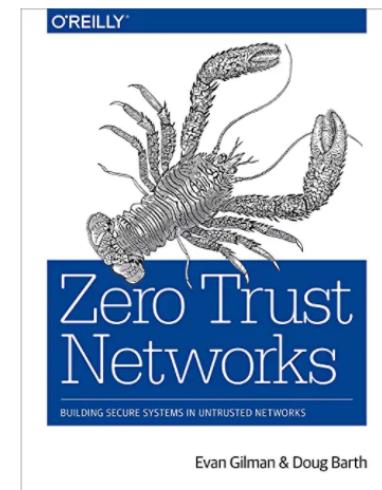
Virtual



Daniel Feldman

Cloud security engineering
Veritas -> Scytale -> HPE

And a huge team with security experience from a variety of companies!



Zero Trust Networks

BUILDING SECURE SYSTEMS IN UNTRUSTED NETWORKS

Evan Gilman & Doug Barth



KubeCon



CloudNativeCon

Europe 2020

Virtual

Why Service Identity

Service Identity Approaches

SPIFFE (the standard)

SPIRE (the implementation)

Next Steps

Why Service Identity

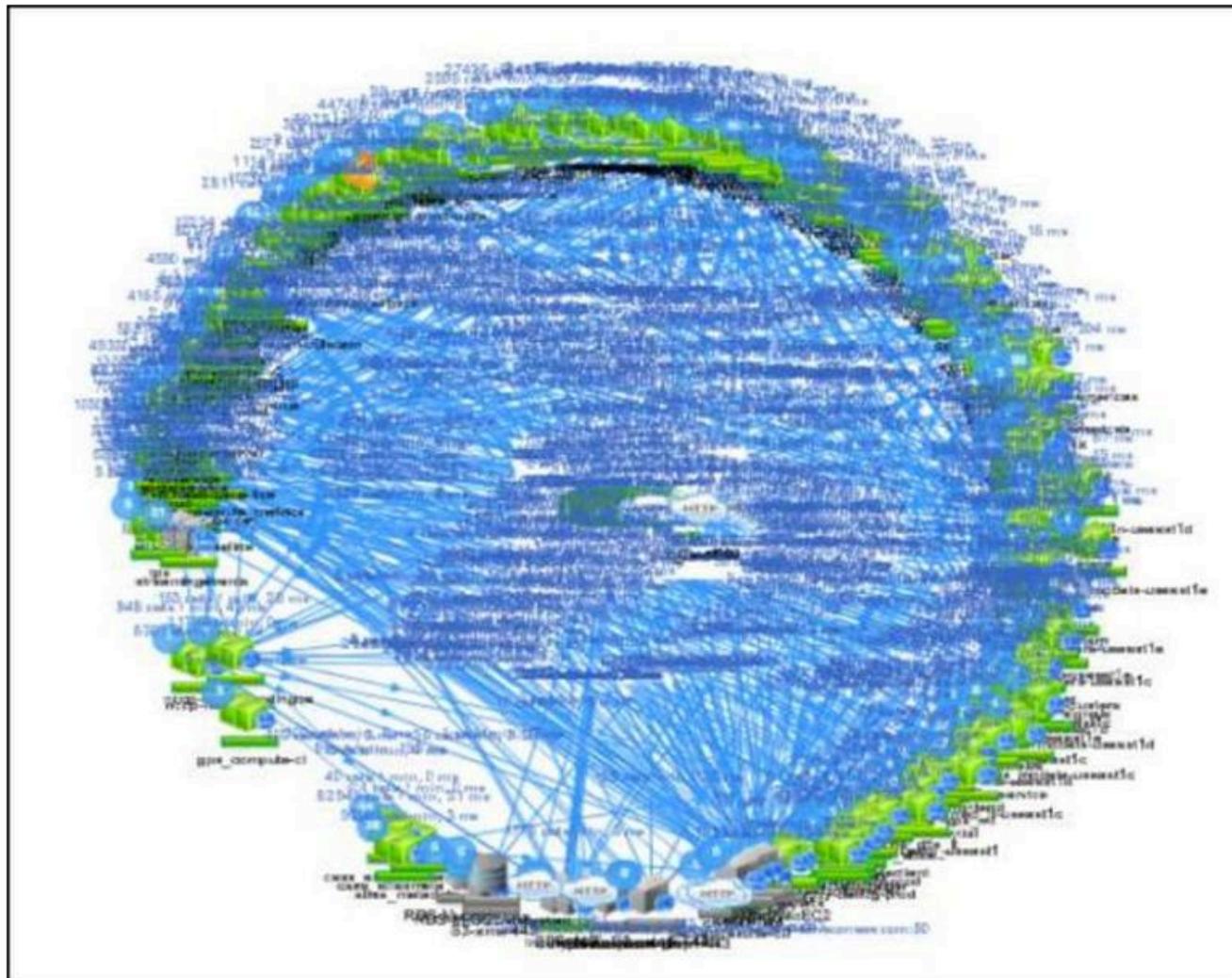


KubeCon



CloudNativeCon
Europe 2020

Virtual



Why Service Identity



KubeCon



CloudNativeCon

Europe 2020

Virtual



ENCRYPTION



INTEGRITY



AUTHENTICATION



AUTHORIZATION

All security rests on a foundation of **identity**

For humans, identity is (mostly) straightforward

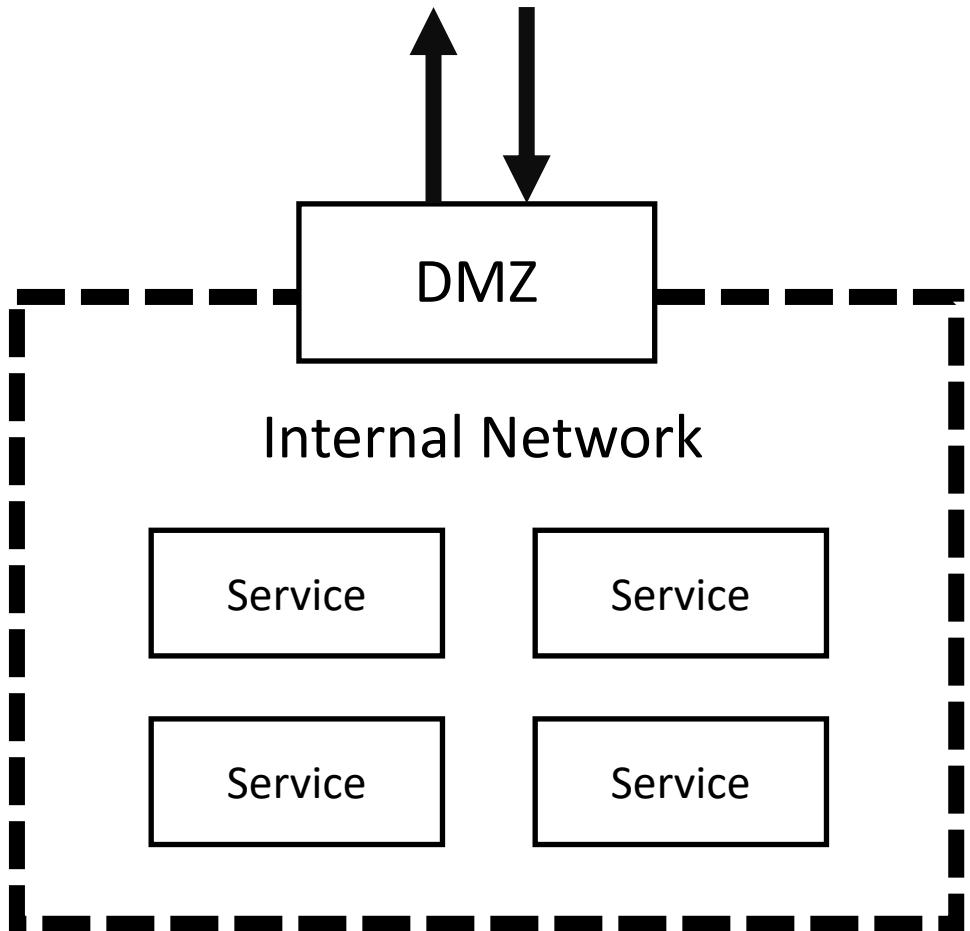
For services...

Service identity approaches



Virtual

Can we just use... **perimeter security**?



- In the perimeter security model, **everything “inside” is trusted and everything “outside” is untrusted**

