Microsoft Azure

Security In Plain Sight: Hardening Systems Via Open Source

Phillip Gibson, Microsoft

opensource.microsoft.com

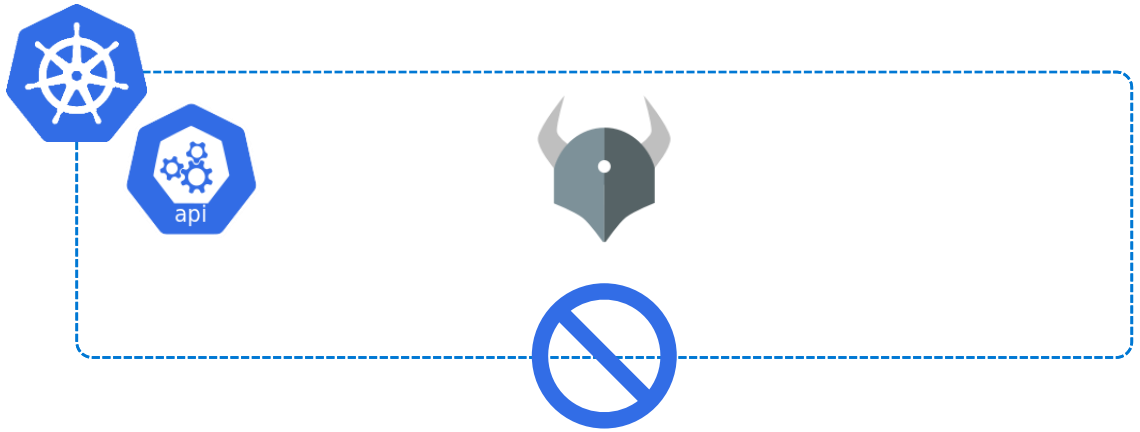
Security and compliance

- The safest code is independently verifiable while still customizable to the org's specific needs
- Industry-standard cloud native technologies are essential for security infrastructure
- Security and transparency go hand in hand
- Microsoft contributes much open source in the K8s security realm

Gatekeeper

Policy Controller for Kubernetes

- Built on Open Policy Agent
- Allows user-defined policy to ensure Kubernetes resources are compliance




```
apiVersion: v1
kind: Pod
metadata:
  name: label-demo
  labels:
    environment: production
    app: nginx
spec:
  containers:
  - name: nginx
    image: nginx:1.14.2
    ports:
    - containerPort: 80
```

