When U.S. Laws Turn Cloud Providers into a Threat

Tomas Kokolevsky

Speaker

- Information Security Officer for Beyond Gravity
- 5+ years securing export-controlled data and Government clouds.
- Before: Biotech, Fintech
- Likes adventure

Agenda

Digital Sovereignty Challenge

U.S. Laws affecting us

Resilience Strategies

Who works for an organization that relies on Cloud Service Providers?

In 2025, 95% of organizations use some form of cloud services

Source: https://spacelift.io/blog/cloud-computing-statistics

Digital Sovereignty Challenge

Strategic Data

Strategic capabilities

Defense and Aerospace

Gov / Public Sector

Critical Infra. Operators

Financial Services

Telecom

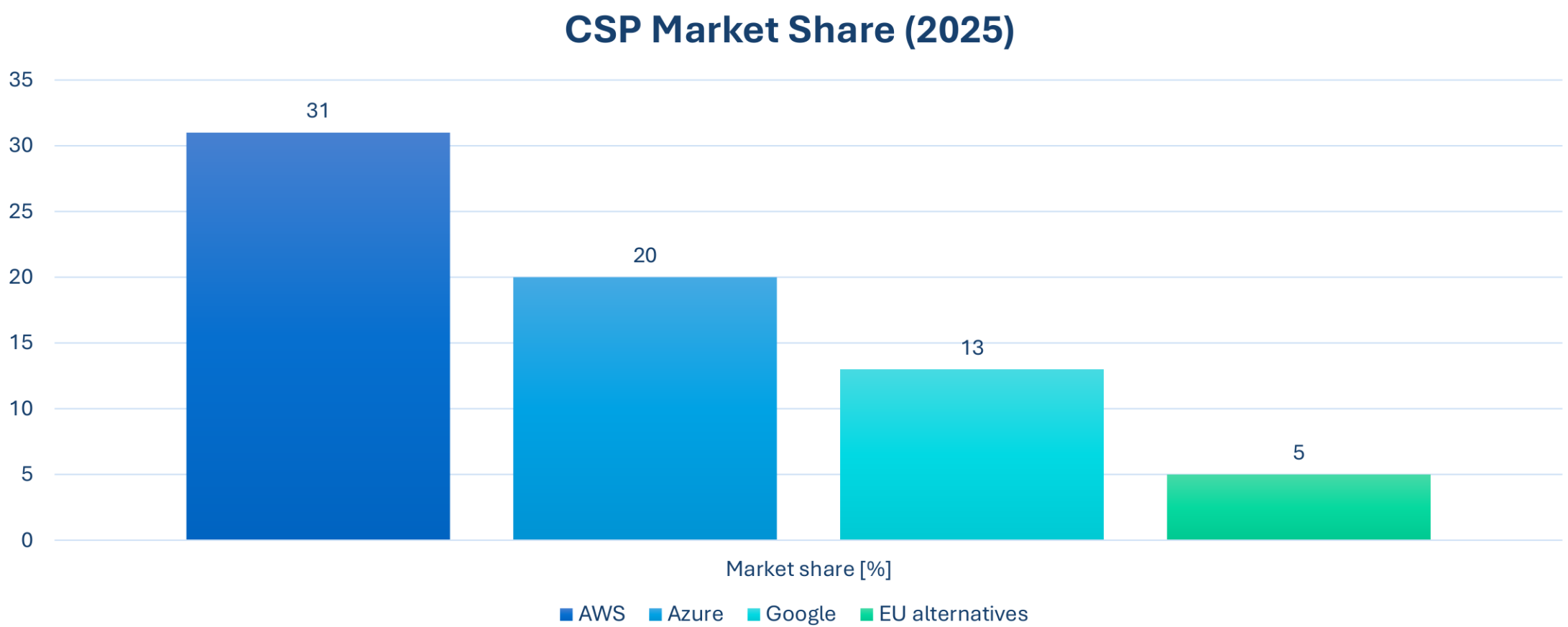
Healthcare

Strategic data

- Nations & orgs depend on their ability to control strategic data
  - Where the data flows.
  - How is the data handled.
  - Which jurisdiction data falls into.

- Sovereign data has more aspects than cybersecurity alone
  - Geo-political & Jurisdictional aspects.
  - Laws & Regulations inform business.
  - We own the data, Government controls the use.

No strategic European Cloud Service Provider



Source: www.statista.com

Can we trust U.S. CSPs with European Sovereign Data?

