SCONE

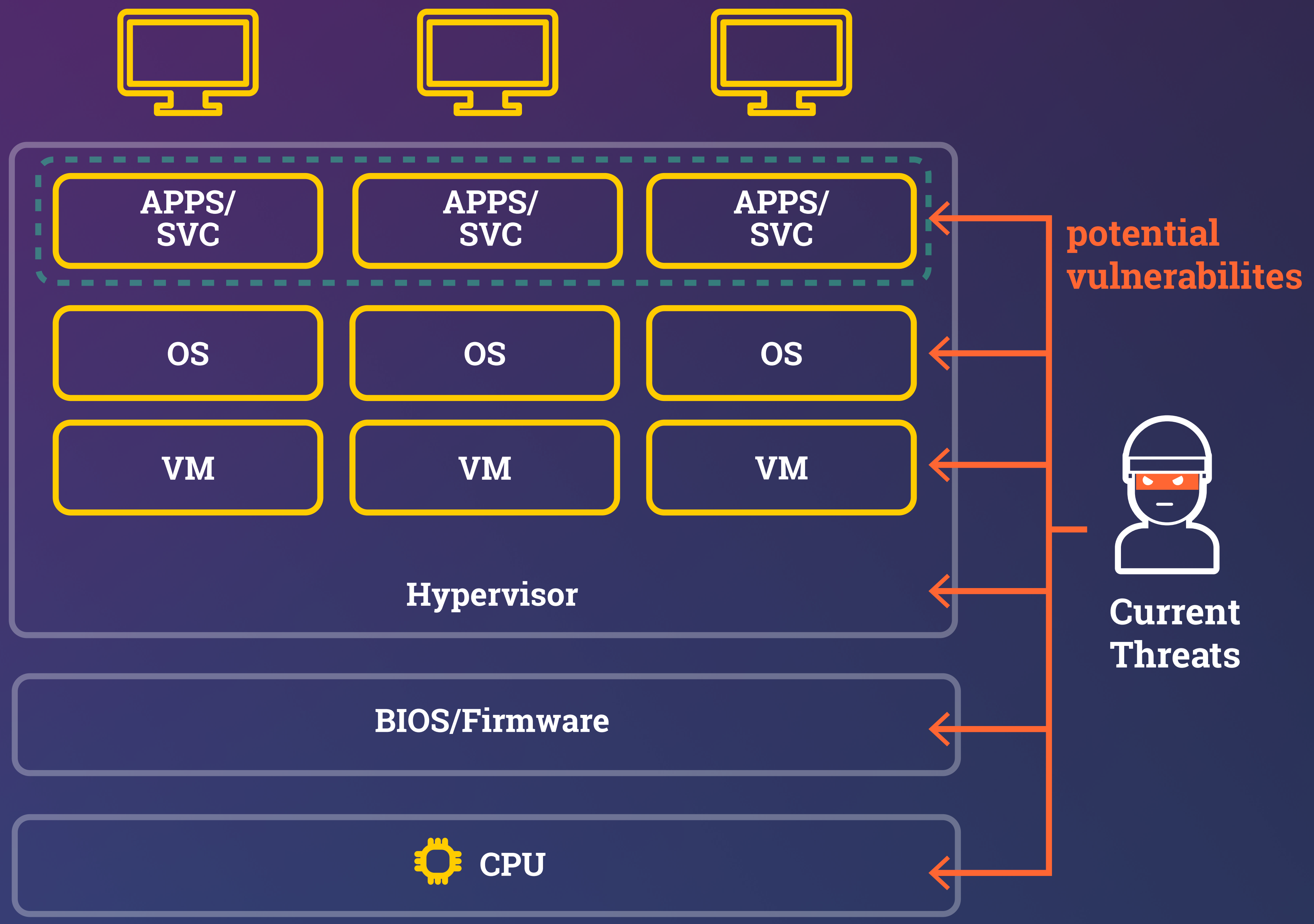
Christof Fetzer, PhD

CONFIDENTIAL COMPUTING WITH SCONE & SGX

christof.fetzer@scontain.com

https://sconedocs.github.io/
https://scontain.com/

SCONE: FOCUS ON APPLICATIONS & SERVICES



APPS/ SVC

APPS/ SVC

APPS/ SVC

OS

OS

OS

VM

VM

VM

Hypervisor

BIOS/Firmware