Why Service Identity



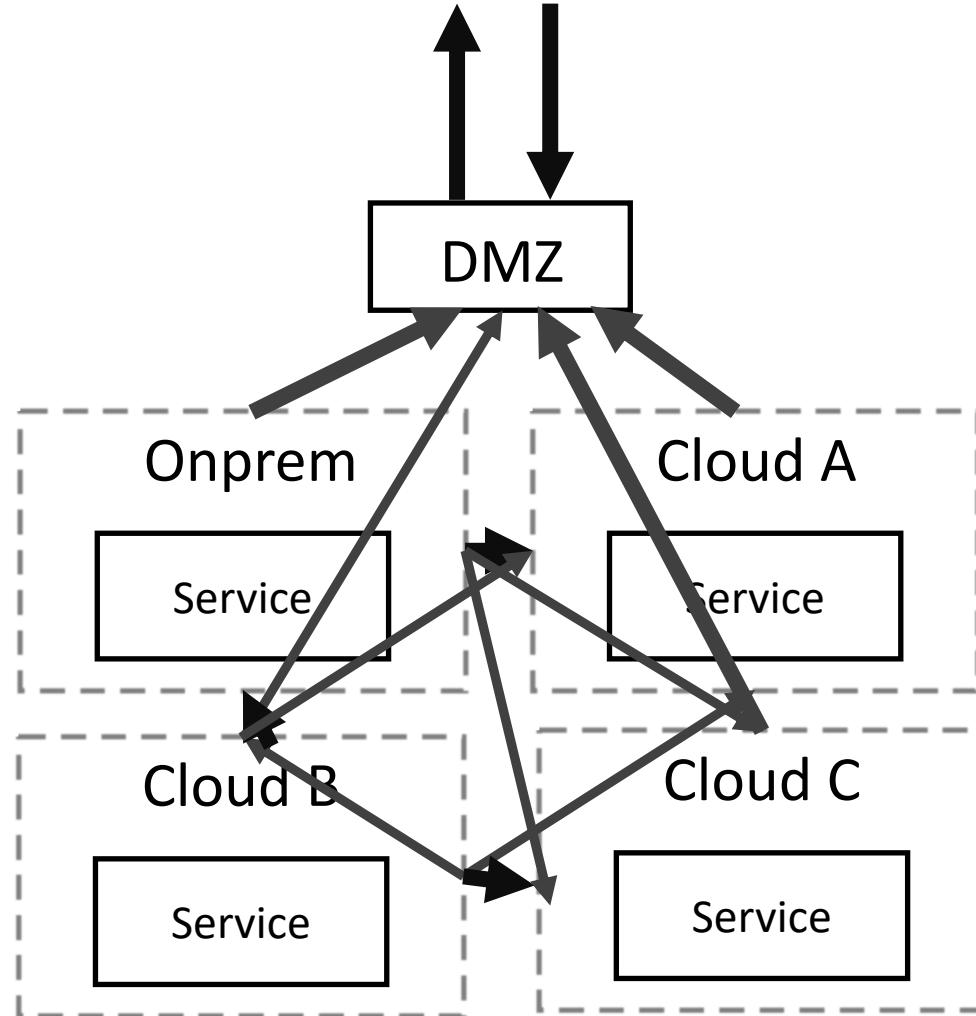
KubeCon



CloudNativeCon
Europe 2020

Virtual

Can we just use... perimeter security?



- In the perimeter security model, everything “inside” is trusted and everything “outside” is untrusted
- As you add multiple datacenters, clouds and regions this becomes **increasingly complex**

Why Service Identity

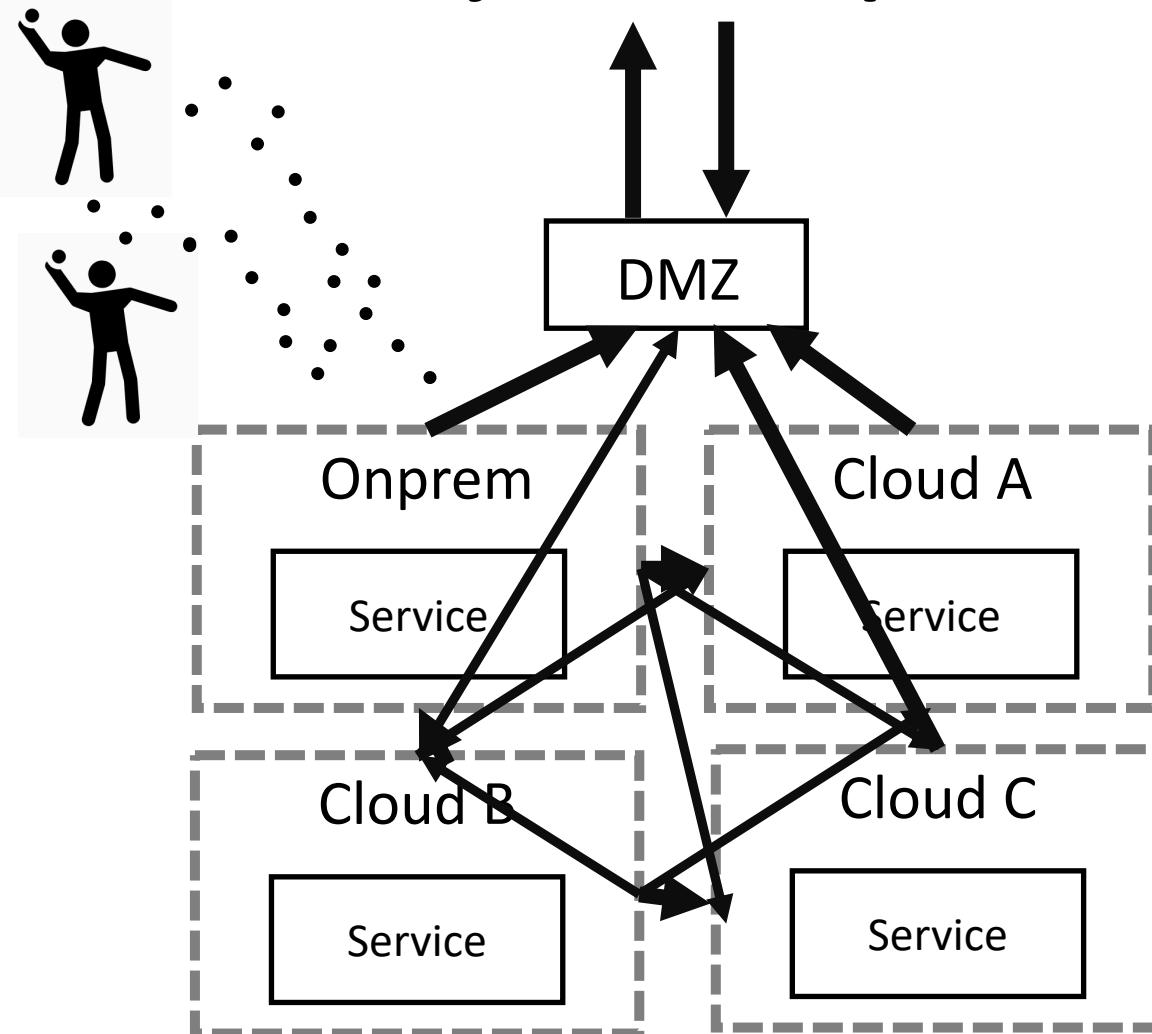


KubeCon

CloudNativeCon
Europe 2020

Virtual

Can we just use... perimeter security?



- In the perimeter security model, everything “inside” is trusted and everything “outside” is untrusted
- As you add multiple datacenters, clouds and regions this becomes increasingly complex
- CI/CD makes it almost impossible

Why Service Identity



KubeCon

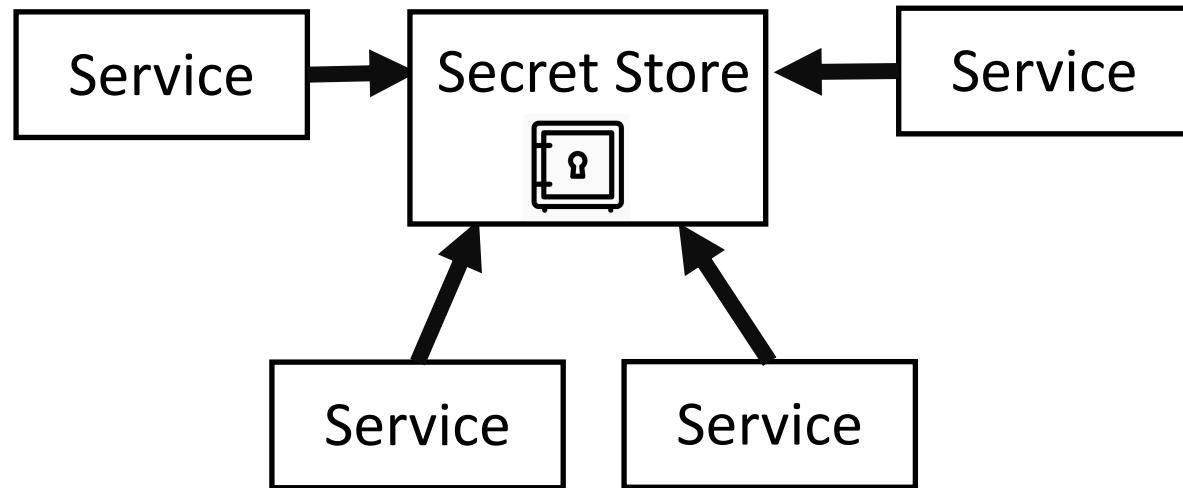


CloudNativeCon

Europe 2020

Virtual

Can we just use... **shared secrets**?



- In the **shared secrets** model, every service has credentials/certificates used to access other services
 - (Hopefully) stored in a secret store
- Maintaining secrets at scale is hard work
- How do you initially authenticate to the secret store?

Why Service Identity



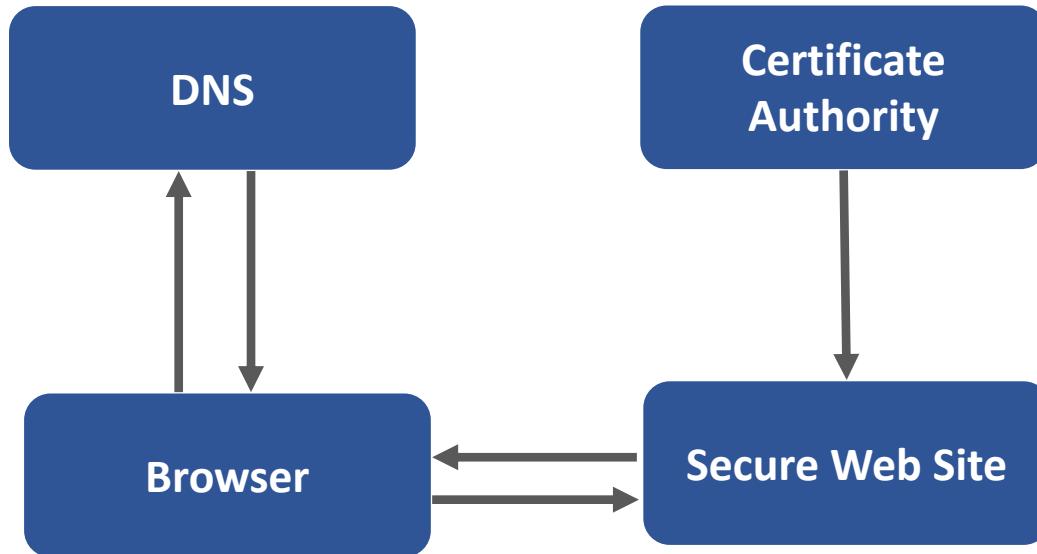
KubeCon



CloudNativeCon
Europe 2020

Virtual

Can we just use... web PKI?