U.S. Laws affecting us

Foreign Intelligence Surveillance Act (s. 702)

- Allows the USG to collect foreign intelligence data outside USA.
- *Shouldn't* be used for economic espionage – but strategic sectors are not economic.
- No need for an individualized warrant. Secret FISC courts approve/deny
  - Success rate 99.97%.
- Broadened scope in 2024: includes all CSPs, ISPs, Datacenters.

Source: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286

Executive Order 12333

- Gag order – CSPs to provide data access **in secret.**
- *“[CSP] to immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition”*

Source: https://www.nsa.gov/Signals-Intelligence/EO-12333/; talk by Doron Zimmermann (2022)

CLOUD Act

- Since 2018.
- Requires U.S. CSPs to provide customer data to U.S. law enforcement regardless of location.
- Difference from FISA s702: Enables *all law enforcement*, not only NSA.

Source: https://www.nsa.gov/Signals-Intelligence/EO-12333/

U.S. CSP legal summary

- How immune is critical / sovereign data to espionage?
  - CSPs under enormous legal pressure.
  - Tools, Laws & Organization ready.
- Strong indicators of geo-political risk
  - Schrems I & Schrems II, invalidated “Safe Harbor”.
  - EU law doesn’t deem surveillance as “*necessary and proportionate*”.
- Is the USA a friend or a competitor?

Does U.S. trust their own CSPs?

- USG CSP certification program
  - Azure GCC High, AWS GovCloud.
- Requires NIST 800-53 & Government audits
  - Example: personnel background checks.
- Organizations **prohibited** from storing U.S. sovereign data in public clouds, even when they are based in the U.S.

CSP claims vs. reality

- Microsoft claims they have a multi-step HSM unlocking process which they will never use.
- Amazon claims AWS NITRO has no operator access system.

