KubeCon | CloudNativeCon
North America 2019

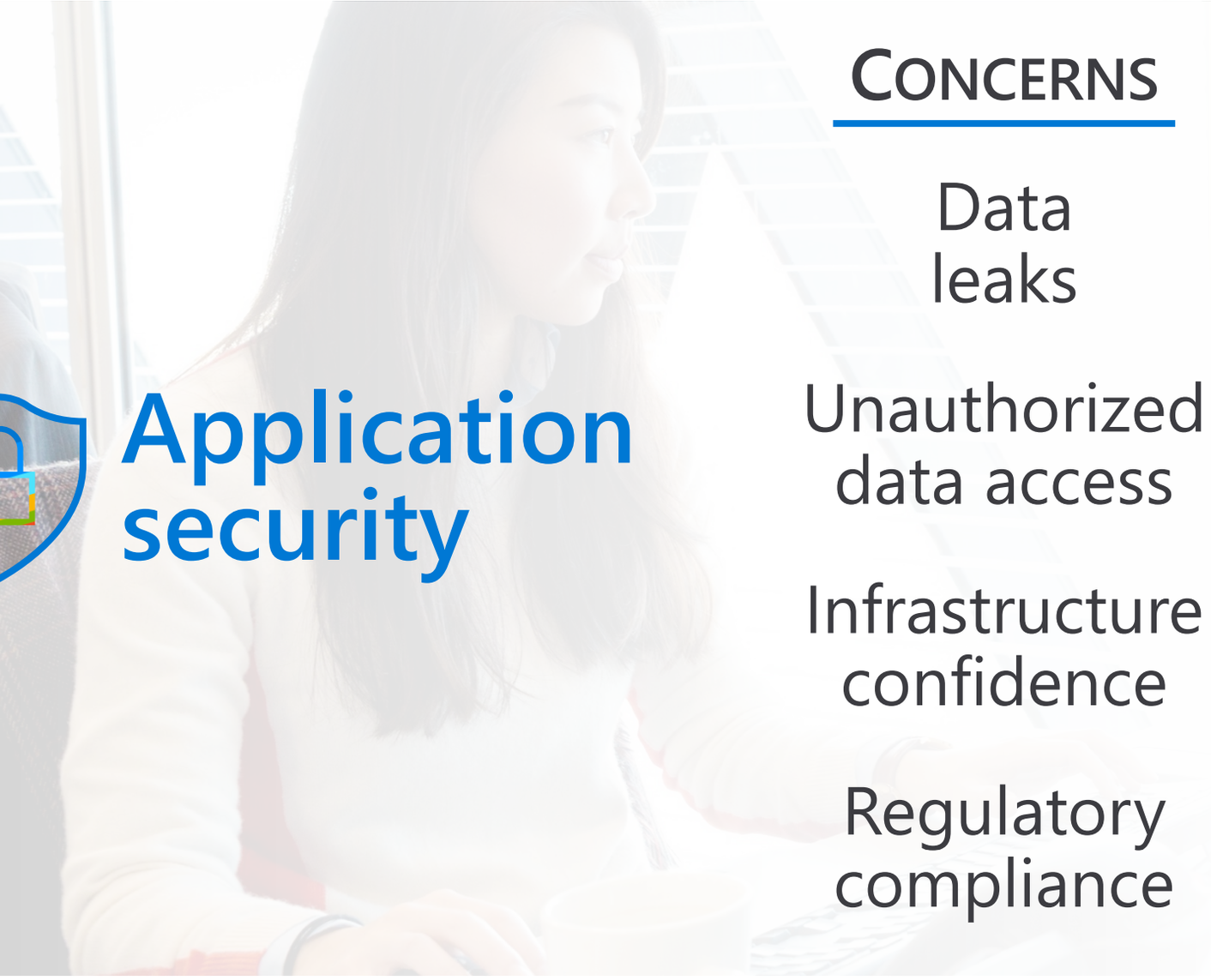
Bringing CONFIDENTIAL COMPUTING to Kubernetes

LACHLAN EVENSON | Microsoft Azure

Principal Program Manager, Azure Container Compute
Board Member, Cloud Native Computing Foundation