CLOUD NATIVE COMPUTING FOUNDATION

github.com/open-policy-agent/gatekeeper

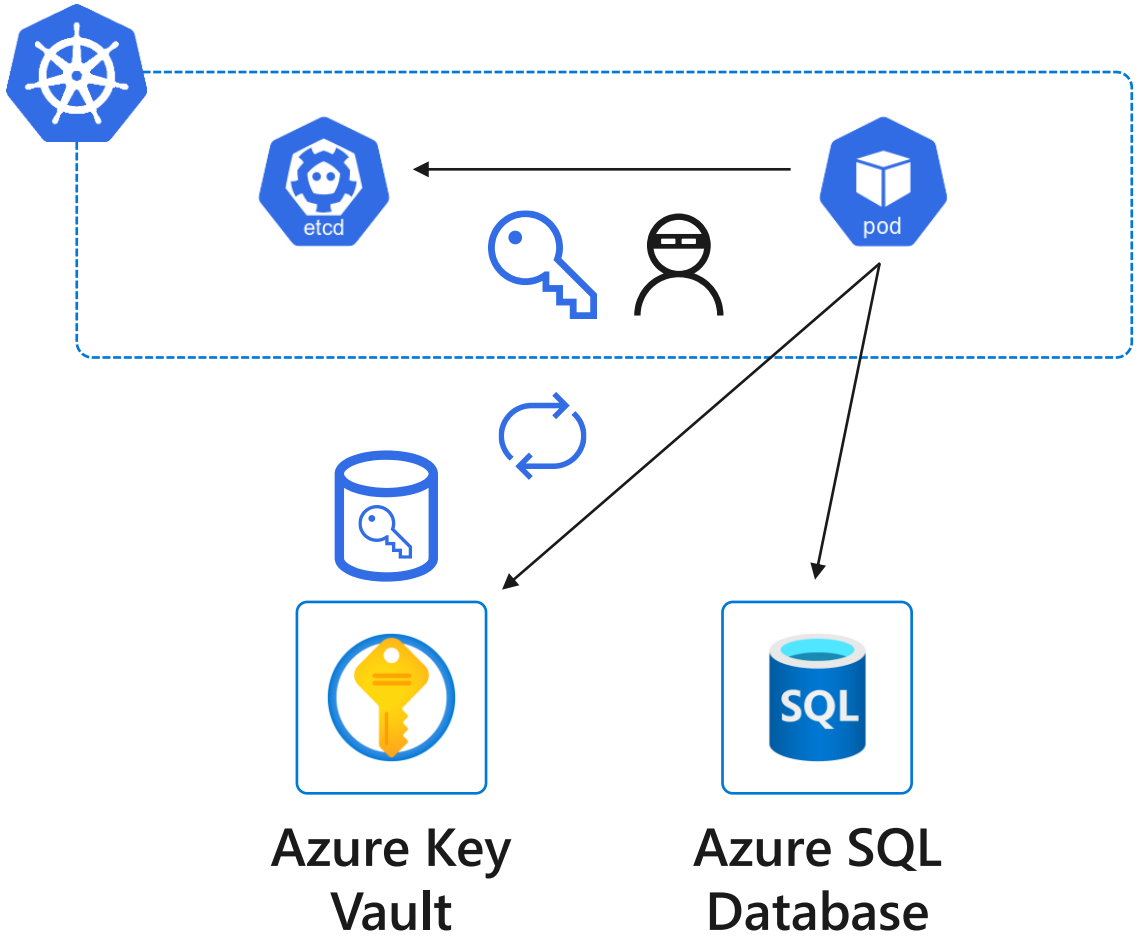
CSI Secrets Store

Integrates secrets stores with Kubernetes via a Container Storage Interface (CSI) volume

Azure Key Vault provider for Secrets Store CSI driver

- Get secret contents stored in Azure Key Vault, HashiCorp Vault, Google Cloud Key, and AWS KMS
- Use Secrets Store CSI driver to mount them into Kubernetes pods

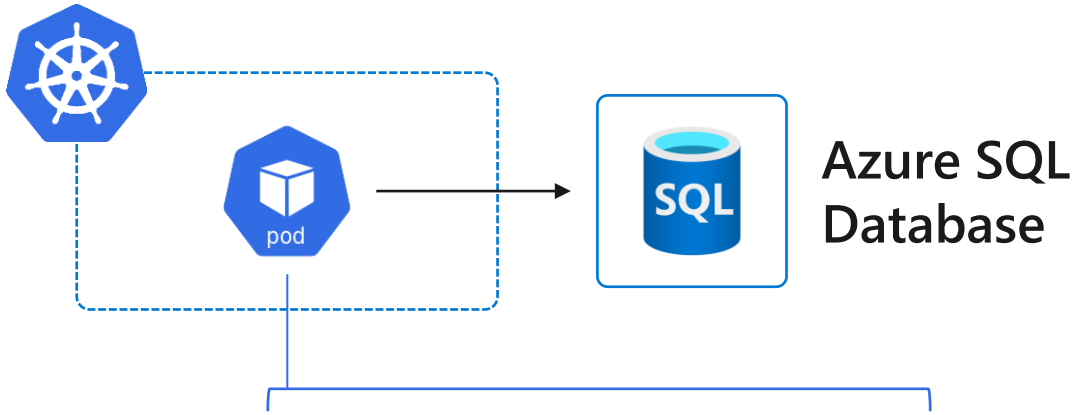
github.com/kubernetes-sigs/secrets-store-csi-driver



Azure AD Pod Managed Identity

Enables Kubernetes applications to access cloud resources securely with Azure Active Directory

- Using Kubernetes primitives, configure identities and bindings to match pods
- Without any code modifications, containerized applications can access resources using AAD as identity provider