- Web Public key infrastructure (PKI) lets you access web sites securely
- But services aren't web sites:
 - Services don't all have hostnames
- Also, no simple way to check the client's identity

Why Service Identity



KubeCon



CloudNativeCon

Europe 2020

Virtual

We need a way to **securely distribute identities to services** without relying on manual effort

Secure Production Identity Framework for Everyone



- SPIFFE is a **platform-agnostic standard** for implementing service identity
- Inspired by Google, Netflix, and Facebook
- It gives your service a “passport” for communicating with other services
- It is partially implemented by several service meshes, and fully implemented in SPIRE

SPIFFE (the standard)



KubeCon



CloudNativeCon

Europe 2020

Virtual

SPIFFE IDs

Standard format for a service ID
spiffe://trustdomain/service

SPIFFE (the standard)



KubeCon
Europe 2020



CloudNativeCon
Europe 2020

Virtual

SPIFFE IDs

Standard format for a service ID
`spiffe://trustdomain/service`

SVIDs

Cryptographically verifiable
documents asserting a SPIFFE ID

SPIFFE (the standard)



KubeCon
Europe 2020



CloudNativeCon
Europe 2020

Virtual

SPIFFE IDs

Standard format for a service ID
`spiffe://trustdomain/service`

SVIDs

Cryptographically verifiable
documents asserting a SPIFFE ID

Trust Bundles

Set of certificates used to
verify SVIDs

SPIFFE (the standard)



Virtual

SPIFFE IDs

Standard format for a service ID
spiffe://trustdomain/service

SVIDs

Cryptographically verifiable
documents asserting a SPIFFE ID

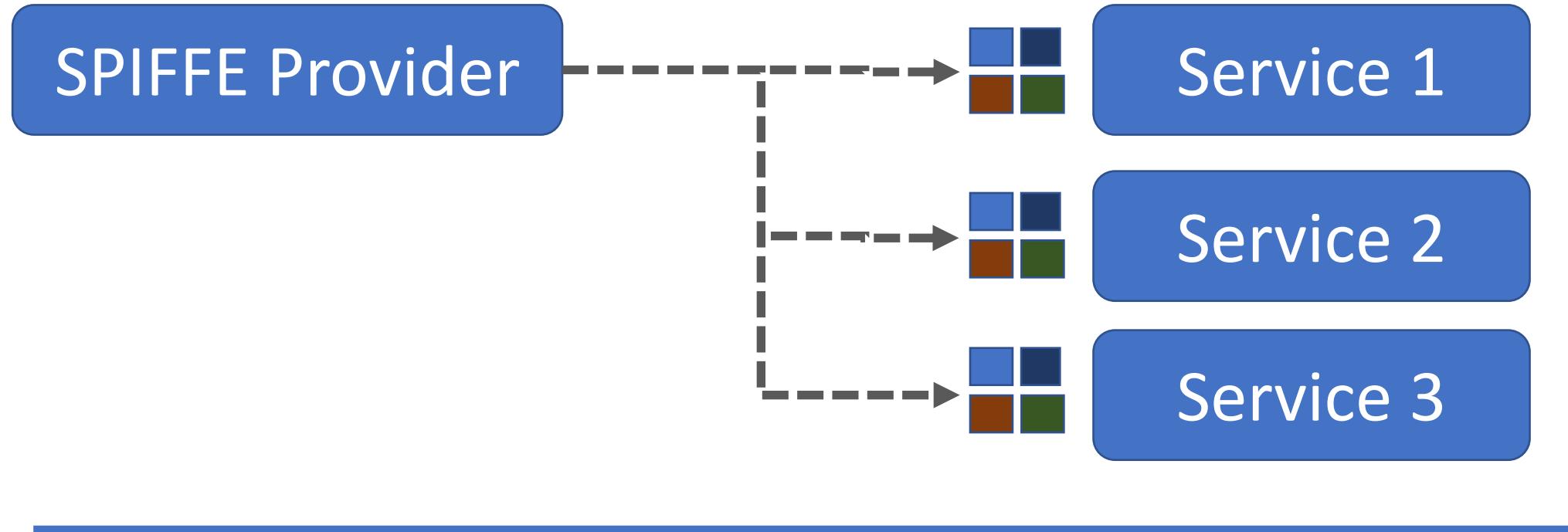
Trust Bundles

Set of certificates used to
verify SVIDs

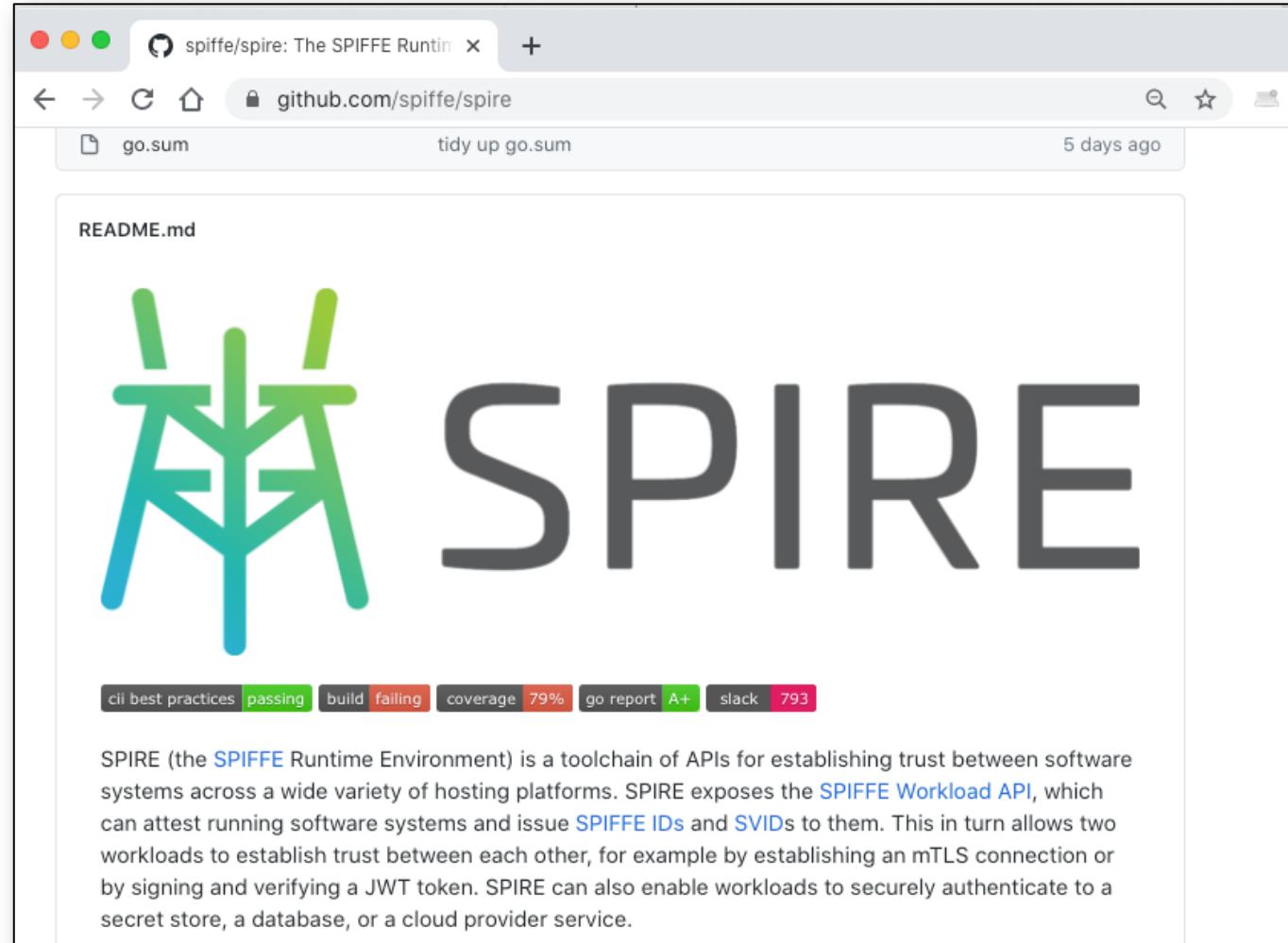
Workload API

Local gRPC API for workloads to
obtain SPIFFE IDs, SVIDs, and
Trust Bundles

SPIFFE (the standard)



SPIRE (our implementation)



SPIRE (our implementation)

