Tyche

Composable Isolation as a Foundation to Manage Trust in the Cloud

Adrien Ghosn[1], *Charly Castes*[2], *Neelu S. Kalani*[2], *Yuchen Qian*[2], *Marios Kogias*[3], *Edouard Bugnion*[2]

[1] Microsoft Azure [2] EPFL [3] IMPERIAL

Composable Isolation

Composable Isolation

Restrict what a piece of software can do.

Composable Isolation

Restrict what a piece of software can do.



Least Privilege

Composable Isolation

Restrict what a piece of software can do.



Least Privilege

=

sandboxes **VMs**



Encapsulation

restrict what it does to **others**

Composable Isolation

Restrict what a piece of software can do.

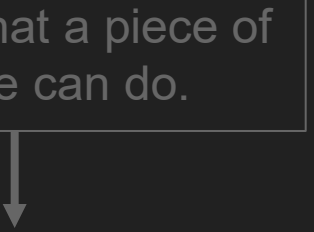


Composable Isolation



Composable Isolation

Restrict what a piece of software can do.



Least Privilege



sandboxes **VMs**

enclaves **CVMs**



Encapsulation



Confidential Computing

Required for Cloud Workloads…

Composable Isolation

Restrict what a piece of software can do.

Least Privilege = **sandboxes** **VMs** + **enclaves** **CVMs** **Confidential Computing**

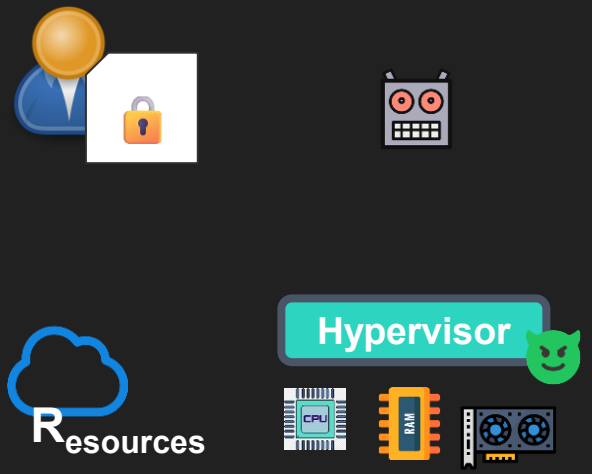
Required for Cloud Workloads… but HARD

Private Inference in Public Cloud



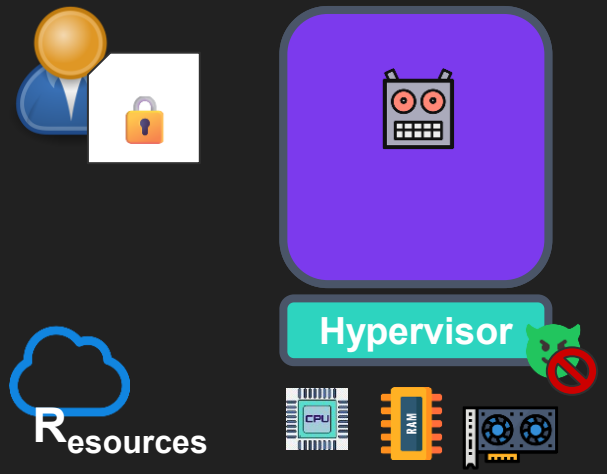
Private Inference in Public Cloud

R



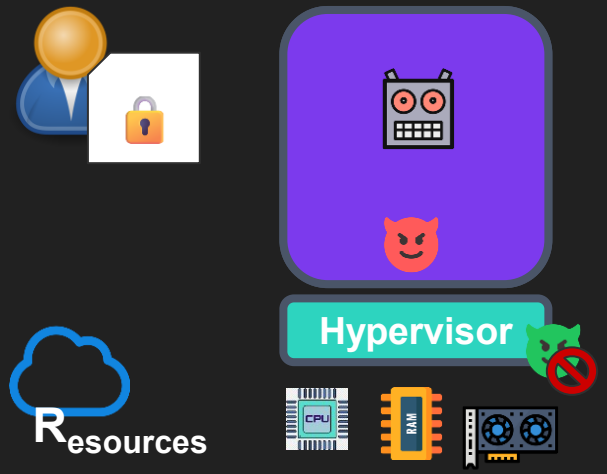
Private Inference in Public Cloud

C_{VM} (R)



Private Inference in Public Cloud

C_{VM} (R)



