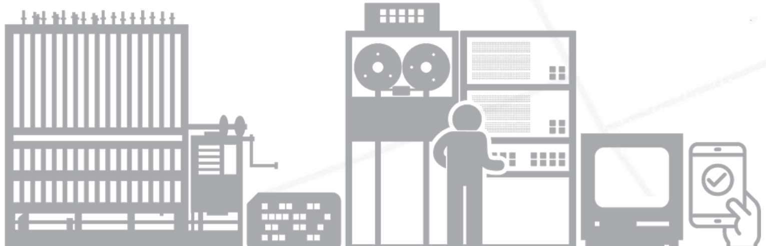
Sentima

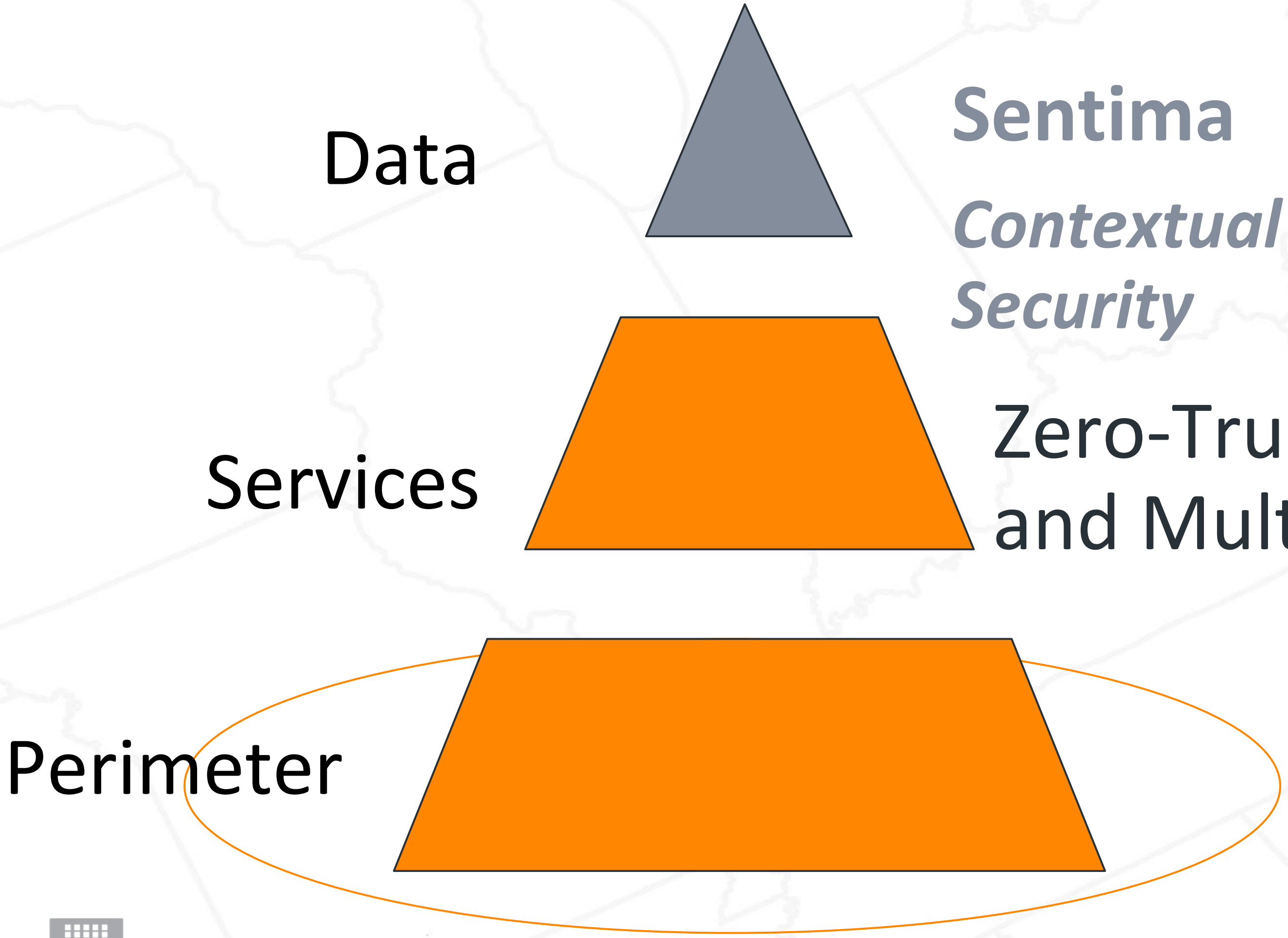
Contextual Aware Converged Security Platform



HOTSOS 2023

10TH ANNUAL
HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 3 - 5, 2023 | *Virtually hosted by* The National Security Agency
hotsos.org

