KubeCon CloudNativeCon India 2026

#KubeCon #CloudNativeCon

Secure GitOps for Regulated Workloads: Argo CD Meets Confidential Containers

Jitendra Singh
Senior Software Engineer, Microsoft

AGENDA

1. GitOps Foundations
2. The Trust Gap in GitOps
3. Closing The Trust Gap
4. Supply Chain Security with Sigstore
5. Confidential Containers & TEEs
6. Secure GitOps Architecture
7. Operational Impact & Takeaways

GitOps Foundations

Declarative Everything

Define desired state in code

Git as Source of Truth

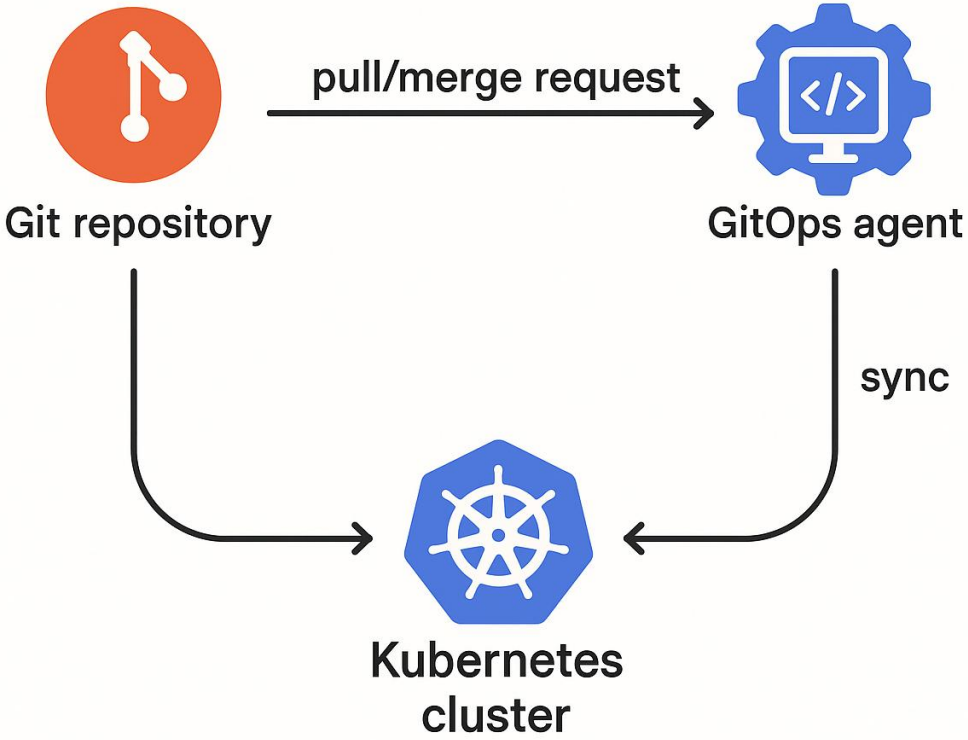
Git is the only source of config

Pull Requests for Changes

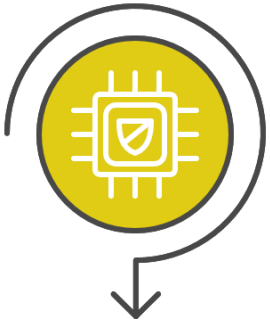
PRs for all updates

Continuous Reconciliation

Automated Sync with Live Systems



The Trust Gap in GitOps



Deployment vs. Trust

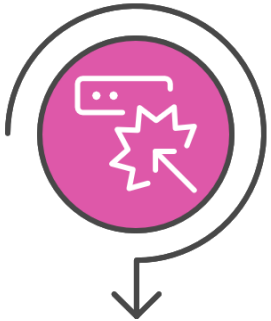
Deployment does not automatically equate to trust. Consider the builder and runtime security.

Signed Malware

Signed malware is a possibility, raising concerns about software integrity.

CI Compromise

CI compromise can lead to vulnerabilities in the deployment process.



Runtime Attacks

Runtime attacks highlight the need for continuous vigilance in maintaining security.