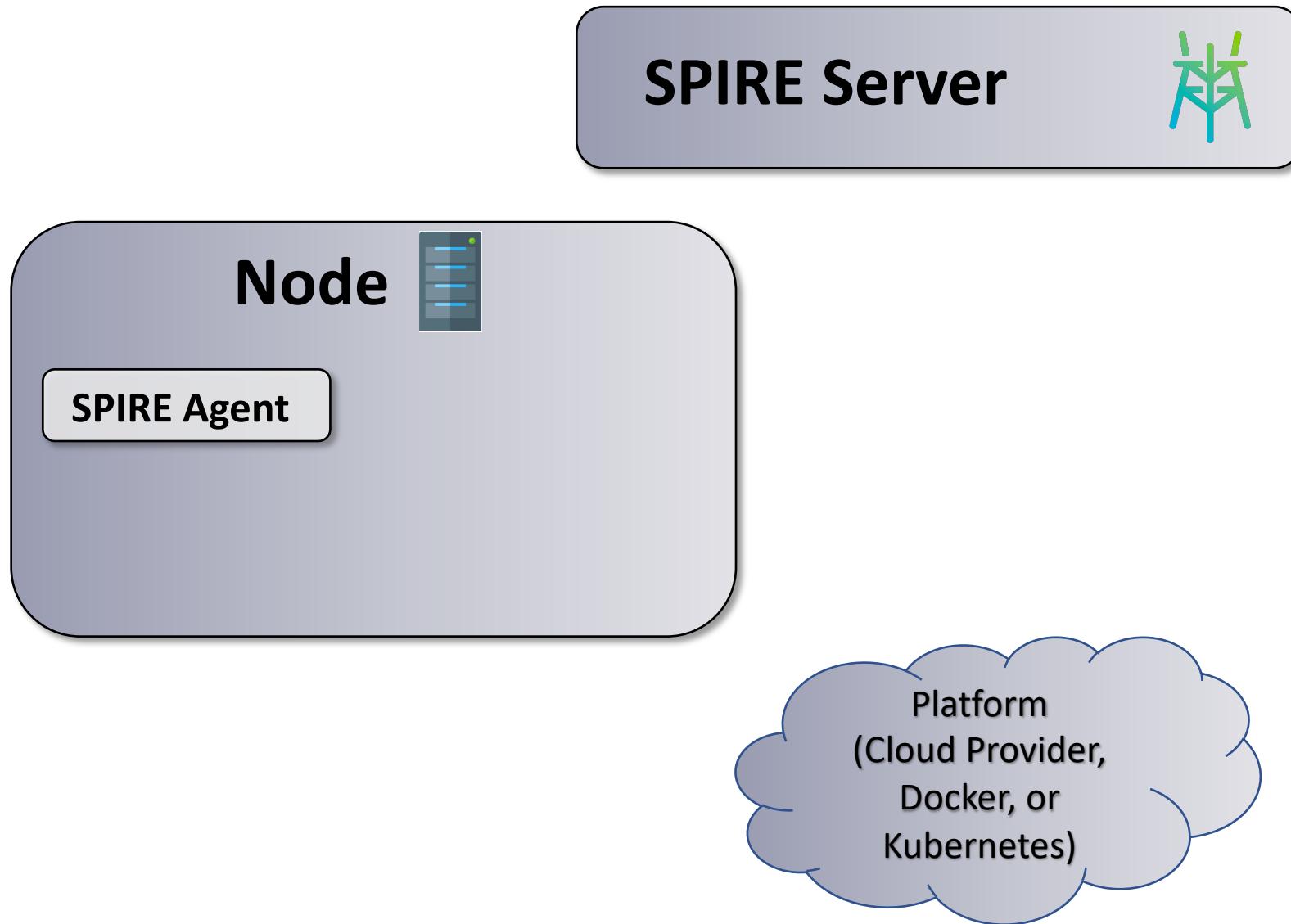


KubeCon

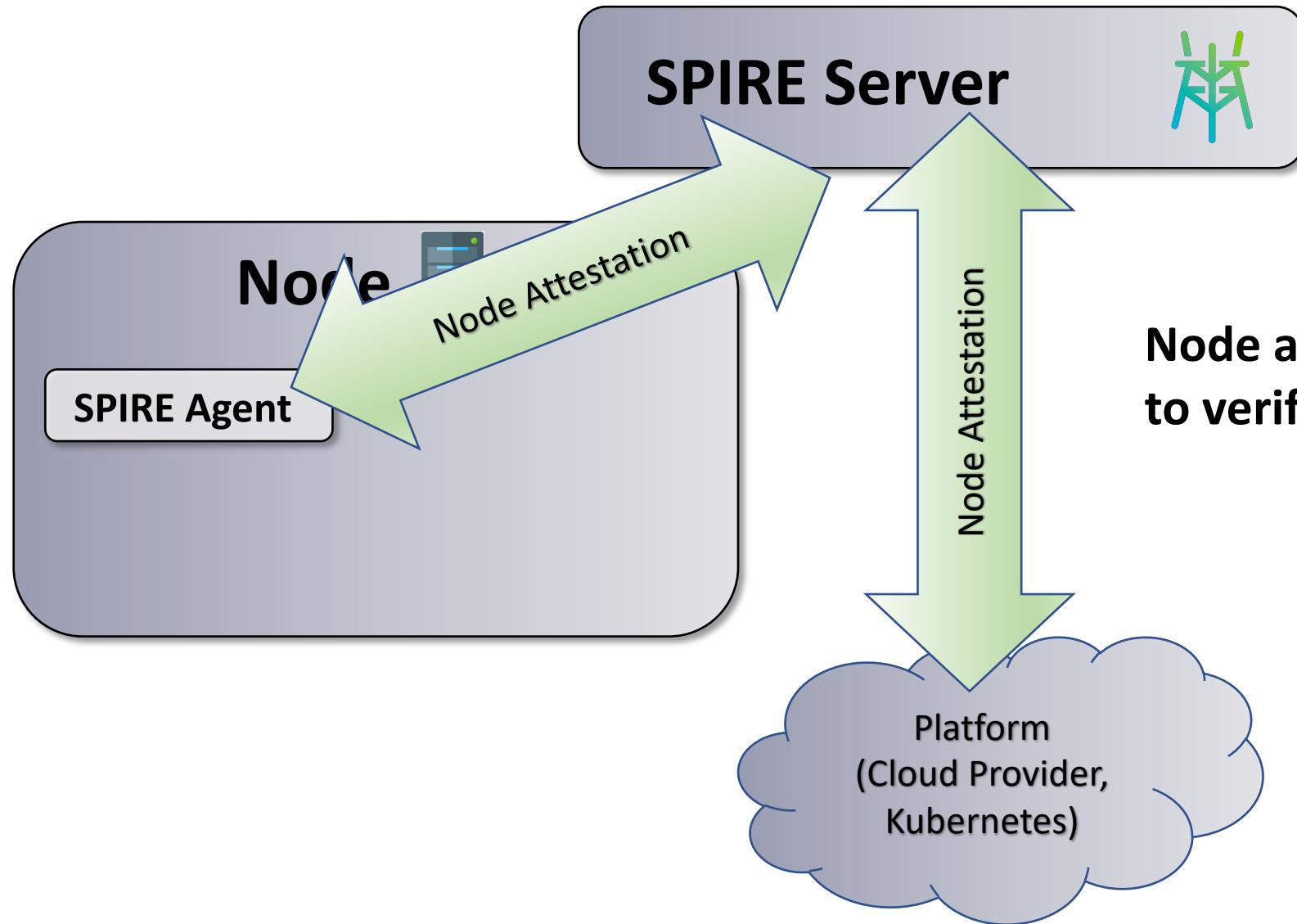


CloudNativeCon
Europe 2020

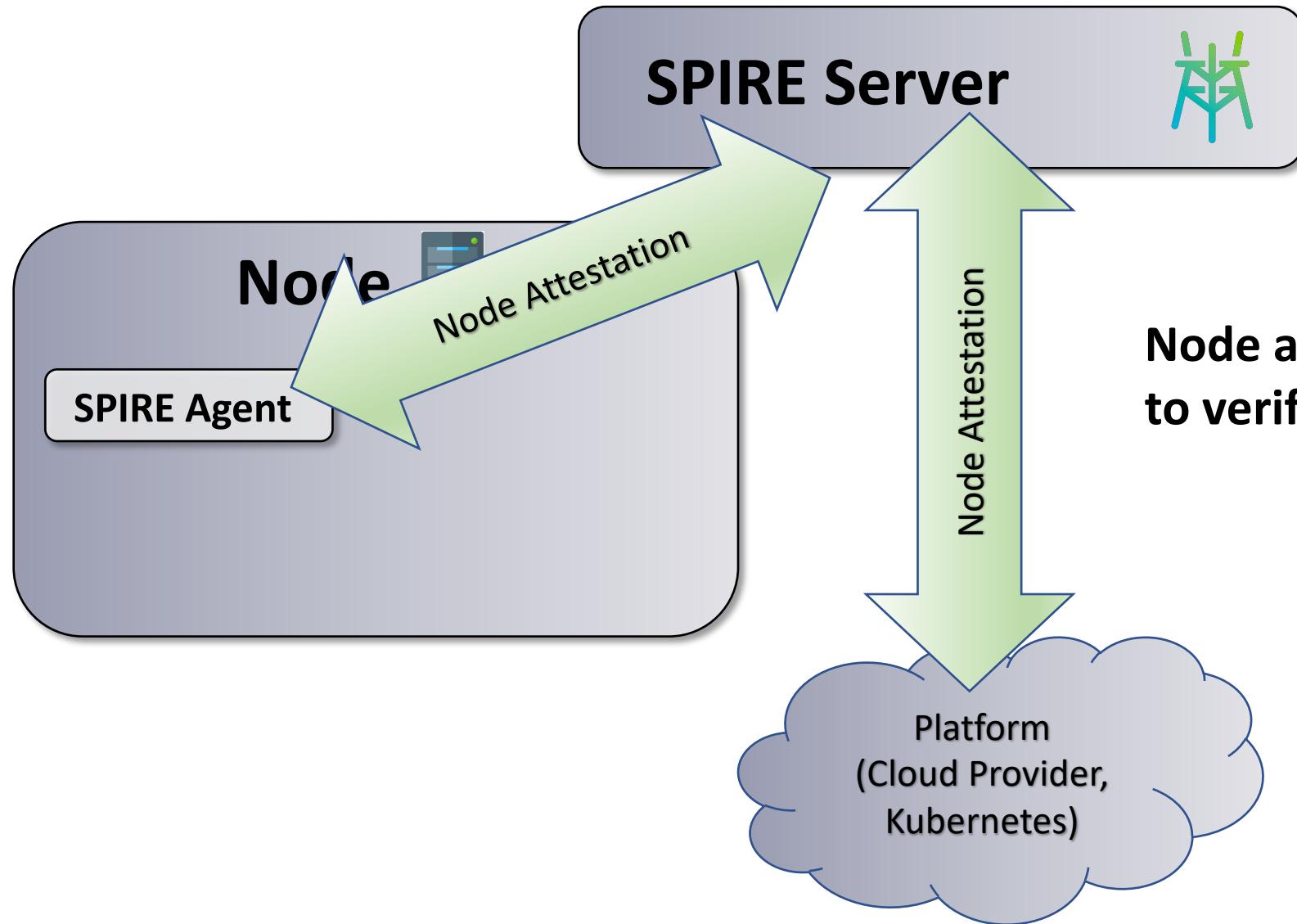