Private Inference in Public Cloud

$$E_{nclave}\ (\ C_{VM}\ (R)\ )$$



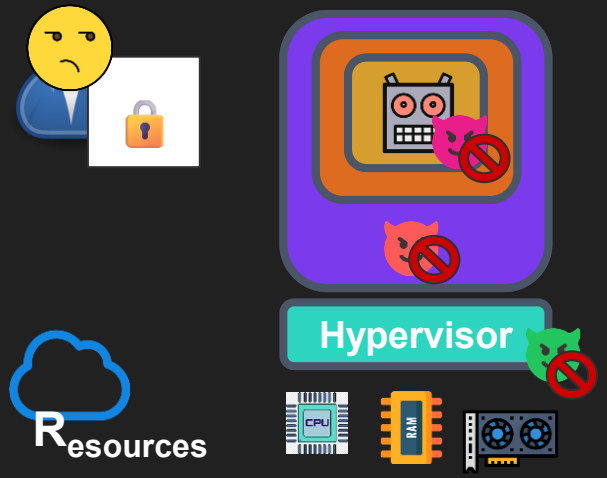
Private Inference in Public Cloud

$$E_{nclave}\ (\ C_{VM}\ (R)\ )$$



Private Inference in Public Cloud

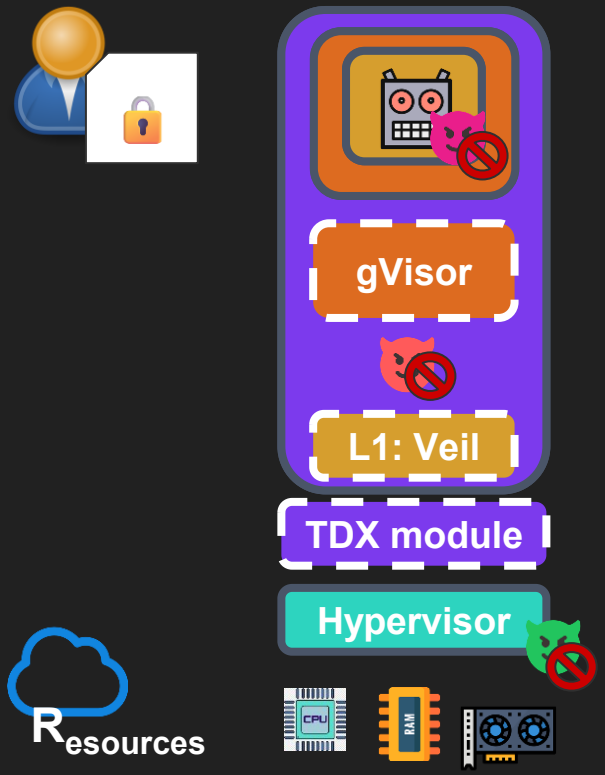
$$S_{andbox}\,(\,E_{nclave}\,(\,C_{VM}\,(R)\,)\,)$$



One Isolation Boundary → One System

Sandbox (Enclave (CVM (R)))

- Sandbox → gVisor+Linux
- Enclave → Veil+L1/L2
- CVM → VTx+TDx



One Isolation Boundary → One System

Sandbox (Enclave (CVM (R)))

- Sandbox → gVisor+Linux
- Enclave → Veil+L1/L2
- CVM → VTx+TDx

✗ Increased TCB



One Isolation Boundary → One System

Sandbox (Enclave (C_{VM} (R)))

- Sandbox → gVisor+Linux
- Enclave → Veil+L1/L2
- C_{VM} → VTx+TDx

✗

- 📈 Increased TCB
- 😓 Deployment complexity



One Isolation Boundary → One System

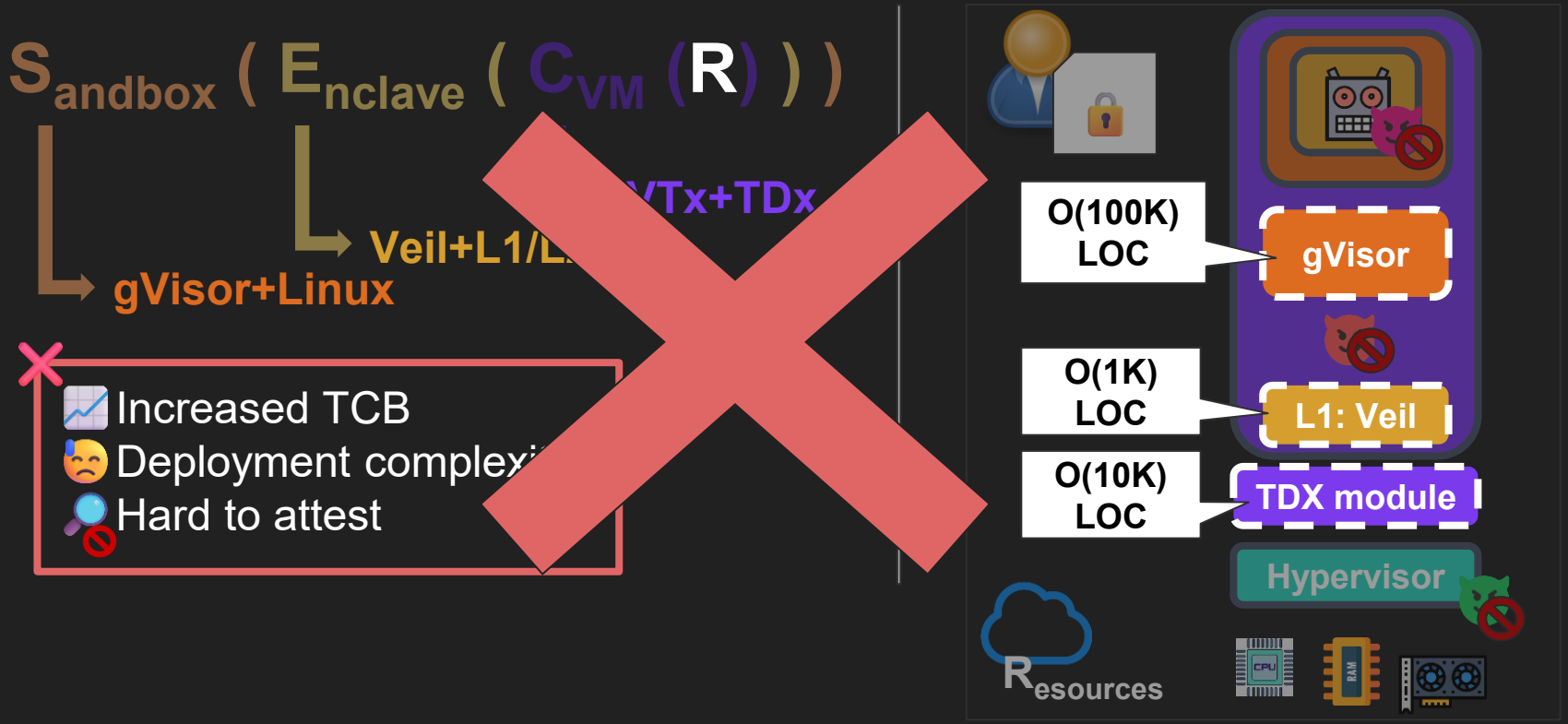
$S_{andbox}\,(\,E_{nclave}\,(\,C_{VM}\,(R)\,)\,)$

