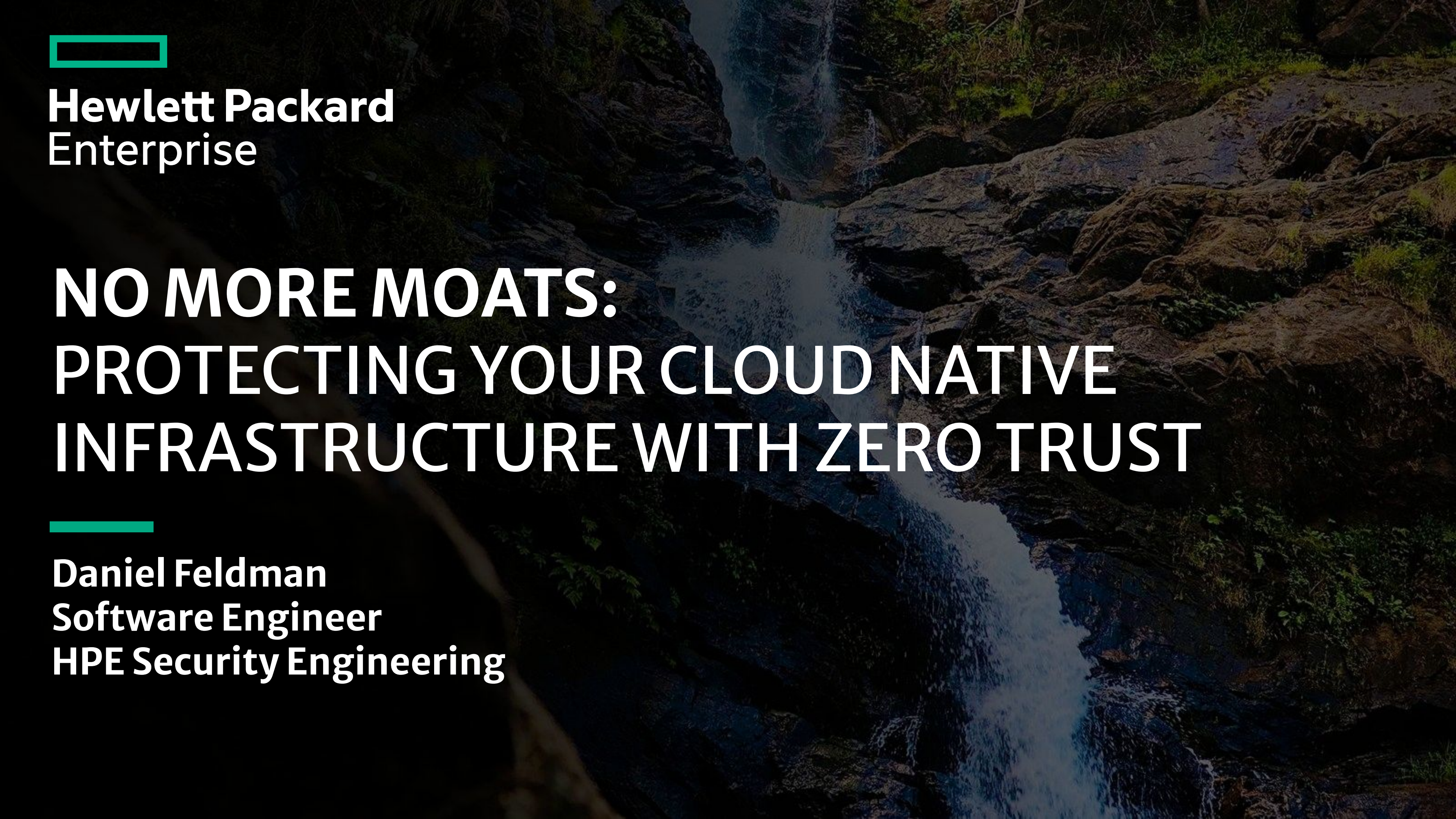


Hewlett Packard
Enterprise

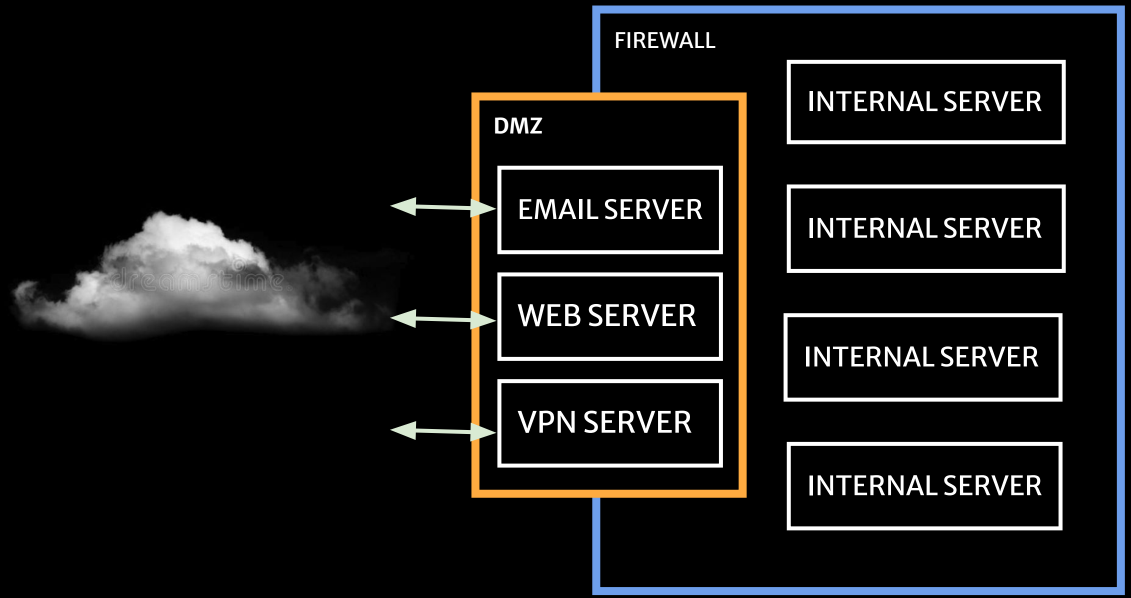
NO MORE MOATS:
PROTECTING YOUR CLOUD NATIVE INFRASTRUCTURE WITH ZERO TRUST

Daniel Feldman
Software Engineer
HPE Security Engineering

AGENDA

1. WHAT IS ZERO TRUST
2. SPIFFE AND SPIRE ARCHITECTURE
3. BUILDING SYSTEMS WITH SPIFFE AND SPIRE
4. ROADMAP
5. NEXT STEPS

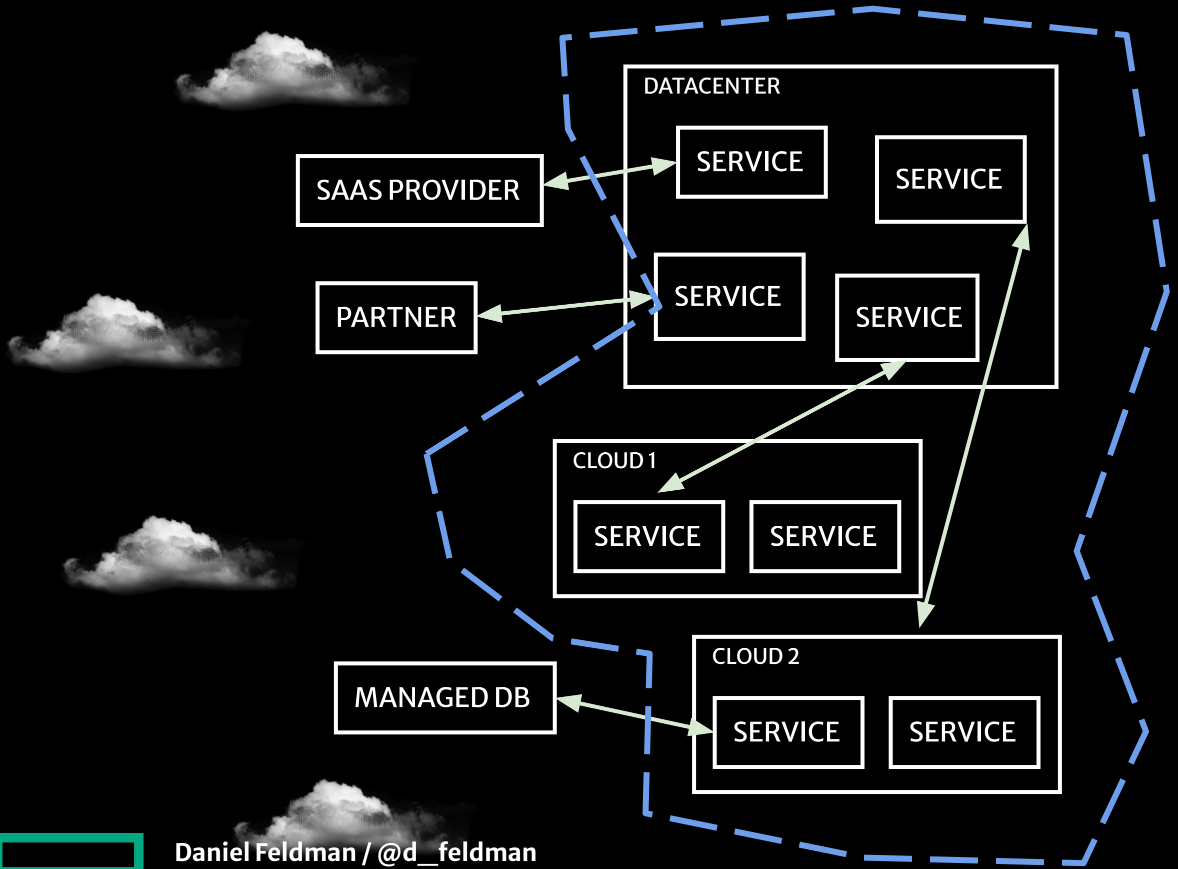
PERIMETER SECURITY



Everything inside the firewall is trusted.