@OpenAtMicrosoft

Microsoft Azure



Application security

Concerns

Data leaks

Unauthorized data access

Infrastructure confidence

Regulatory compliance

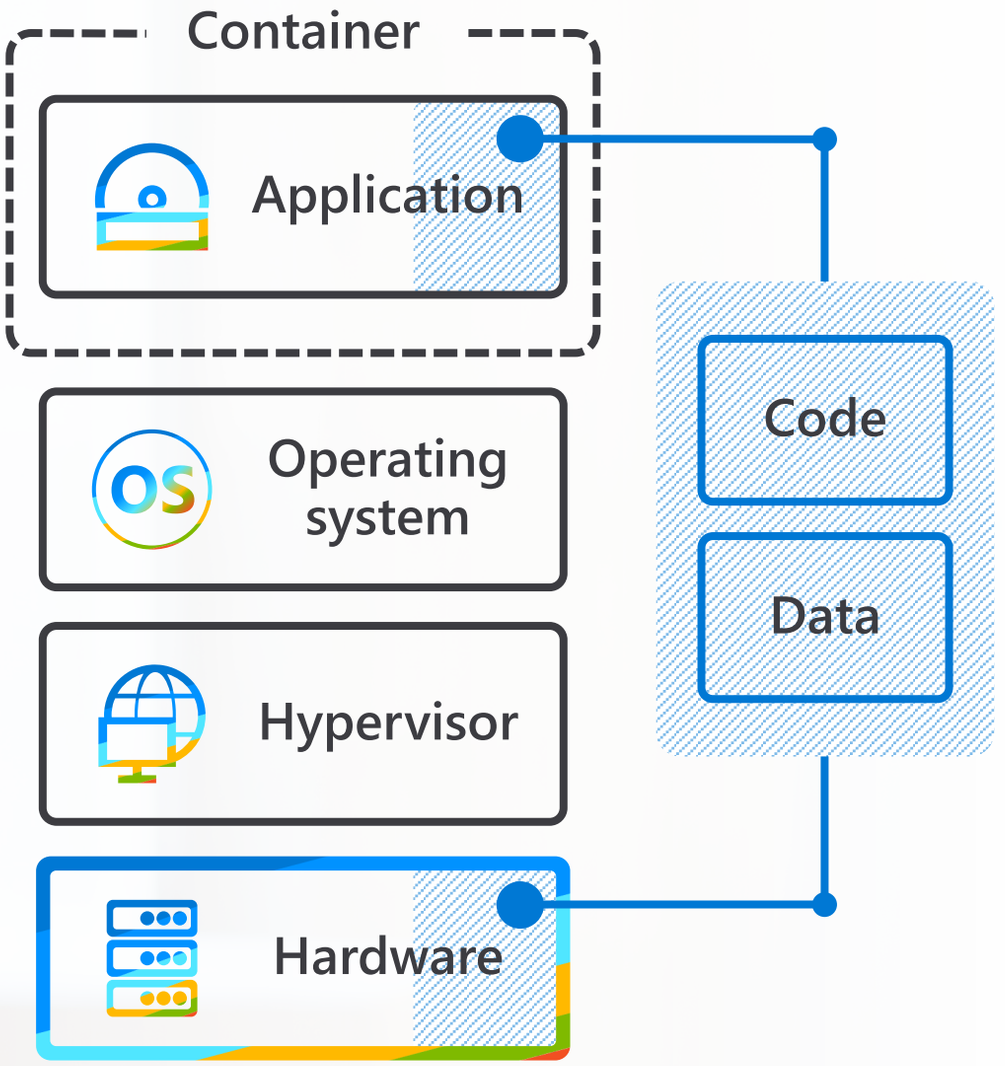
Goals

Hardware-level data protection

Confident processing of multi-tenant data

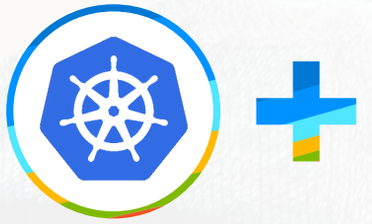
Safer sensitive and confidential data IP