CPU

potential vulnerabilites

Current Threats

Protect the DATA & CODE

At rest

In flight

In use

ATTEST the Platform & Code

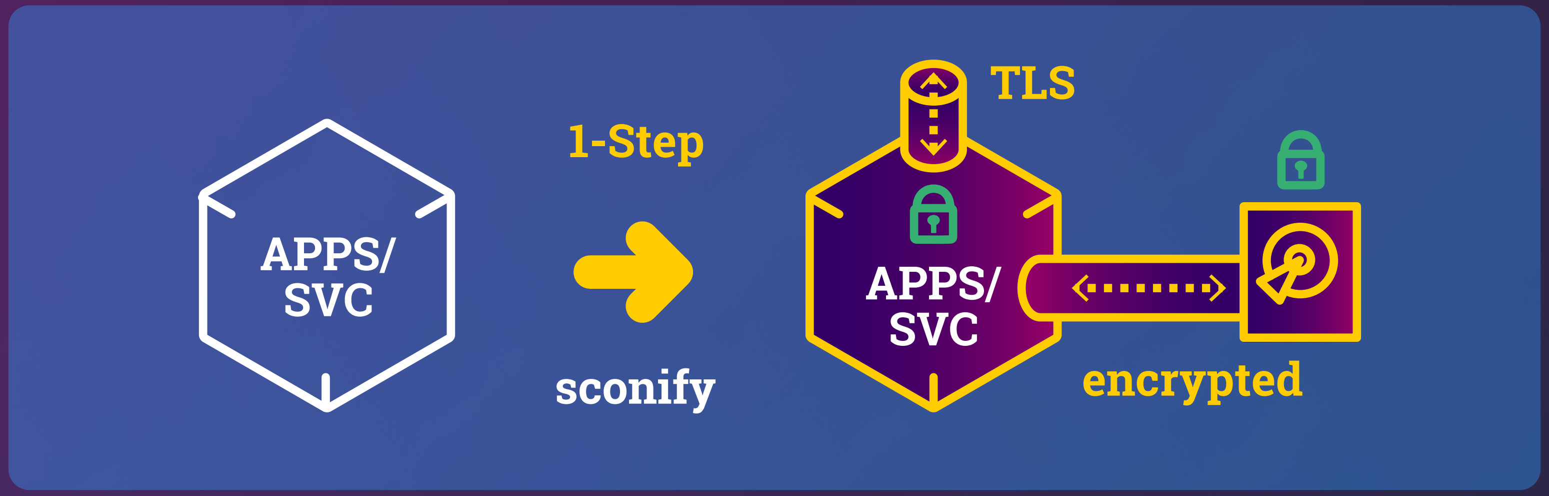
Trust

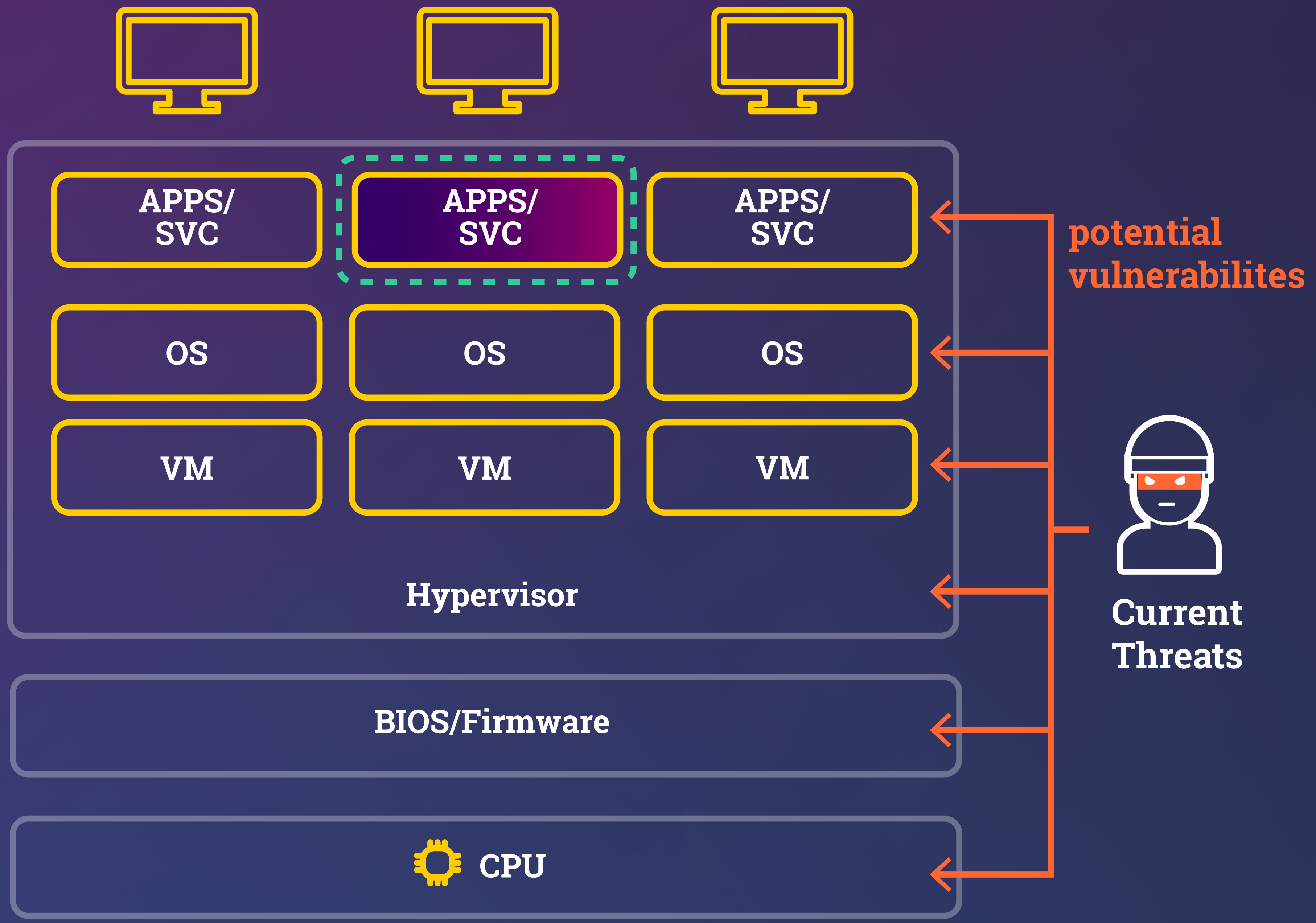
Resilience

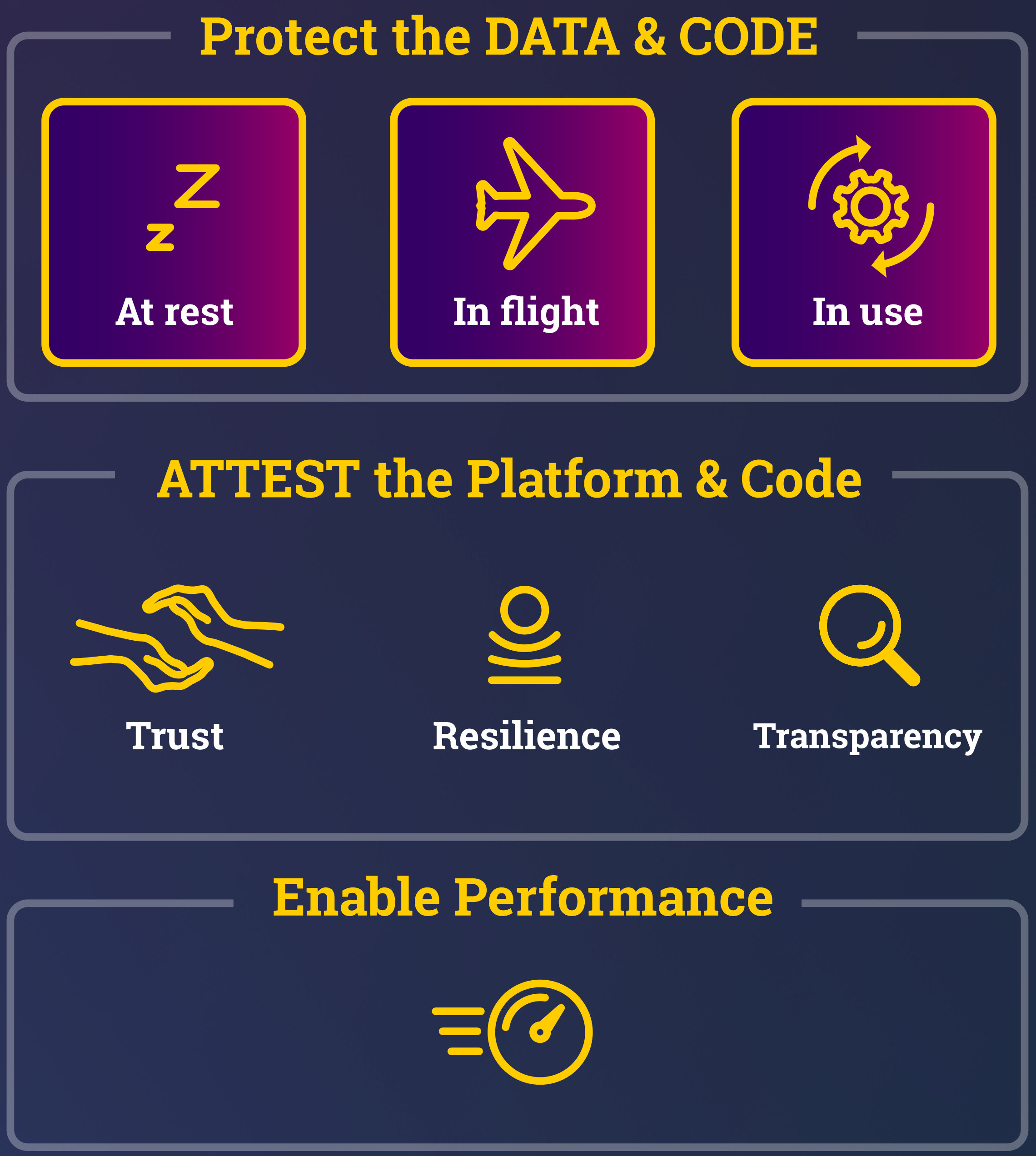
Transparency

Enable Performance