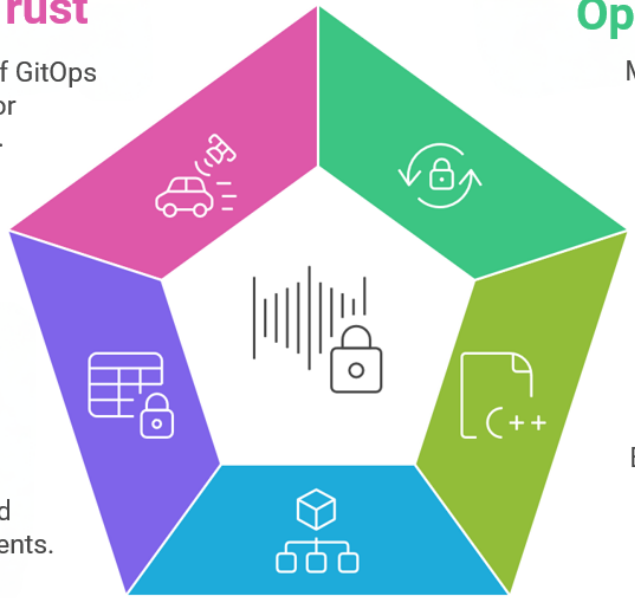
Closing the Trust Gap

Speed and Trust

Balancing the speed of GitOps with the need for verifiable trust.

Operational Trust

Making trust a measurable and actionable operational signal.



Hardware Isolation

Providing secure, isolated runtime execution environments.

Software Signing

Ensuring software authenticity and provenance through cryptographic verification.

GitOps Orchestration

Enforcing trust policies within the GitOps workflow.

Supply Chain Security with Sigstore

KubeCon CloudNativeCon India 2026

Keyless Signing
Sign artifacts without managing keys.

Identity-Based Verification
Verify using trusted identities (OIDC).

Provenance & Transparency
Record and verify how software is built.

Modern Cloud-Native CI/CD Pipelines

Secures the Software Supply Chain
Ensures integrity from code to runtime.

Prevents Tampering & Attacks
Detects unauthorized changes early.

Provides Audit Logs & Policy Enforcement
Delivers verifiable logs and supports policies.

Confidential Containers & TEEs

KubeCon CloudNativeCon India 2026

Protects Data While It's Being Used

Data at Rest

Disk Encryption

Data in Transit

Secure Transfer

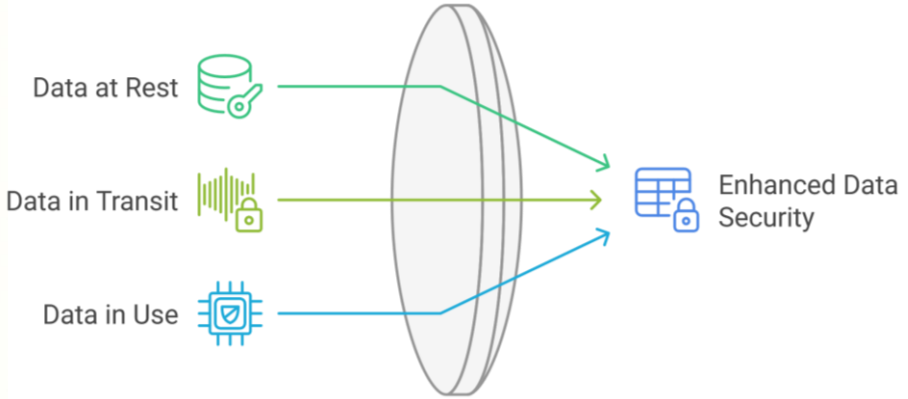
Data in Use

UNPROTECTED

Confidential Computing:

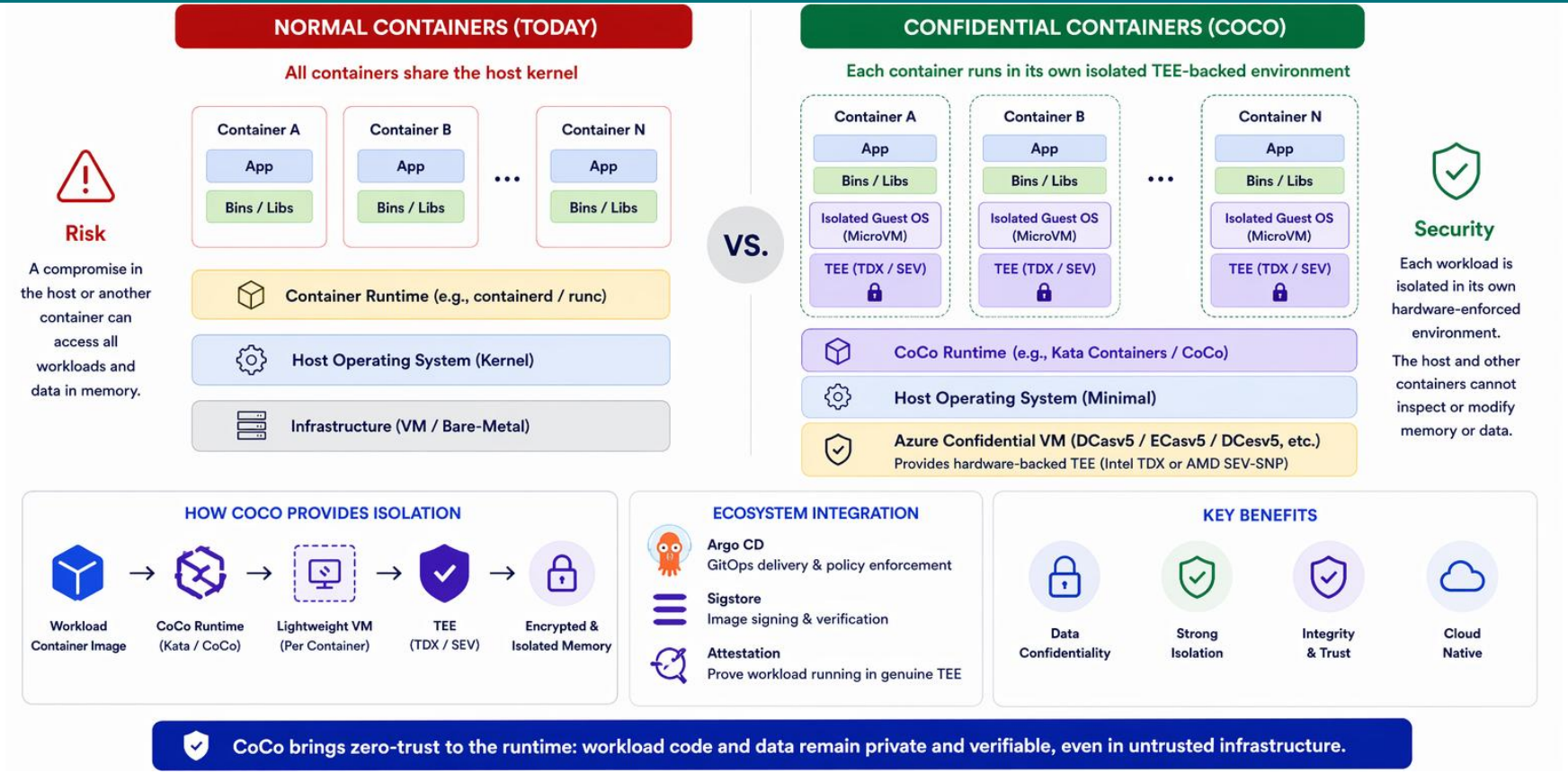
Encryption + Isolation During Processing