Everything outside is untrusted

PERIMETER SECURITY



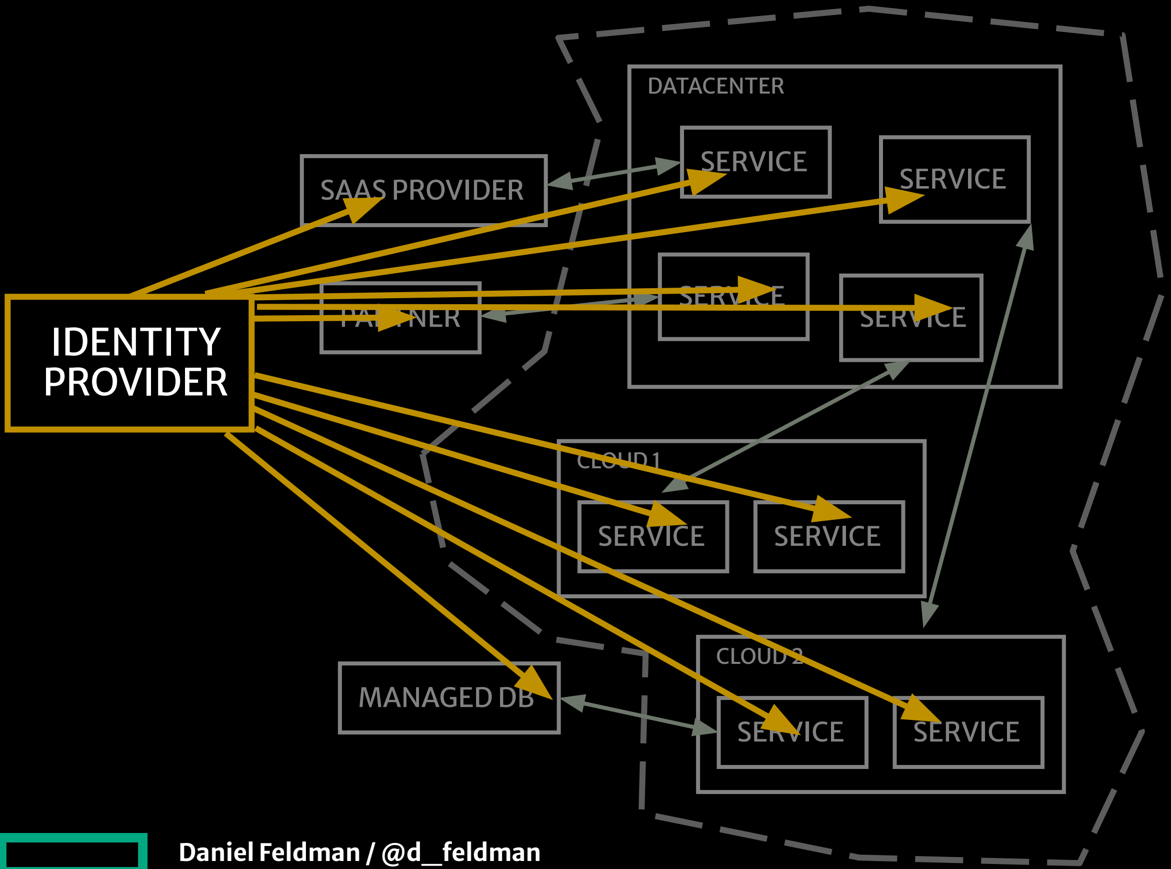
As we add:

- services
- datacenters
- clouds
- regions inside clouds

perimeter security becomes increasingly untenable

> We’re protecting 21st-century infrastructure with 14th-century technology!
>
> - *Frederick Kautz*

ZERO TRUST



Each service gets its own
- unique
- secure
- provable

identity

Daniel Feldman / @d__feldman

SPIFFE AND SPIRE

spiffe

Standard for applications to use a service identity provider

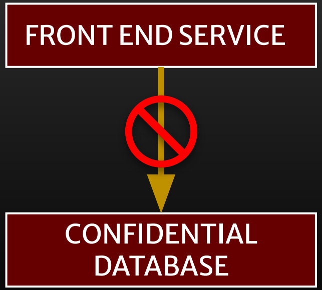
SPIRE

Production-ready implementation of SPIFFE

KEY BENEFITS OF ZERO TRUST

DEFENSE IN DEPTH

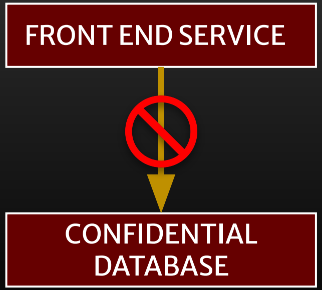
If one service is compromised, attackers can't move laterally within the network.



KEY BENEFITS OF ZERO TRUST

DEFENSE IN DEPTH

If one service is compromised, attackers can’t move laterally within the network.



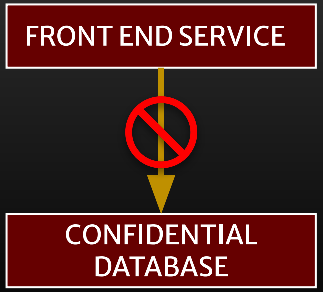
REDUCE SECURITY OVERHEAD

Security teams don’t have to maintain perimeters and manually create and rotate credentials.

KEY BENEFITS OF ZERO TRUST

DEFENSE IN DEPTH

If one service is compromised, attackers can't move laterally within the network.

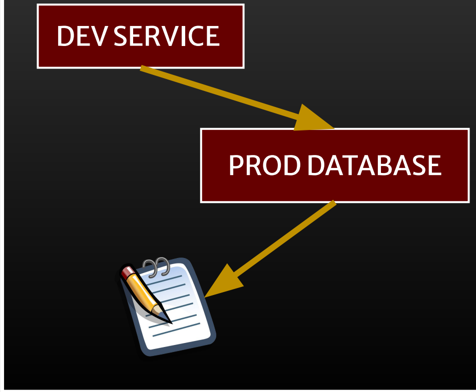


REDUCE SECURITY OVERHEAD

Security teams don't have to maintain perimeters and manually create and rotate credentials.

OBSERVABILITY AND LOGGING

Services can't operate without an explicit identity, which can be logged



AGENDA

1. WHAT IS ZERO TRUST
2. SPIFFE AND SPIRE ARCHITECTURE
3. BUILDING SYSTEMS WITH SPIFFE AND SPIRE
4. ROADMAP
5. NEXT STEPS

SPIFFE AND SPIRE

spiffe

Standard for applications to use a service identity provider

SPIRE

Production-ready implementation of SPIFFE

SPIFFE IN FOUR PIECES

SPIFFE ID

Standard format for a service identifier

```
spiffe://trustdomain/service
```

SPIFFE IN FOUR PIECES

SPIFFE ID

Standard format for a service identifier

```
spiffe://trustdomain/service
```

SPIFFE VERIFIABLE IDENTITY DOCUMENT

(SVID)

Cryptographically verifiable document asserting a SPIFFE ID

SPIFFE IN FOUR PIECES

SPIFFE ID

Standard format for a service identifier

`spiffe://trustdomain/service`

SPIFFE VERIFIABLE IDENTITY DOCUMENT

(SVID)

Cryptographically verifiable document asserting a SPIFFE ID

TRUST BUNDLE

Set of public keys used to verify SVIDs

SPIFFE IN FOUR PIECES

SPIFFE ID

Standard format for a service identifier

`spiffe://trustdomain/service`

SPIFFE VERIFIABLE IDENTITY DOCUMENT

(SVID)

Cryptographically verifiable document asserting a SPIFFE ID

TRUST BUNDLE

Set of public keys used to verify SVIDs

WORKLOAD API

Local API for workloads to retrieve their SPIFFE IDs, SVIDs, and Trust Bundles

SPIFFE IN FOUR PIECES

SPIFFE ID

Standard forn

`spiffe://`

SPIFFE VERIFIABLE IDENTITY DOCUMENT

t asserting a

TRU

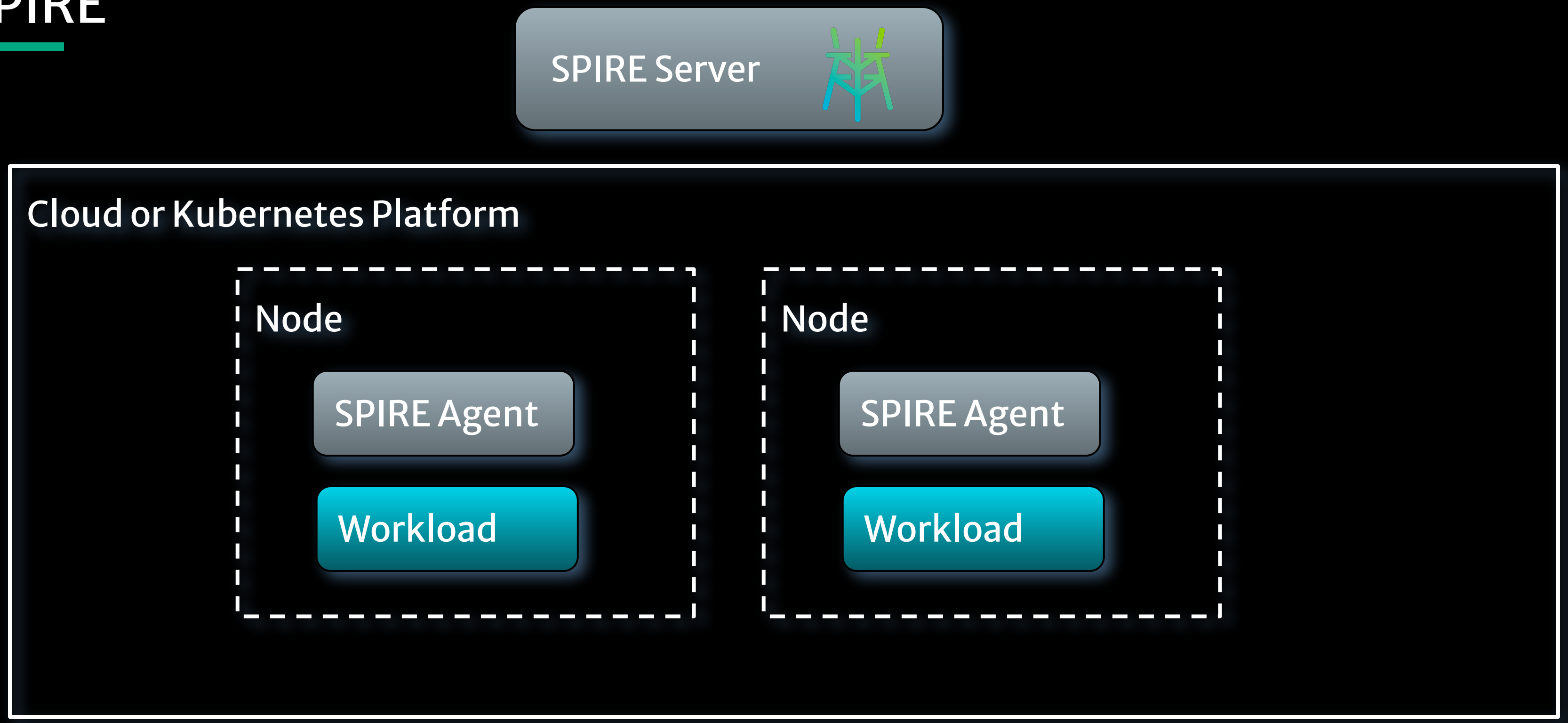
Set of public

PI

etrieve their SPIFFE IDs, SVIDs, and Trust Bundles

SVIDs and Trust Bundles expire frequently (every few hours) for improved security