SCONIFY: Native » Confidential Container Image

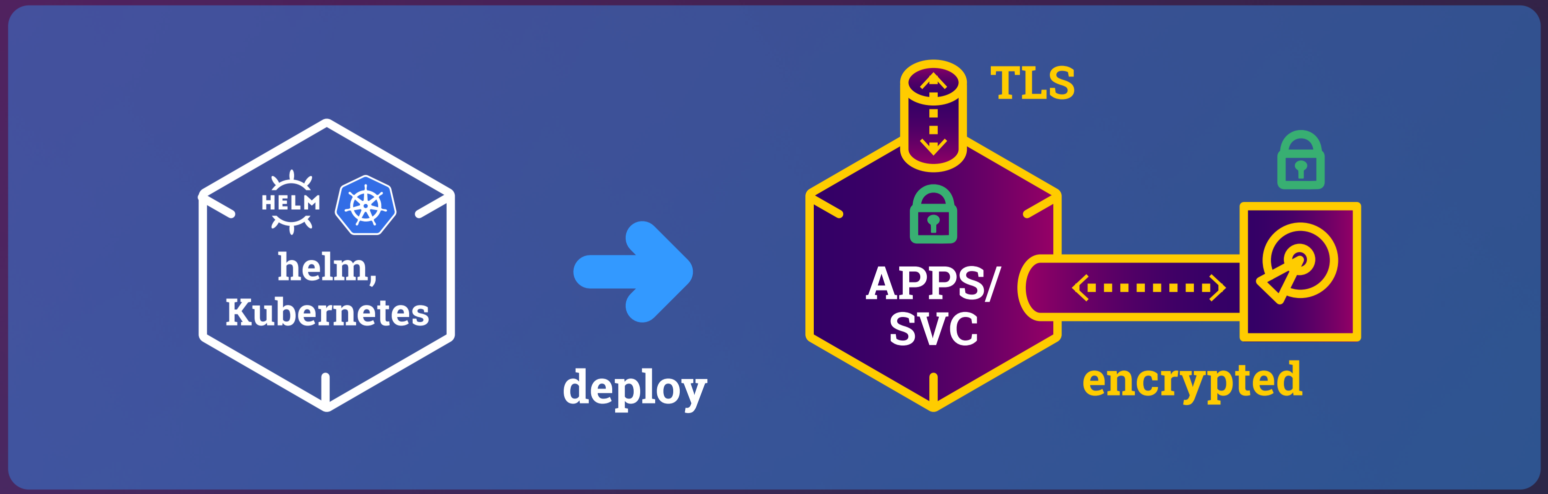


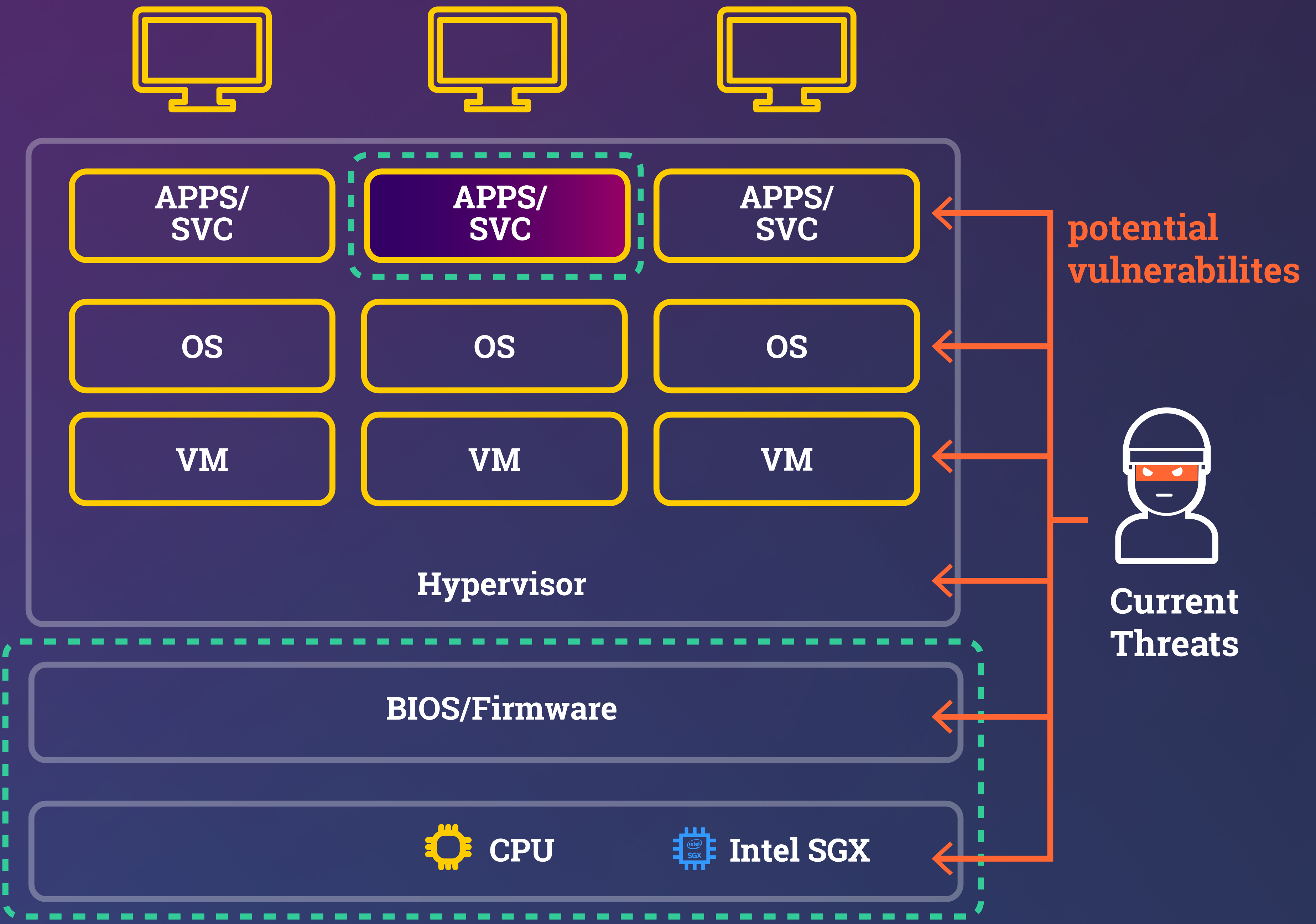


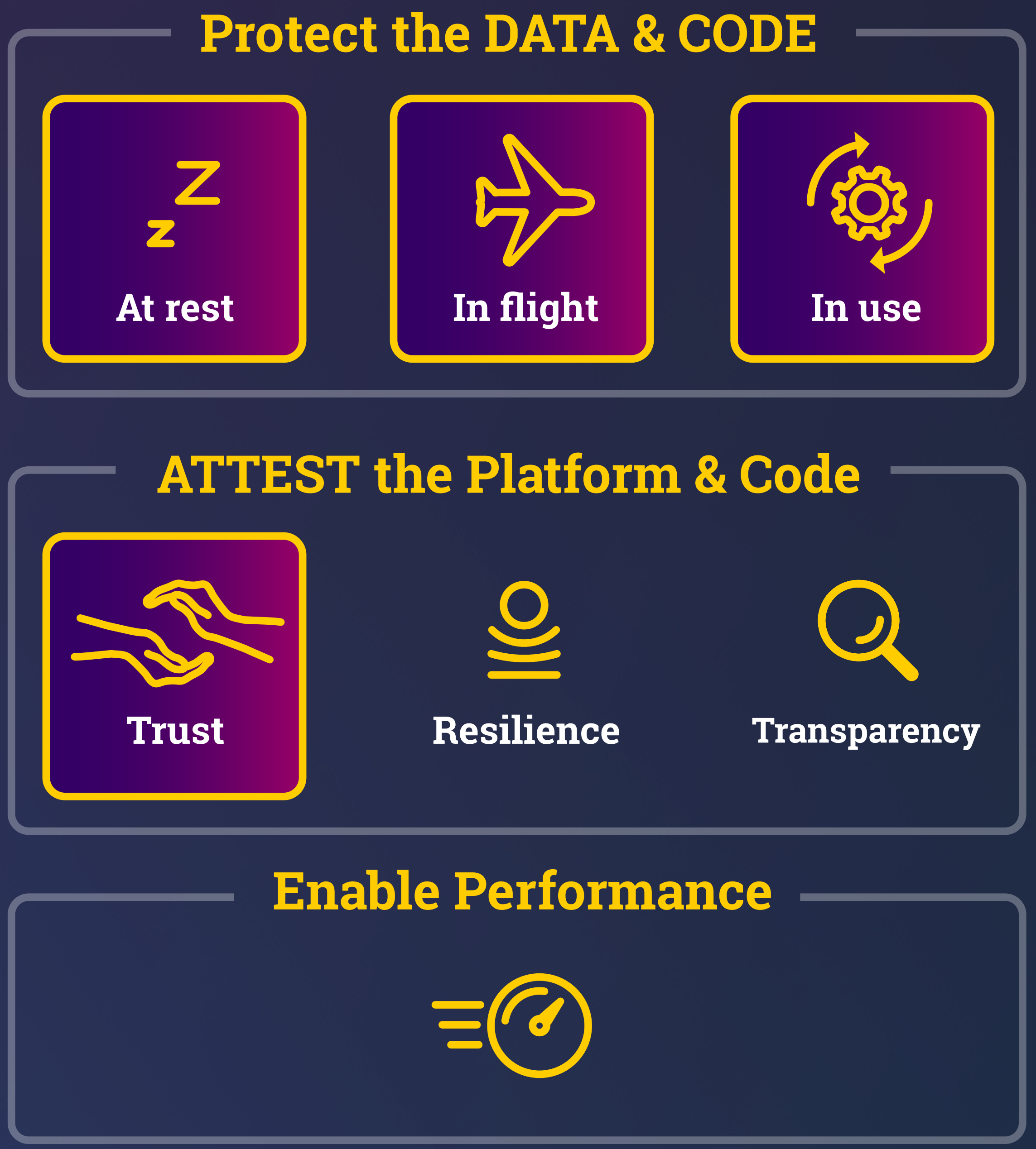


TRANSPARENT ATTESTATION: Enforcing Cyber Hygiene

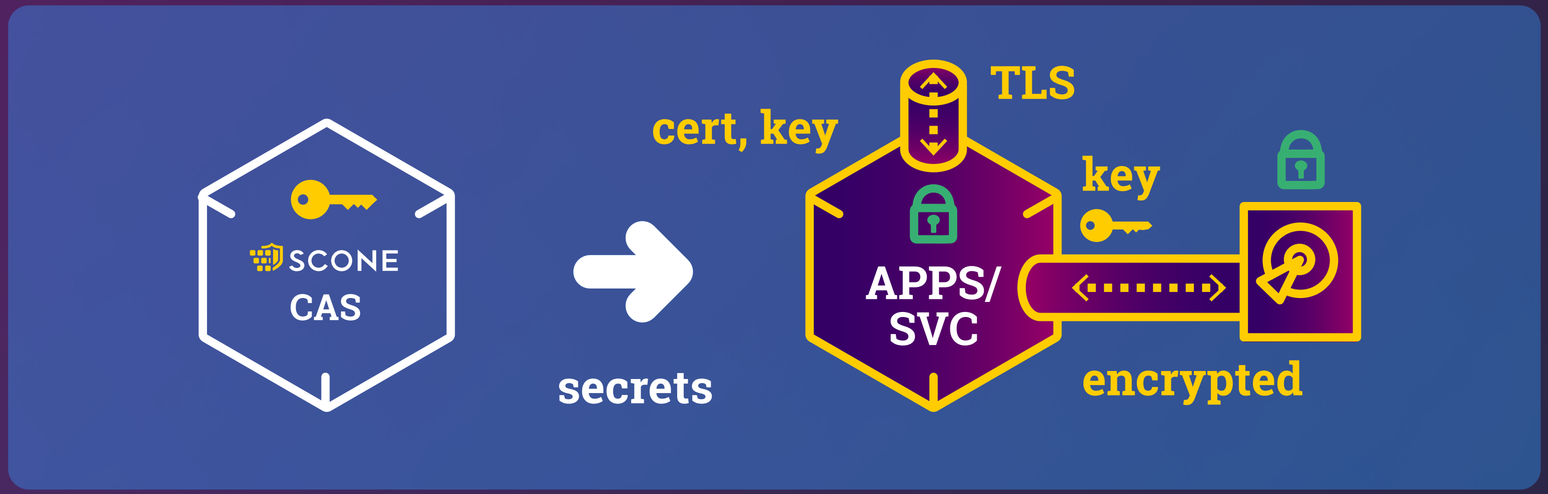
attest that genuine SGX,
up-to-date firmware
& app code