Virtual



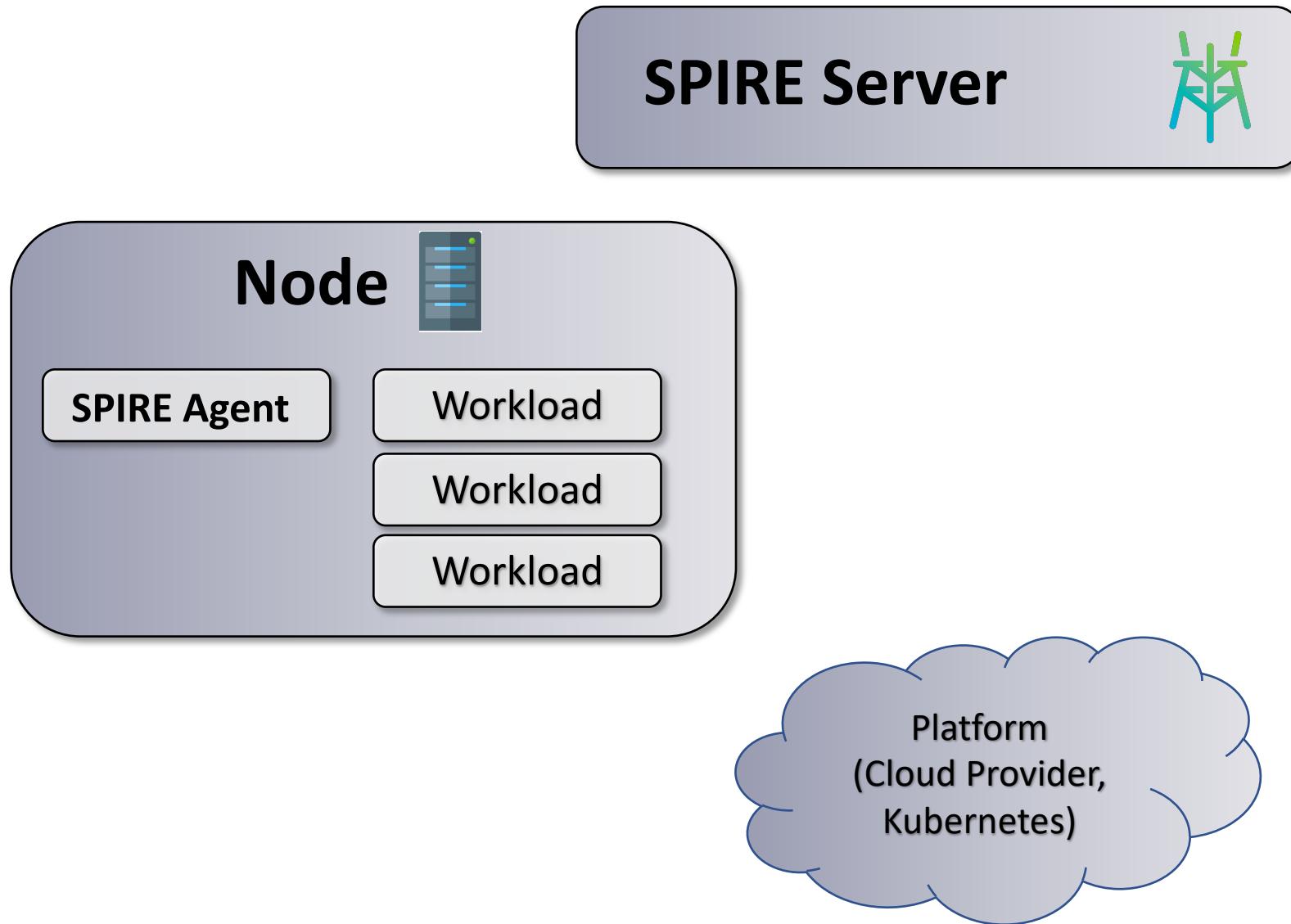
SPIRE (our implementation)



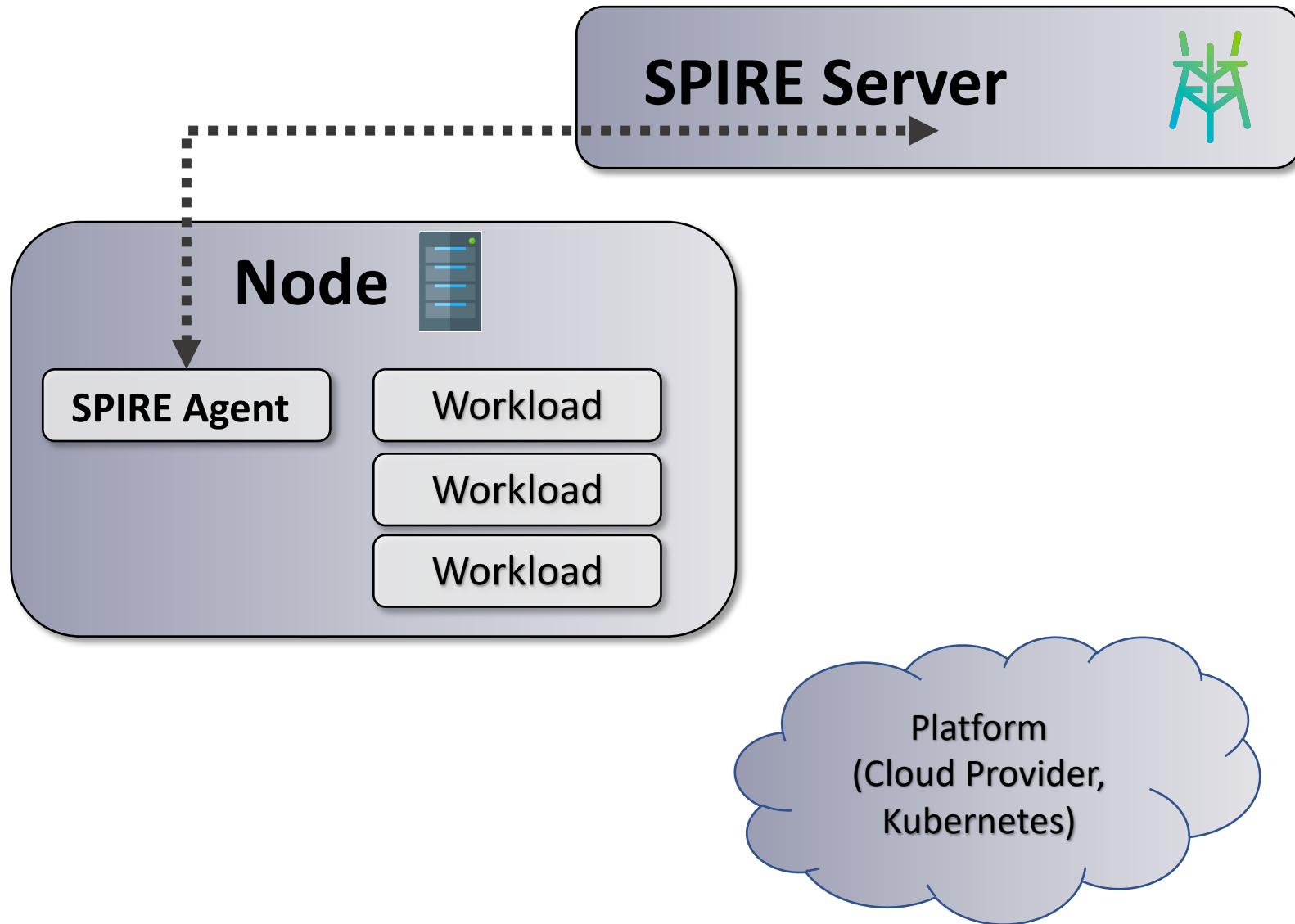
SPIRE (our implementation)