SPIRE


SPIRE Server

Cloud or Kubernetes Platform

Node

SPIRE Agent

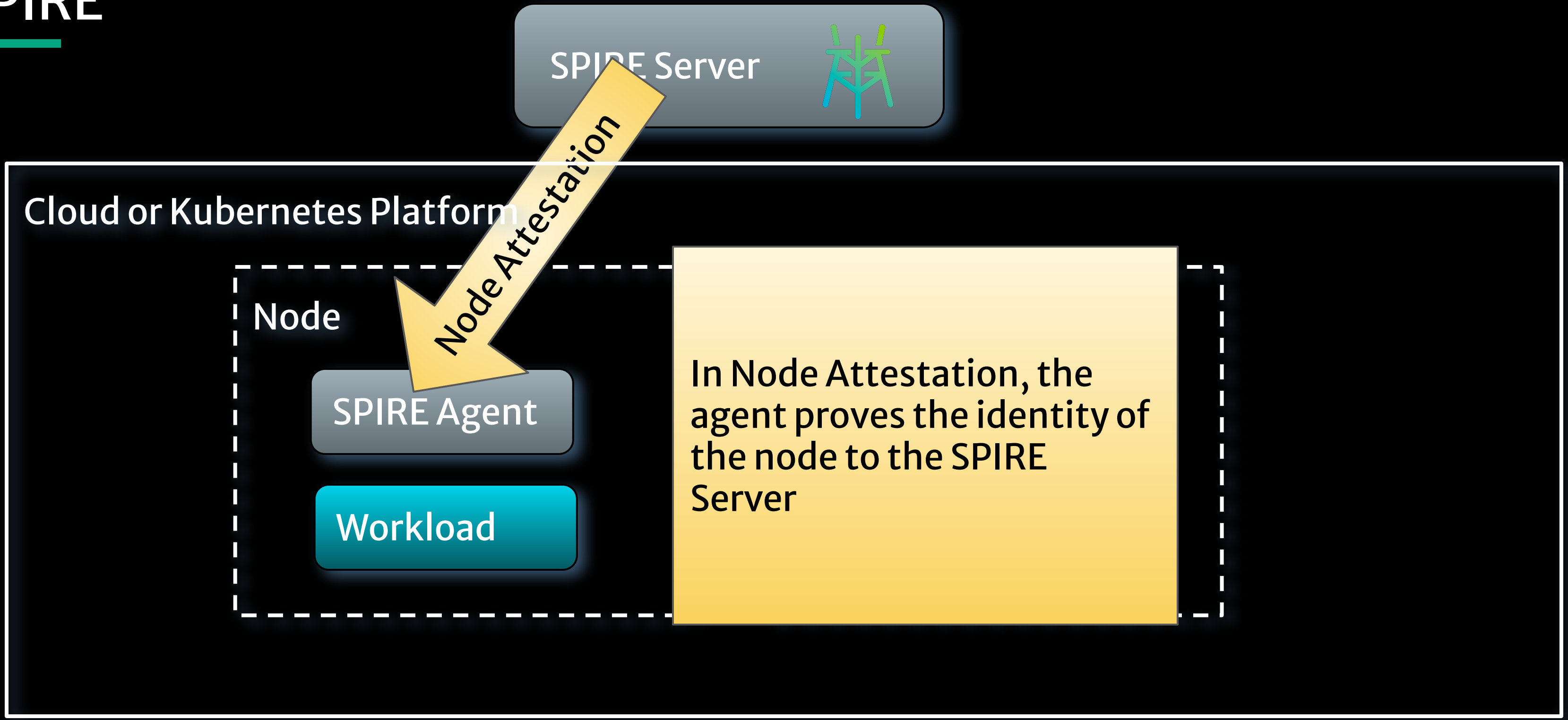
Workload

Node

SPIRE Agent

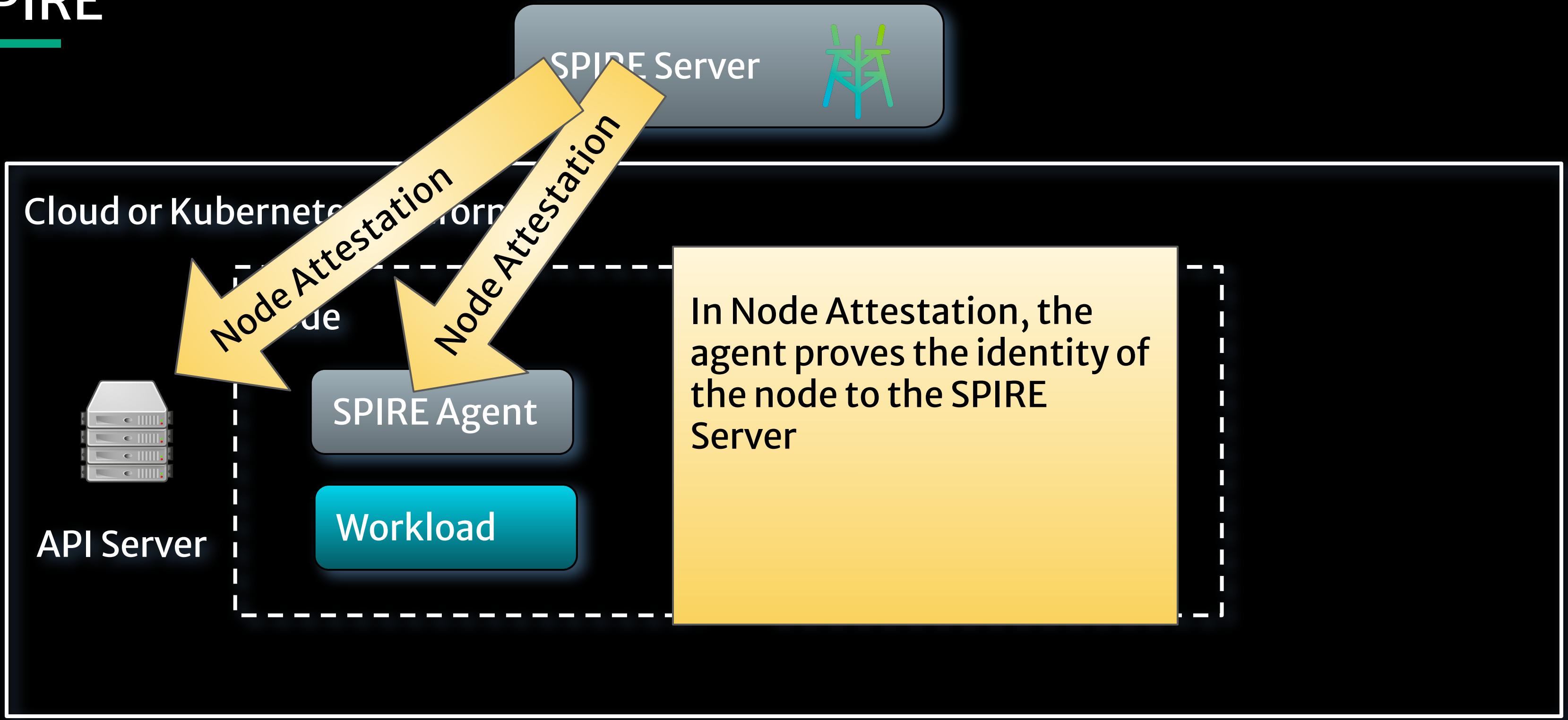
Workload

SPIRE



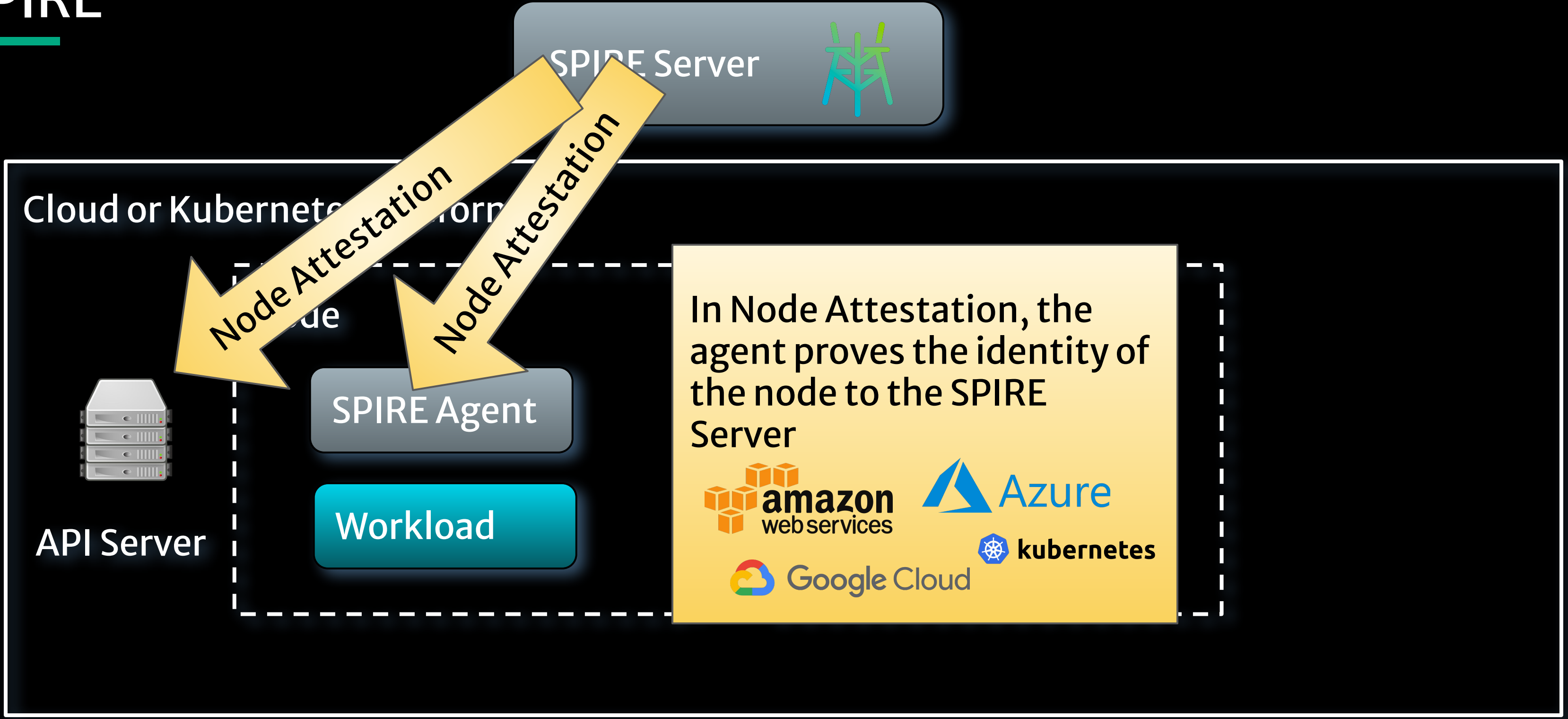
In Node Attestation, the agent proves the identity of the node to the SPIRE Server

