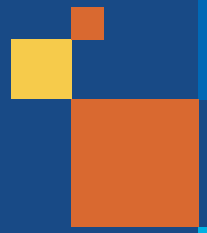
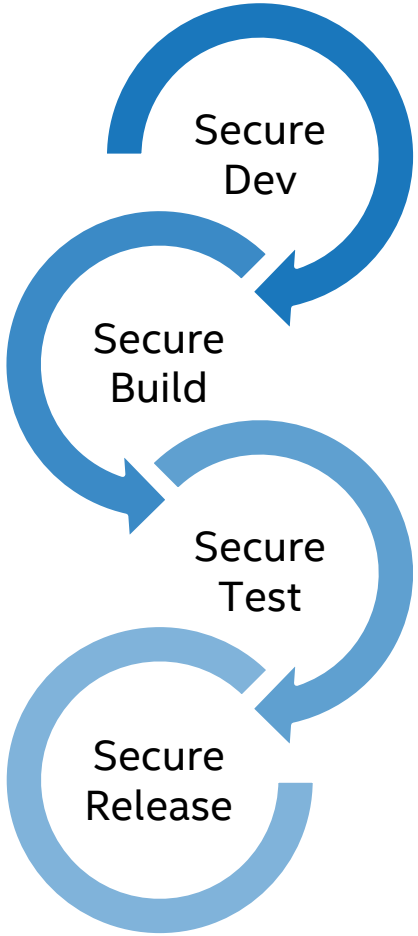
An Ecosystem Solution for Confidential Computing



intel®

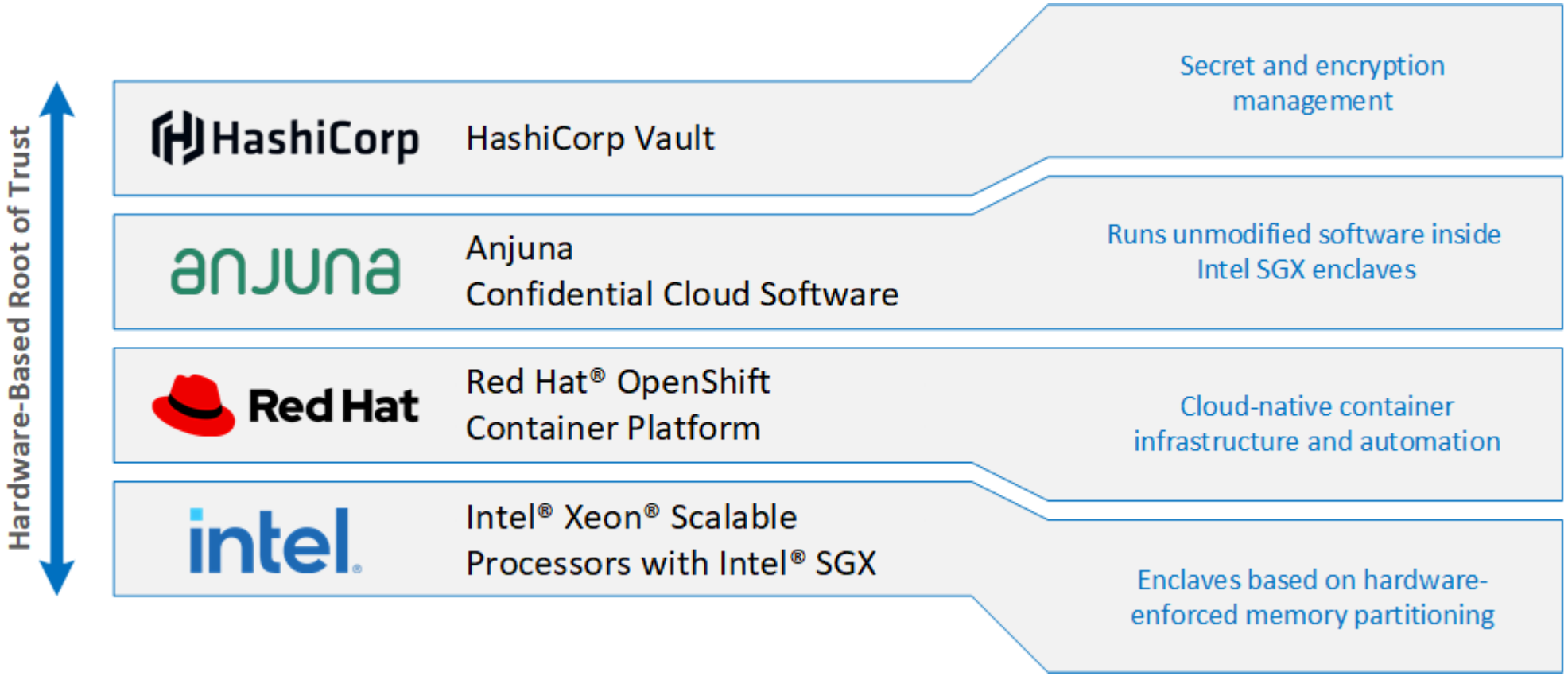
The Growing Threat of Supply Chain Attacks