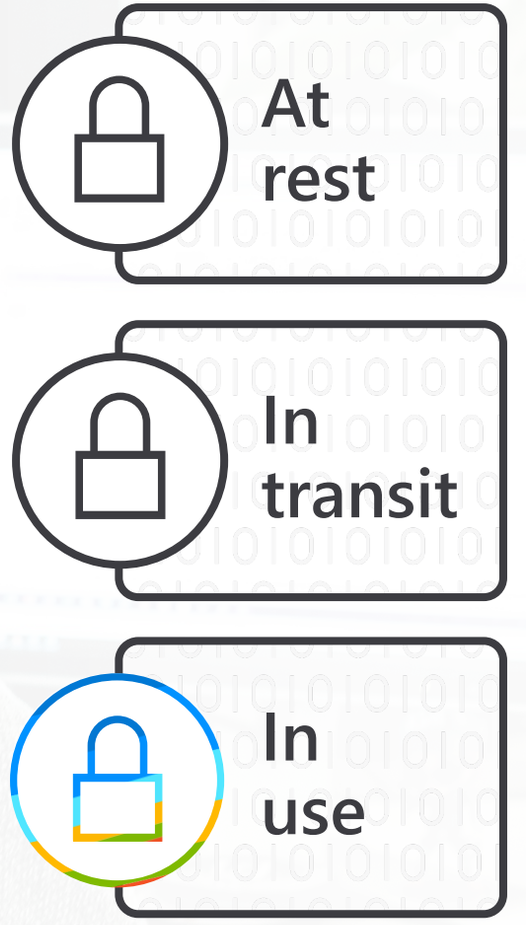
Layers of abstraction



Announcing!

Confidential Computing
for Kubernetes





Existing encryption

Trusted Execution Environment

Confidential Computing use cases

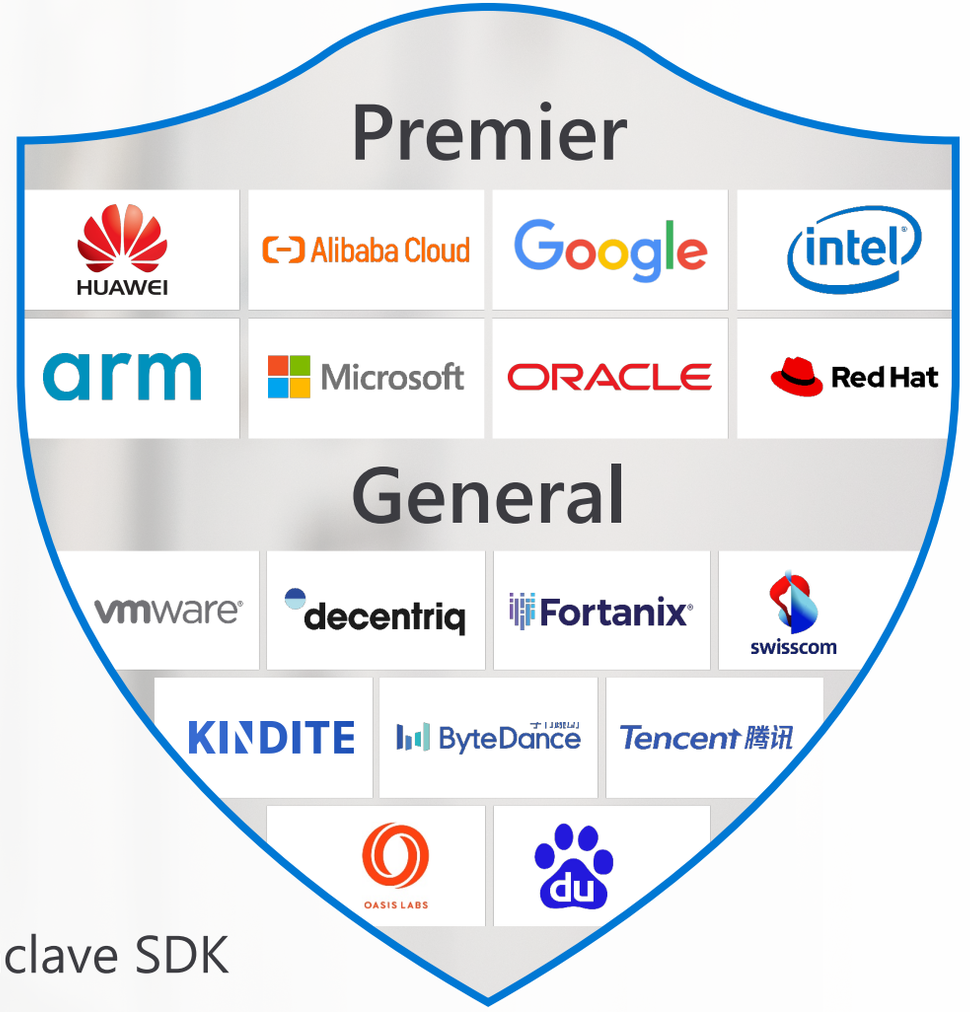
Scenario	Use Case
Securing LOB workloads	Payment processing
Targeted benefits	Credit card offers
Reducing the need for trust	Distributed consensus
Multi-party ML	New medicines