Safe Enclave



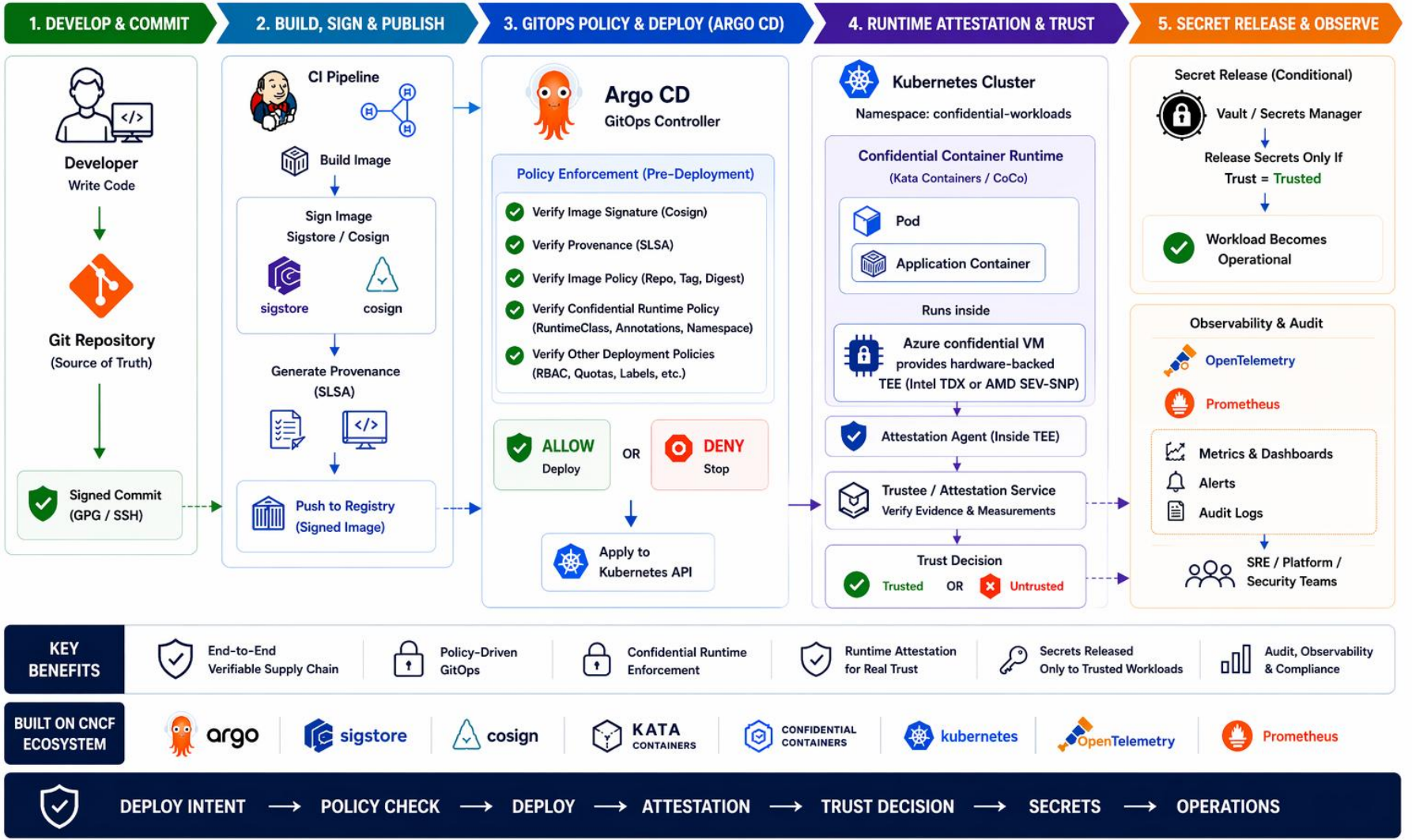
Confidential Containers & TEEs…

KubeCon CloudNativeCon India 2026



KubeCon CloudNativeCon India 2026

Secure GitOps Architecture


1. DEVELOP & COMMIT
2. BUILD, SIGN & PUBLISH
3. GITOPS POLICY & DEPLOY (ARGO CD)
4. RUNTIME ATTESTATION & TRUST
5. SECRET RELEASE & OBSERVE
Developer
Write Code
Git Repository
(Source of Truth)
Signed Commit
(GPG / SSH)
CI Pipeline
Build Image
Sign Image
Sigstore / Cosign
sigstore
cosign
Generate Provenance
(SLSA)
Push to Registry
(Signed Image)
Argo CD
GitOps Controller
Policy Enforcement (Pre-Deployment)
Verify Image Signature (Cosign)
Verify Provenance (SLSA)
Verify Image Policy (Repo, Tag, Digest)
Verify Confidential Runtime Policy
(RuntimeClass, Annotations, Namespace)
Verify Other Deployment Policies
(RBAC, Quotas, Labels, etc.)
ALLOW
Deploy
OR
DENY
Stop
Apply to
Kubernetes API
Kubernetes Cluster
Namespace: confidential-workloads
Confidential Container Runtime
(Kata Containers / CoCo)
Pod
Application Container
Runs inside
Azure confidential VM
provides hardware-backed
TEE (Intel TDX or AMD SEV-SNP)
Attestation Agent (Inside TEE)
Trustee / Attestation Service
Verify Evidence & Measurements
Trust Decision
Trusted
OR
Untrusted
Secret Release (Conditional)
Vault / Secrets Manager
Release Secrets Only If
Trust = Trusted
Workload Becomes
Operational
Observability & Audit
OpenTelemetry
Prometheus
Metrics & Dashboards
Alerts
Audit Logs
SRE / Platform /
Security Teams
KEY BENEFITS
End-to-End
Verifiable Supply Chain
Policy-Driven
GitOps
Confidential Runtime
Enforcement
Runtime Attestation
for Real Trust
Secrets Released
Only to Trusted Workloads
Audit, Observability
& Compliance
BUILT ON CNCF ECOSYSTEM
argo
sigstore
cosign
KATA
CONTAINERS
CONFIDENTIAL
CONTAINERS
kubernetes
OpenTelemetry
Prometheus
DEPLOY INTENT → POLICY CHECK → DEPLOY → ATTESTATION → TRUST DECISION → SECRETS → OPERATIONS