Bring Security Closer to the Real Value Resource

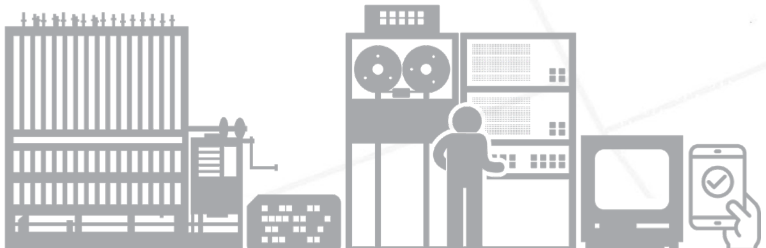


Sentima

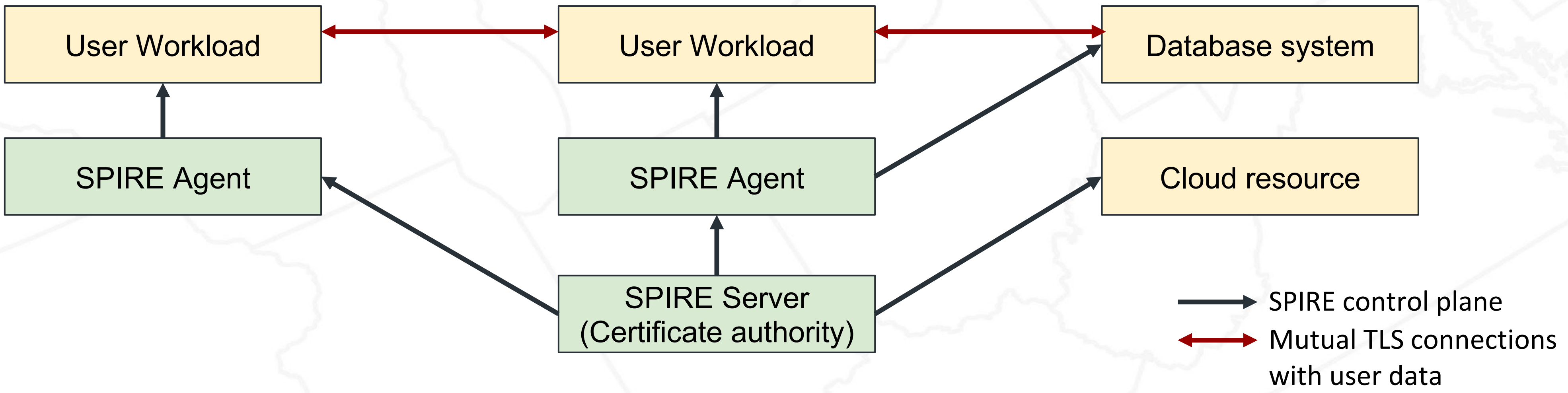
Contextual Converged Security

Zero-Trust for Hybrid and Multi-Cloud

Existing Security models are Reactive and Segmented, and lack context



Phase 1: Point-to-point zero trust



- Our team previously developed **SPIFFE/SPIRE, a widely used open source set of tools** for point-to-point zero trust security.

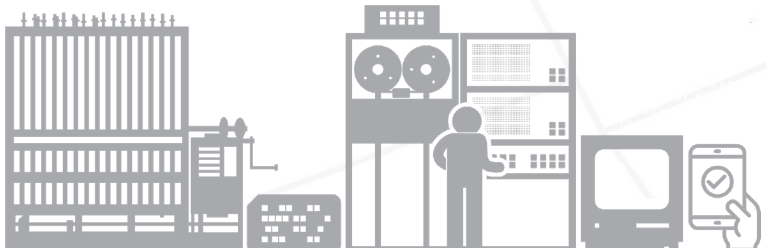
- SPIRE **automatically distributes and rotates client and server certificates** from a CA to every server/VM, user workload, or cloud API within large-scale distributed cloud infrastructure.

- These certificates are used to create **mutual TLS connections.**

- SPIRE c**hecks the detailed properties of a workload** including service account and binary signature. If they match a configured profile, it grants the needed credentials.