- S_{andbox} → gVisor+Linux
- E_{nclave} → Veil+L1/L2
- C_{VM} → VTx+TDx

- Increased TCB
- Deployment complexity
- Hard to attest



One Isolation Boundary → One System



Insight

Composable	Isolation
Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))	sandboxes VMs Encapsulation
	enclaves CVMs Confidential Computing

Insight

	Composable	Isolation
Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))	sandboxes VMs	enclaves CVMs
= S_{andbox} ∘ E_{nclave} ∘ C_{VM} (R)	Encapsulation	Confidential Computing

Insight

Composable

Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))

= S_{andbox} ∘ E_{nclave} ∘ C_{VM} (R)

Isolation

sandboxes VMs — **Encapsulation**

enclaves CVMs — **Confidential Computing**

= What is shared

Insight

Composable | **Isolation**

Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))

= S_{andbox} ∘ E_{nclave} ∘ C_{VM} (R)

sandboxes VMs — **Encapsulation** = **What is shared**

enclaves CVMs — **Confidential Computing** = **What is exclusive**

Insight

Composable | **Isolation**

Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))

= S_{andbox} ∘ E_{nclave} ∘ C_{VM} (R)

sandboxes **VMs** — **Encapsulation** = **What is shared**

enclaves **CVMs** — **Confidential Computing** = **What is exclusive**

✅ **Access & Boundary Control**

Insight

Composable | **Isolation**

Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))

= S_{andbox} ∘ E_{nclave} ∘ C_{VM} (R)

~~sandboxes~~ ~~VMs~~ → Encapsulation = What is shared

~~enclaves~~ ~~CVMs~~ → Confidential Computing = What is exclusive

✅ Access & Boundary Control → SD

Insight

Composable

Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))

= S_{andbox} ∘ E_{nclave} ∘ C_{VM} (R)

= SD ∘ SD ∘ SD (R)