SPIRE



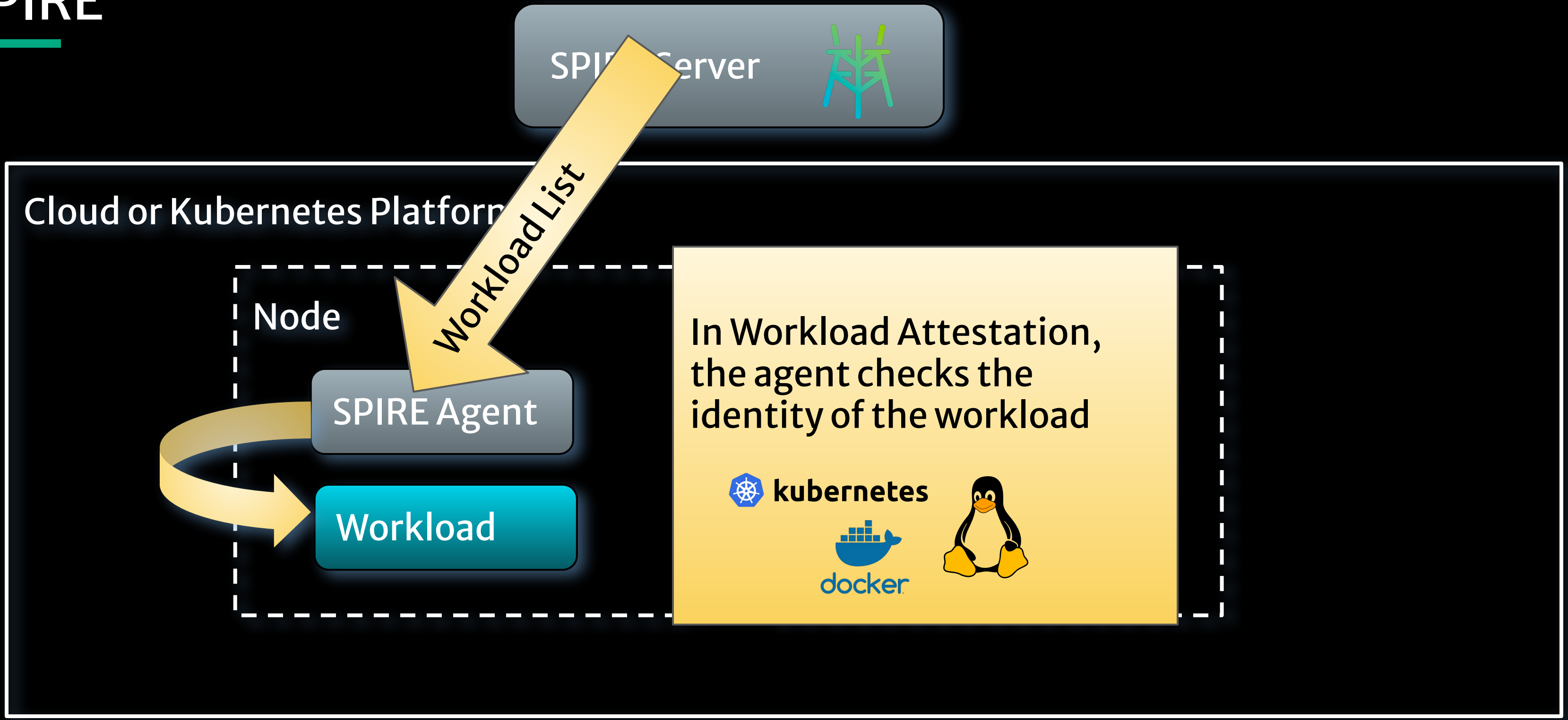
In Node Attestation, the agent proves the identity of the node to the SPIRE Server

SPIRE



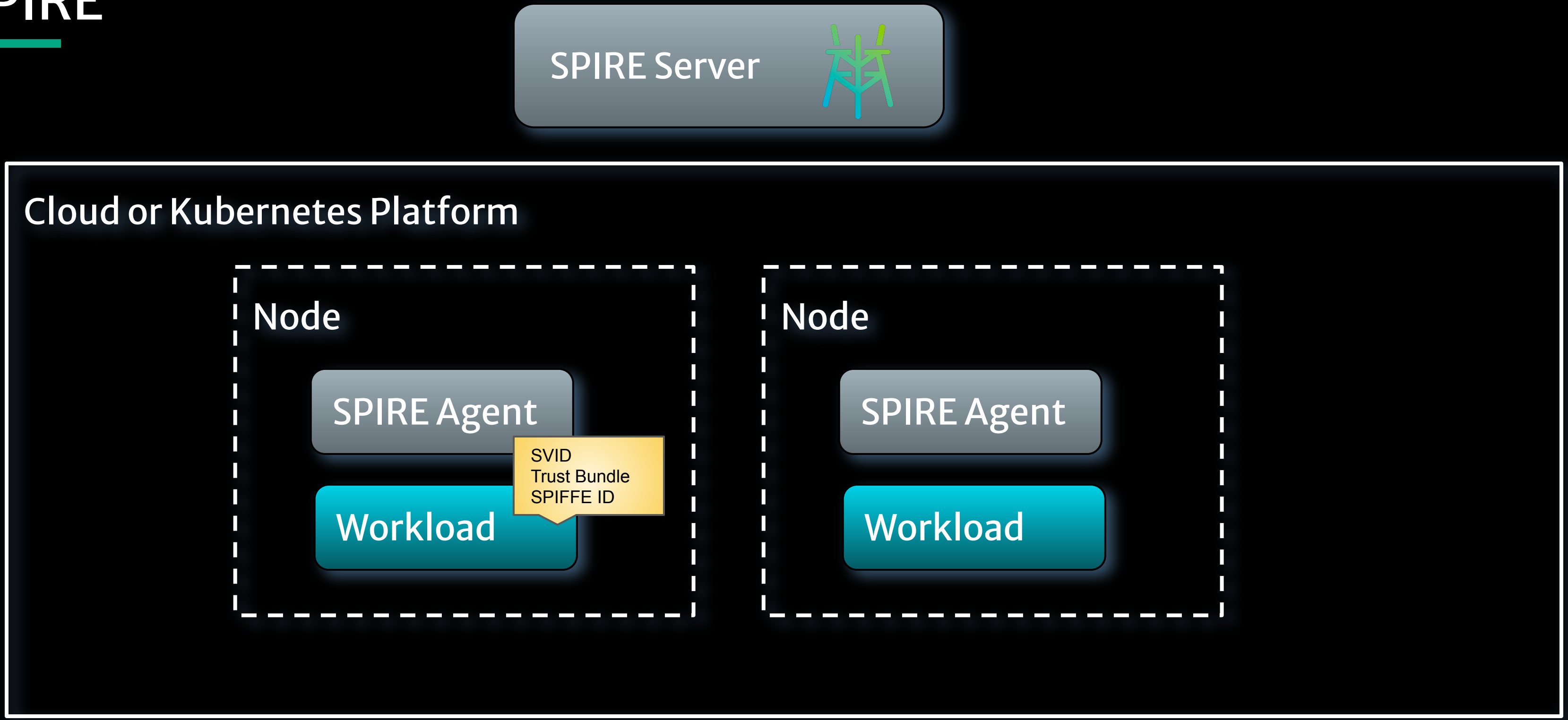
In Node Attestation, the agent proves the identity of the node to the SPIRE Server