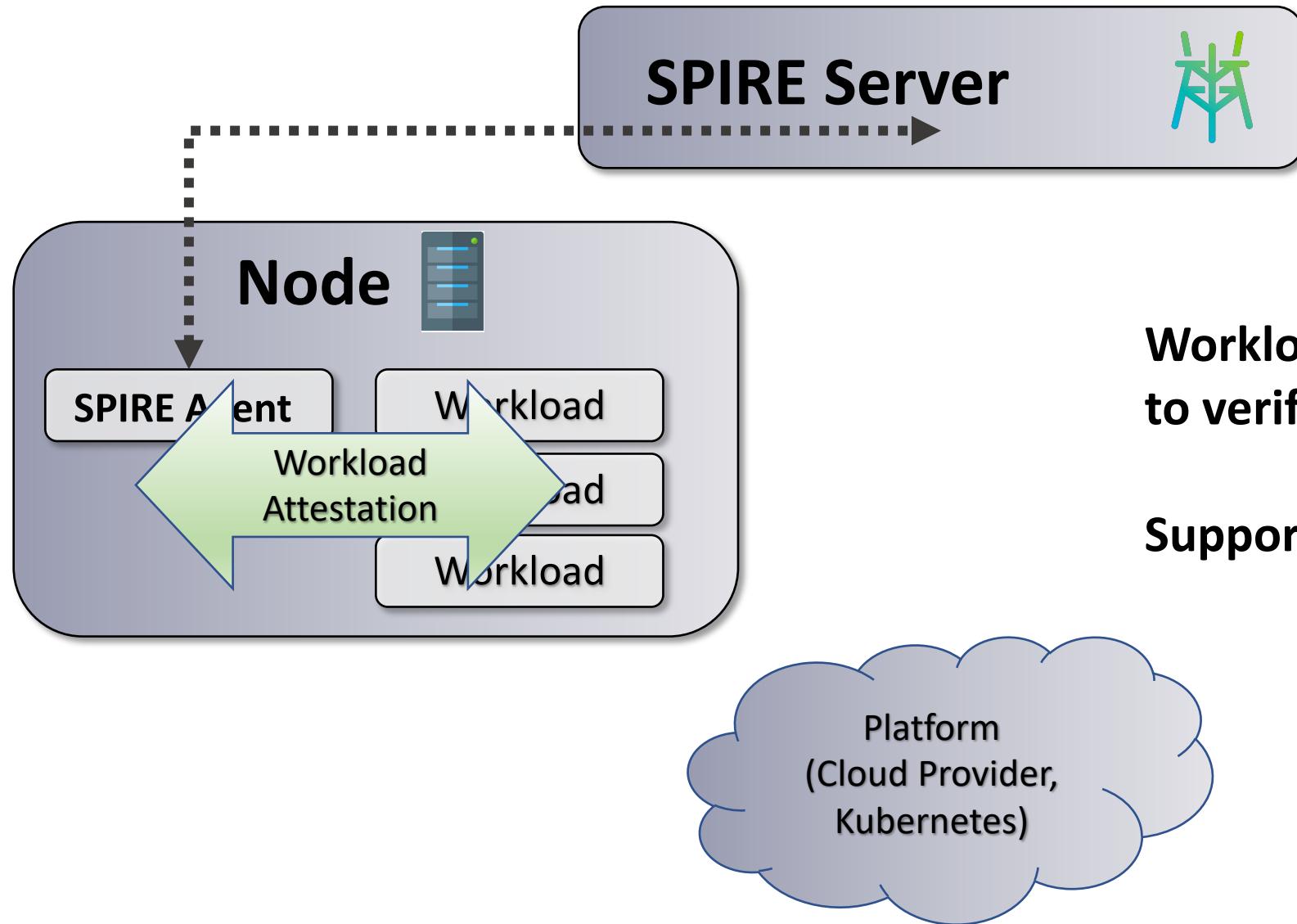
SPIRE (our implementation)



SPIRE (our implementation)



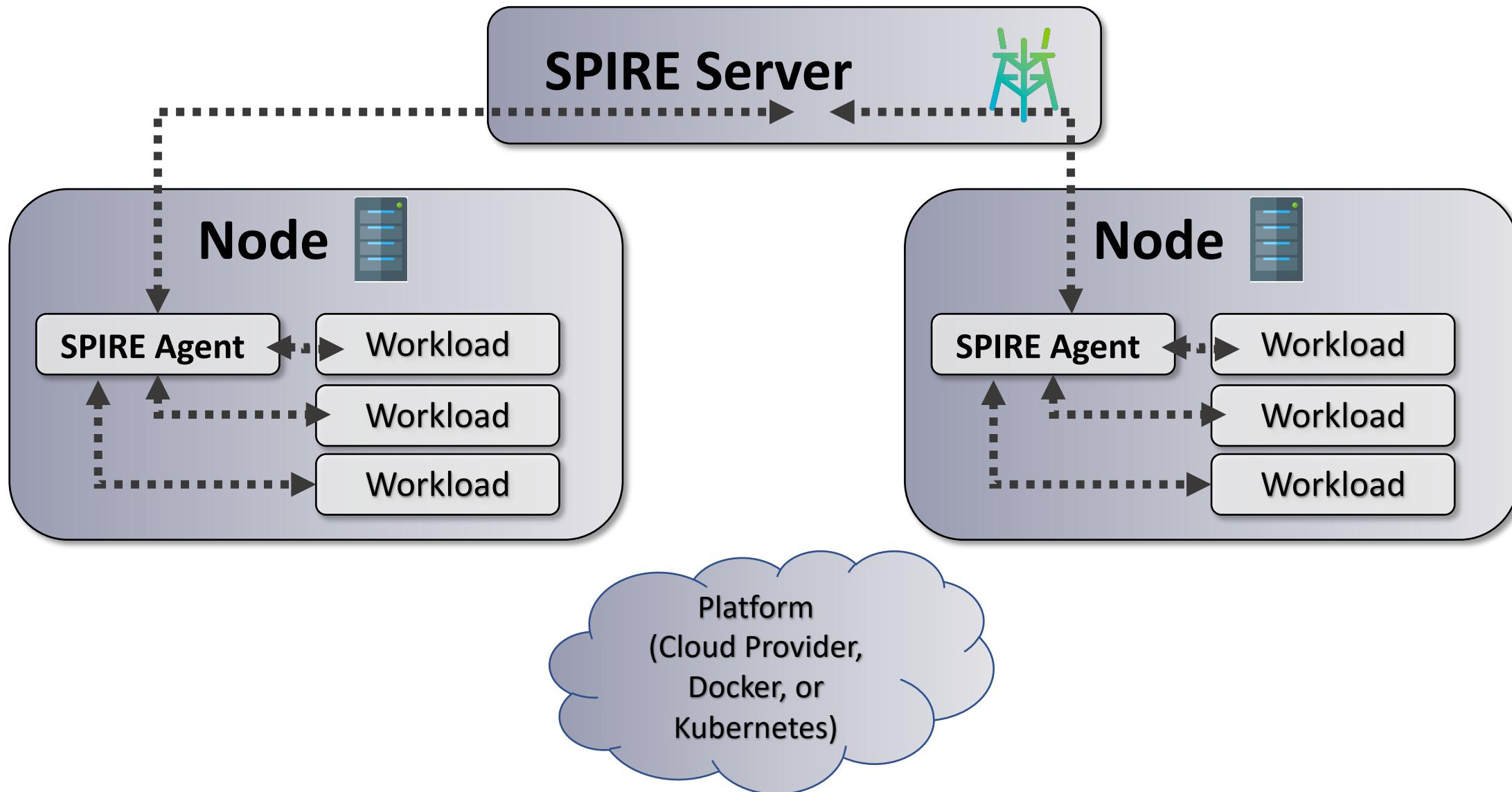
SPIRE (our implementation)



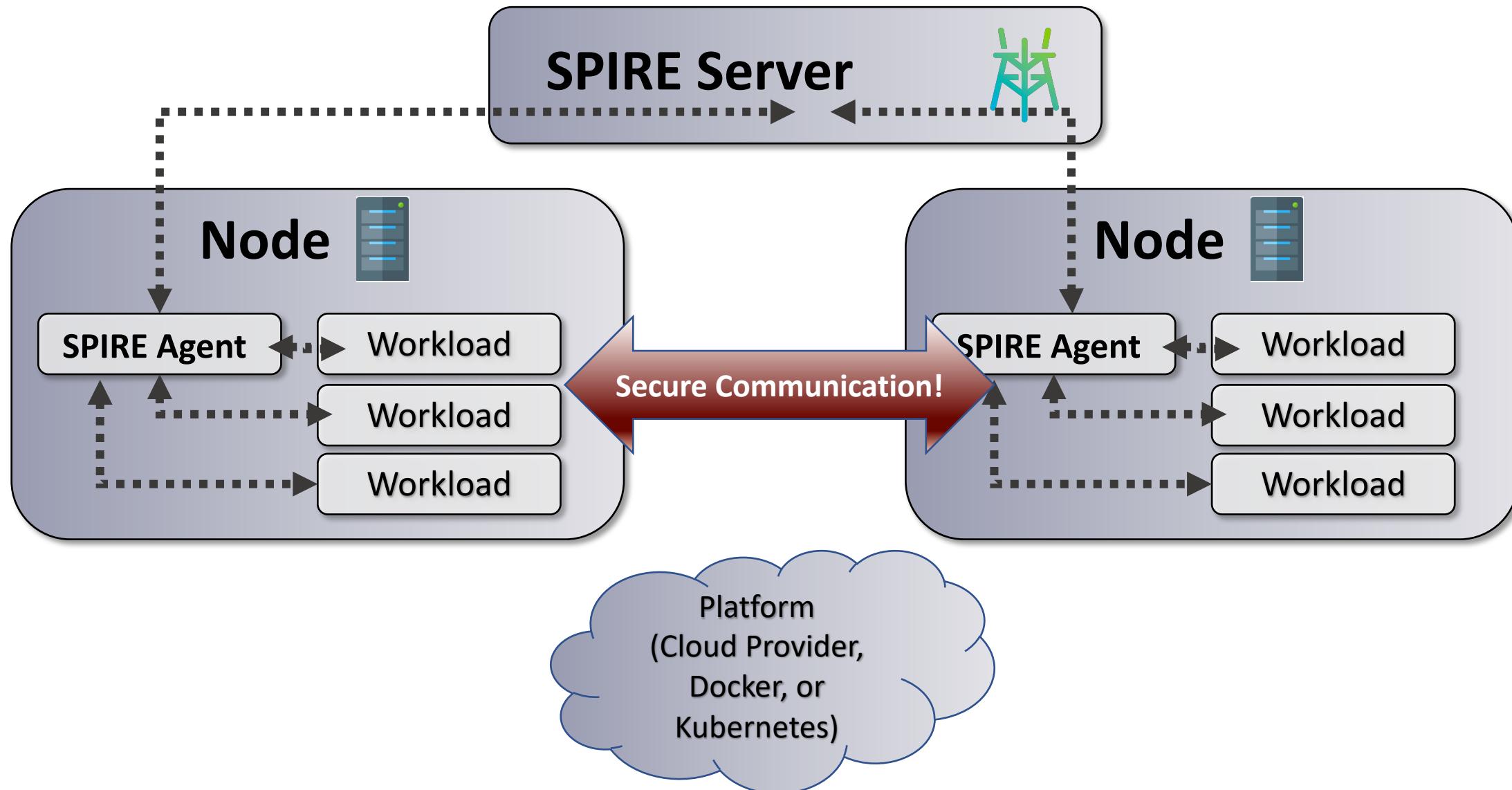
Workload attestation uses the kernel to verify the identity of the process