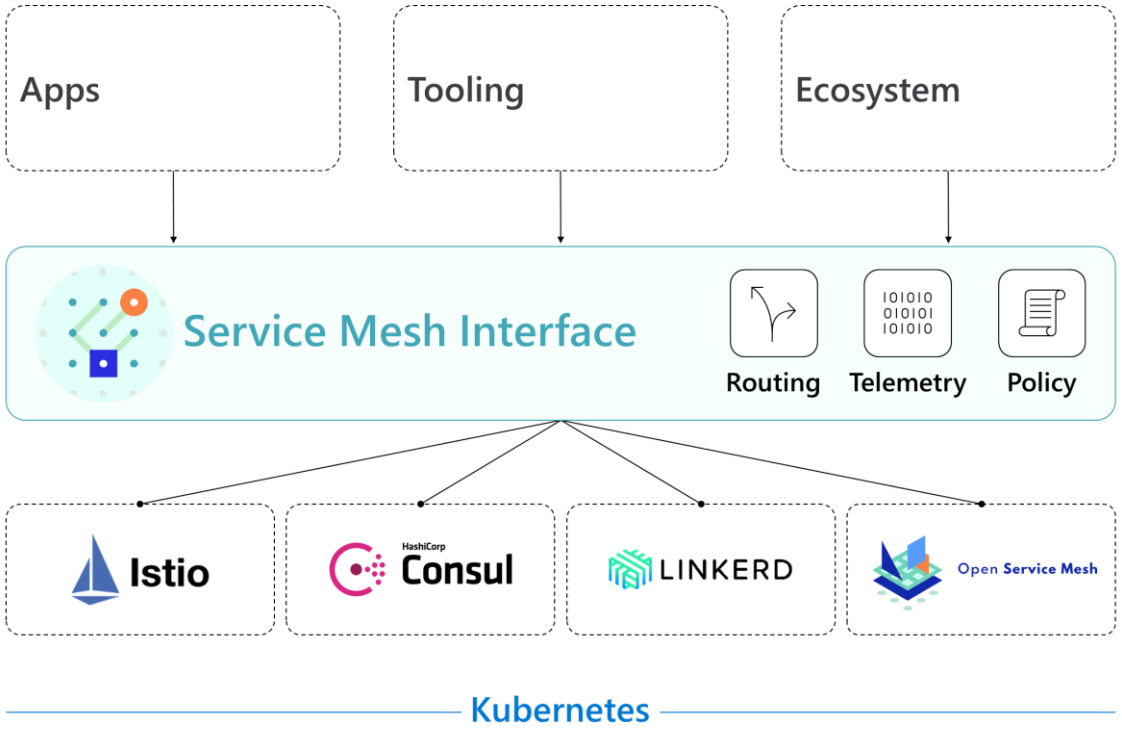



```
# MSAL (Microsoft Authentication Library)

using Microsoft.Identity.Client;

IConfidentialClientApplication app;
app = ConfidentialClientApplicationBuilder.Create(config.ClientId)
                        .WithClientSecret(config.ClientSecret)
                        .WithAuthority(new Uri(config.Authority))
                        .Build();

AuthenticationResult result = null;

try
{
   result = await app.AcquireTokenForClient(scopes)
                     .ExecuteAsync();
   // TODO Access something
}
{
   catch(MsalServiceException ex)
{
    // TODO Can't access service
}
```

azure.github.io/aad-pod-identity

Service Mesh Interface

- A standard interface for service meshes on Kubernetes
- A basic feature set of the most common service mesh use cases
- Flexibility to support new service mesh capabilities over time
- Space for the ecosystem to innovate with service mesh technology

