BUILDING CONFIDENTIAL CLOUD-NATIVE APPLICATIONS WITH THE SCONE PLATFORM

Christof Fetzer, PhD
christof.fetzer@scontain.com
https://scontain.com

MOTIVATION

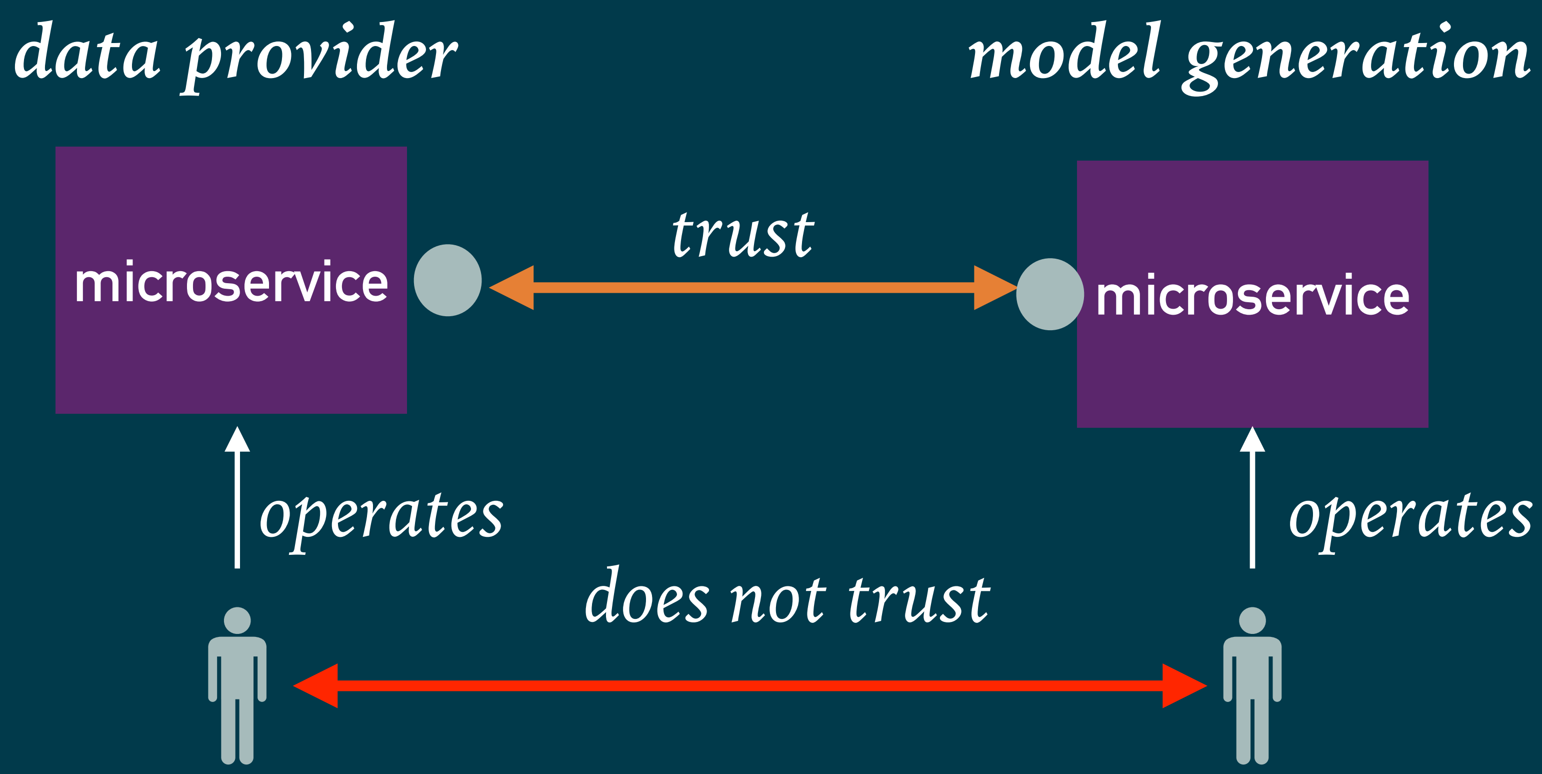
- **Data-Driven Economy** requires the collaboration
  - between non-trusting entities

- **Approach:**
  - **Establish trust in the interaction between non-trusting entities**

IN CODE WE TRUST
WITH SCONE

- establishing trust in untrusted environments between mutually untrusting parties -