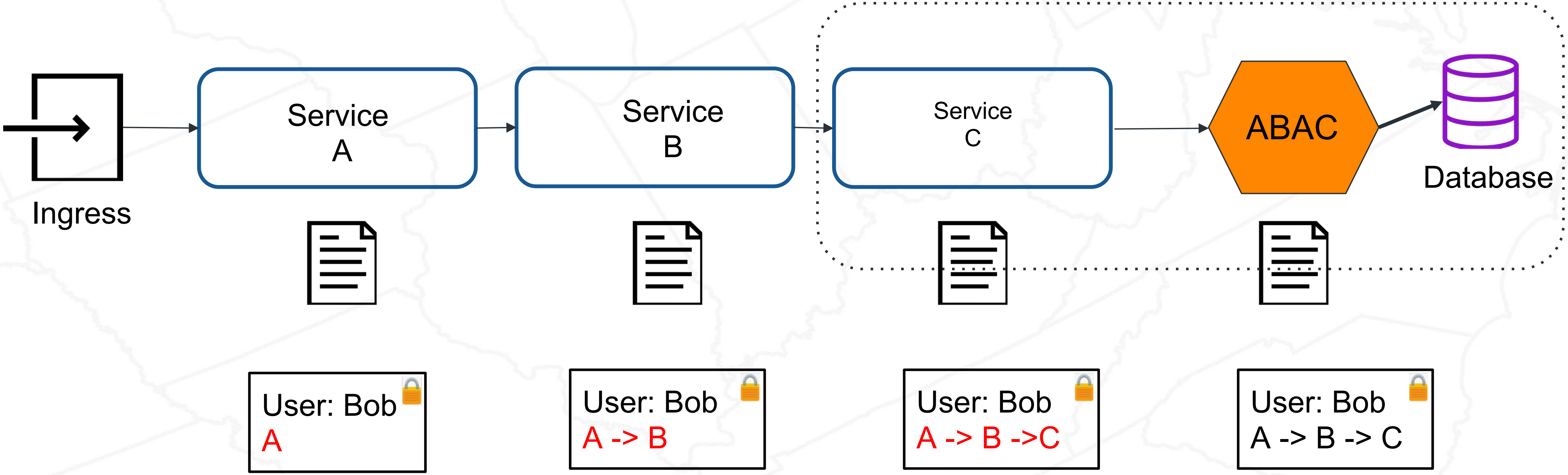
- SPIRE **authenticates** database connections, public cloud services like S3 and RDS, and **integrates** with Istio, SIGSTORE, Kubernetes, and many other systems.

- **SPIFFE/SPIRE is the starting point for Sentima.**



Point-to-point zero trust eliminates service accounts, secrets management, and helps mitigate persistent threats

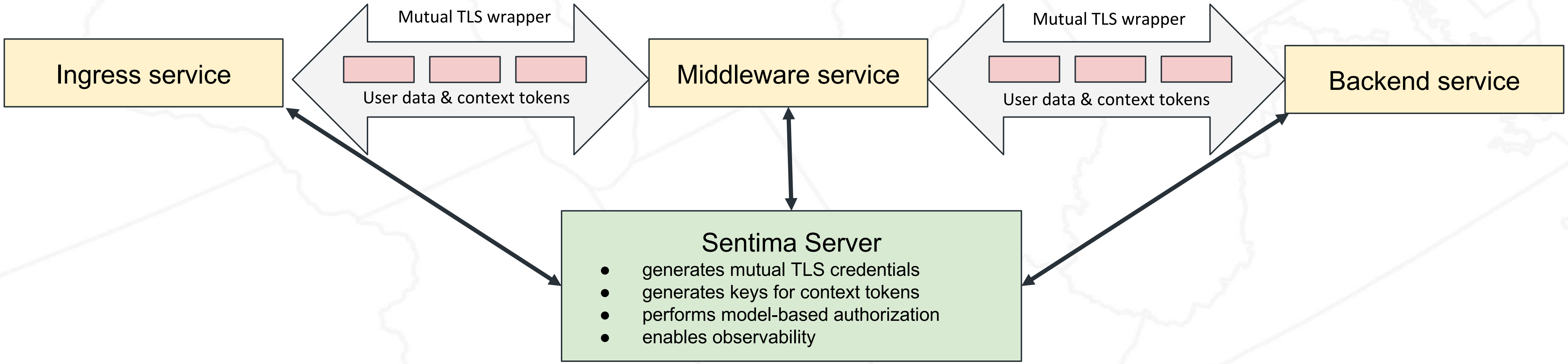
Phase 2: Chain of Custody



(Cryptographically verified Chain of Trust)

Limit any movements to the intended purpose of that digital communication or transaction, thus preventing any breach. Eliminates need for many security tools. Creates a cryptographically verifiable Chain of Trust.

Phase 3: Contextual Awareness



Sentima Server

- generates mutual TLS credentials
- generates keys for context tokens
- performs model-based authorization
- enables observability

- With certificates for mutual TLS, and chain of custody encoded in signed tokens, **each service can now make informed authorization decisions.**
- Authorization can use an existing rule-based authorization engine such as Open Policy Agent or XACML, or **Sentima's own model-based authorization tool.**

- In model-based authorization, services use the **"who, what, when, where, and why"** of each incoming request (including the complete chain of custody) to make an authorization decision based on a learning model of expected behavior.

Incorporates intelligent decision making based on context and threshold scoring at each step of the way.

Team

Eugene Weiss - CEO

Pioneer, Innovator and Cybersecurity Technologist. 20-year Expert in Security Intelligence, Zero Trust and AI.
eugene@sentima.io

Yogi Porla - CTO

Impacted over 40 organizations with IT vision and strategy. Delivered and Integrated Zero Trust, AI, Ops, and Cloud solutions
yogi@sentima.io

Daniel Feldman - COO

Software engineer with 10 years experience delivering security solutions; SPIFFE steering committee
daniel@sentima.io