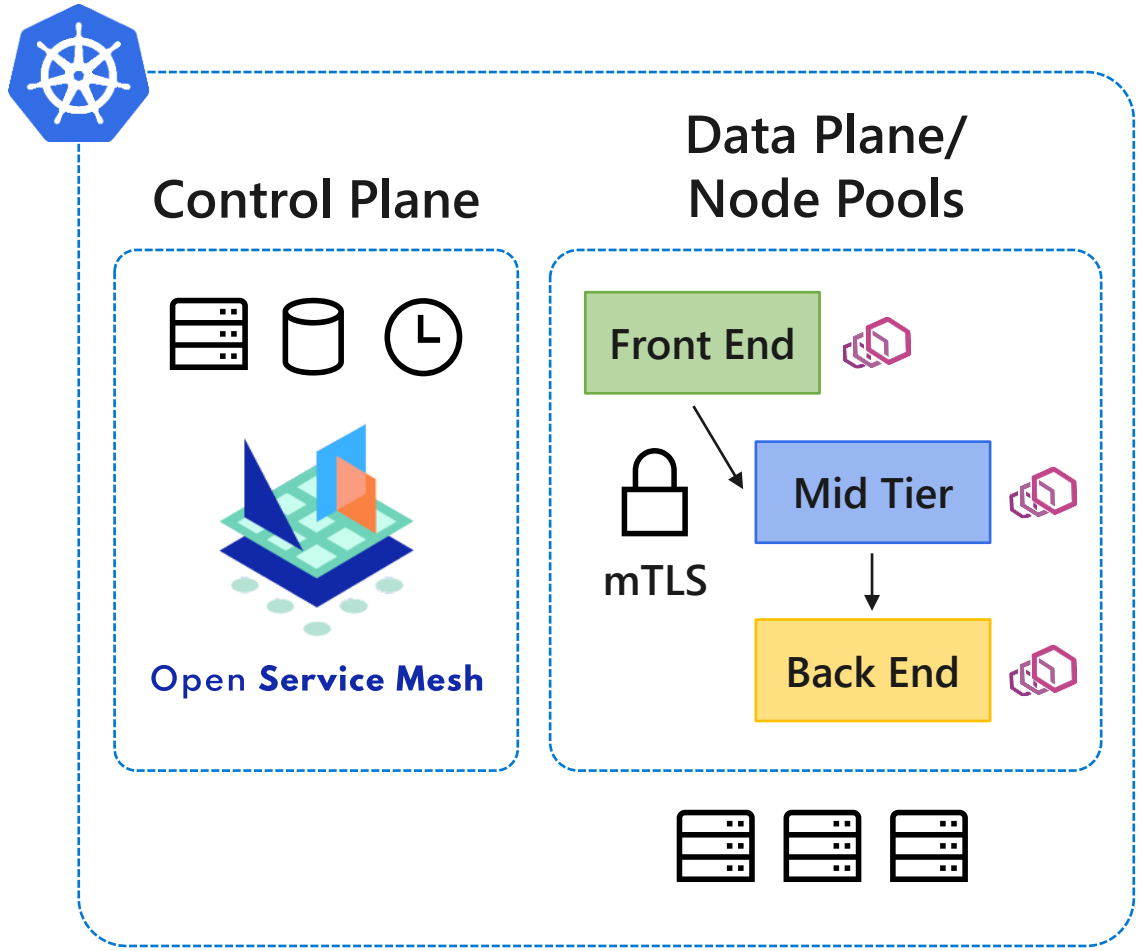


CLOUD NATIVE COMPUTING FOUNDATION

smi-spec.io

Open Service Mesh (OSM)

- **Simple** to understand and contribute to
- **Effortless** to install, maintain, and operate
- **Painless** to troubleshoot
- **Easy** to configure via Service Mesh Interface (SMI)



