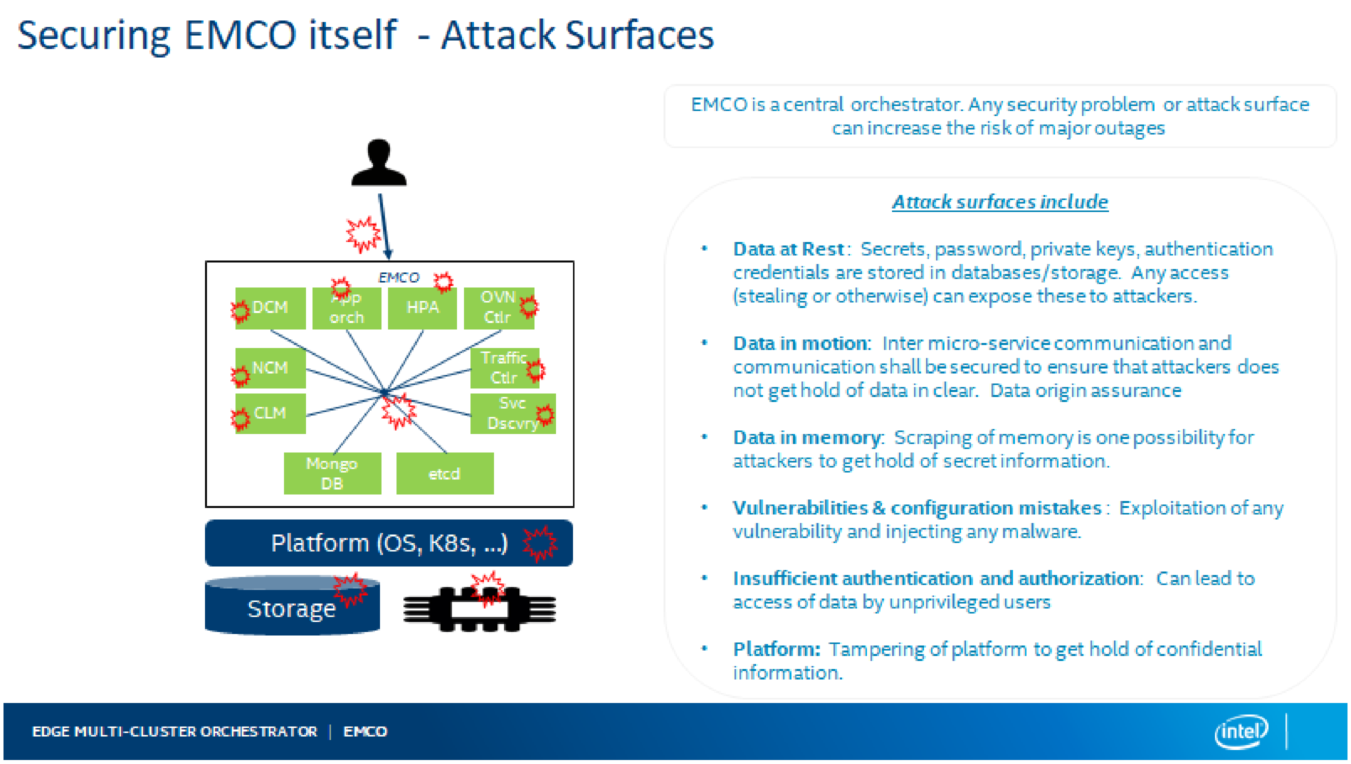
Securing EMCO

Some of the best practices EMCO uses today.



Securing EMCO itself - Attack Surfaces

EMCO is a central orchestrator. Any security problem or attack surface can increase the risk of major outages

Attack surfaces include

- **Data at Rest**: Secrets, password, private keys, authentication credentials are stored in databases/storage. Any access (stealing or otherwise) can expose these to attackers.
- **Data in motion**: Inter micro-service communication and communication shall be secured to ensure that attackers does not get hold of data in clear. Data origin assurance
- **Data in memory**: Scraping of memory is one possibility for attackers to get hold of secret information.
- **Vulnerabilities & configuration mistakes**: Exploitation of any vulnerability and injecting any malware.
- **Insufficient authentication and authorization**: Can lead to access of data by unprivileged users
- **Platform:** Tampering of platform to get hold of confidential information.

EDGE MULTI-CLUSTER ORCHESTRATOR | EMCO

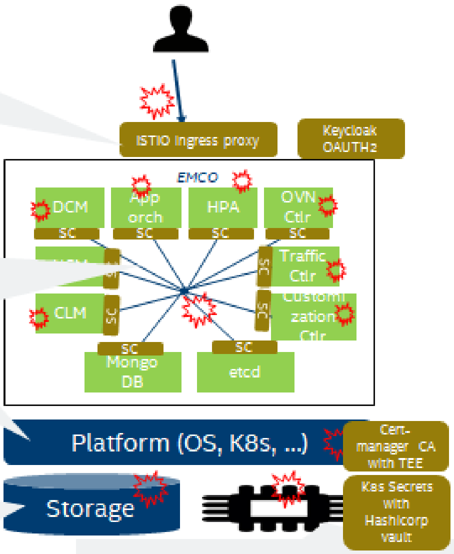
Securing EMCO itself - Solutions that it (would) leverages

ISTIO/Envoy Security via ingress proxy:
JWT/Certificate authentication; TLS; OAUTH2, Request authorization; ModSecurity WAF, IDS/IPS as WASM Plugin in Service Mesh
→ Protects from attacks from Internet

ISTIO/Envoy Security via sidecars (Zero trust)
Inter Micro-service communication security (Mutual TLS, Authentication and Authorization, WAF, IDS/IPS) -> protects from other micro-services (avoid any lateral attacks) and protects from stealing information on the wire

Secure boot and Platform attestation:
To ensure that platform is booted with right software and configuration

Storage data security:
Encrypted file system (example: dm-crypt) with symmetric key secured in outside vault



Confidential Computing:
Ensure that critical micro-services are run in TEE

EMCO uses CN best practices to secure the micro-services via Service meshes (ISTIO/Envoy)

Centralized Authentication and Authorization at ISTIO, thereby reducing errors by developers and to simplify DevSecOps

EMCO uses Keycloak instead of local database. Deployers can replace keycload with their own OAUTH2 server

EMCO will leverage secured ISTIO (Private key security in cert-manager/TEE) as and when it is ready