Isolation

~~sandboxes~~ ~~VMs~~ → Encapsulation

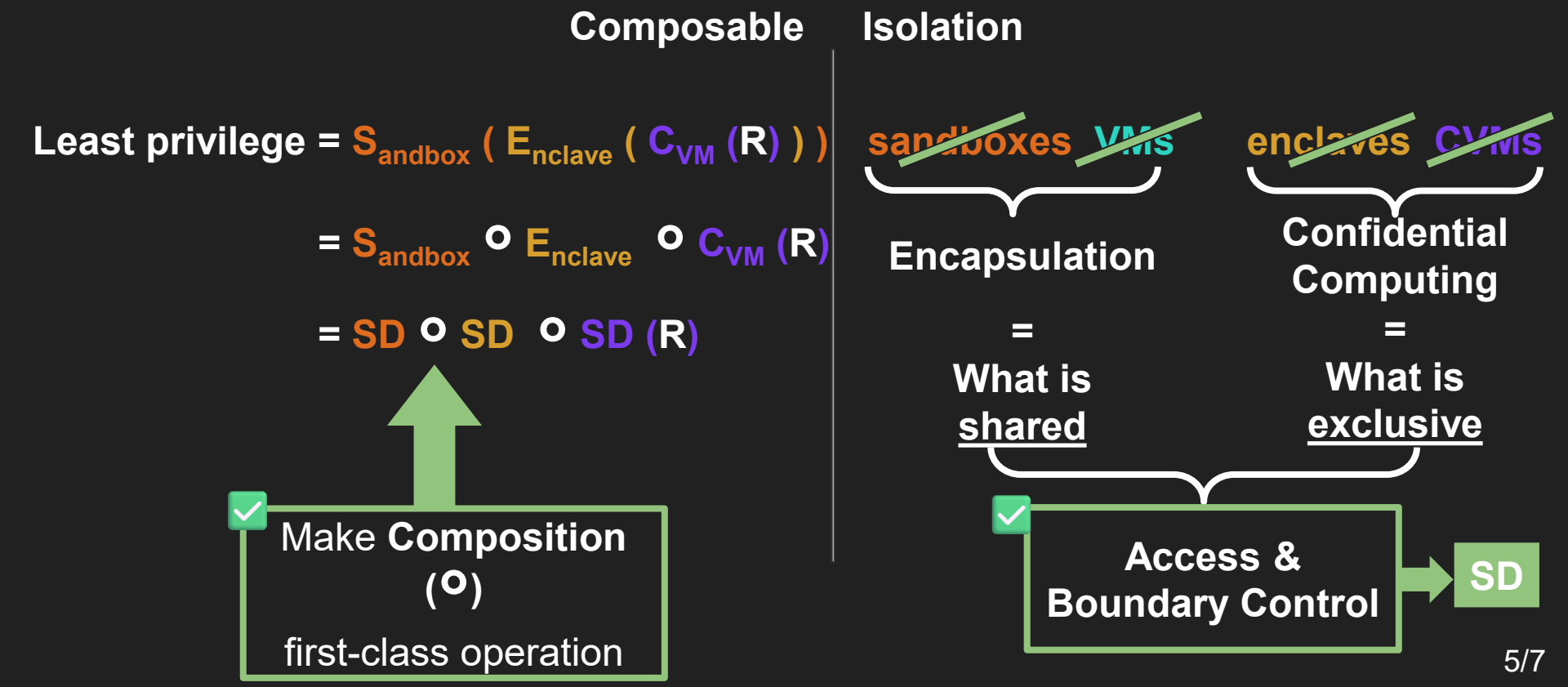
~~enclaves~~ ~~CVMs~~ → Confidential Computing

= What is <u>shared</u>

= What is <u>exclusive</u>

✅ Access & Boundary Control → SD

Insight


Composable
Isolation
Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))
= S_{andbox} ∘ E_{nclave} ∘ C_{VM} (R)
= SD ∘ SD ∘ SD (R)
sandboxes VMs
enclaves CVMs
Encapsulation
Confidential Computing
=
What is shared
=
What is exclusive
Make Composition (∘)
first-class operation
Access & Boundary Control
SD

Insight

Composable

Least privilege = S_{andbox} (E_{nclave} (C_{VM} (R)))

= S_{andbox} ∘ E_{nclave} ∘ C_{VM} (R)

= SD ∘ SD ∘ SD (R)

= SD_{S+E+C} (R)

Make **Composition** (∘)