DATA-DRIVEN ECONOMY



Example

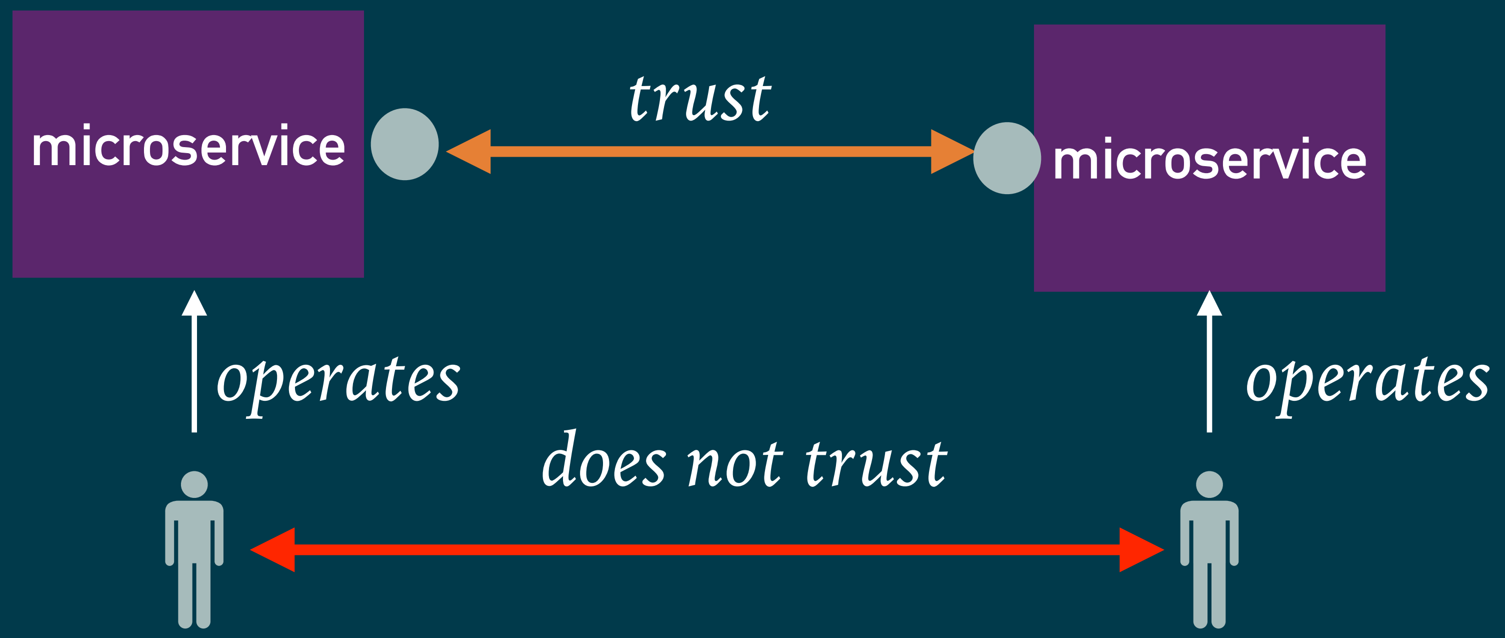
*Use **training data***

- *of a **data provider,***
- *to create **AI model,***

Protecting the IP of all parties!

ESTABLISHING TRUST WITH SCONE

mutual attestation to establish trust



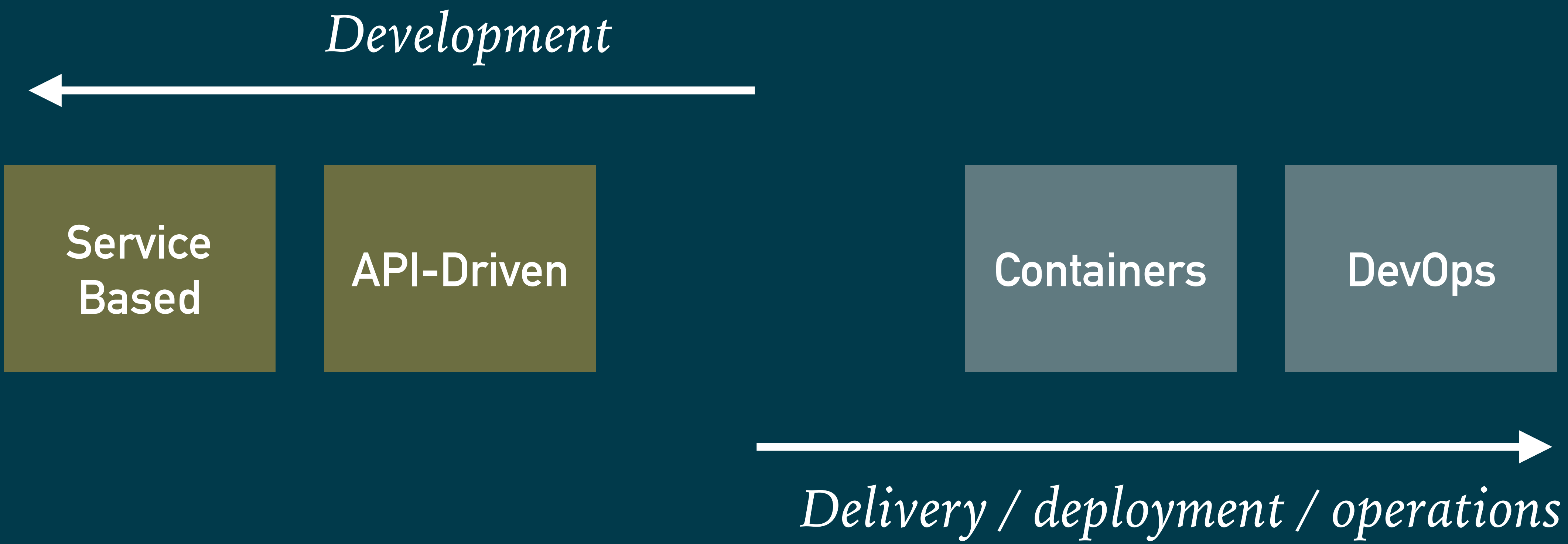
Establishing trust

SCONE helps to ensure that communication partners

- *run the correct code base,*
- *are properly initialized,*
- *run inside of TEEs*