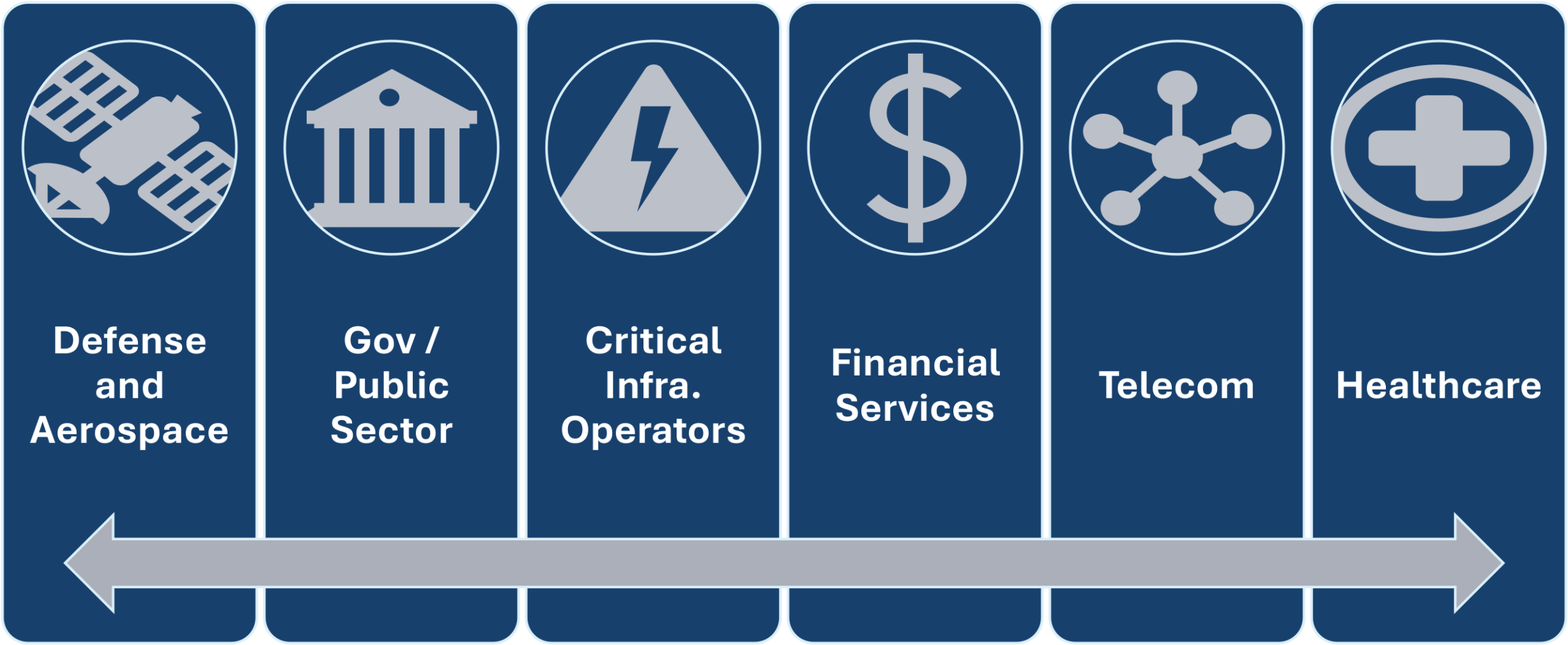
CSP claims vs. reality

- No reasonable CSP will ever claim their services are compromised, even when they are *legally forced* to do so.
- No 3rd party audits of the implementation that proves the claim.
- U.S. ITAR & CUI example:
  - Not allowed in public cloud despite “no operator access”.
  - Cloud contracts insufficient, FedRAMP required for all U.S. sovereign data.

(Slow) EU regulatory evolution

- Limited EU sovereign clouds / EU FedRAMP.
- Slow evolution in jurisdiction from GDPR to NIS2/DORA.
  - Data residency alone insufficient to address remote access concerns.
  - Hard to make strong requirements with U.S. Cloud dependency.
- DORA
  - 3rd party supplier risk assessment requirements on foreign jurisdictions
  - Interesting: Critical 3rd Party Providers designation.

Exposed strategic capabilities

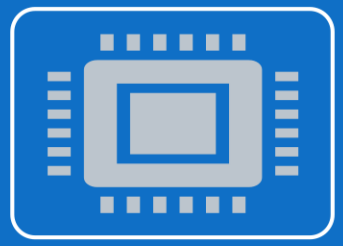


Resilience strategies

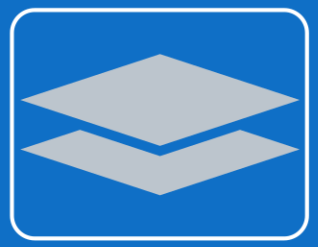
Sovereignty by design

Many options available

Hold Your Own Key (HYOK)



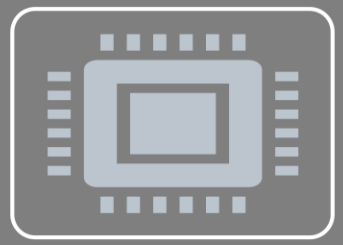
Confidential Compute



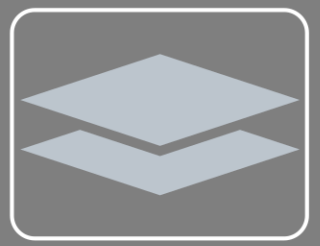
Hybrid Architectures

Many options available

Hold Your Own Key (HYOK)



Confidential Compute



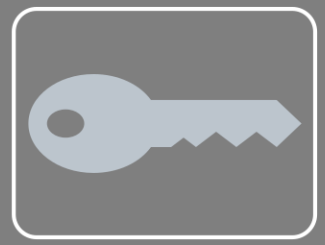
Hybrid Architectures

BYOK vs. HYOK

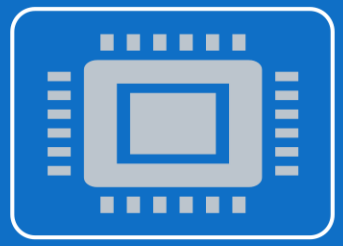
- Bring Your Own Key:
  - You control the key, CSP stores it *active* in their HSM.
  - Administrative control, not access control against espionage.
  - “Wrapper" Data Encryption Keys.
  - Once you upload the key, it’s over.

- Hold Your Own Key:
  - Keys never leave your infrastructure.
  - HSMs & Key Proxy needed.
  - Very limiting and possibly expensive.