first-class operation

Isolation

~~sandboxes~~ ~~VMs~~

Encapsulation

=

What is shared

~~enclaves~~ ~~CVMs~~

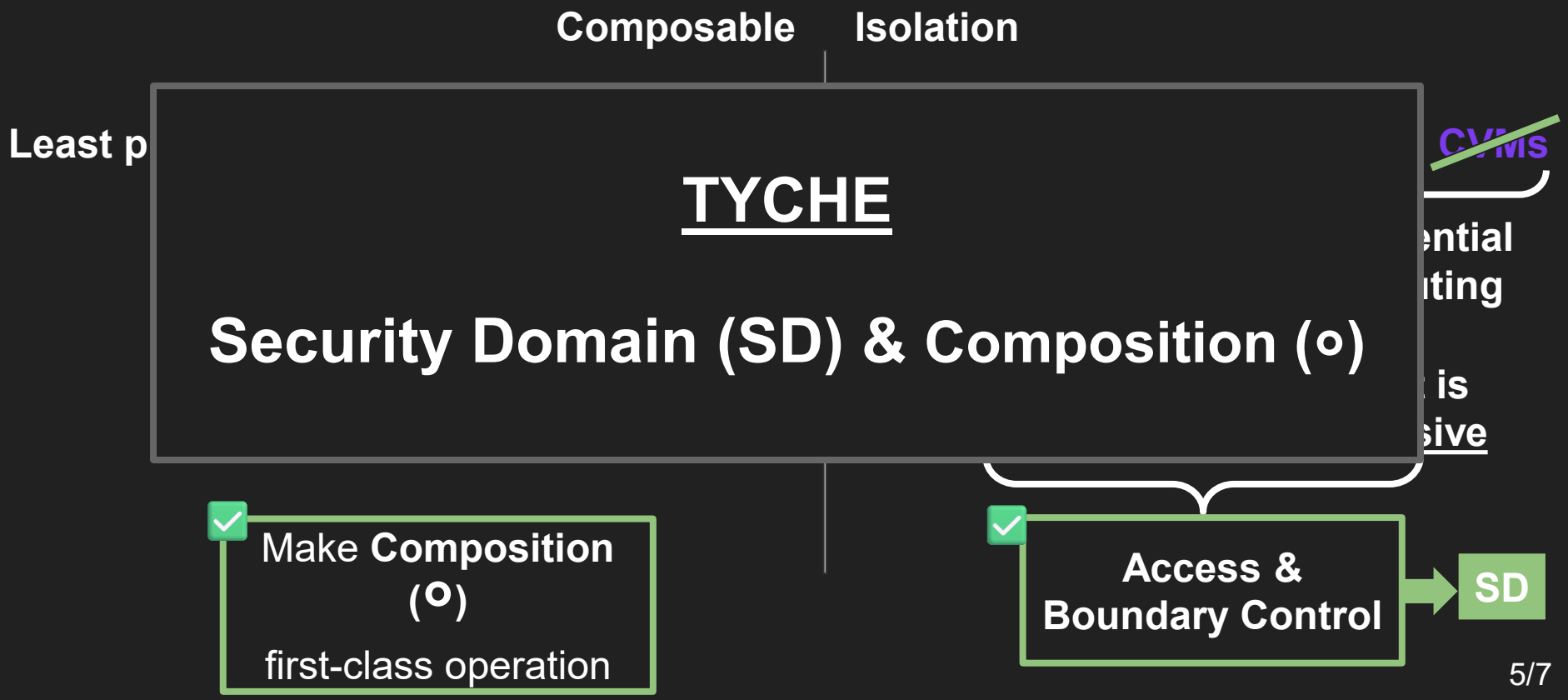
Confidential Computing

=

What is exclusive

Access & Boundary Control → **SD**

Insight


Composable
Isolation
Least p
TYCHE
Security Domain (SD) & Composition (∘)
CVMs
ential
uting
is
sive
Make Composition (∘)
first-class operation
Access & Boundary Control
SD

Tyche Security Monitor

Tyche Security Monitor

✅

📌 Fixed TCB + Commodity Hardware



Tyche Security Monitor

- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API

Tyche



Tyche Security Monitor

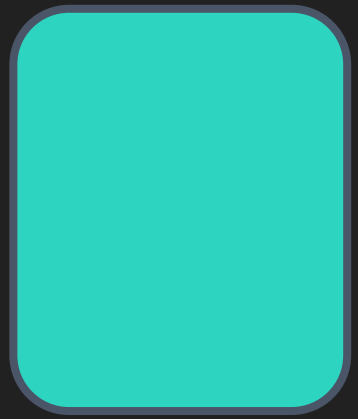
- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API



Tyche

Tyche Security Monitor

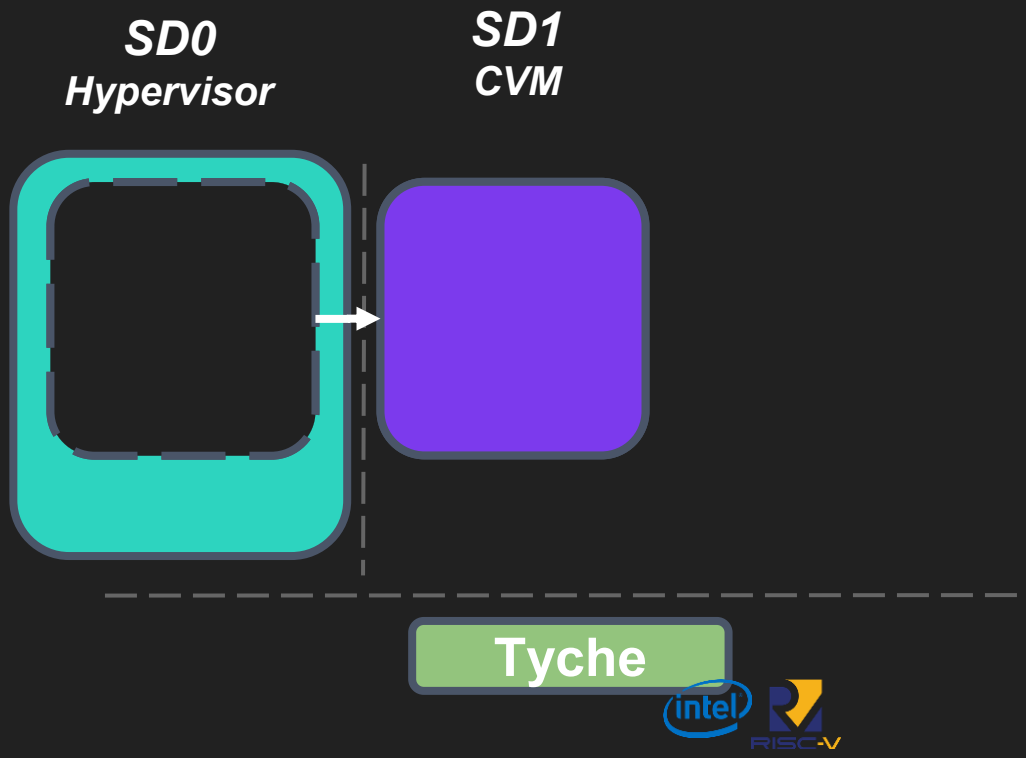
- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API
  - Backward-compatible
    - QEMU+KVM