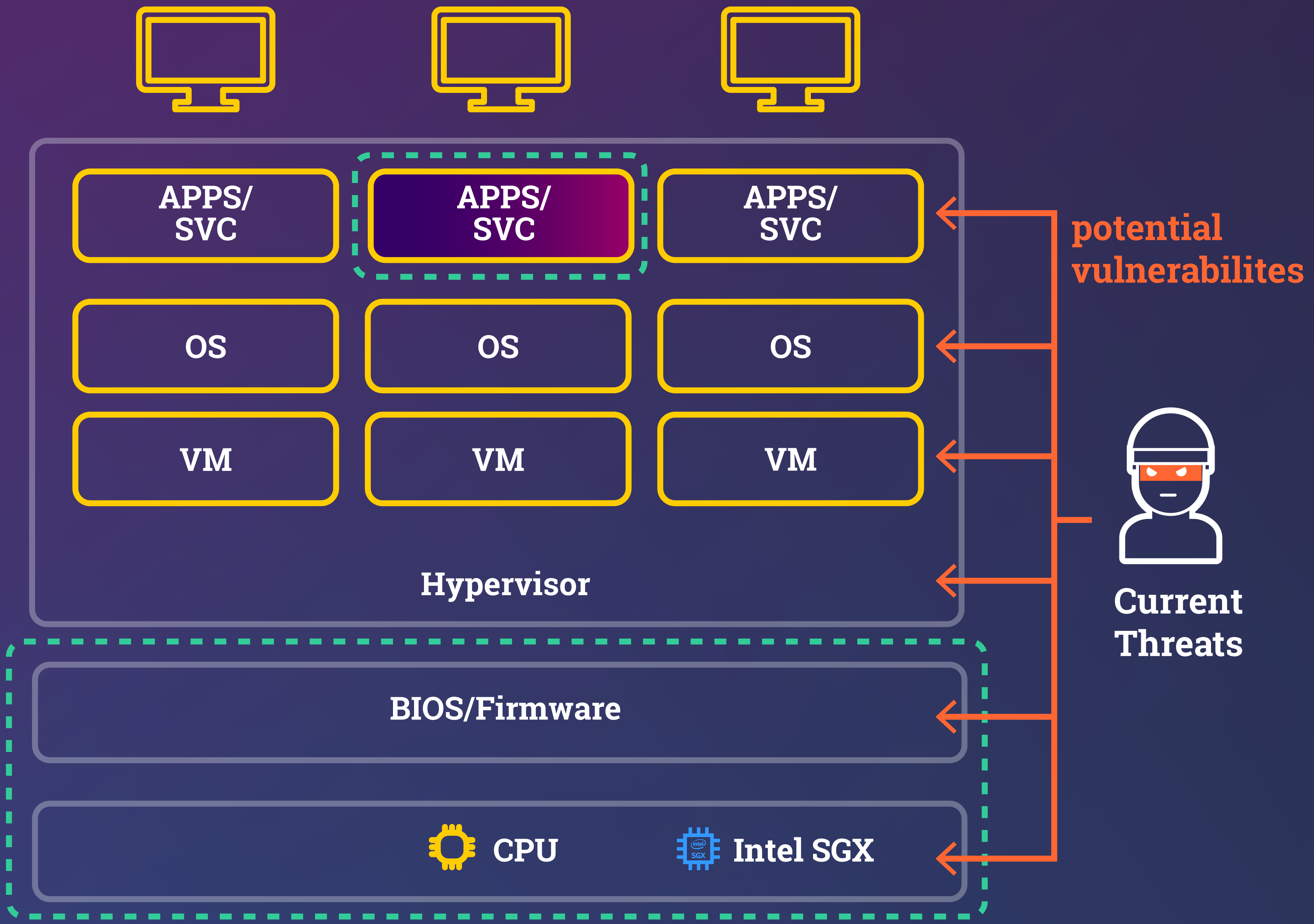


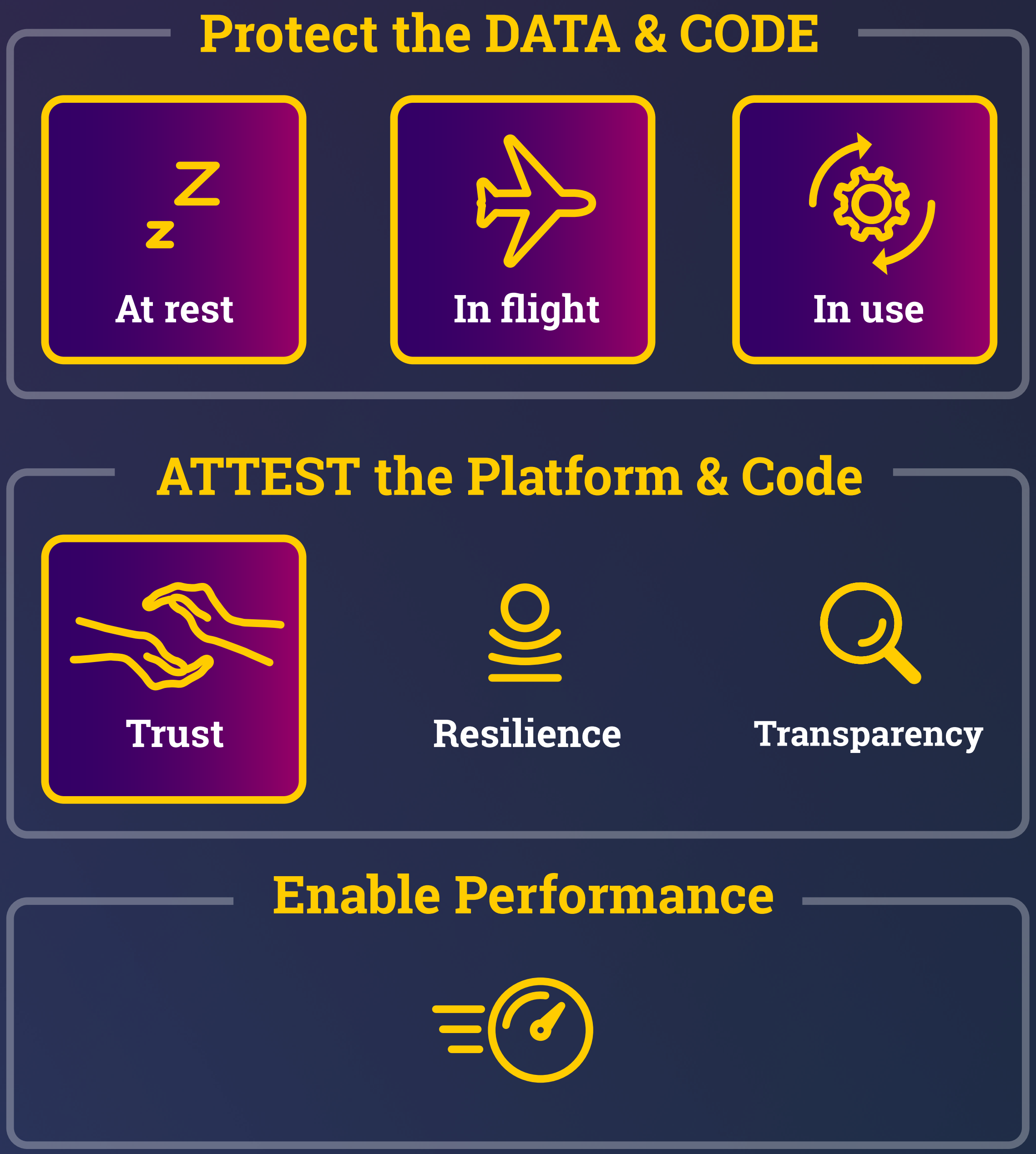


Transparent Secret Provision



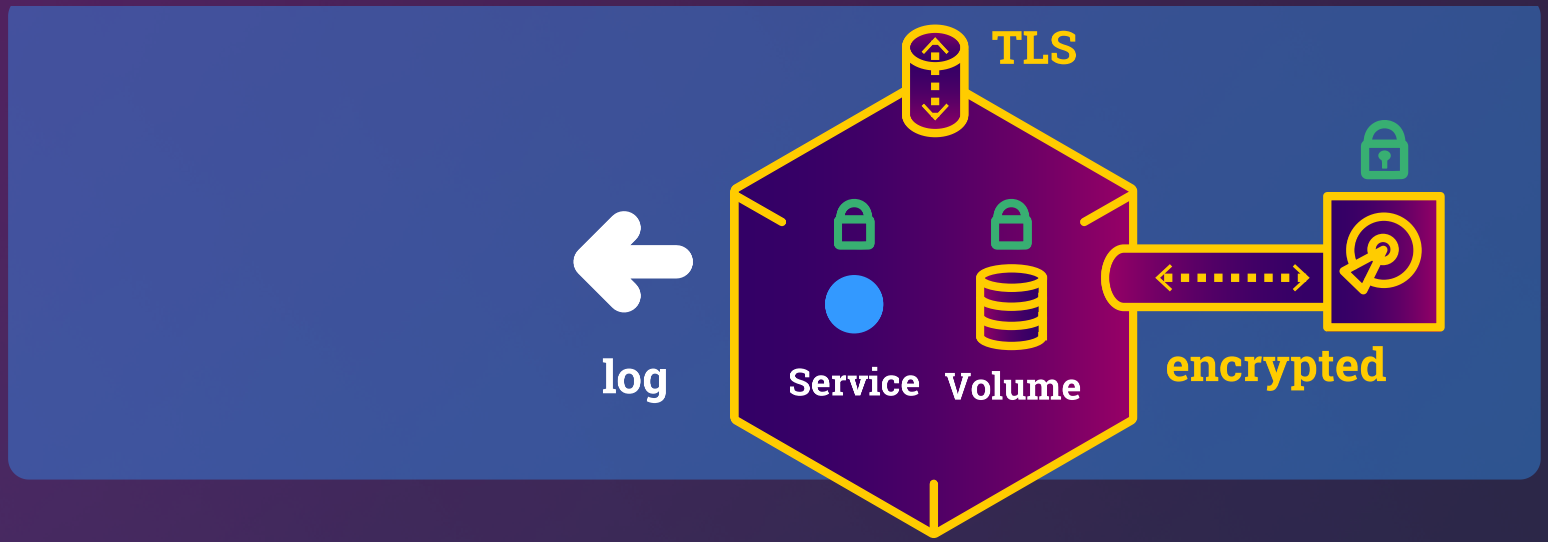
generate certs/keys & provisioning of secrets & certs