christof.fetzer@scontain.com

CLOUD-NATIVE APPLICATIONS



Cloud-Native Application

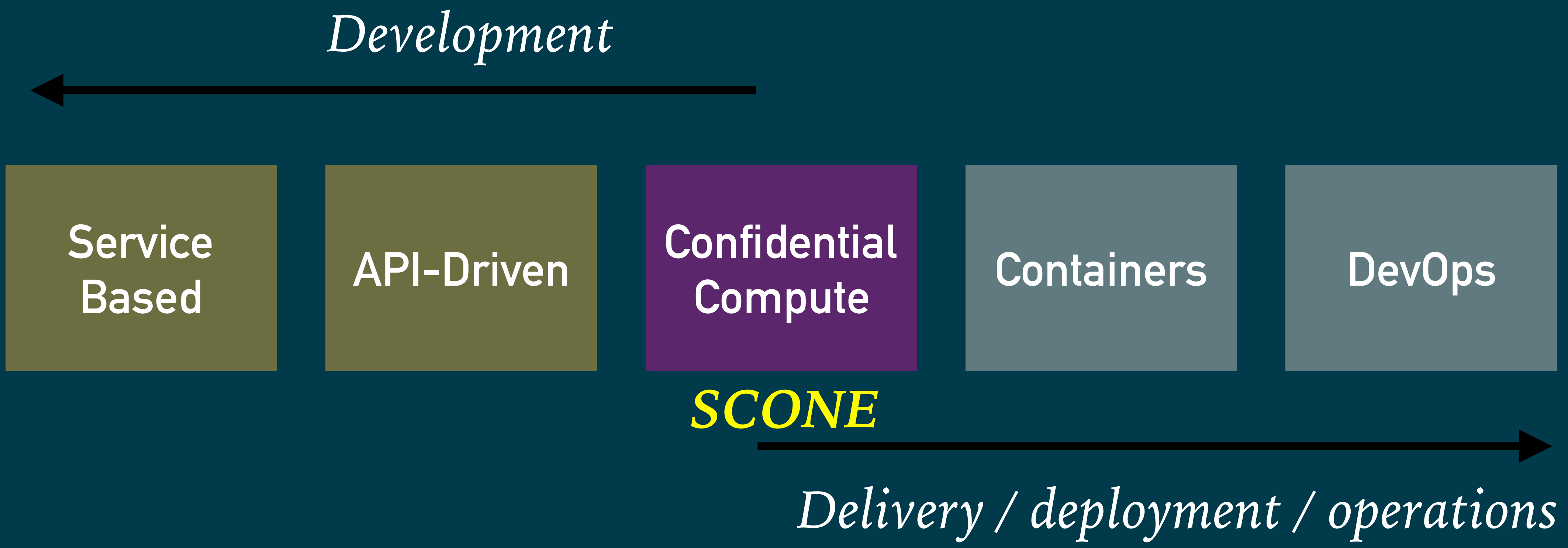
- an application developed and operated using the cloud-native development/operation model

Adapted from Qvarnstrom, Saavedra: „PATH TO CLOUD-NATIVE APP DEV"

CONFIDENTIAL CLOUD-NATIVE APPLICATIONS

	Confidential Cloud-Native Application Development
Security	**data**, **code**, and **keys** are **always encrypted** *NEW* - at rest, in transit, in main memory -
Focus	Speed to market
Development Methodology	Agile development, DevOps
Teams	Collaborative DevOps team
Delivery Cycle	Short and continuous
Application Architecture	Loosely coupled, service-based, API-based communication
Infrastructure	Container-centric, portable, scales horizontally, on-demand capacity