Supports Linux, BSD, Kubelet

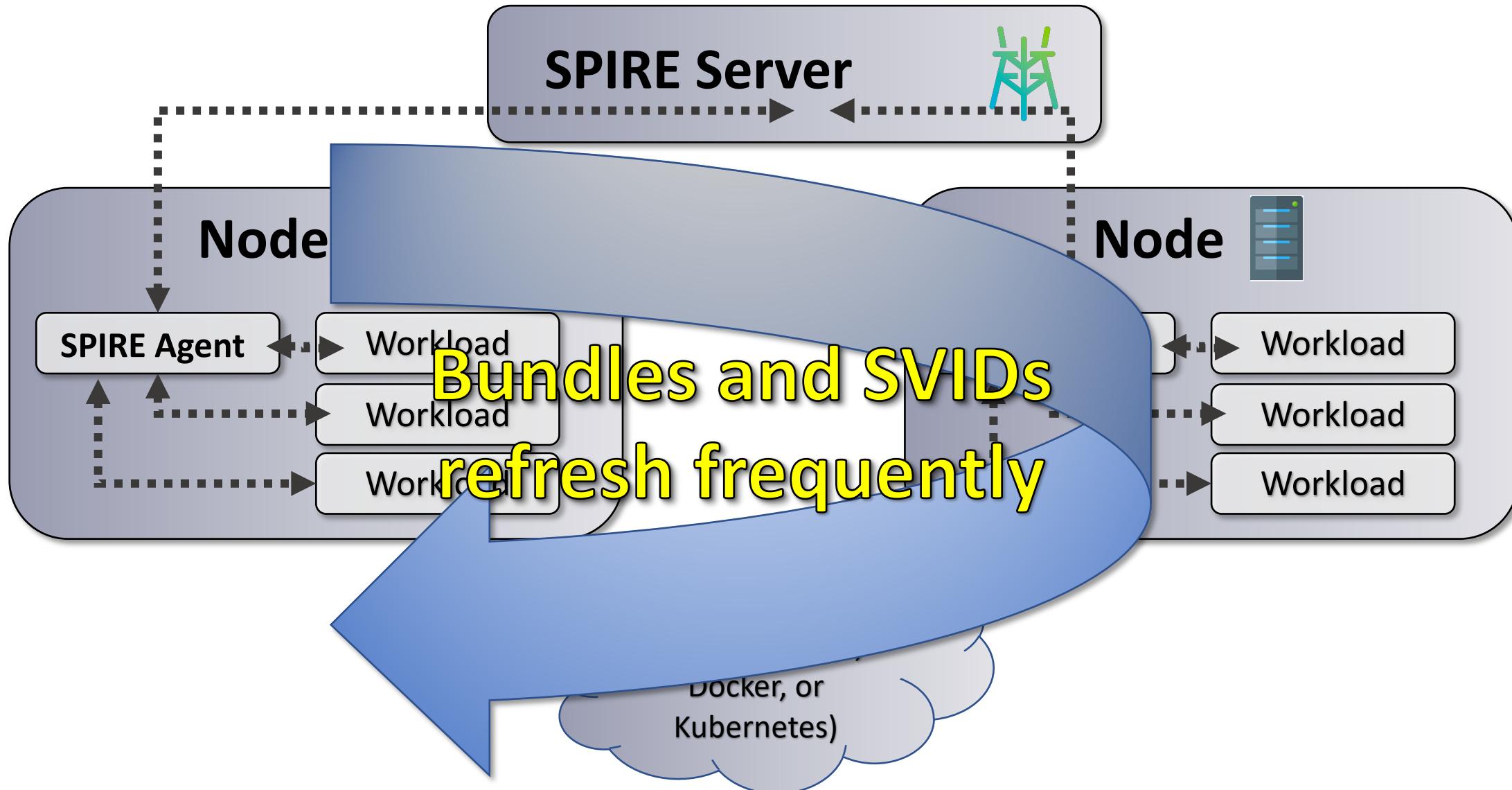
SPIRE (our implementation)



SPIRE (our implementation)



SPIRE (our implementation)



SPIRE (our implementation)