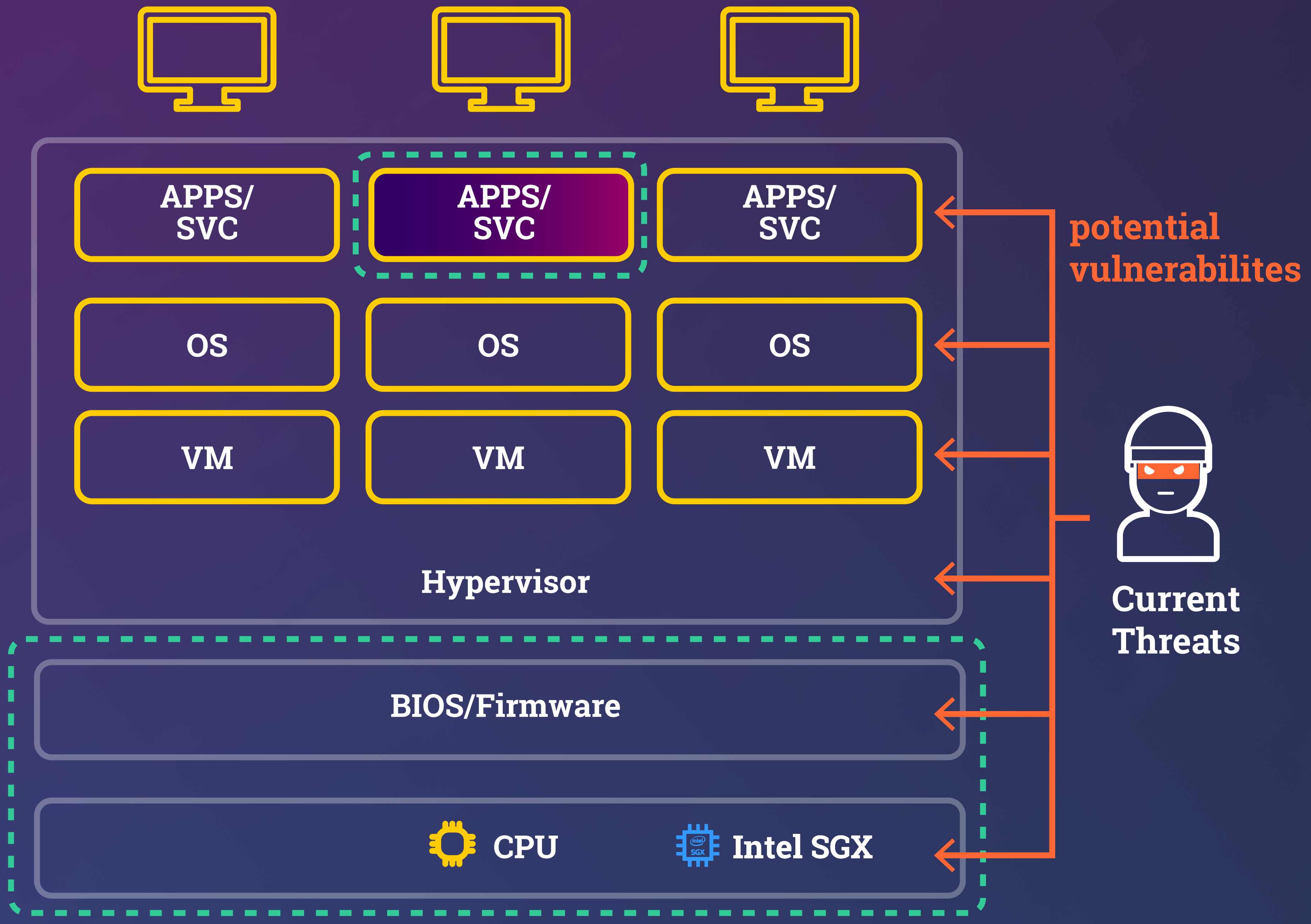


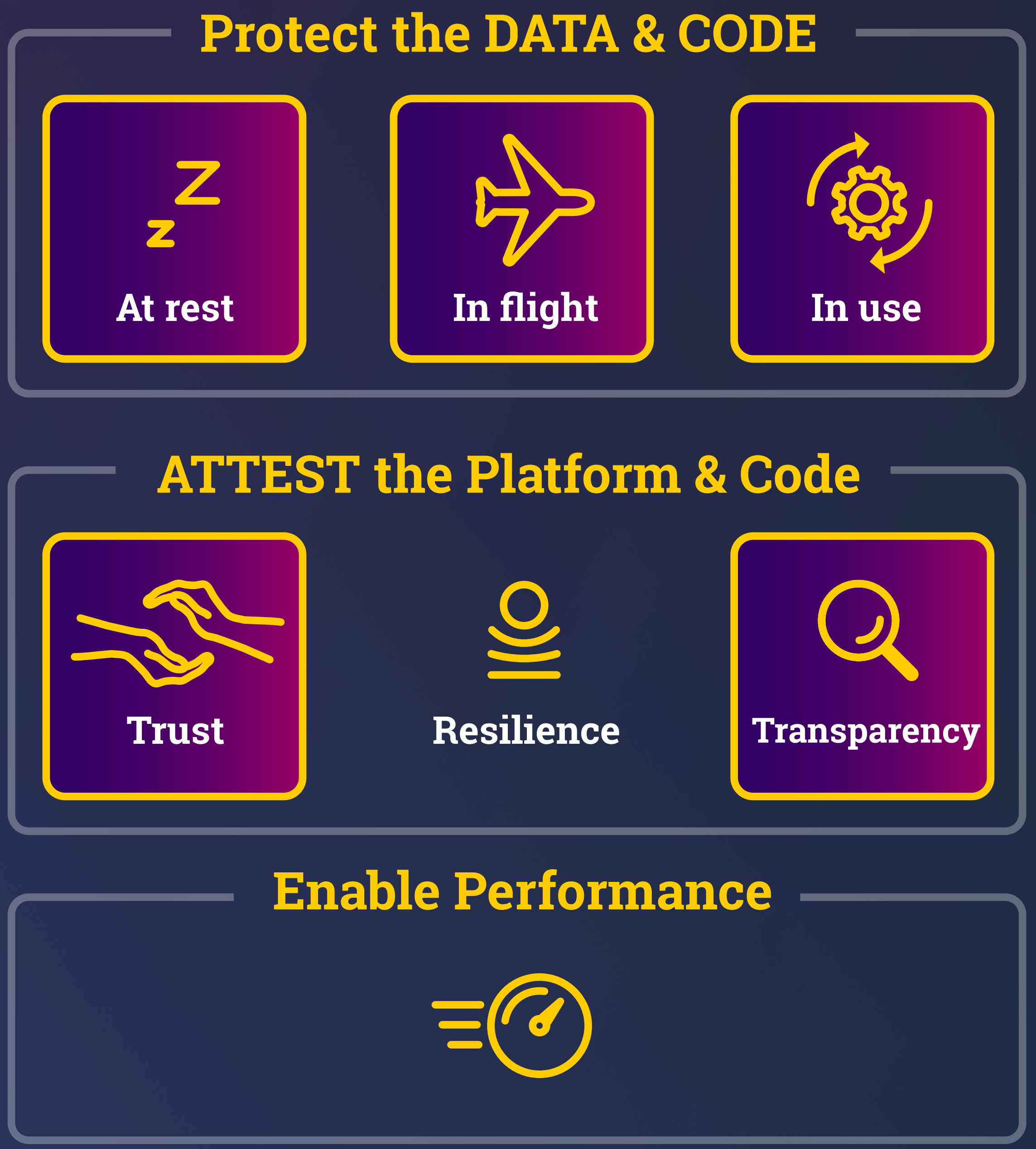


SCONE: Transparency of usage & changes

audit log of all attestations, policy changes,…

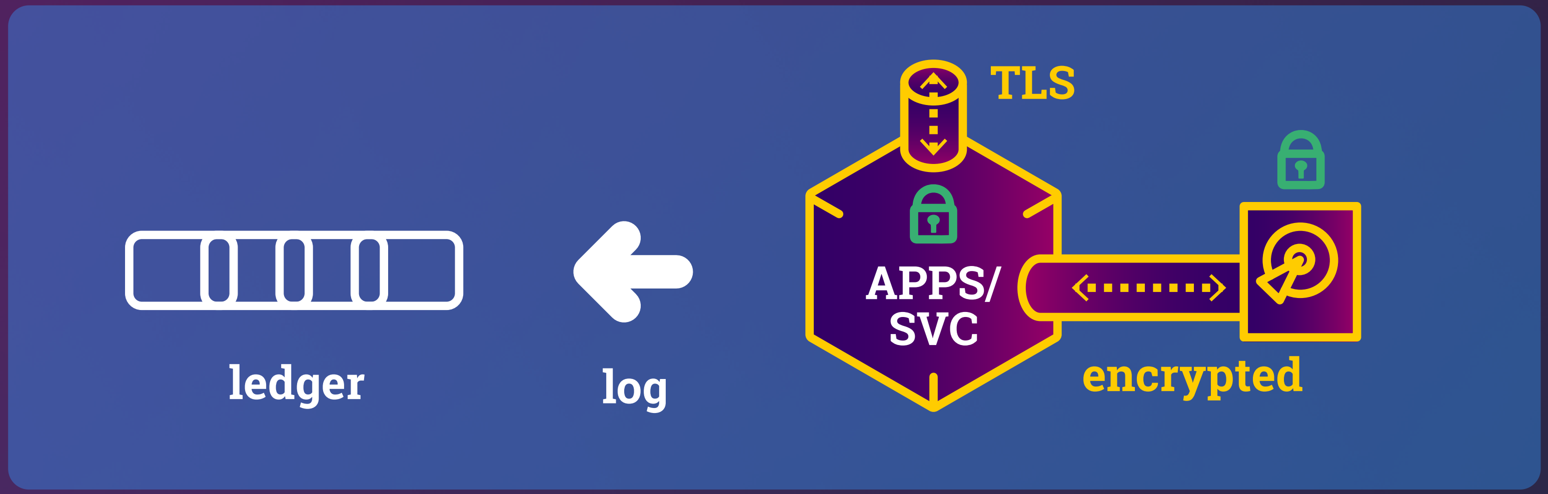






SCONE: Ledger to enforce transparency

audit log of all
attestations,
policy changes,... **in ledger**



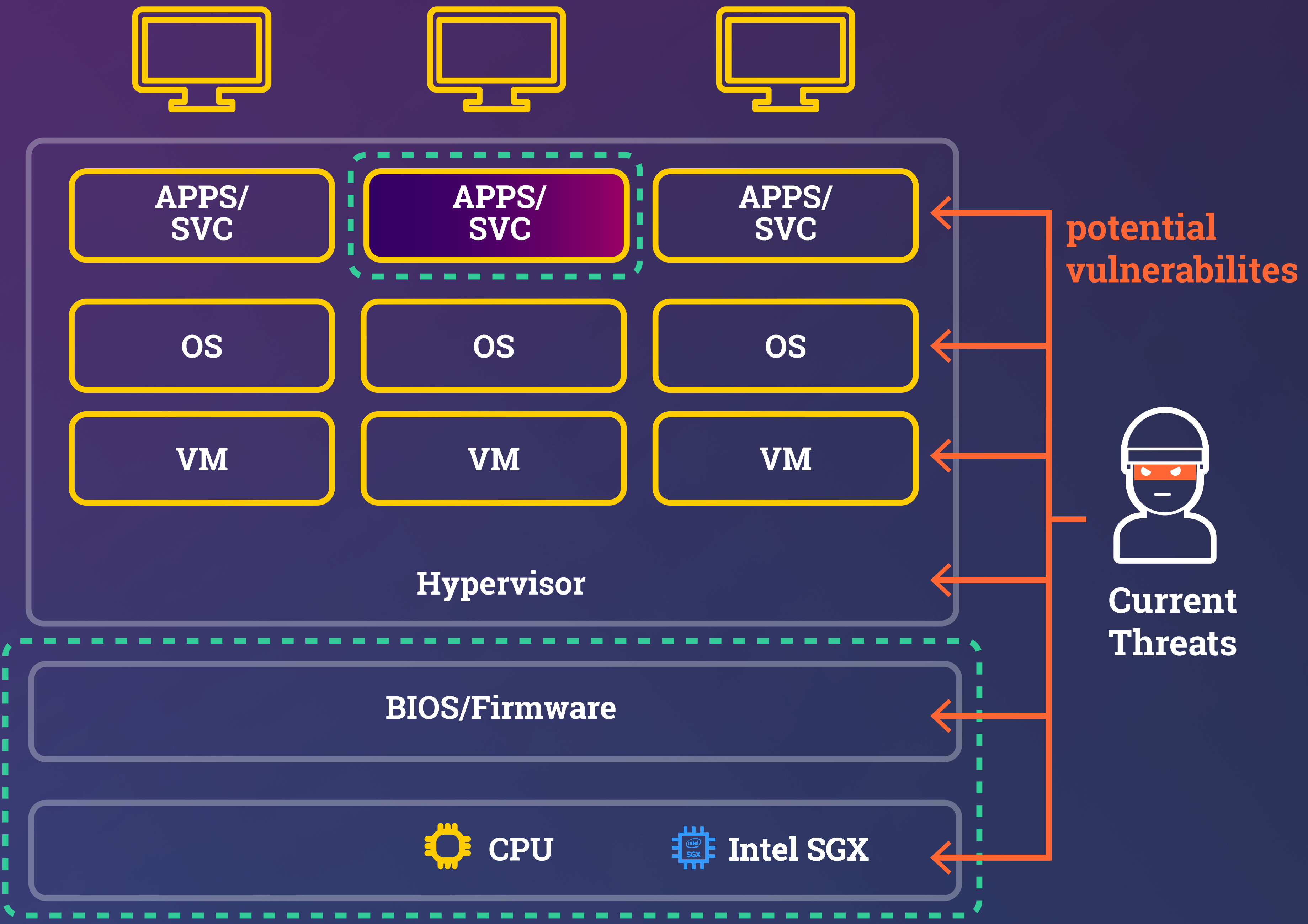
TLS

APPS/
SVC

encrypted

ledger

log



APPS/
SVC

APPS/
SVC

APPS/
SVC

OS

OS