Tyche

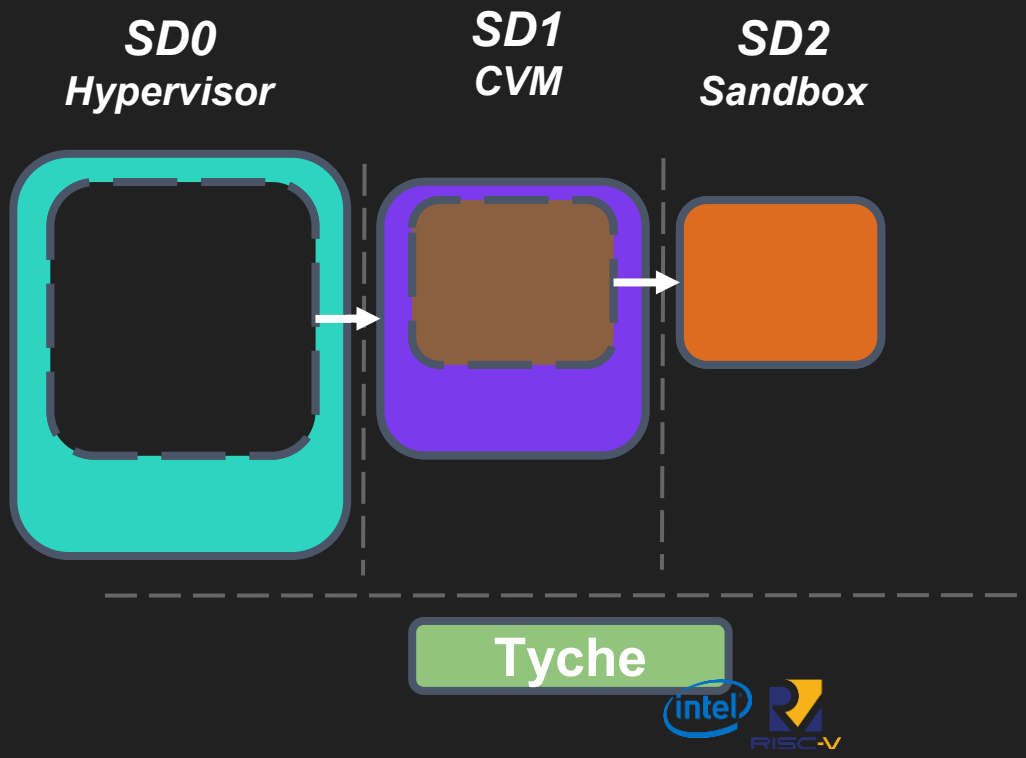
Tyche Security Monitor

- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API
  - Backward-compatible
    - QEMU+KVM



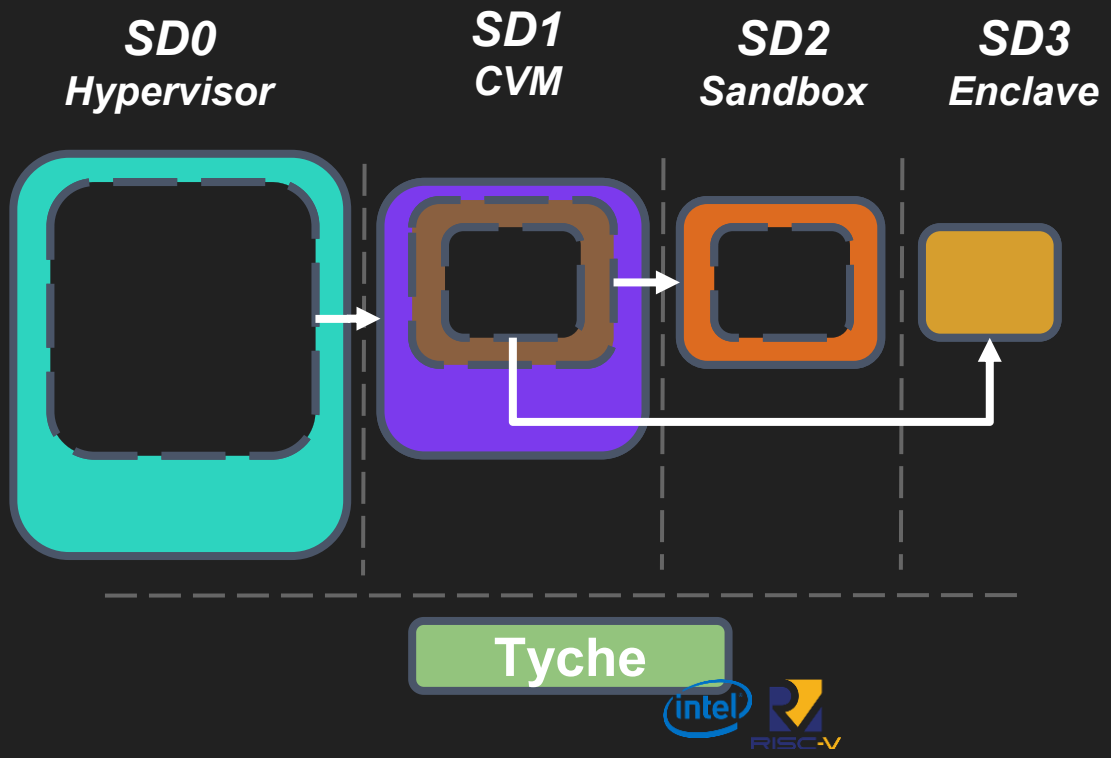
Tyche Security Monitor

- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API
  - Backward-compatible
    - QEMU+KVM
    - Gramine