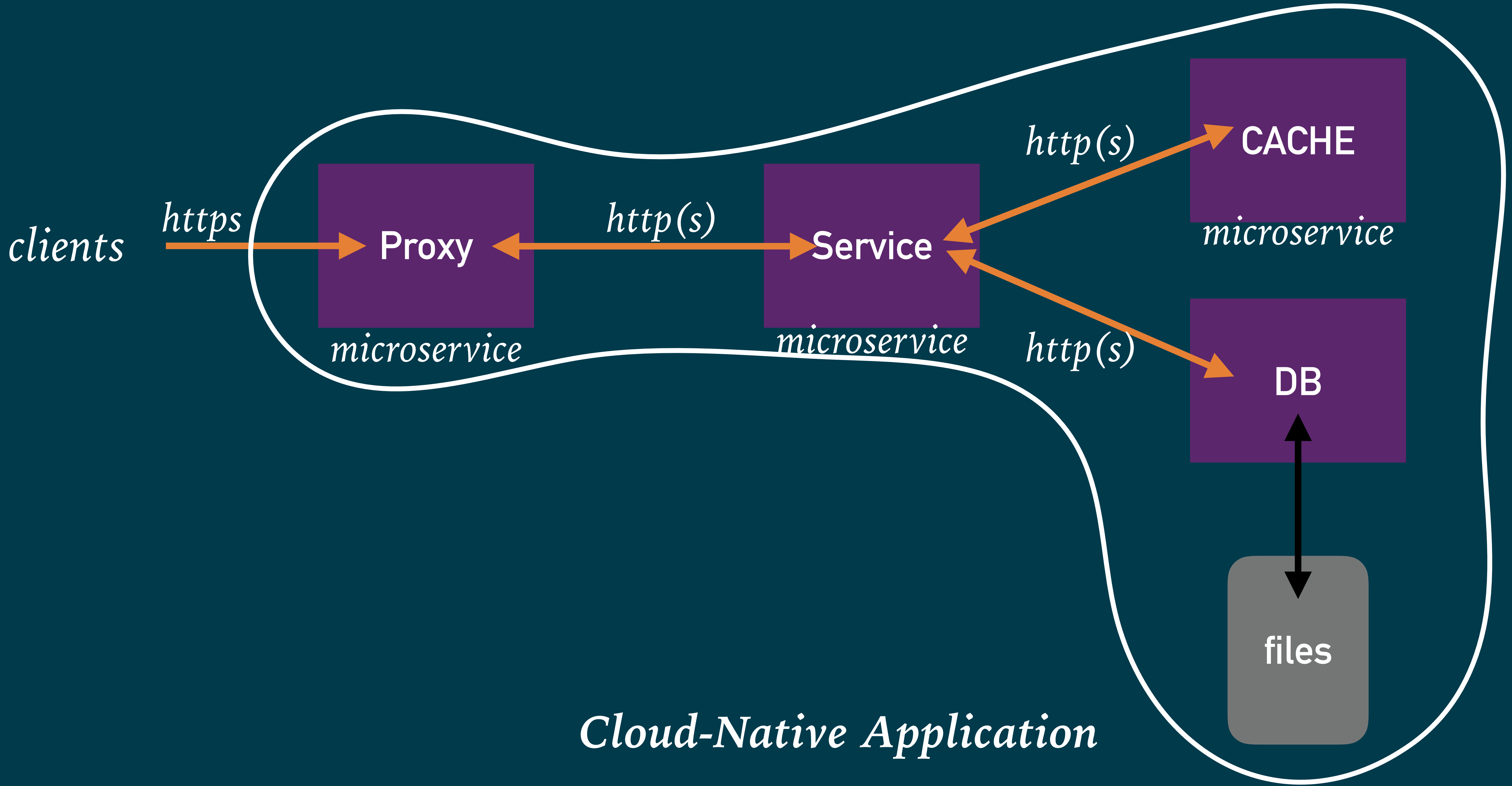
CONFIDENTIAL CLOUD-NATIVE APPLICATIONS



Confidential Cloud-Native Application

- *cloud-native application*
- *protect code, data and keys of application*

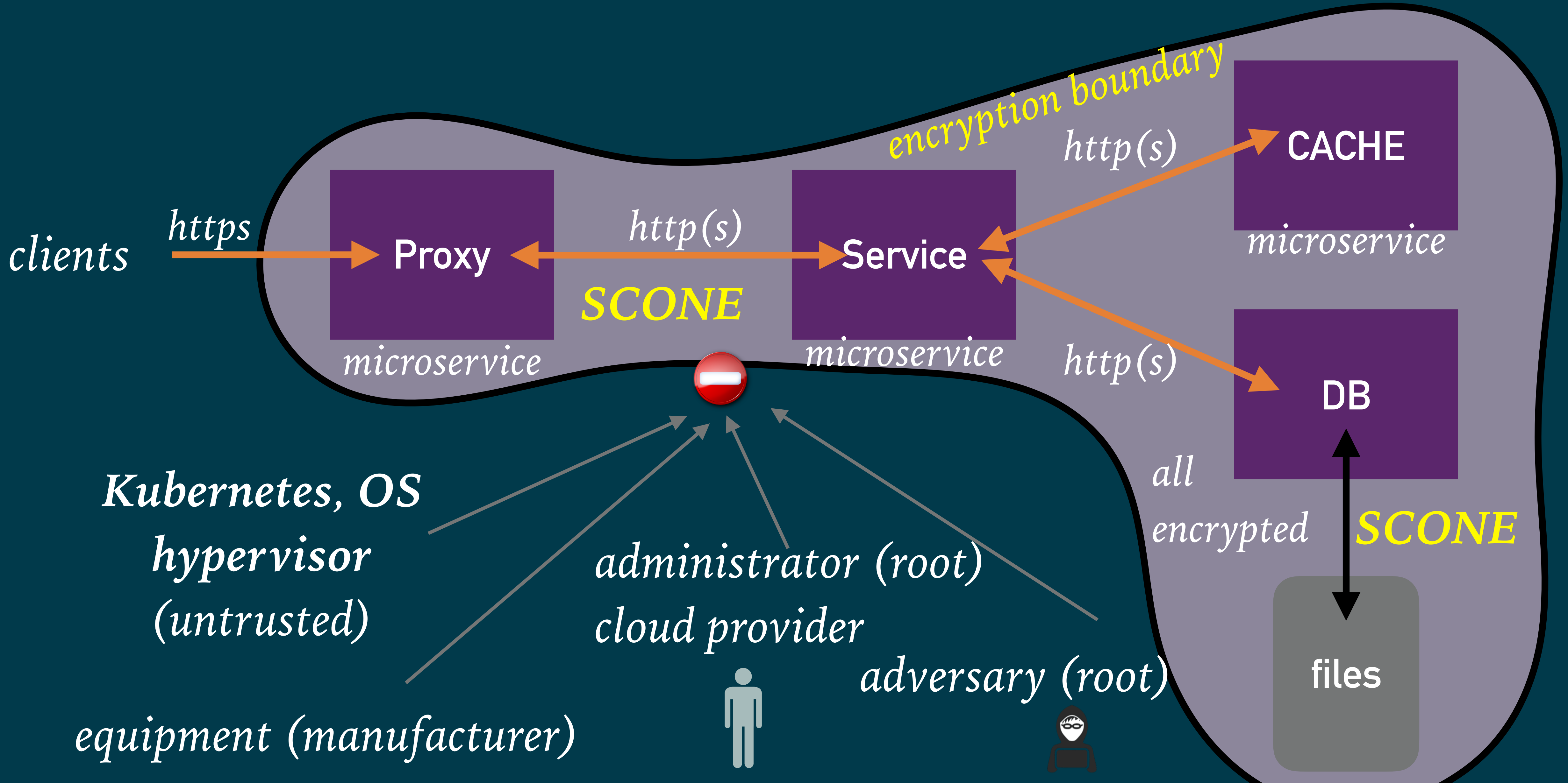
CLOUD-NATIVE APPLICATION



Cloud-Native Application

- an application developed and operated using the cloud-native development/operation model