OS

VM

VM

VM

Hypervisor

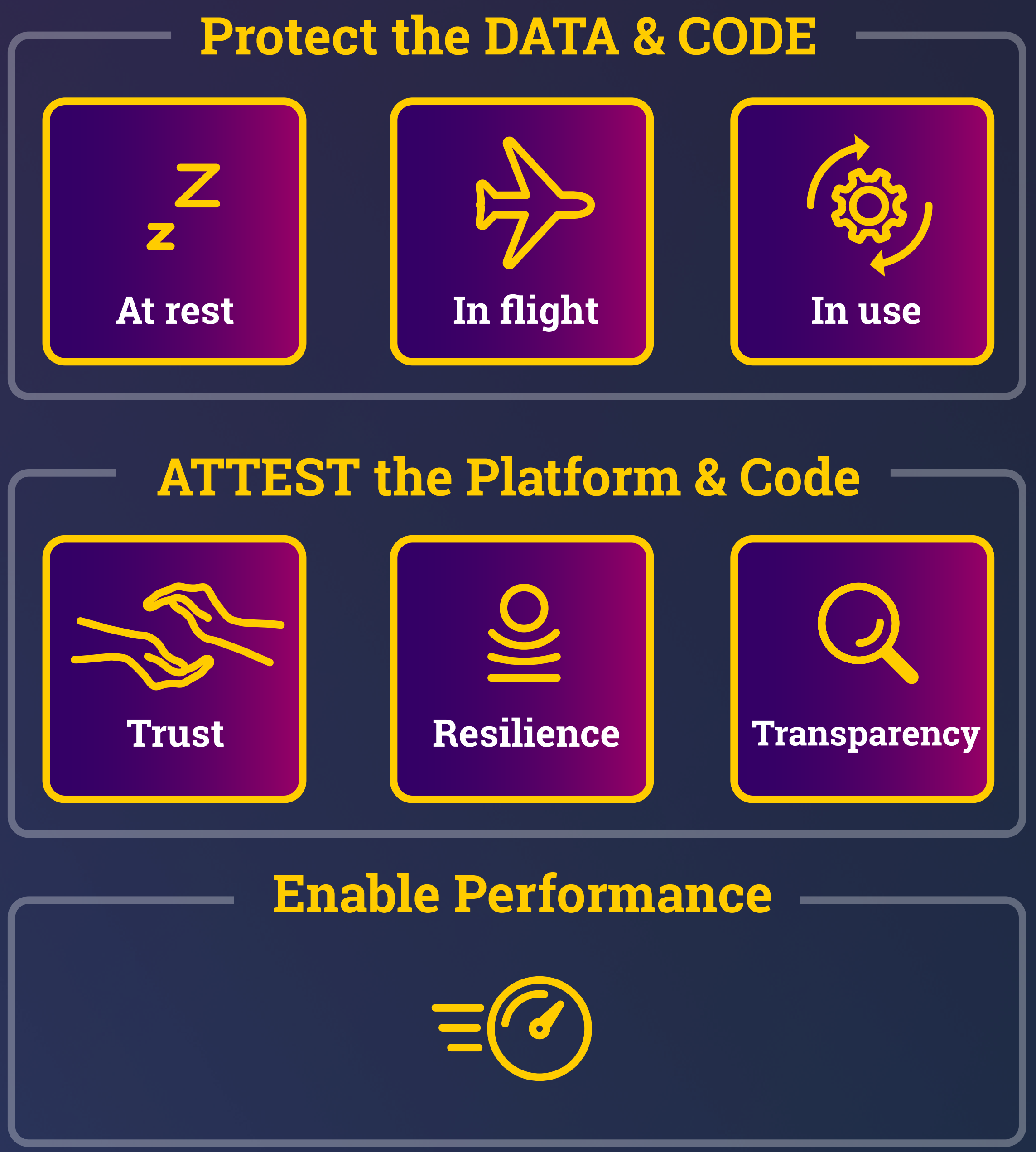
BIOS/Firmware

CPU

Intel SGX

potential
vulnerabilites

Current
Threats



Protect the DATA & CODE

At rest

In flight

In use

ATTEST the Platform & Code

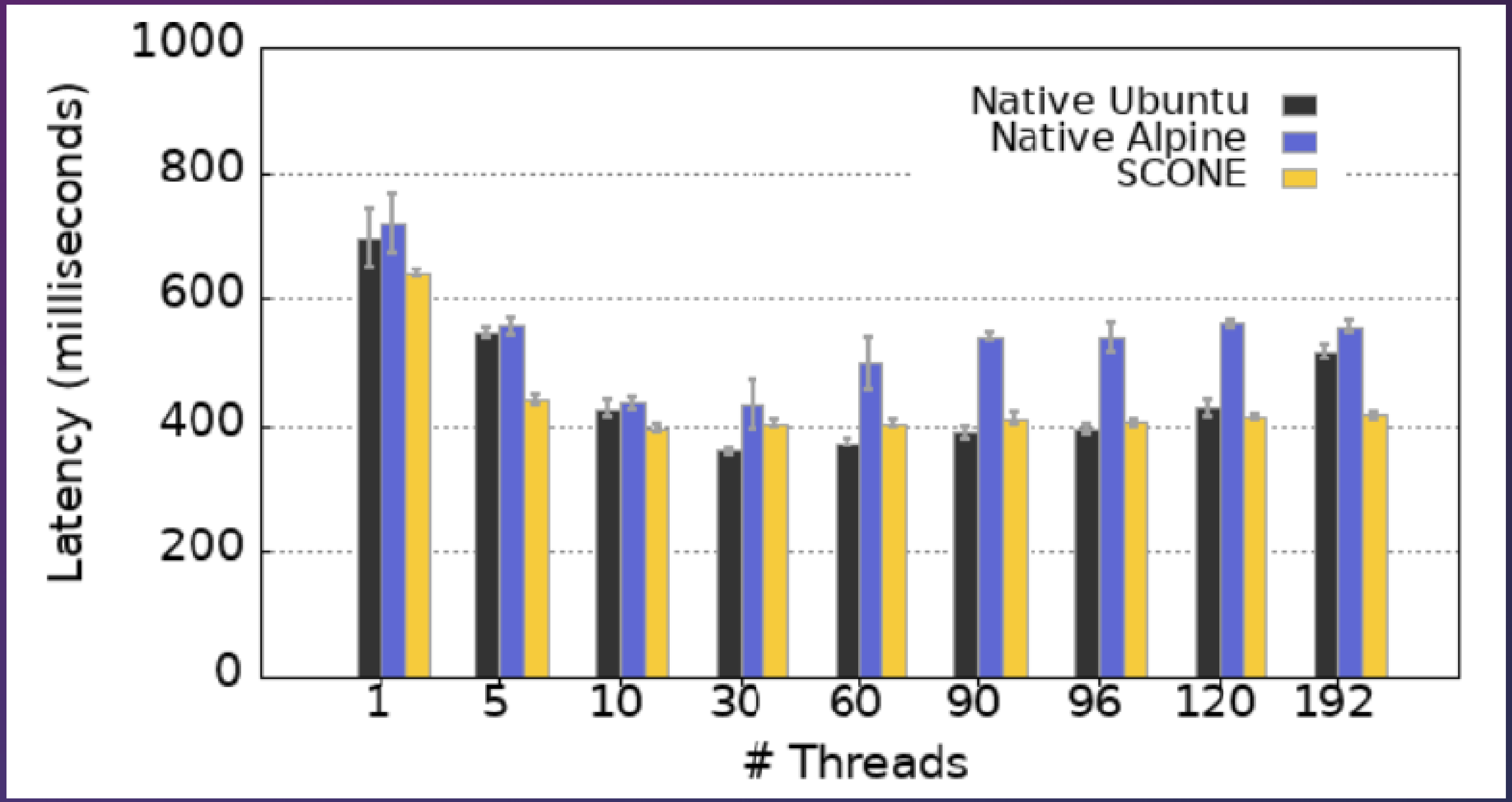
Trust

Resilience

Transparency

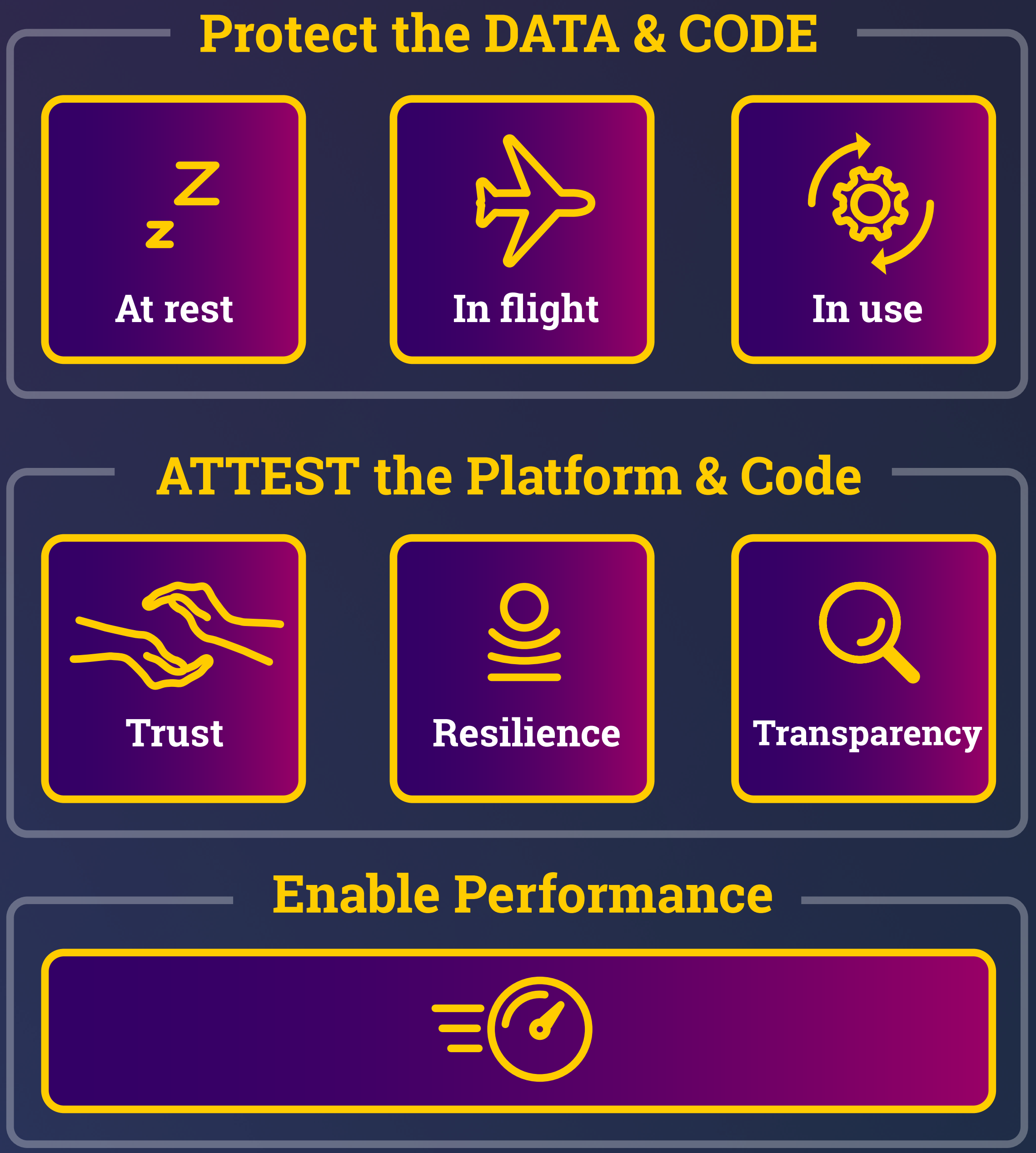
Enable Performance

SCONE : Excellent Performance



Intel Icelake:
close to native performance

TensorFlow Lite