SPIRE

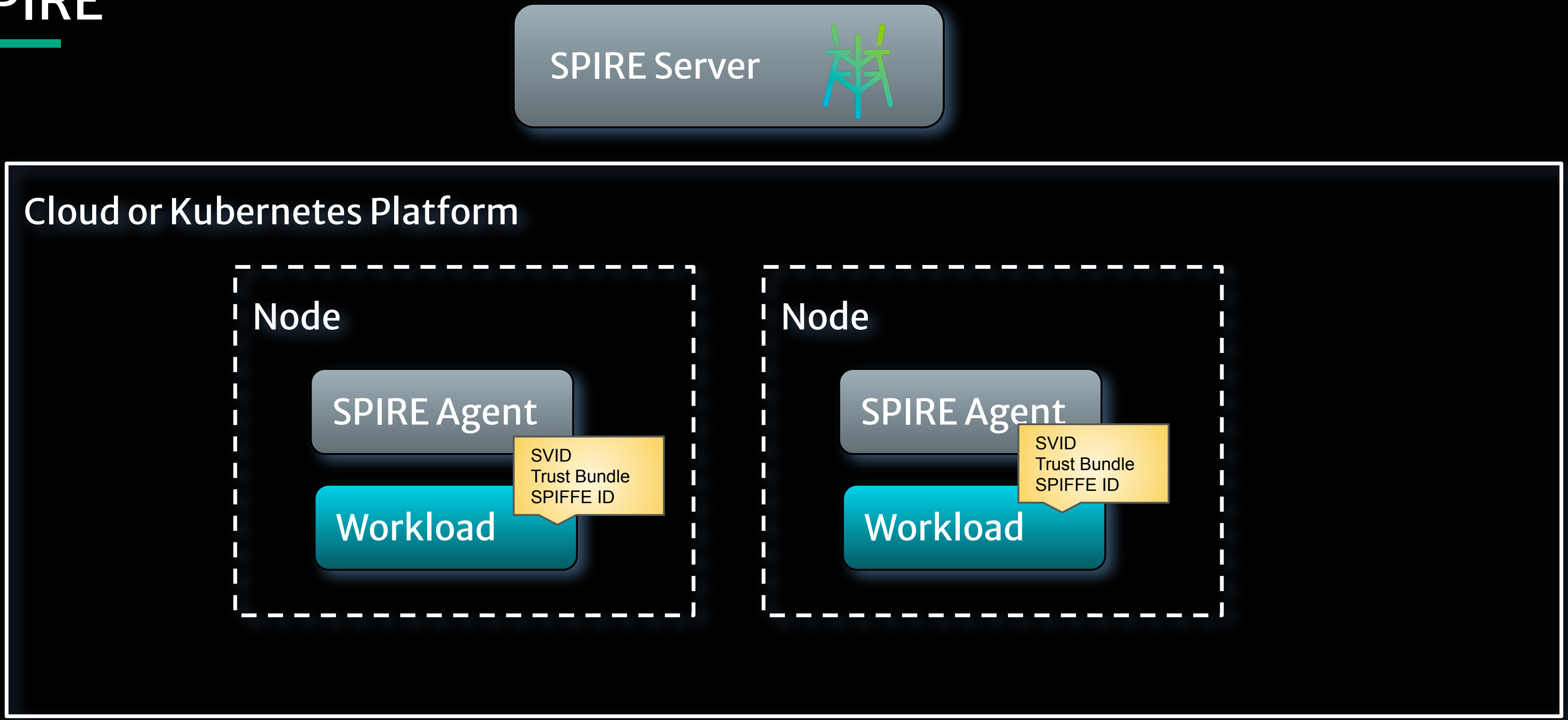


In Workload Attestation, the agent checks the identity of the workload

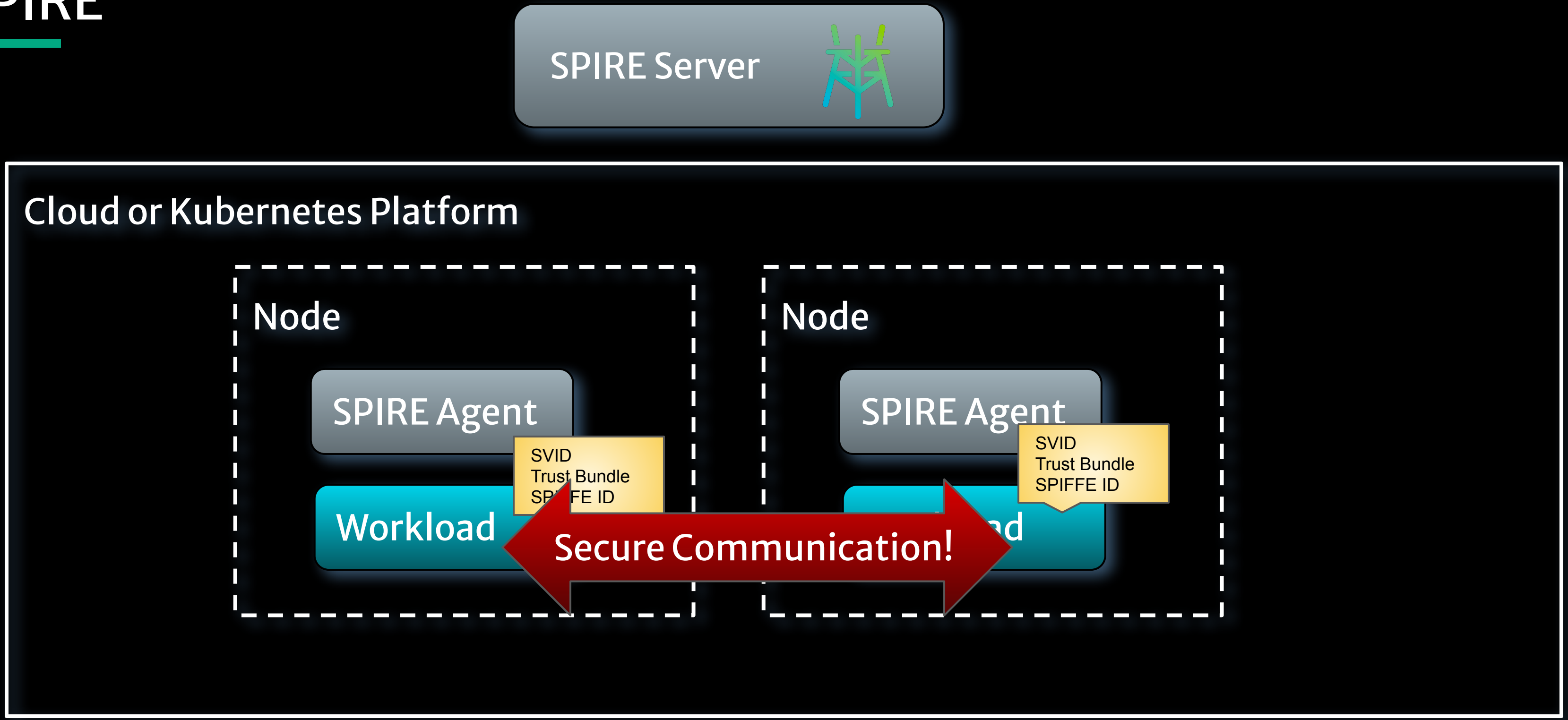
SPIRE


SPIRE Server
Cloud or Kubernetes Platform
Node
SPIRE Agent
SVID
Trust Bundle
SPIFFE ID
Workload
Node
SPIRE Agent
Workload

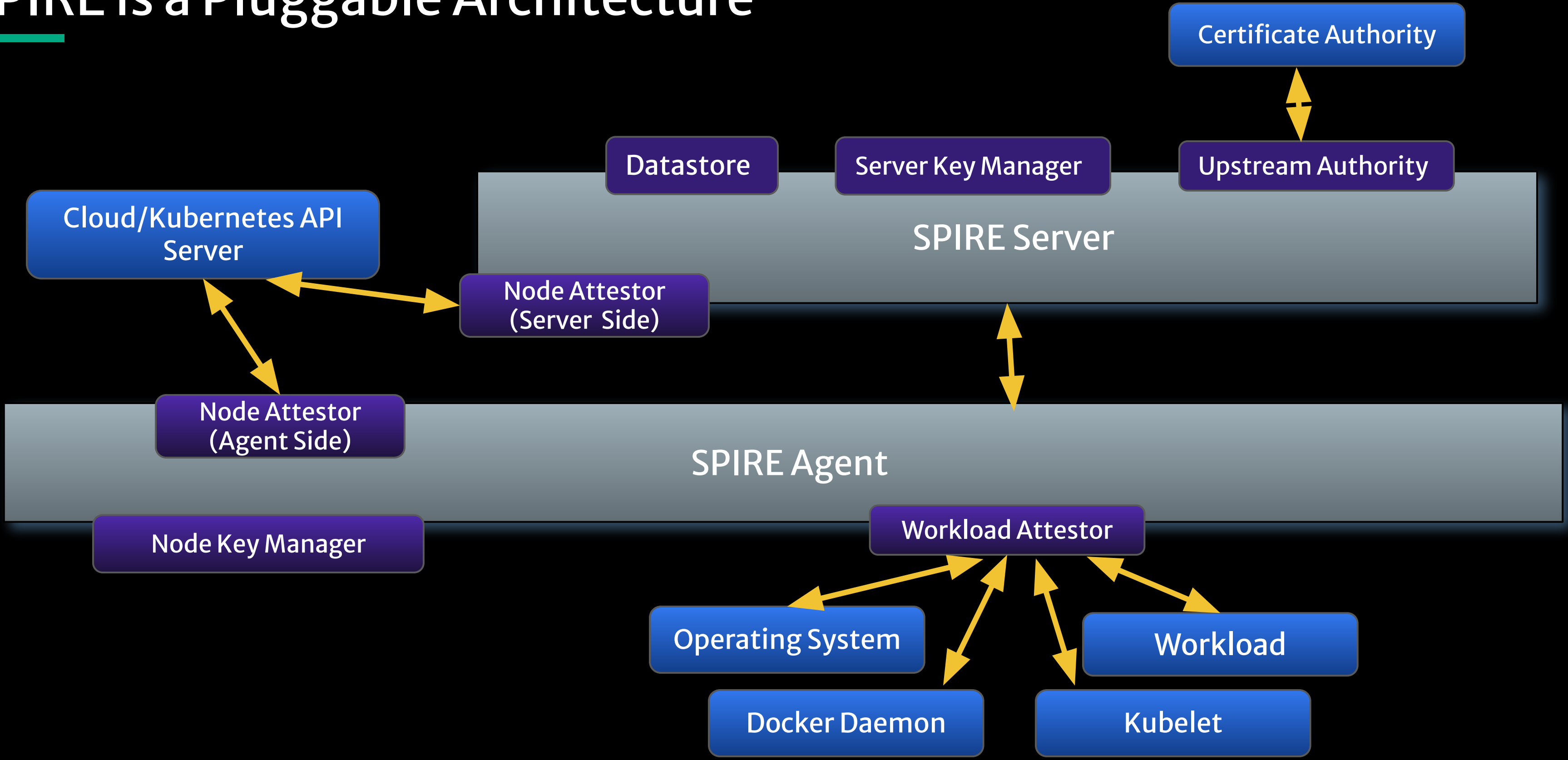
SPIRE


SPIRE Server
Cloud or Kubernetes Platform
Node
SPIRE Agent
SVID
Trust Bundle
SPIFFE ID
Workload
Node
SPIRE Agent
SVID
Trust Bundle
SPIFFE ID
Workload

