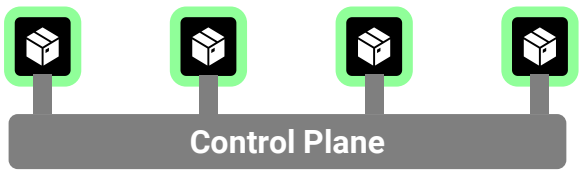
Confidential Kubernetes
Security Analysis

Managed Kubernetes with Confidential VMs or Secure Enclaves

Concept

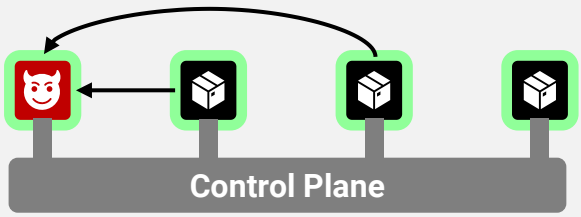


At most, worker nodes are protected with confidential computing. The nodes are not verified. This only protects against direct access to node memory and cold-boot attacks.
This is how **AKS**, **EKS**, and **GKE** work.

Attack #1: Compromised control plane

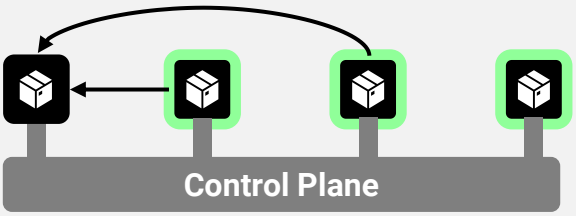
A compromised control plane has full control over worker nodes via *kubelet* and can thus access all data.

Attack #2: Manipulated node



A node running manipulated software is added to the cluster. This goes unnoticed due to the lack of proper attestation.

Attack #3: Unprotected node



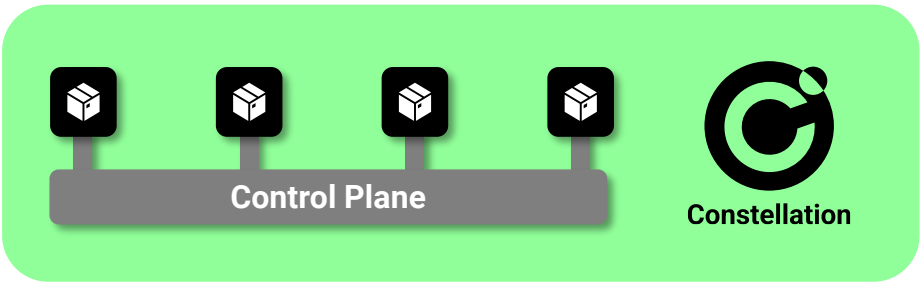
An unprotected node is added to the cluster. This goes unnoticed due to the lack of proper attestation.

Many other possible attacks exist

- Manipulation of node parameters
- Interception of K8s admin connections
- Access to cloud-based key management
- ...

Constellation

Concept



The control plane and all worker nodes are protected with Confidential VMs. Constellation ensures the integrity of the entire deployment using remote attestation. Constellation ensures that all data is always encrypted – at rest, in transit, and during processing. Constellation transparently manages the corresponding cryptographic keys.

All attacks above are prevented by Constellation.

Learn more at https://edgeless.systems/.