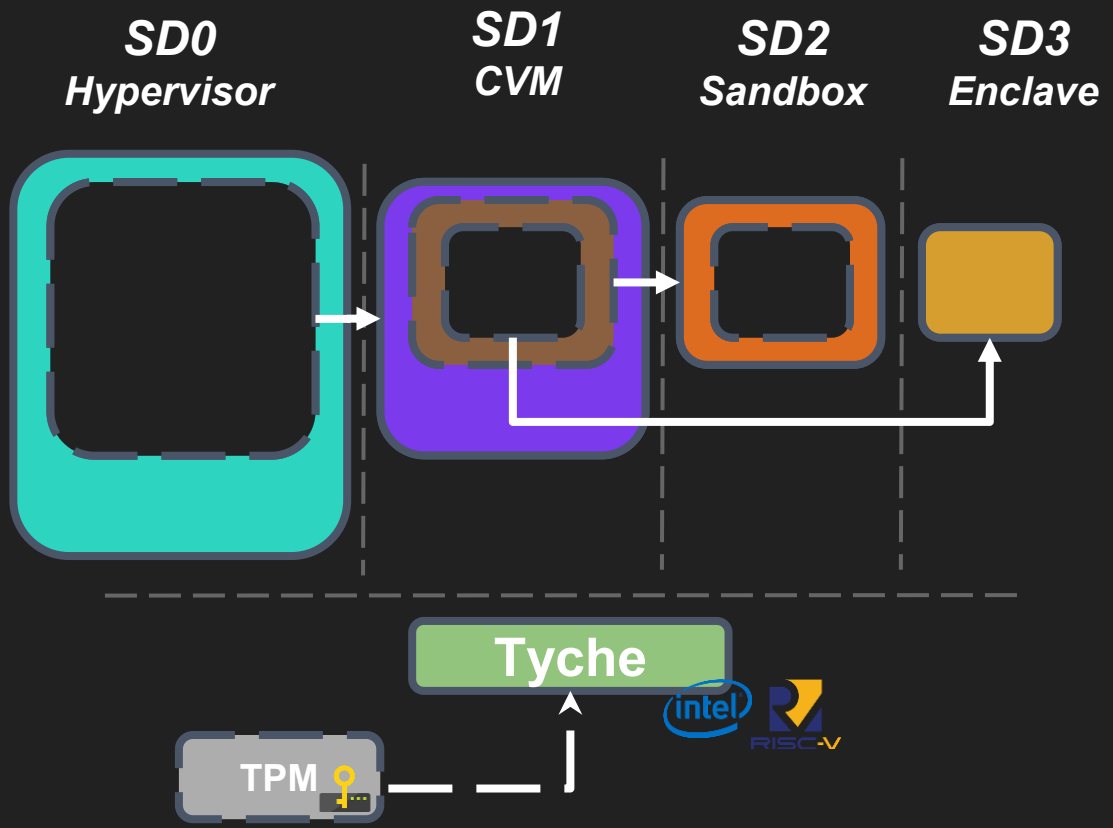
Tyche Security Monitor

- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API
  - Backward-compatible
    - QEMU+KVM
    - Gramine