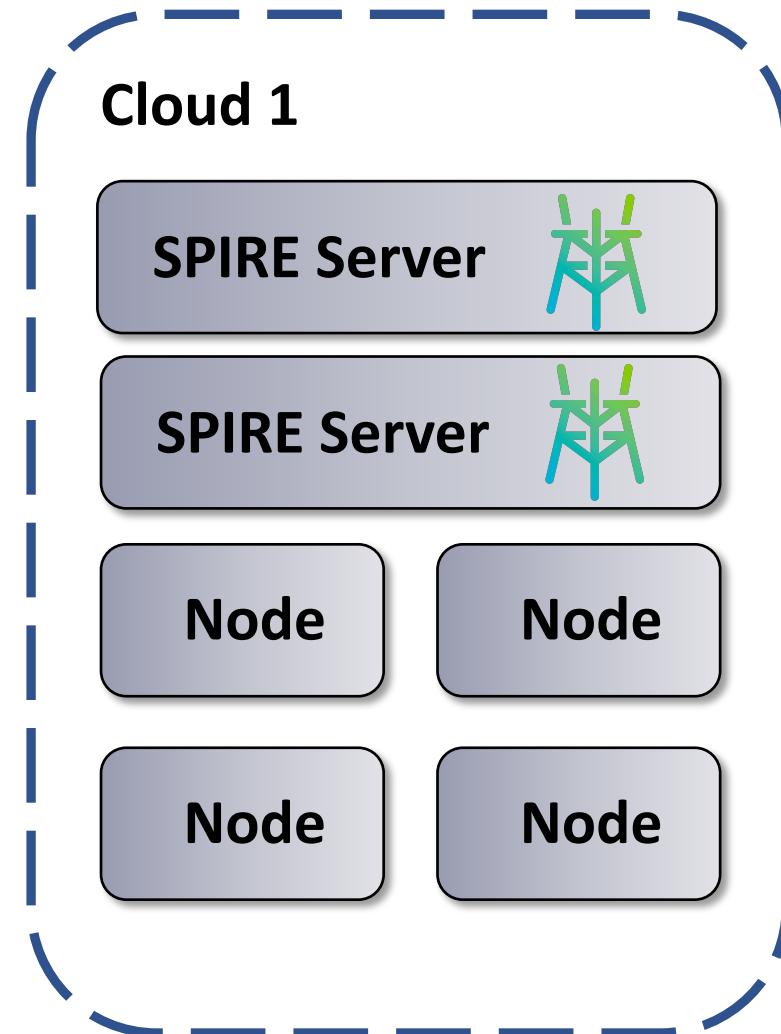


KubeCon

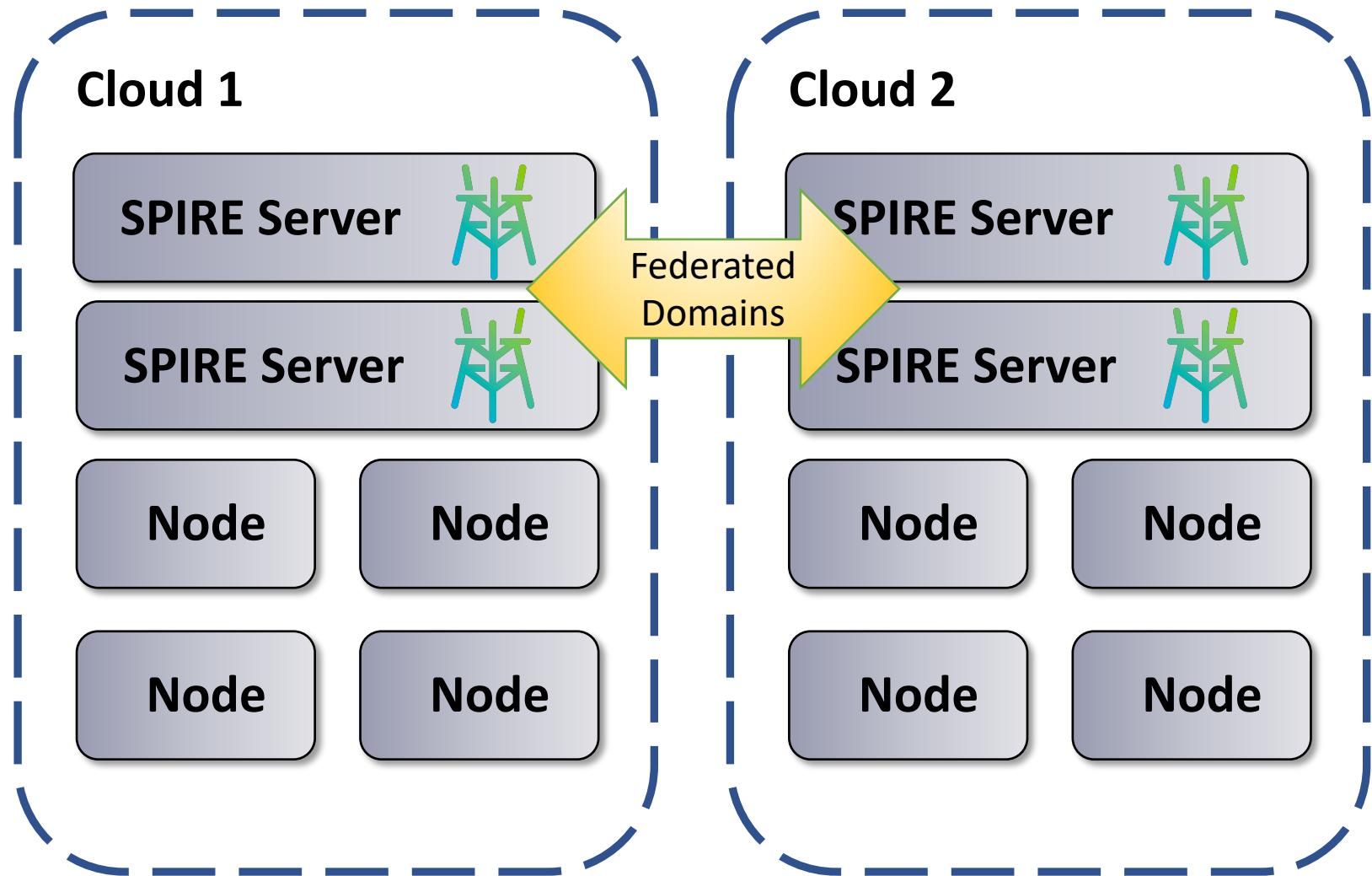


CloudNativeCon
Europe 2020

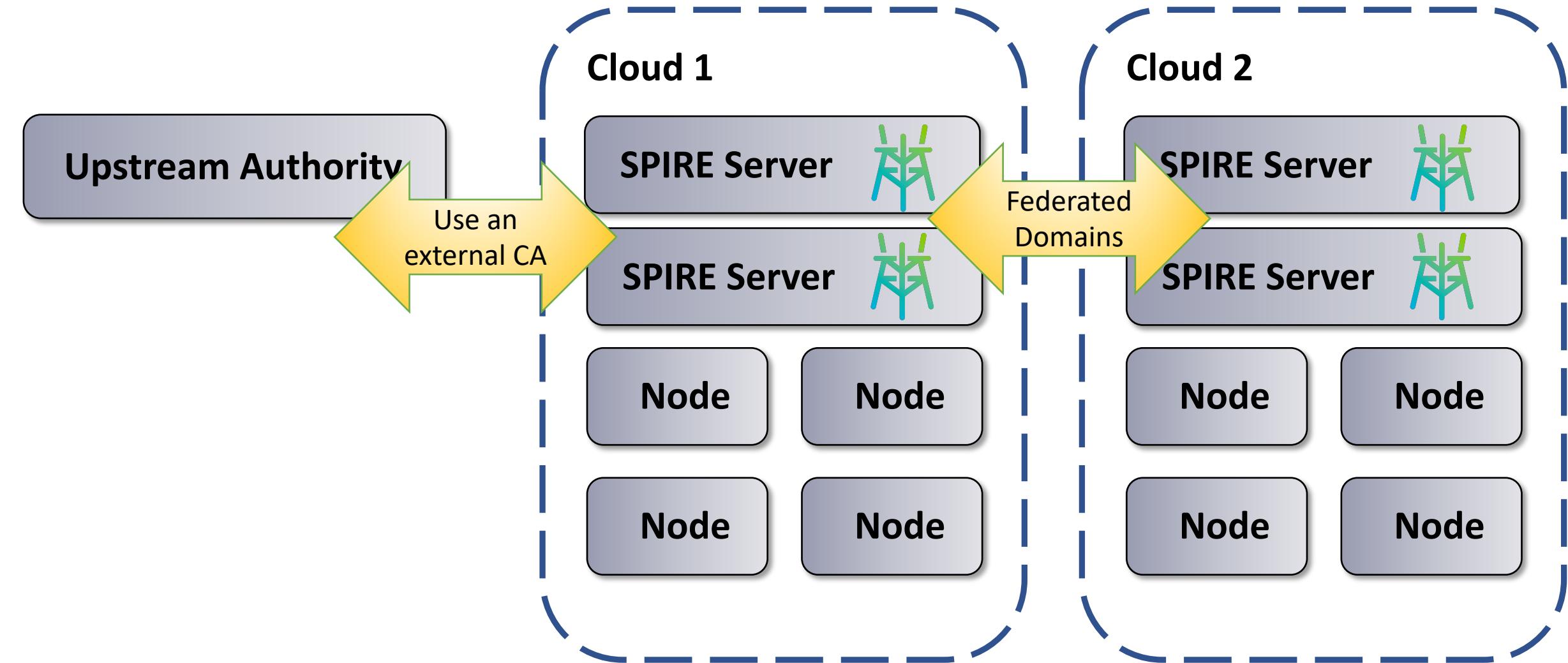
Virtual



SPIRE (our implementation)



SPIRE (our implementation)



SPIRE (our implementation)



KubeCon



CloudNativeCon

Europe 2020

Virtual

- Why do I need one SPIRE Agent per node?

SPIRE (our implementation)



KubeCon



CloudNativeCon
Europe 2020

Virtual

- Why do I need one SPIRE Agent per node?
- What if the SPIRE Agent is compromised?

- Why do I need one SPIRE Agent per node?
- What if the SPIRE Agent is compromised?
- What about my old workload that I don't want to change?

- Why do I need one SPIRE Agent per node?
- What if the SPIRE Agent is compromised?
- What about my old workload that I don't want to change?
- How do I specify which workloads get which SPIFFE IDs?

Registration Entries

Node Registration Entry

If a node has:

The aws tag “database”

Then give it the SPIFFE ID:

spiffe://mycompany/database

Registration Entries

Node Registration Entry

If a node has:

The aws tag “database”

Then give it the SPIFFE ID:

spiffe://mycompany/database

Workload Registration Entry

If a workload has:

The parent ID spiffe://mycompany/database

The UID “payments”

Then give it the SPIFFE ID:

spiffe://mycompany/database/payments

SPIRE (our implementation)



KubeCon



CloudNativeCon
Europe 2020

Virtual

- Why do I need one SPIRE Agent per node?
- What if the SPIRE Agent is compromised?
- What about my old workload that I don't want to change?
- How do I specify which workloads get which SPIFFE IDs?
- What if the SPIRE Server goes down?

SPIRE Ecosystem



KubeCon



CloudNativeCon

Europe 2020

Virtual

[bloomberg / spire-tpm-plugin](#)

Watch 6 Star 29 Fork 4

Code Issues 2 Pull requests 1 Actions Security Insights

master Go to file Add file Code

 pawalt Merge pull request #10 from bloombe... ... ✓ on May 22 18

ci add tests 3 months ago

cmd move agent/server logic to pkg 3 months ago

pkg add comments to common_test files 2 months ago

About

Provides agent and server plugins for SPIRE to allow TPM 2-based node attestation.

spiffe spire tpm2
tpm-attestation

SPIRE Ecosystem



KubeCon



CloudNativeCon

Europe 2020

Virtual

The screenshot shows two GitHub repository pages side-by-side.

Left Repository: spire-tpm-plugin

- Owner: bloomberg
- Name: spire-tpm-plugin
- Watched by 6 users
- 29 stars
- 4 forks
- Code tab is selected
- Issues: 2
- Pull requests: 1
- Actions, Security, Insights tabs are present
- Branch: master
- Last commit by pawalt: Merge pull request #10 from bloomber...
- Commits: ci, cmd, pkg

Right Repository: vault-auth-spire

- Owner: bloomberg
- Name: vault-auth-spire
- Watched by 6 users
- 22 stars
- 5 forks
- Code tab is selected
- Actions, Security, Insights tabs are present
- Bloomberg logo: New York, NY
- 148 repositories, 50 members
- Last commit by dennisgove: Updates README with new co... on Nov 8, 2019 (21)
- Commits: cmd/plugin, internal/common, .gitignore

About

vault-auth-spire is an authentication plugin for Hashicorp Vault which allows logging into Vault using a Spire provided SVID.

Tags: spire, plugin, authn

SPIRE Ecosystem



KubeCon



CloudNativeCon

Europe 2020

Virtual

The screenshot shows three GitHub repository pages overlaid:

- bloomberg / spire-tpm-plugin**: Watched by 6 users, 29 stars, 4 forks. Issues: 2, Pull requests: 1. Shows a merge pull request from pawalt.
- bloomberg / vault-auth-spire**: Watched by 6 users, 22 stars, 5 forks. Shows a commit from dennisgove.
- github / emissary**: Watched by 72 users, 20 stars, 0 forks. Issues: 1. Shows a commit from joewilliams.

Next Steps



KubeCon



CloudNativeCon

Europe 2020

Virtual

Who's Using SPIFFE?

Anyone using Istio, Kuma, NSM, Consul Connect, Hamlet, or several other service mesh technologies is using at least part of SPIFFE!

Who's Using SPIRE?

ByteDance (TikTok)

Square

Bloomberg

Anthem (Health Insurance)

Uber

GitHub

Stripe

TransferWise

Others we don't know about....

Next Steps

Learn More:

Find out more at spiffe.io

Regular Community Days

Join the SPIFFE Slack: slack.spiffe.io

More Talks:

Evan Gilman – [Introduction to SPIFFE and SPIRE](#)

Andrew Harding – [Running SPIRE In Large Scale, Enterprise-Grade Environments](#)

[Building Zero Trust based Authentication in Healthcare with SPIRE](#)

SPIRE Deep Dives at [HPE Discover](#)

Contribute!



KubeCon



CloudNativeCon

Europe 2020

Virtual

Why Service Identity

Service Identity Approaches

SPIFFE (the standard)

SPIRE (the implementation)

Next Steps

Thank You!

[@d feldman](https://twitter.com/d_feldman)

dan.feldman@hpe.com

Time for Questions



KubeCon



CloudNativeCon

Europe 2020

Virtual



KEEP CLOUD NATIVE CONNECTED