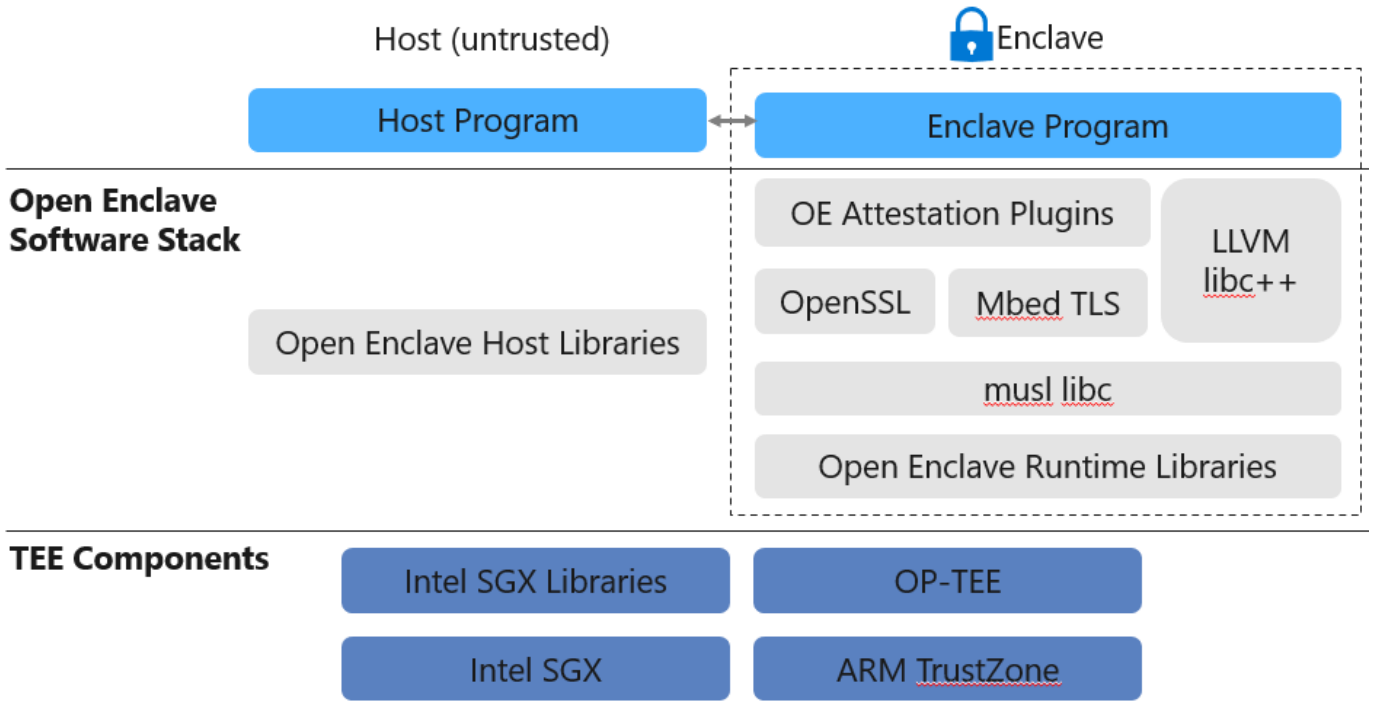
CLOUD NATIVE COMPUTING FOUNDATION

openservicemesh.io

Open Enclave SDK

Enables building applications based on Trusted Execution Environments

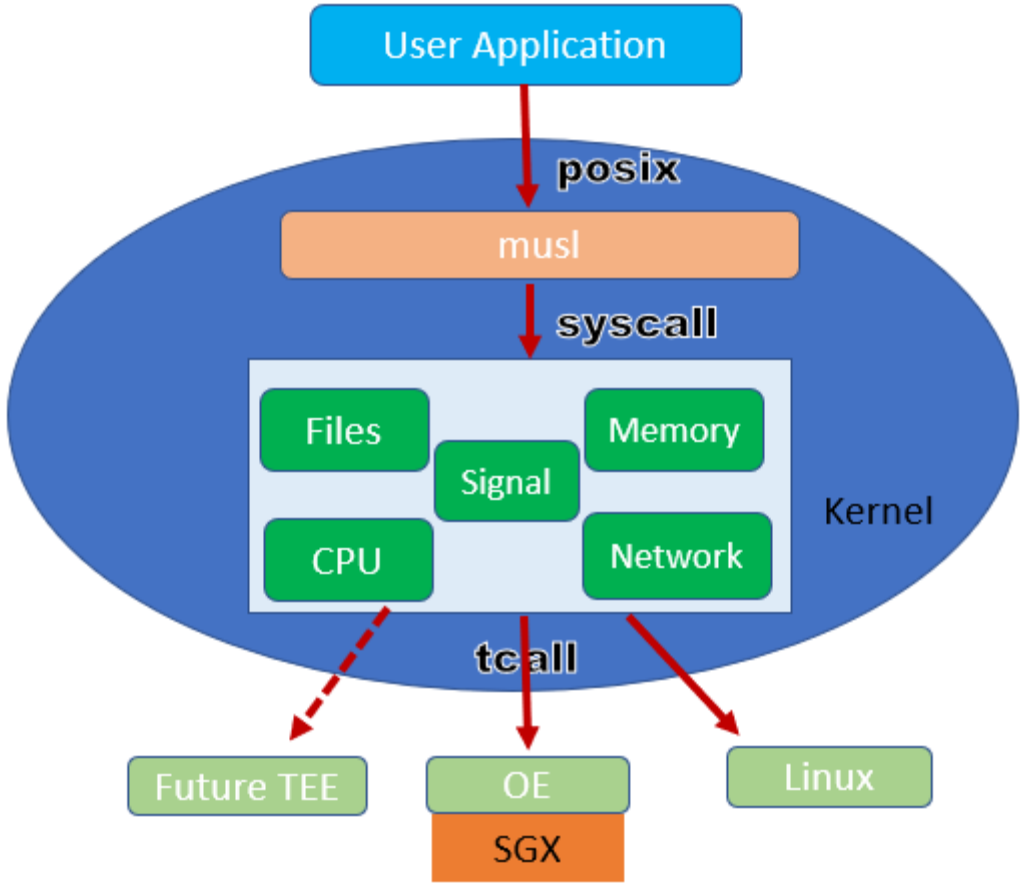
Provides consistent API surface across enclave technologies as well as all platforms from cloud to edge