Protect the DATA & CODE

At rest

In flight

In use

ATTEST the Platform & Code

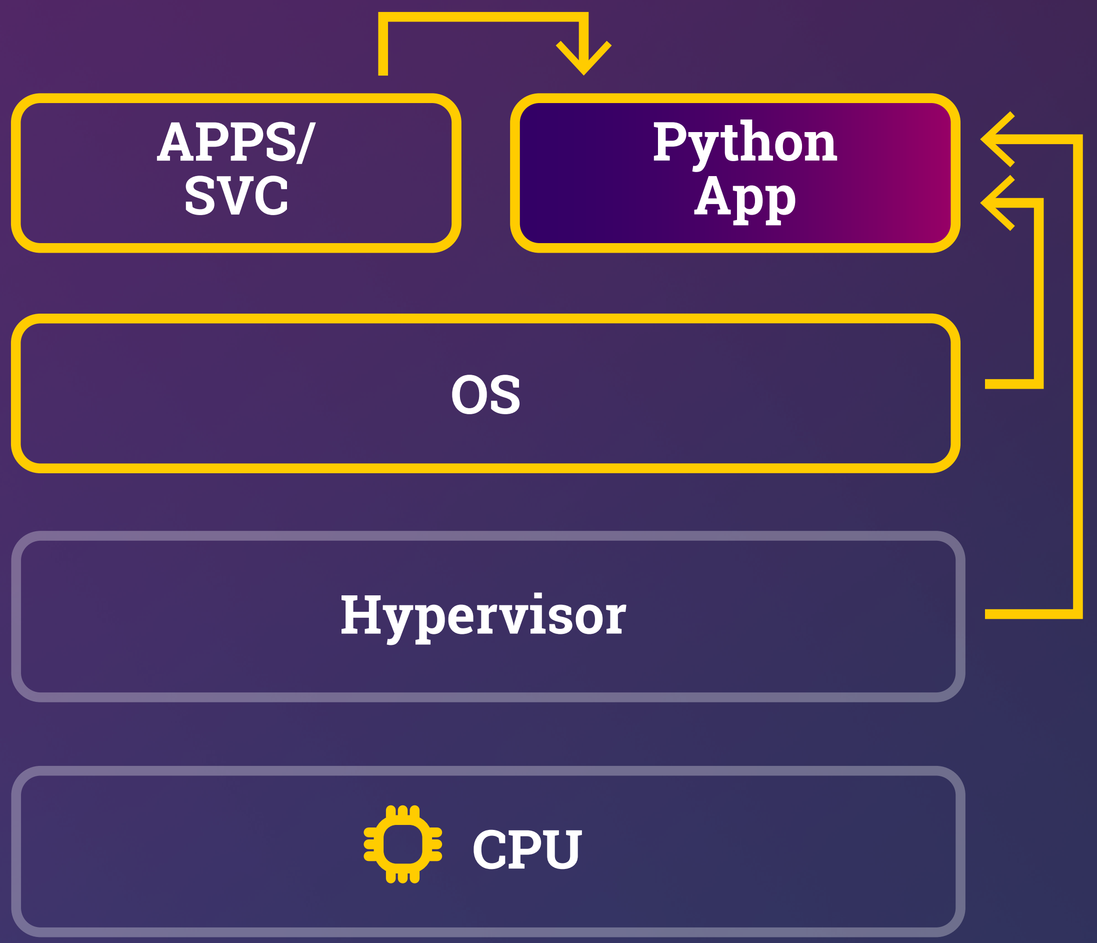
Trust

Resilience

Transparency

Enable Performance

Why Protect Data and Code?



Protect against

Malicious insiders with escalated admin privileges

Hackers exploiting bugs in the hypervisor/OS

Third parties accessing data without owner`s consent

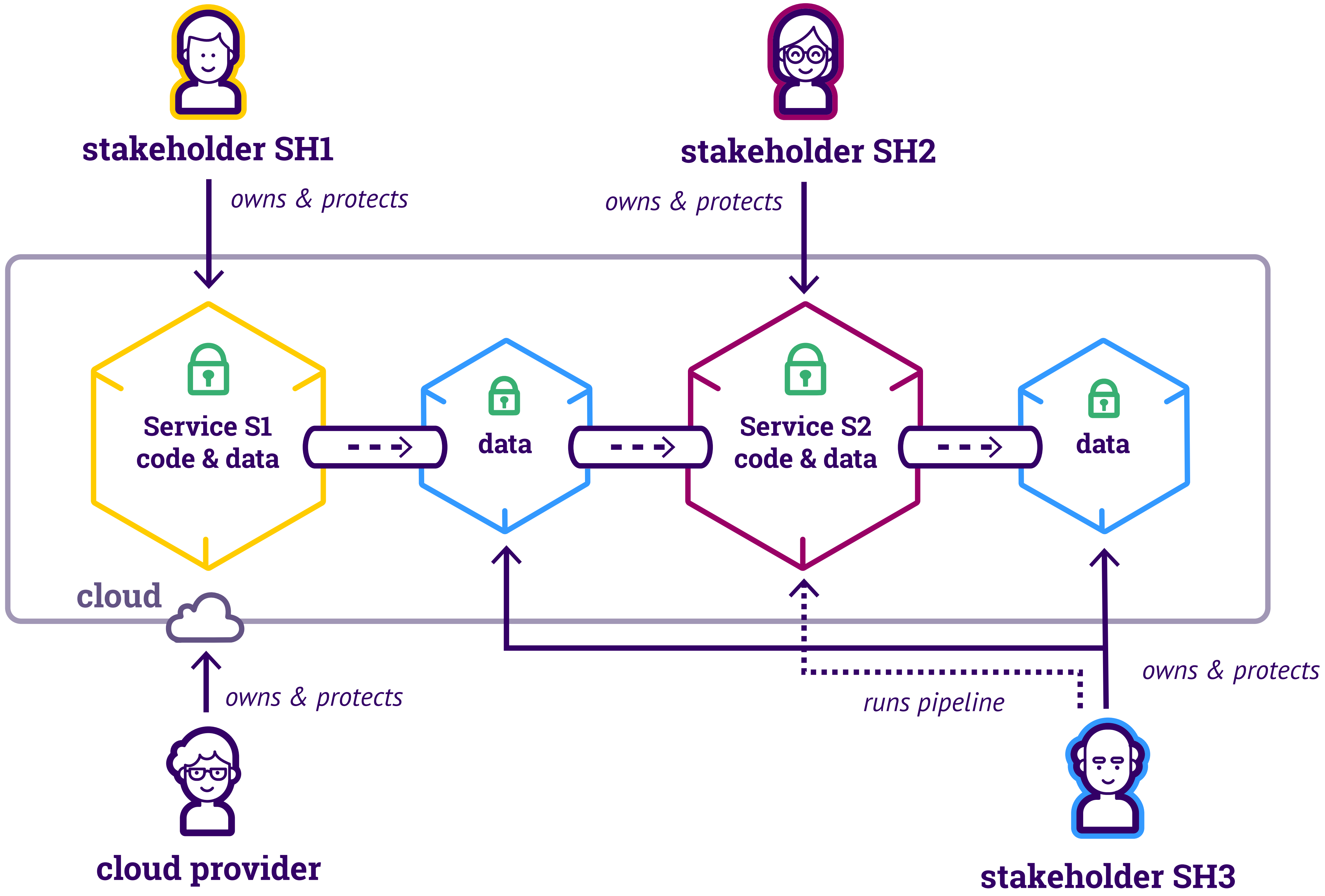
Data & Computation exposed to...