SPIRE

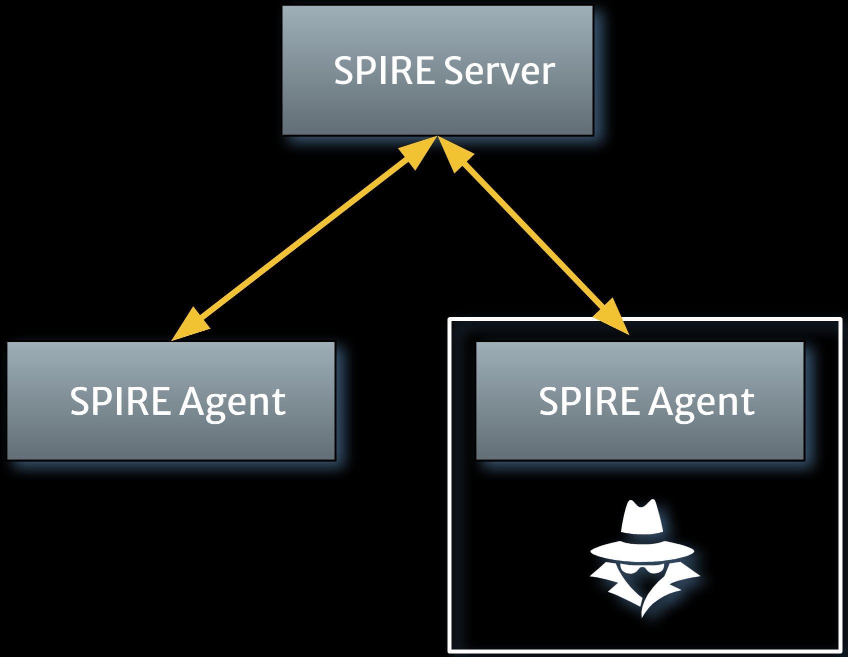

SPIRE Server
Cloud or Kubernetes Platform
Node
SPIRE Agent
SVID
Trust Bundle
SPIFFE ID
Workload
Node
SPIRE Agent
SVID
Trust Bundle
SPIFFE ID
Workload
Secure Communication!

SPIRE is a Pluggable Architecture

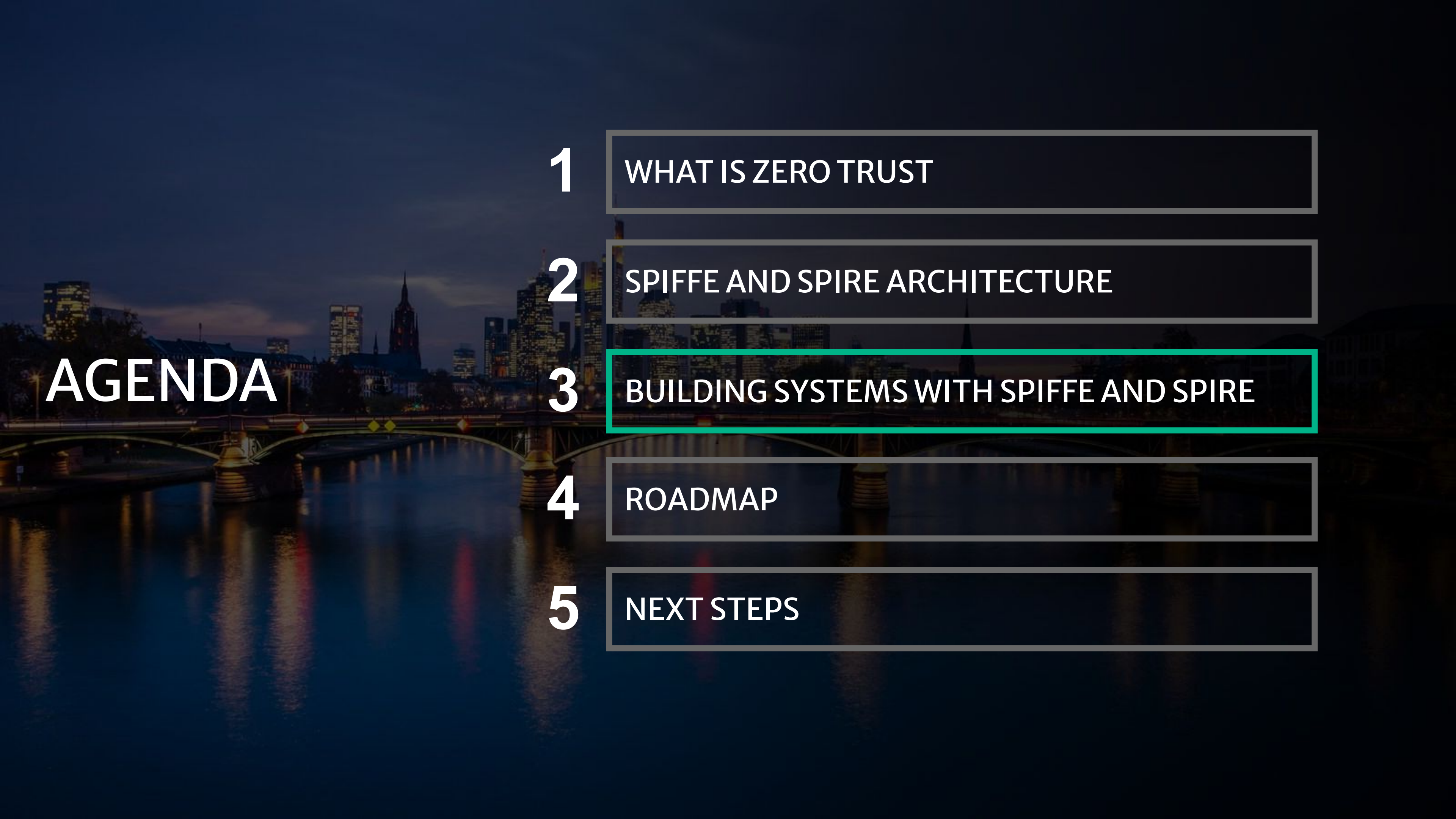


Daniel Feldman / @d__feldman

SPIRE is Defense in Depth



Even if one agent is compromised, it can’t issue identities assigned to the other agents



AGENDA

1 WHAT IS ZERO TRUST

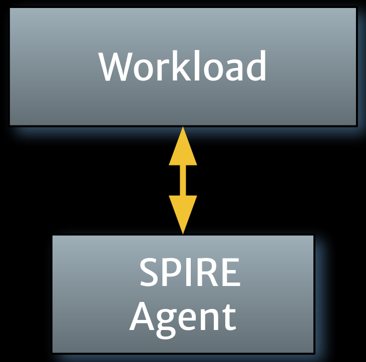
2 SPIFFE AND SPIRE ARCHITECTURE

3 BUILDING SYSTEMS WITH SPIFFE AND SPIRE

4 ROADMAP

5 NEXT STEPS

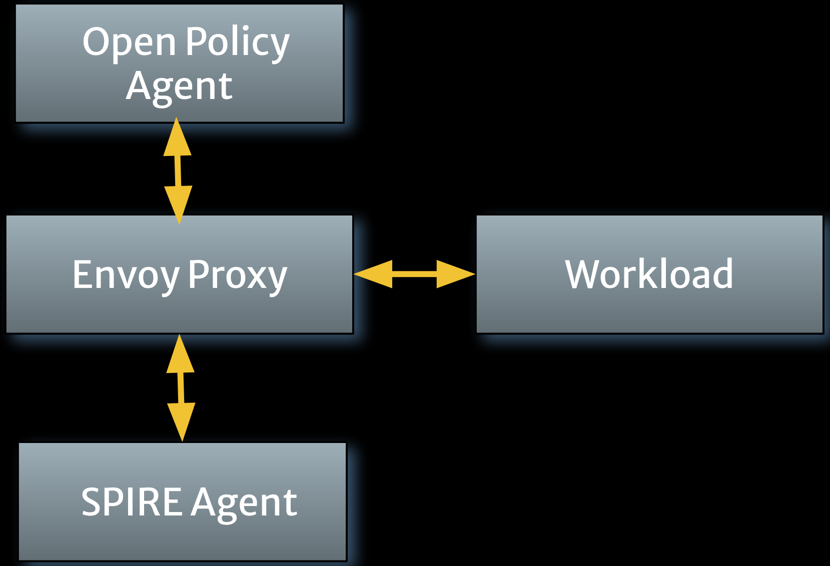
Three Ways to Use SPIFFE



DIRECT WORKLOAD API ACCESS

We have libraries for Java and Go (Python planned)

Three Ways to Use SPIFFE

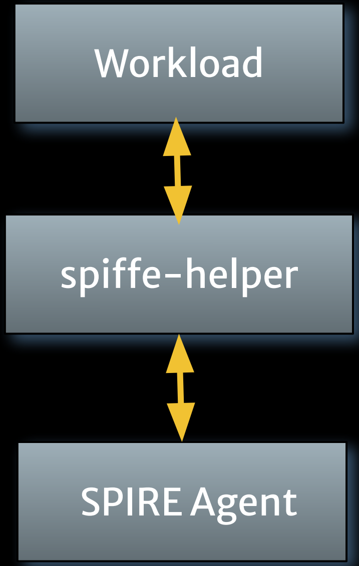


SIDECAR PROXY

Envoy can integrate with SPIRE.

Optionally, you can use Open Policy Agent (OPA) to make complex authorization rules.

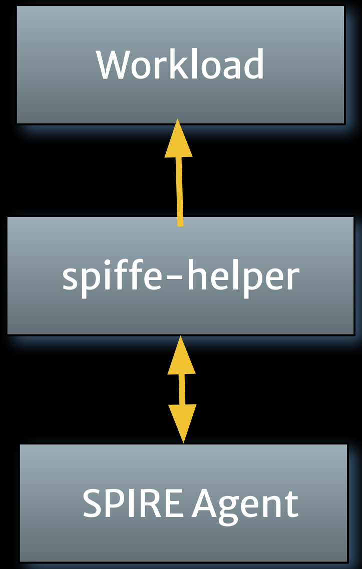
Three Ways to Use SPIFFE



SPIFFE HELPER

The SPIFFE Helper can put SPIFFE certificates and trust bundles in files that are compatible with non-SPIFFE-aware workloads.