openenclave.io/sdk

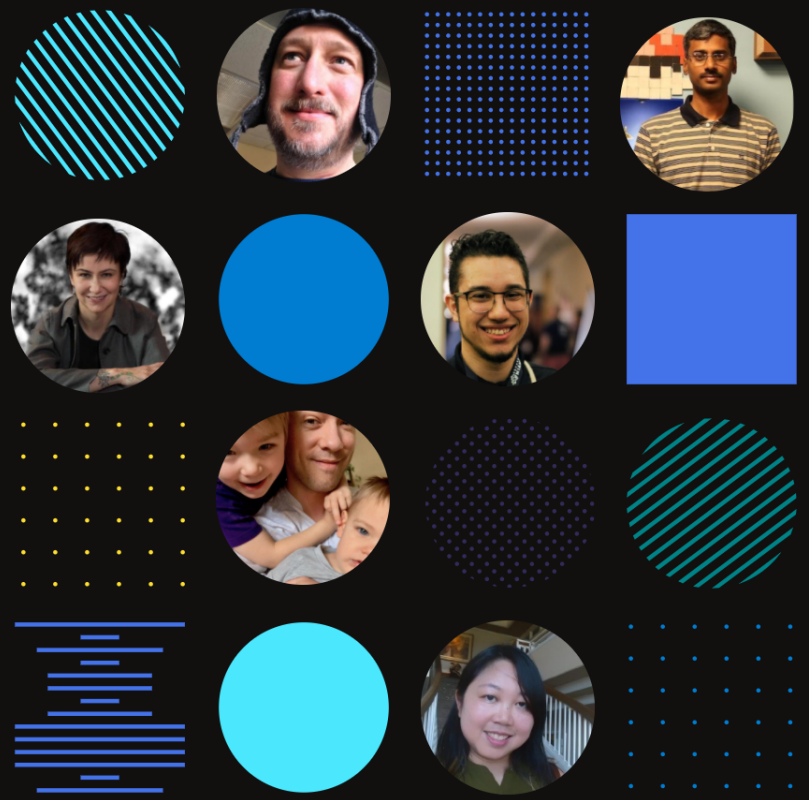
Mystikos: Bringing TEEs to Cloud Native

- Secure your Linux apps by using Trusted Execution Environments, with little or no modification in many cases
- Designed for the cloud-native deployment paradigm
- Simplifies re-targeting to other TEE architectures through a plugin system, and aim for a "build once; run anywhere" model



github.com/deislabs/mystikos

Open. Collaborative. Flexible.



Open Source enables Microsoft products and services to bring choice, technology and community to our customers.

opensource.microsoft.com