CONFIDENTIAL COMPUTING CONSORTIUM

confidentialcomputing.io

Confidential Computing Consortium

A community effort under the Linux Foundation to secure data in use



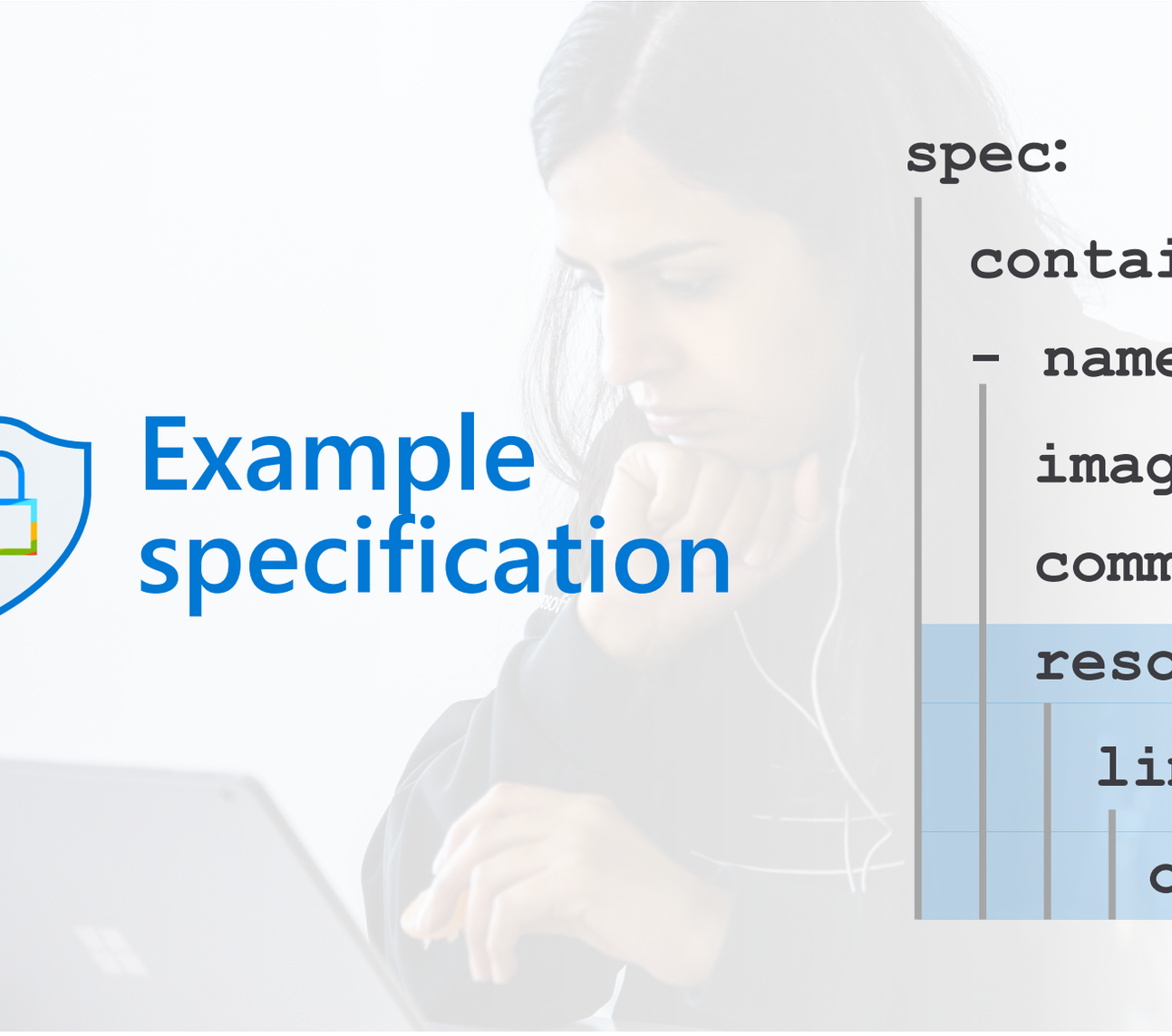
PROJECTS: Intel Software Guard Extensions SDK | Open Enclave SDK

@OpenAtMicrosoft

Microsoft Azure

Using Open Enclave SGX device plugin

```
$ kubectl get nodes node01 -o yaml
[...]
status:
  allocatable:
    cpu: "4"
    memory: 15656620Ki
    openenclave.io/sgx_epc_MiB: "82"
[...]
```



Example specification

```
spec:
  containers:
  - name: <image_name>
    image: <image_reference>
    command: <exec>
    resources:
      limits:
        openenclave.io/sgx_epc_MiB: 64
```

Next steps

VISIT the Azure booth to talk about Confidential Computing and related open source projects

aka.ms/kubecon2019SD