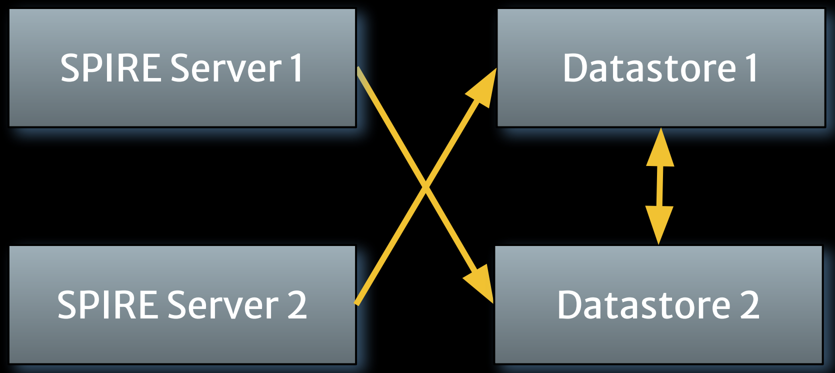
Three Ways to Use SPIFFE



SPIFFE HELPER

The SPIFFE Helper can put SPIFFE certificates and trust bundles in files that are compatible with non-SPIFFE-aware workloads.

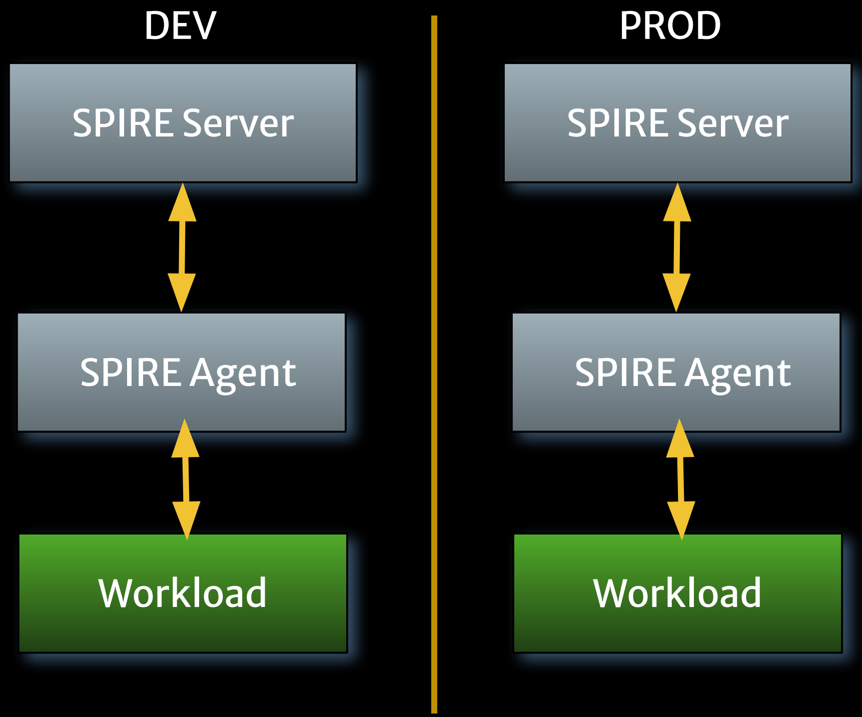
Zero Trust Design Patterns



HIGH AVAILABILITY

SPIRE stores all its data in an external datastore. If this is a distributed database, the SPIRE server can be an active-active high availability cluster.

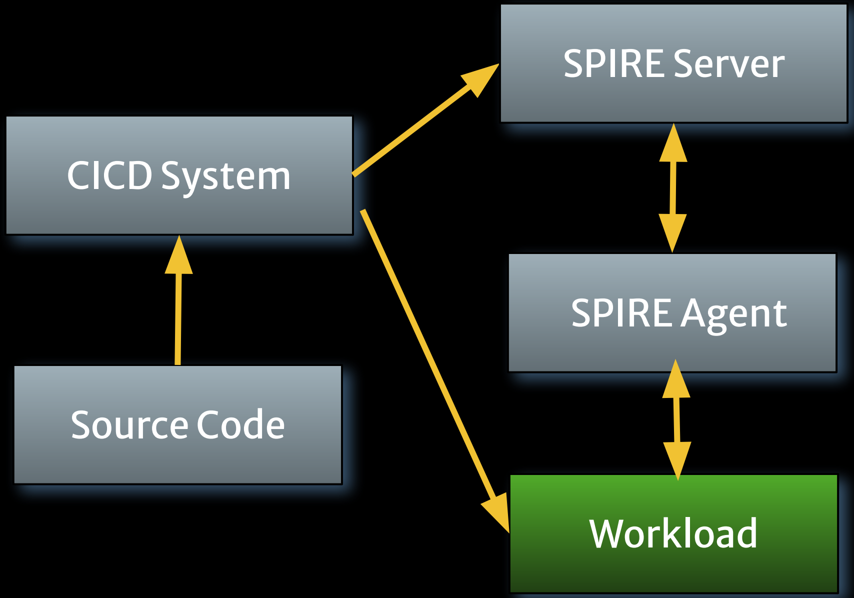
Zero Trust Design Patterns



SEPARATE TRUST DOMAINS

Use separate SPIRE domains for dev and prod workloads, in order to ensure isolation of prod workloads.

Zero Trust Design Patterns

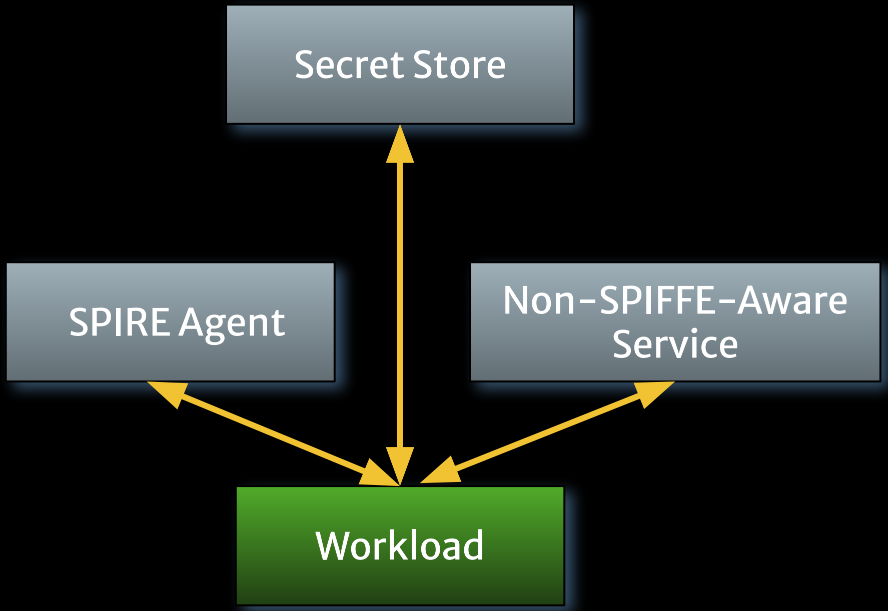


CICD BASED IDENTITY CREATION

As containers are built in a CICD system, identities are automatically updated.

This allows identities to be tied to a specific build hash.

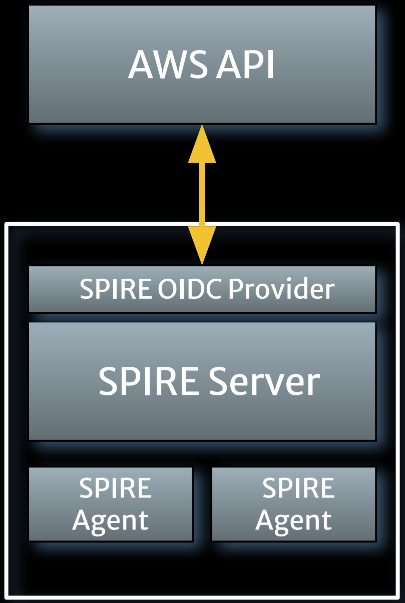
Zero Trust Design Patterns



SECRET STORE ACCESS

SPIFFE Identities can be used to access secrets in a secret store, which can then be used to access non-SPIFFE-aware resources.

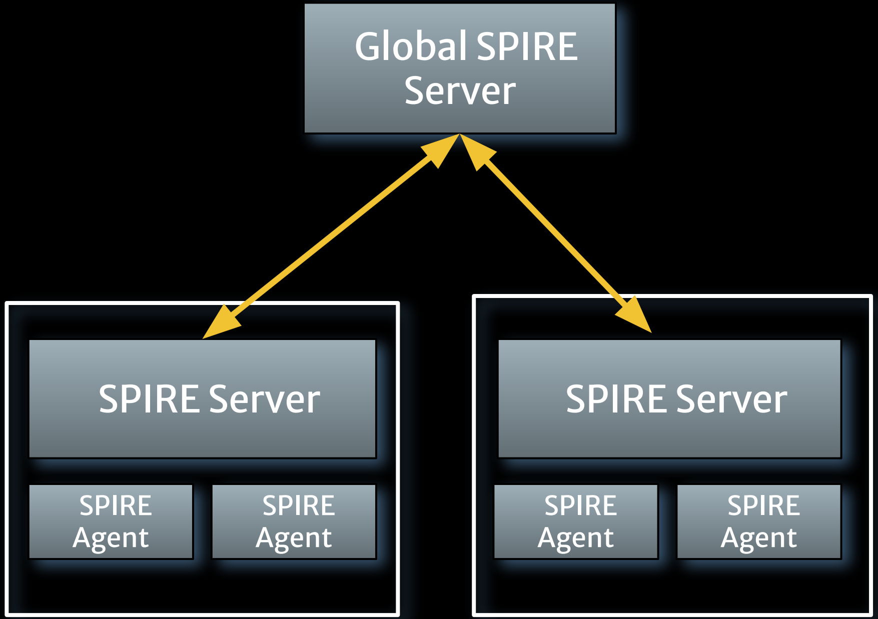
Zero Trust Design Patterns



OIDC FEDERATION

OIDC Federation lets your services authenticate to many common external APIs (like AWS)

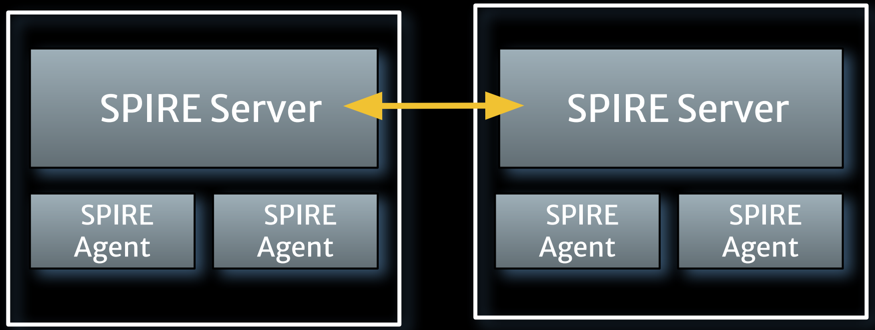
Zero Trust Design Patterns



NESTED SPIRE

Nested SPIRE can help you separate failure domains between multiple data centers or clouds

Zero Trust Design Patterns



FEDERATION

Federation lets you separate security domains between two independent SPIRE servers.