CONFIDENTIAL CLOUD-NATIVE APPLICATION



Confidential Cloud-Native Application

- *cloud-native application*
- *protect code, data and keys of application*

PROTECTION GOALS OF CONFIDENTIAL COMPUTE

- Protection of

SCONE

  - **Confidentiality**: information is not made available or disclosed to unauthorized individuals, entities, or processes
  - **Integrity**: information cannot be modified by unauthorized individuals, entities, or processes
  - **Freshness**: information cannot be replaced by old information by unauthorized individuals, entities, or processes

- **Additional Protection goals:**

Kubernetes, Ceph

  - **Availability**: probability that information is available when it is needed (verifiable via monitoring)
  - **Durability**: probability that information will survive for one year (verifiable via monitoring)

WHAT INFORMATION TO PROTECT?

- Protection of
  - **Code**, e.g., modern AI programs written in Python
  - **Data**, e.g., training data to create AI models
  - **Keys**, e.g., keys used to encrypt databases

WHAT INFORMATION TO PROTECT?

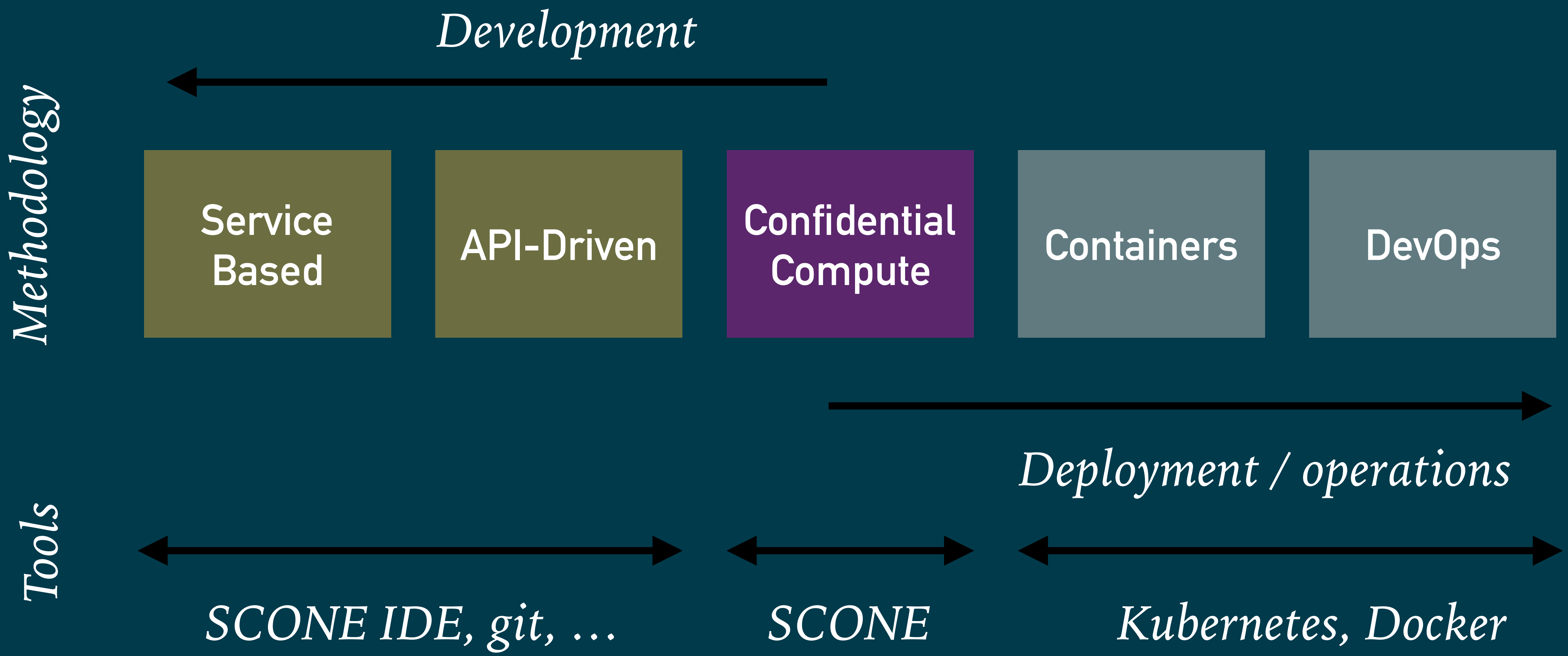
- Protection of
  - **Code**, e.g., modern AI programs written in Python
  - **Data**, e.g., training data to create AI models
  - **Keys**, e.g., key used to encrypt database
- **Example: Cannot protect encryption key in native execution**
  - *MariaDB* supports encryption of database
  - encryption key is stored in configuration file
  - configuration file protected via access control:
    - i.e., can be read and written by MariaDB (user) as well as any root (=privileged) user

PROTECTION WITH SCONE

- Protection of
  - **Code**, e.g., modern AI programs written in Python
  - **Data**, e.g., training data to create AI models
  - **Keys**, e.g., key used to encrypt database
- **Example**: Confidential Cloud-Native Application with SCONE
  - *MariaDB* encrypts database and runs in SGX enclave
  - encryption key is stored in configuration file encrypted/decrypted by SCONE inside of MariaDB enclave
  - SCONE configuration attestation service ensures that only this MariaDB can access the encrypted configuration file

HOW?