- Guest OS
- Host OS
- Hypervisor
- Physical hardware access
- Host admin
- VM admin
- Kubernetes admin
- Service admin
- Collaborator

example

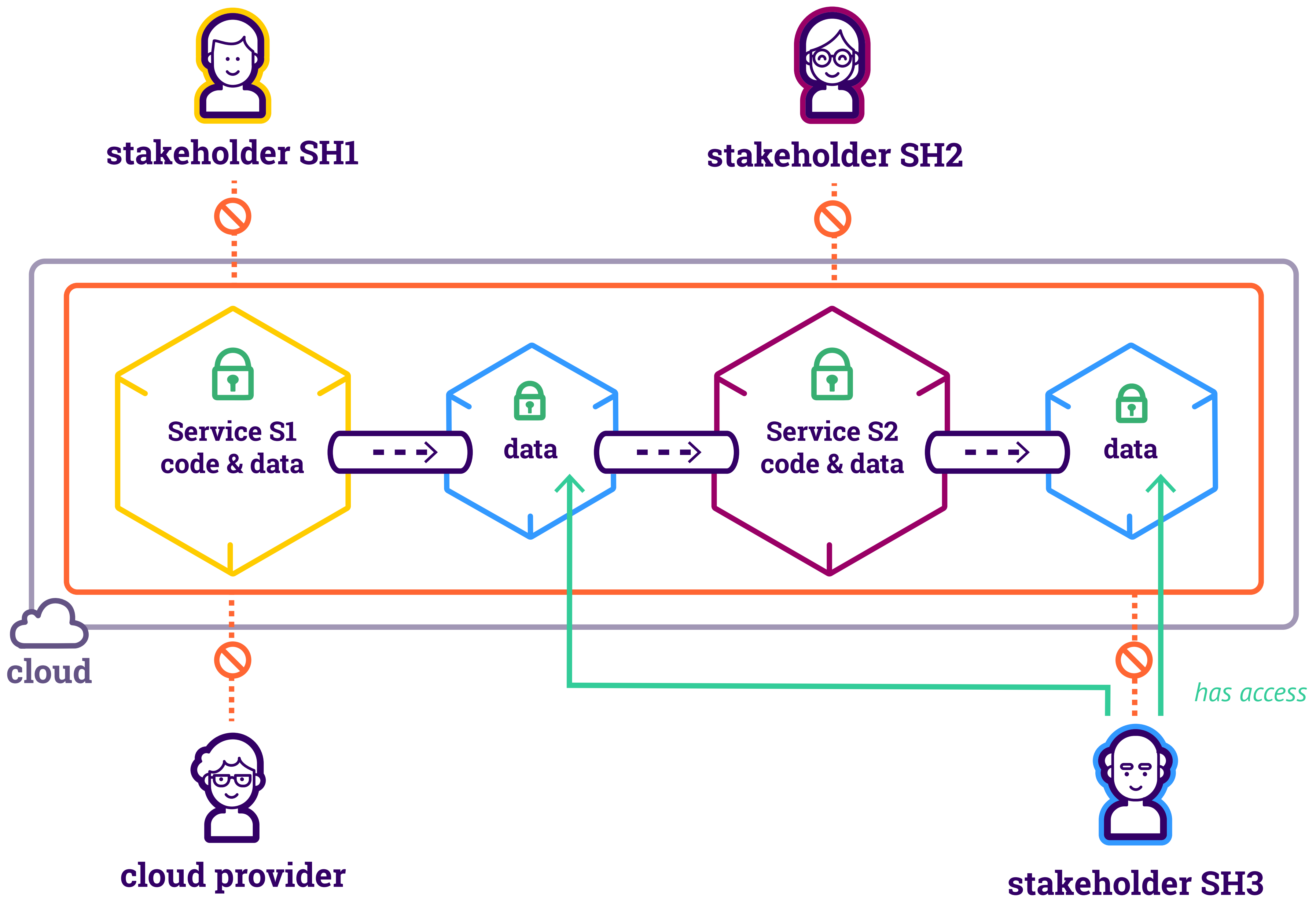
USE CASE: Multiple Stakeholder Computation I

- Computations encompassing multiple stakeholders
- Each stakeholder protects its own IP
- Classical RBAC insufficient to protect IP



Managed Kubernetes cluster

USE CASE: Multiple Stakeholder Computation II



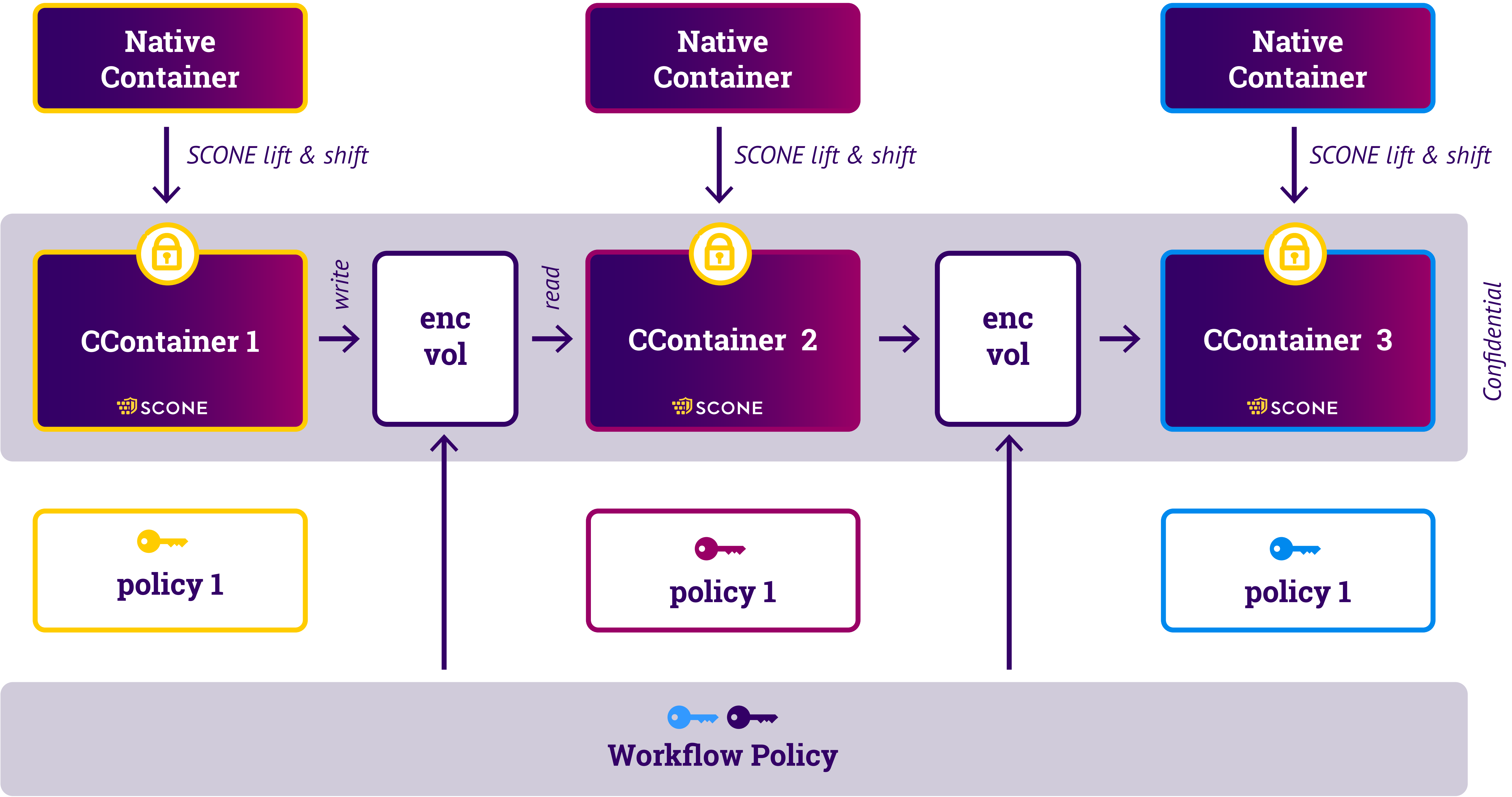
Managed Kubernetes cluster

- Confidential workflow connects confidential services
- Each stakeholder controls its IP via own policies
- Even operator of workflow cannot look into individual service

USE CASE: Multiple Stakeholder Computation III

1-step binary transformation images

Each policy protects resources of its stakeholders



A policy can connect a workflow

Application Domains:
Federated Learning, eHealth, Manufacturing

SCONTAIN

Products

https://sconedocs.github.io

https://scontain.com

Contact

info@scontain.com