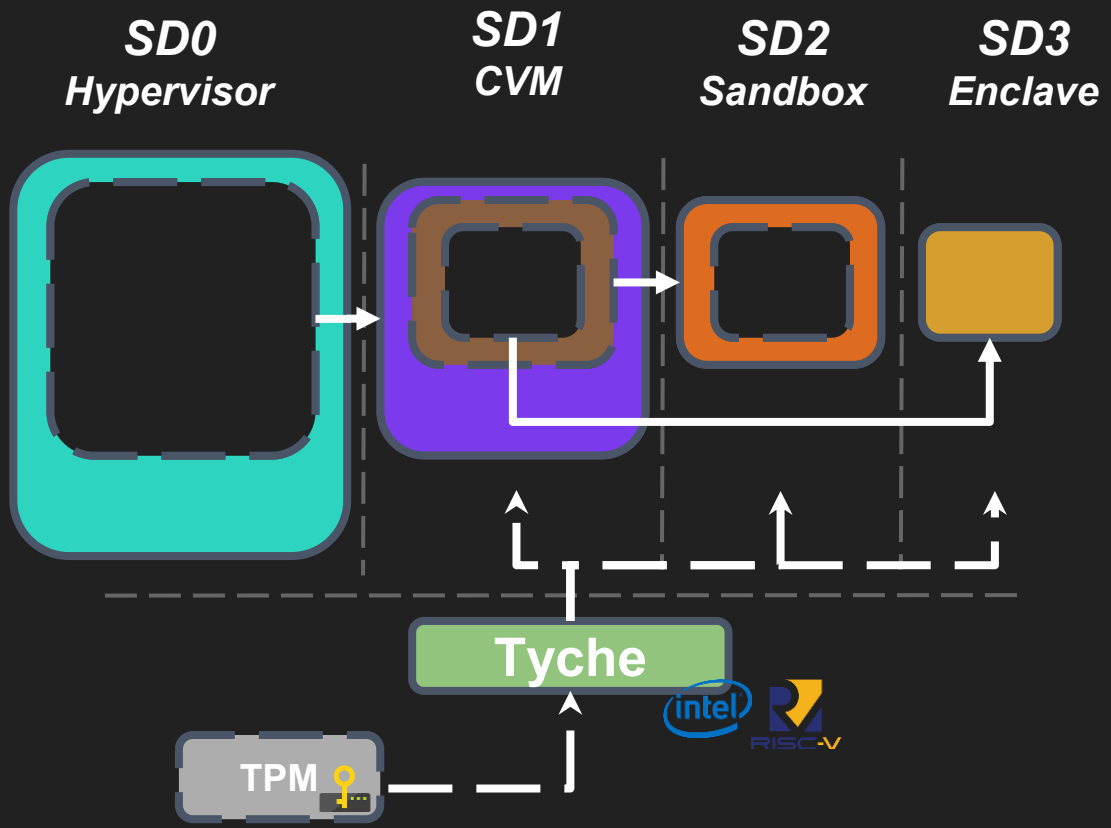
Tyche Security Monitor

- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API
  - Backward-compatible
    - QEMU+KVM
    - Gramine
- 🔏 Rich, fine-grained attestation



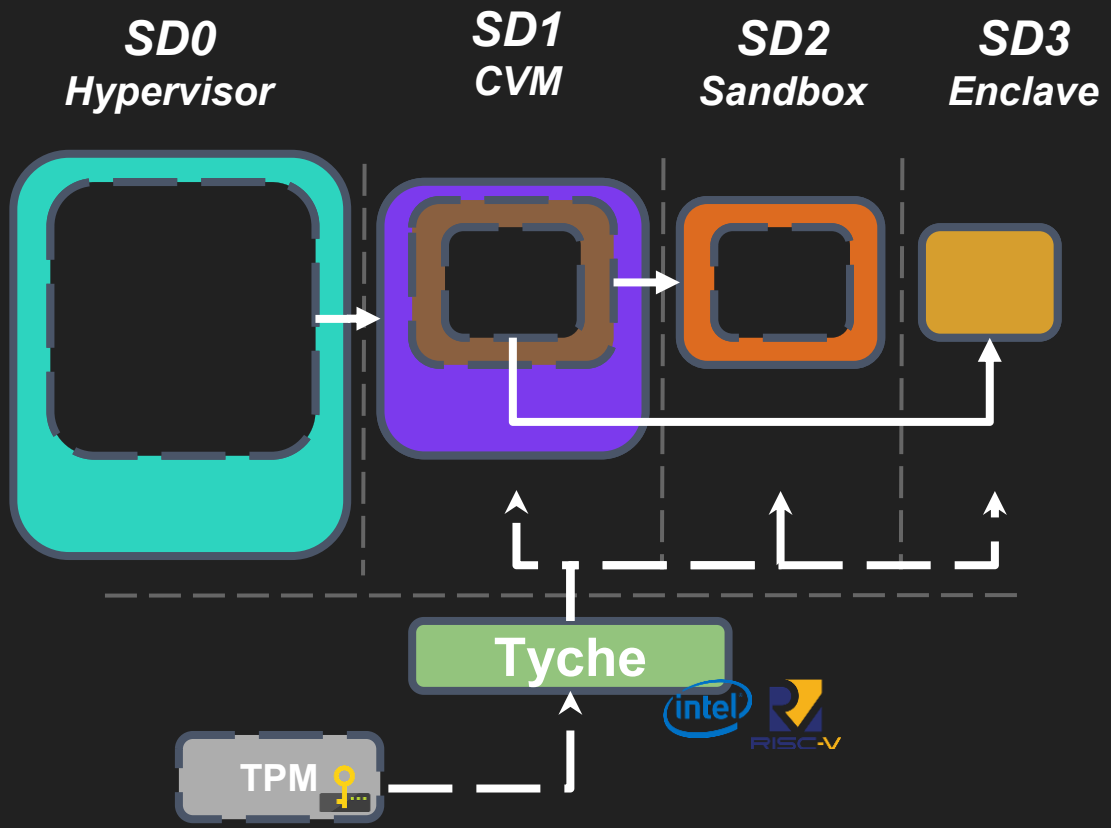
Tyche Security Monitor

- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API
  - Backward-compatible
    - QEMU+KVM
    - Gramine
- 🔬 Rich, fine-grained attestation
  - Multi-SDs



Tyche Security Monitor

- 📌 Fixed TCB + Commodity Hardware
- 👍 Simple Capability-based API
  - Backward-compatible
    - QEMU+KVM
    - Gramine
- 🔏 Rich, fine-grained attestation
  - Multi-SDs
  - Capabilities & policies



Tyche

- Come see our poster
- More details in the paper
- Extra features
  -
  -
  -
  - >_