CONFIDENTIAL CLOUD-NATIVE APPLICATION DEVELOPMENT



Development

Methodology

Service Based

API-Driven

Confidential Compute

Containers

DevOps

Deployment / operations

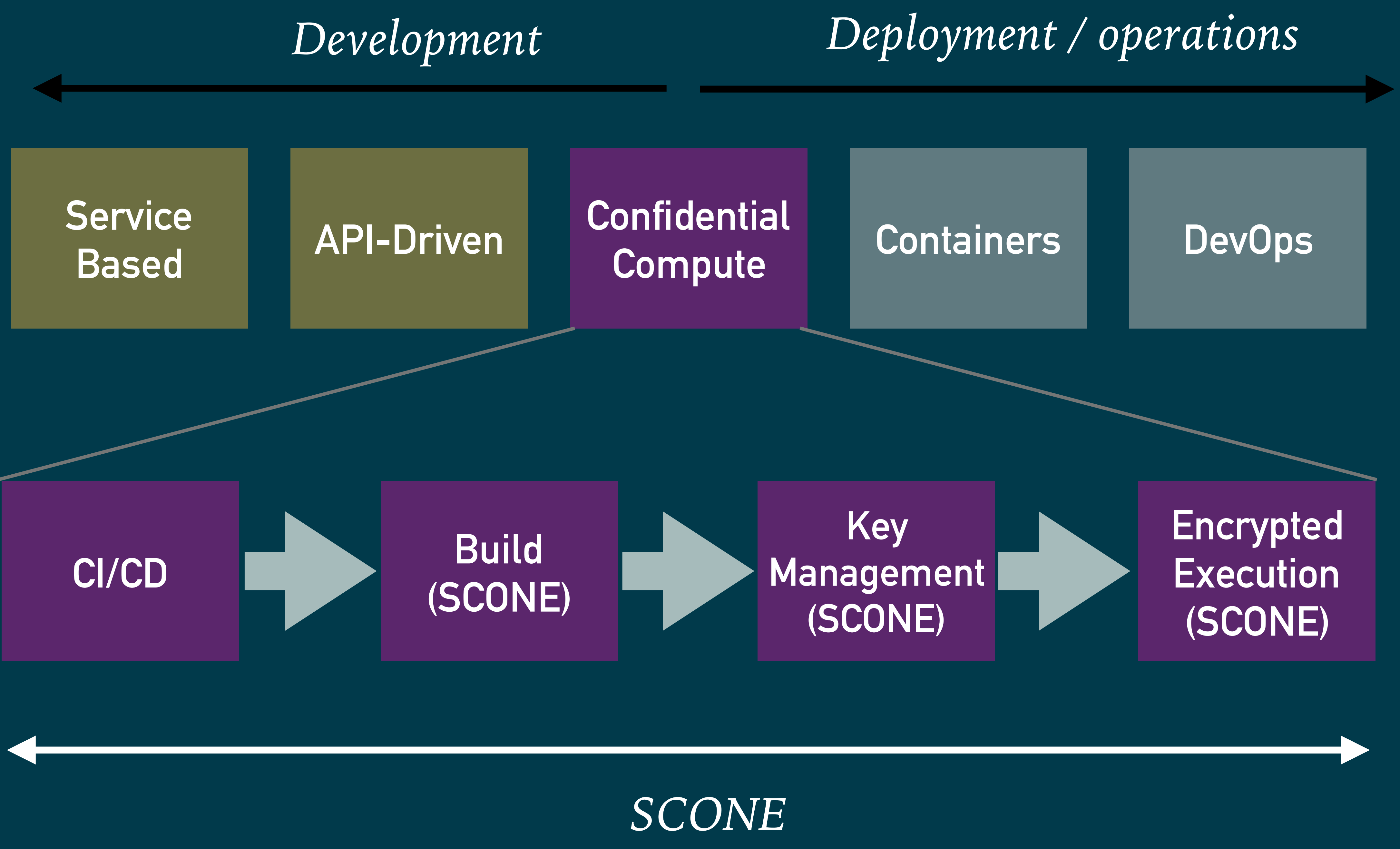
Tools

SCONE IDE, git, …

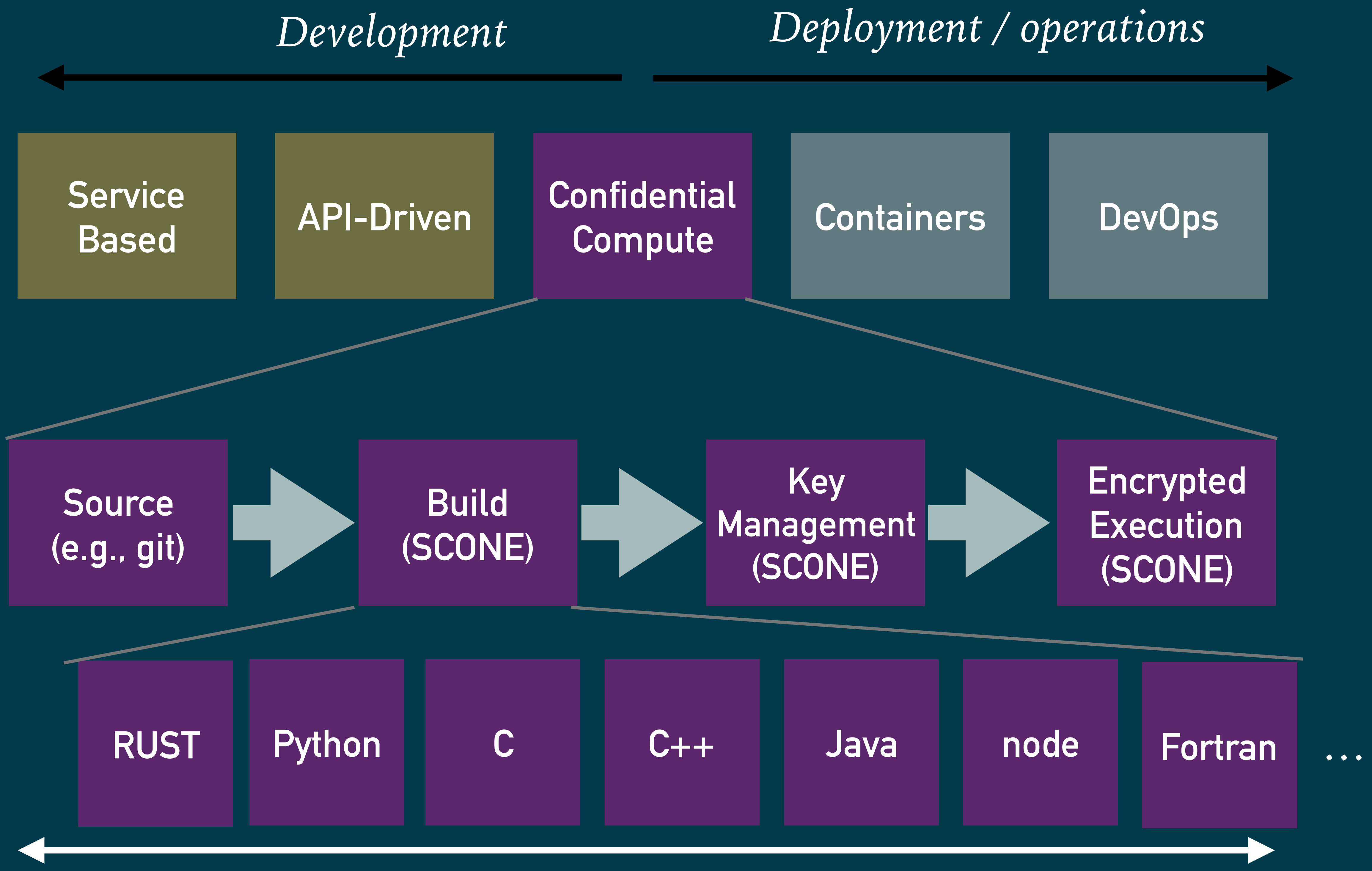
SCONE

Kubernetes, Docker

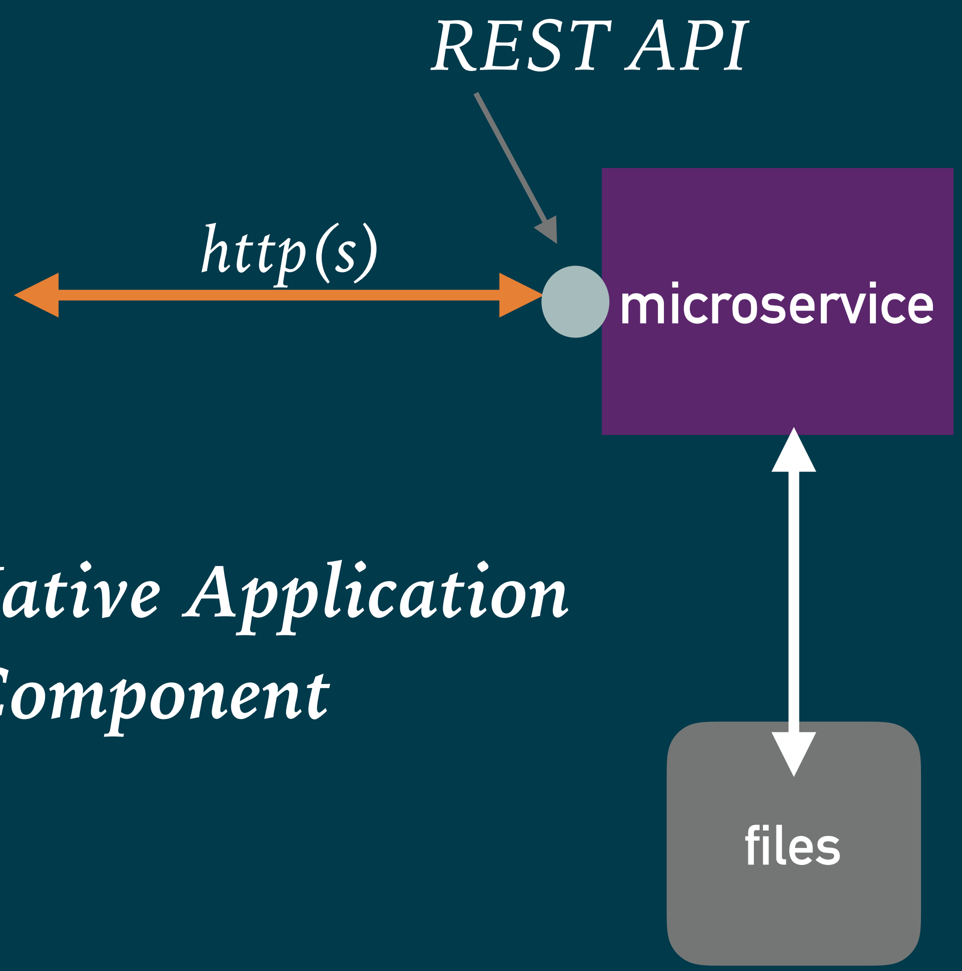