AGENDA

1 WHAT IS ZERO TRUST

2 SPIFFE AND SPIRE ARCHITECTURE

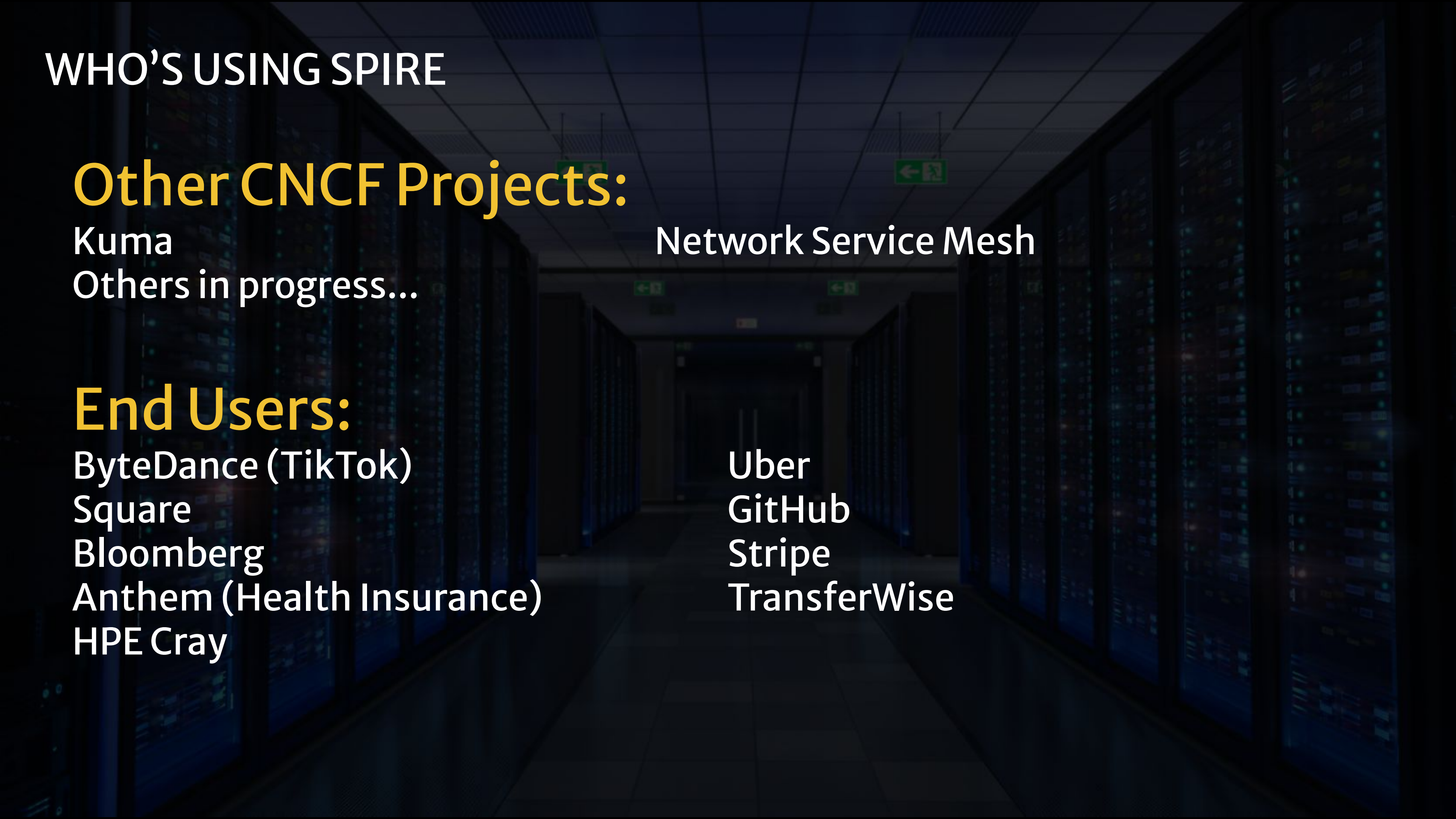
3 BUILDING SYSTEMS WITH SPIFFE AND SPIRE

4 ROADMAP

5 NEXT STEPS

ROADMAP

- IMPROVED DATASTORE LAYER
- SUPPORT FOR TRUSTED PLATFORM MODULES
- SUPPORT FOR SERVERLESS FUNCTIONS
- CERTIFICATE TRANSPARENCY
- IMPROVED KUBERNETES SUPPORT



WHO’S USING SPIRE

Other CNCF Projects:

Kuma

Others in progress...

Network Service Mesh

End Users:

ByteDance (TikTok)

Square

Bloomberg

Anthem (Health Insurance)

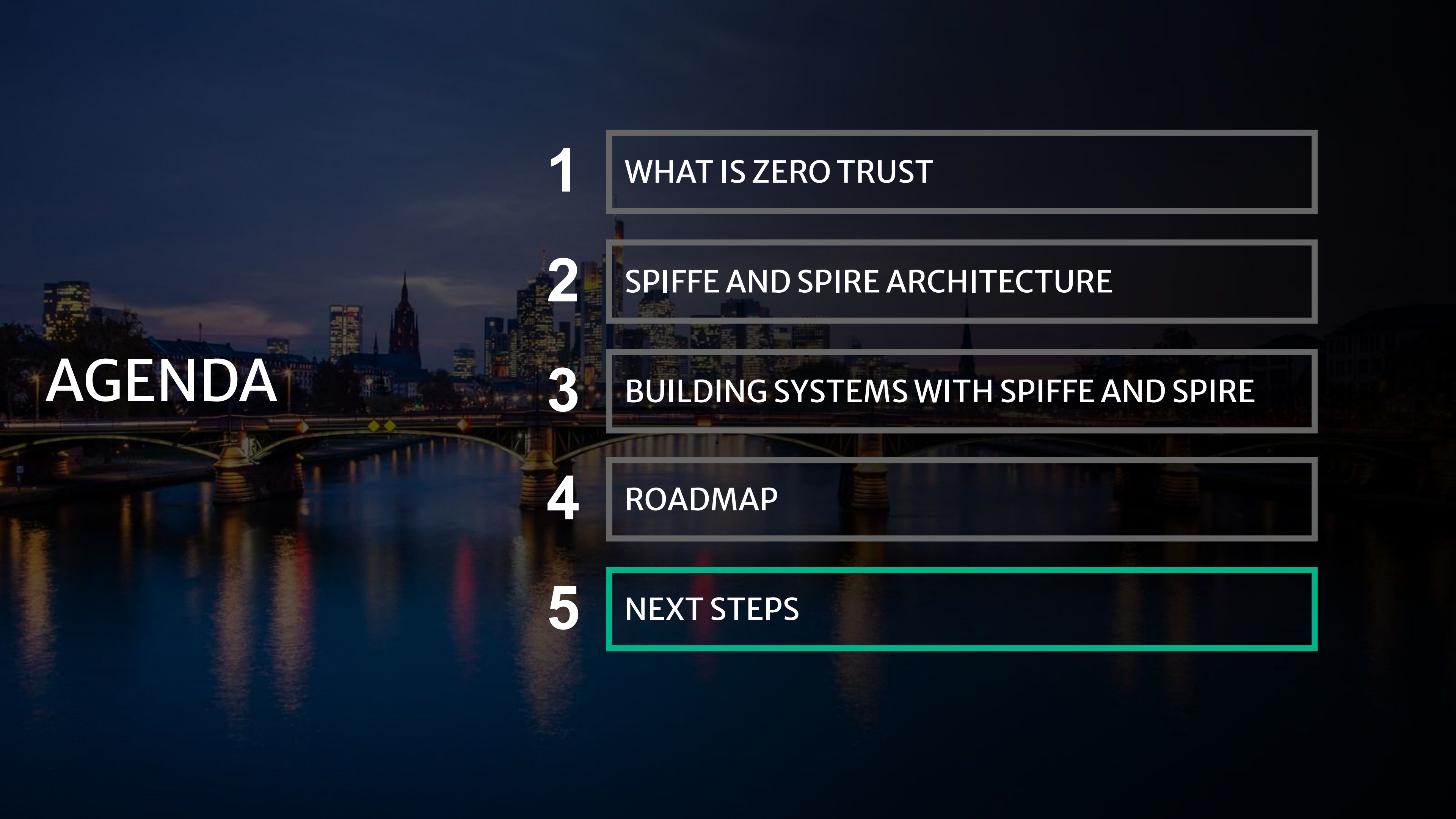
HPE Cray

Uber

GitHub

Stripe

TransferWise

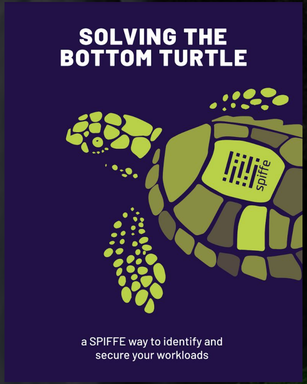


AGENDA

1. WHAT IS ZERO TRUST
2. SPIFFE AND SPIRE ARCHITECTURE
3. BUILDING SYSTEMS WITH SPIFFE AND SPIRE
4. ROADMAP
5. NEXT STEPS

NEXT STEPS

- spiffe.io
- spiffe.slack.com
- @spiffeio
- Book coming out soon!


SOLVING THE BOTTOM TURTLE
spiffe
a SPIFFE way to identify and secure your workloads

THANK YOU

Daniel Feldman
HPE Security Engineering
dan.feldman@hpe.com
@d__feldman