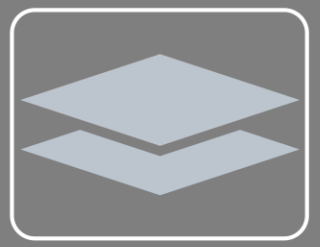
Many options available



Hold Your Own Key (HYOK)



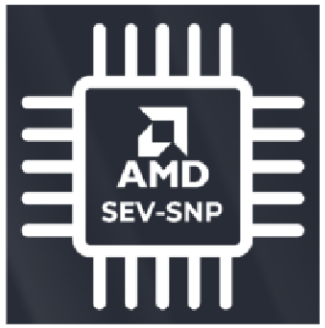
Confidential Compute



Hybrid Architectures

Confidential Compute

Confidential VMs
Powered by AMD SEV-SNP

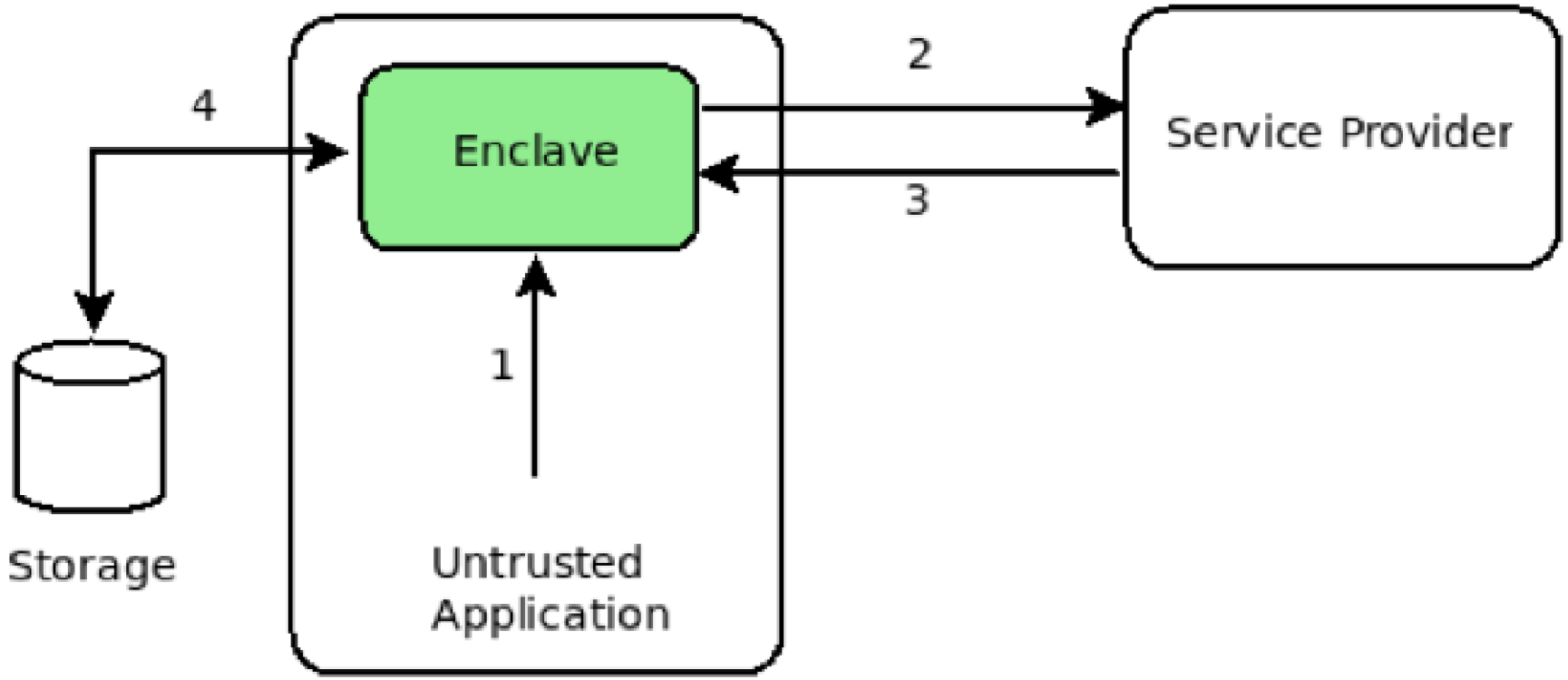


Application Enclaves
Powered by Intel SGX

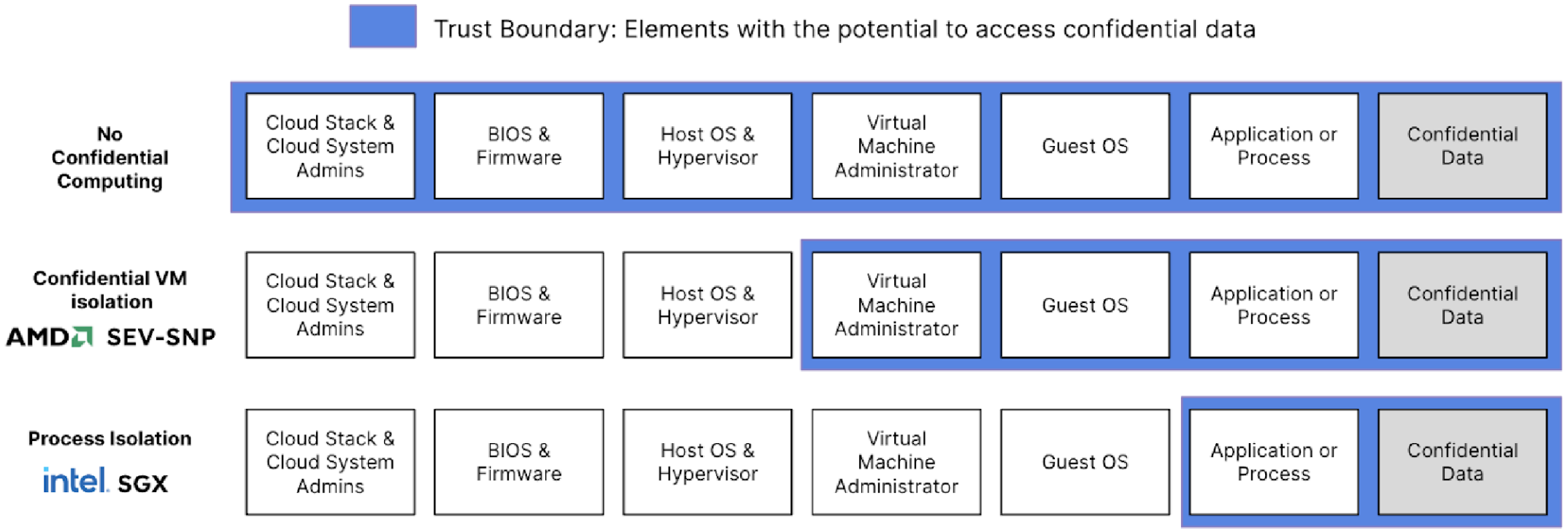
Ease of use

Data isolation

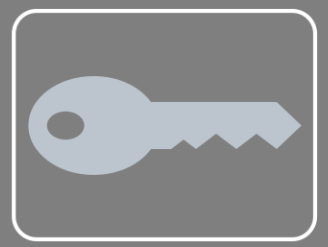
Confidential Compute



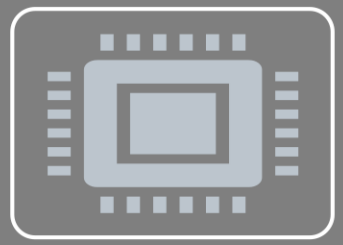
Confidential Compute



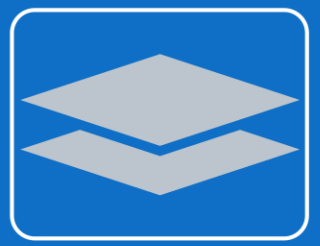
Many options available



Hold Your Own Key (HYOK)

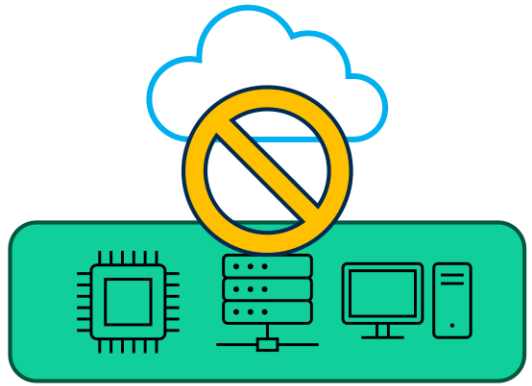


Confidential Compute



Hybrid Architectures

Hybrid Architectures



- Architecture requirements:
  - Sensitive data stays on-prem.
  - Security / Metadata / Support tools may use cloud.
  - Ensure data flows (routing) avoid data processing in the cloud.
- Component choice and configuration matters:
  - NO direct upload of controlled data to CSP.
  - NO admin from CSP.
  - OK to use local processing services from CSP (EDR)
  - OK to share metadata / security data.

Thank you.

Tomas Kokolevsky
Information Security Officer @ Beyond Gravity | CMMC, ISO 27001, NIST 800-171