INTEGRATION IN CI/CD PROCESS



WE SUPPORT MOST POPULAR PROGRAMMING LANGUAGES



MICROSERVICE

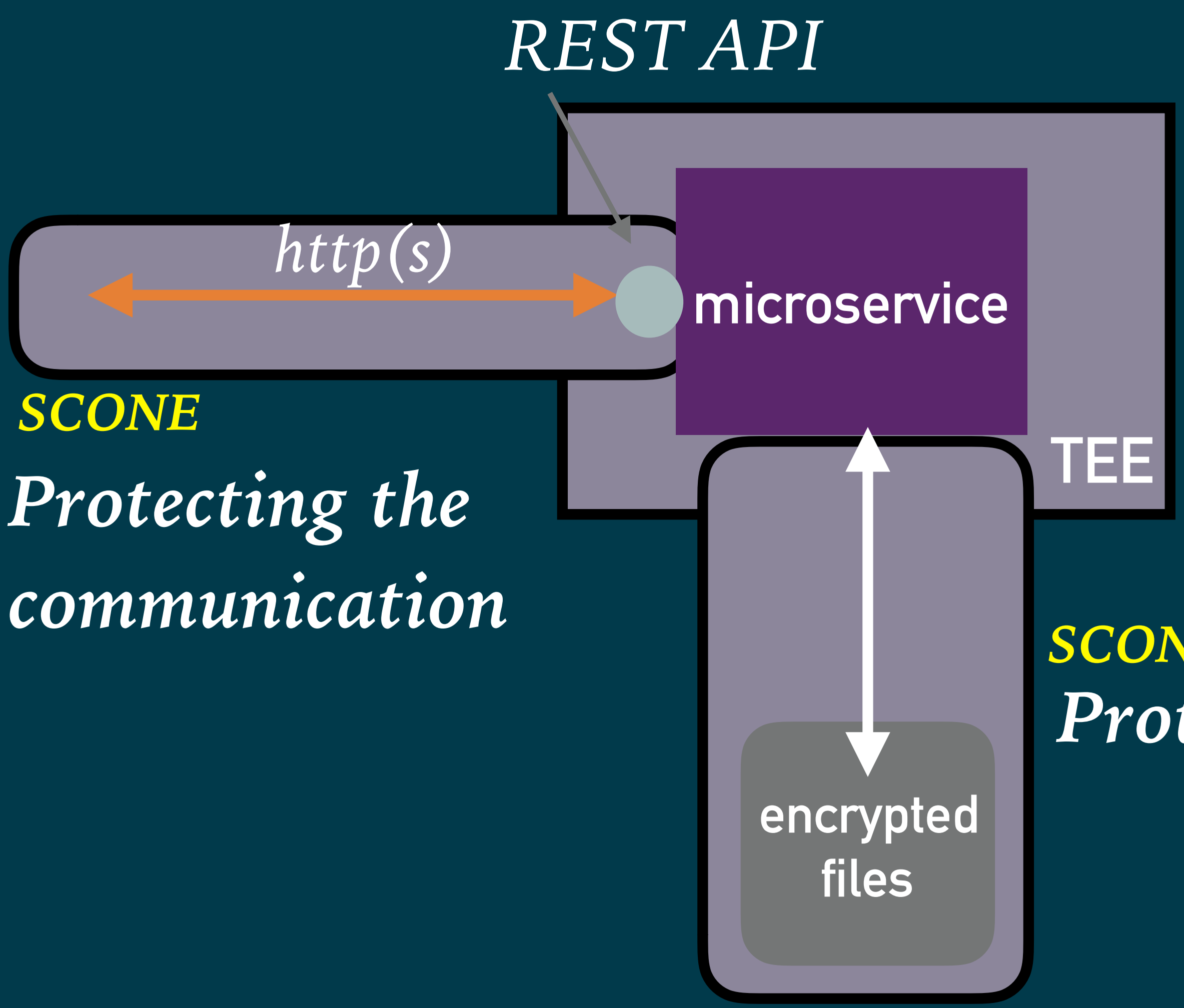


Cloud-Native Application Component

microservice

- *focus on a single aspect*
- *microservices are small, autonomous services that work together*

CONFIDENTIAL MICROSERVICE



SCONE

Protecting the computation

SCONE

Protecting the communication

SCONE

Protecting the files

SCONE

Protecting Confidential Cloud-Native Applications

without source code changes

CONCLUSION

SCONE supports the development & operation of **confidential cloud-native applications**

SCONE

info@scontain.com

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