Sigstore and TEEs : Closing the Security Gaps

KubeCon CloudNativeCon India 2026

Relying on only one security component leaves critical security gaps

The Vault

TEEs: Trusted Execution Environments

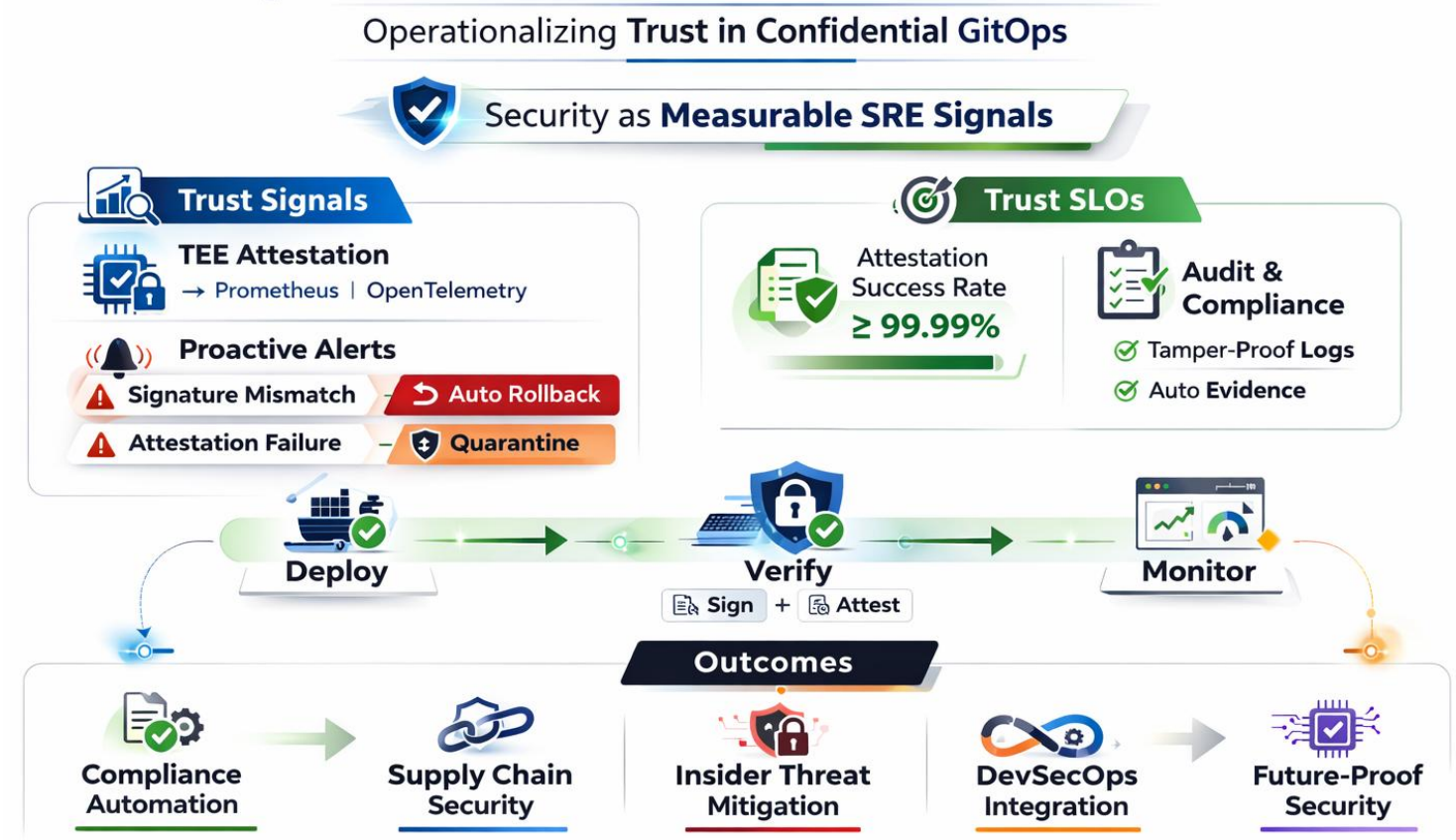
- **Protects** Data During Execution
- **Encrypts** and **Isolates** Code and Secrets
- **Provides** Runtime Attestation

Sigstore

Image Signing and Verification

- **Ensures** Supply Chain Security
- **Verifies** Origin of Images
- **Detects** Tampering Before Deployment

Operational Impact & Key Takeaways



KubeCon CloudNativeCon India 2026

Thank You !