- The global software supply chain is under attack:
  - Attacks tripled from 2020 to 2021[1]
  - Large organizations are attacked almost weekly[2]
- DevSecOps provides coordinated joint resistance:
  - Unifies security, development, and operations
- Confidential computing provides trusted execution:
  - Hardens DevSecOps pipelines
  - Hardware root of trust, beyond the reach of software



1 Security Week, January 20, 2022. "Software Supply Chain Attacks Tripled in 2021: Study." https://www.securityweek.com/software-supply-chain-attacks-tripled-2021-study.
2 Abnormal Security, April 13, 2022. "New Research Shows 67% Chance of Supply Chain Compromise Attack." https://abnormalsecurity.com/blog/new-research-supply-chain-compromise-attack.

Root of Trust for Confidential Computing

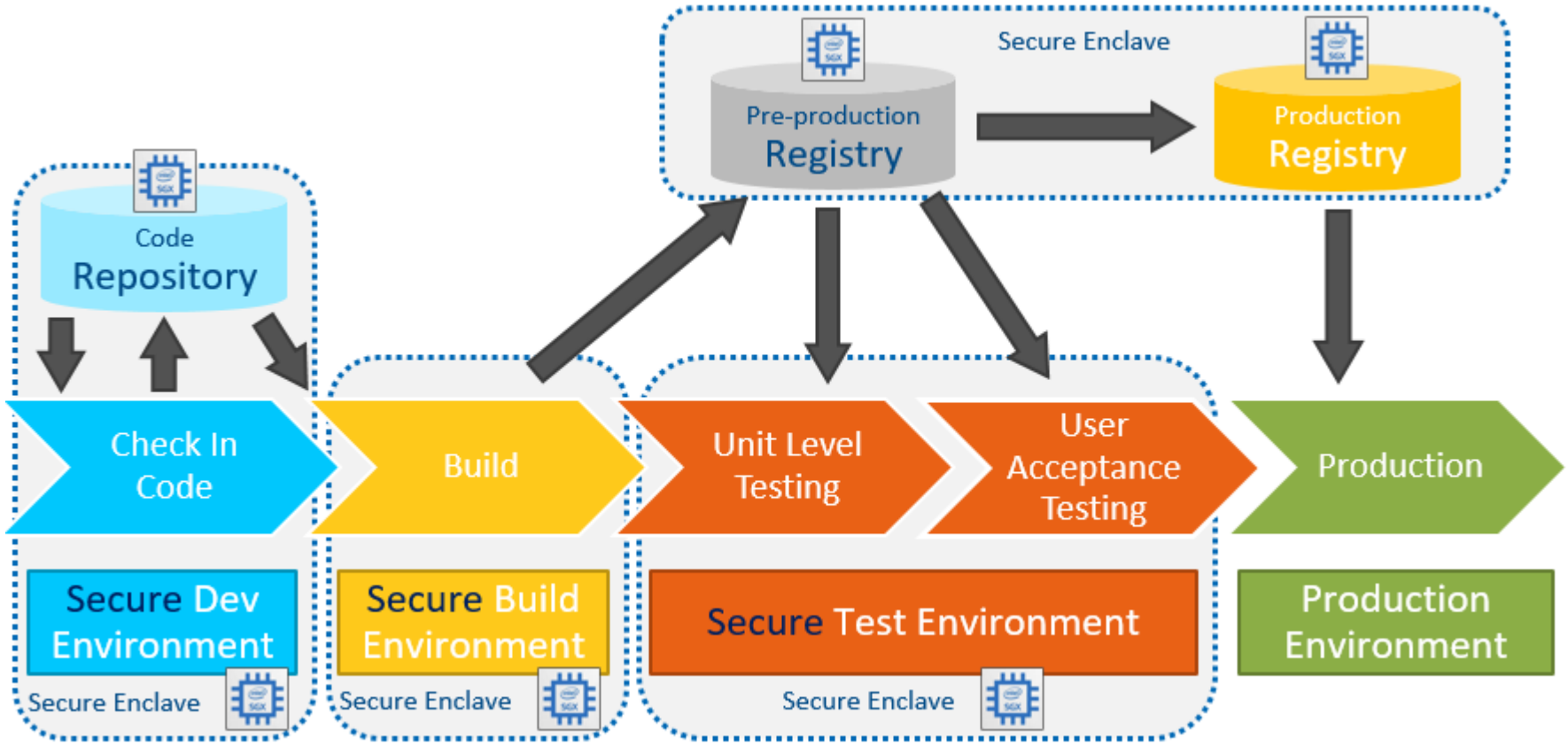


The Confidential Computing Consortium

- Industry initiative to promote cloud-era protection for data in use
- Open source initiative hosted at The Linux Foundation
- Embodies open governance and collaboration

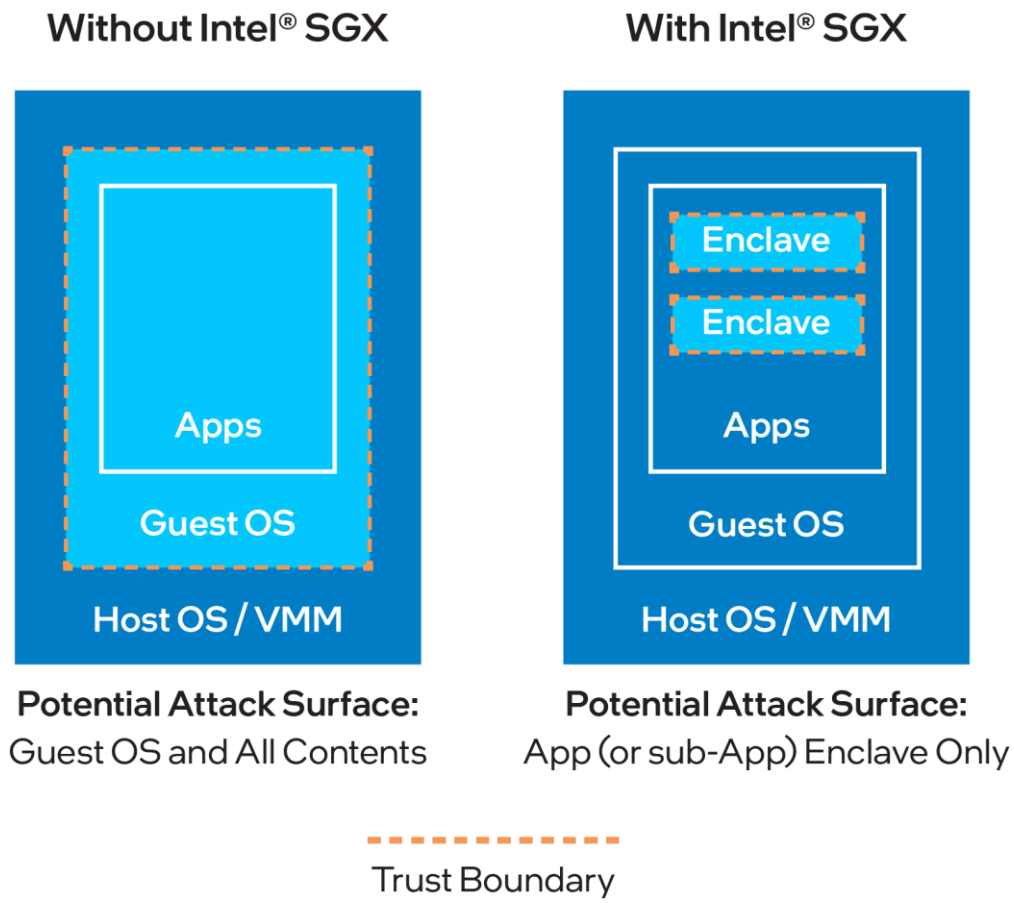
confidentialcomputing.io/

Use Case: Hardening the DevSecOps Pipleine

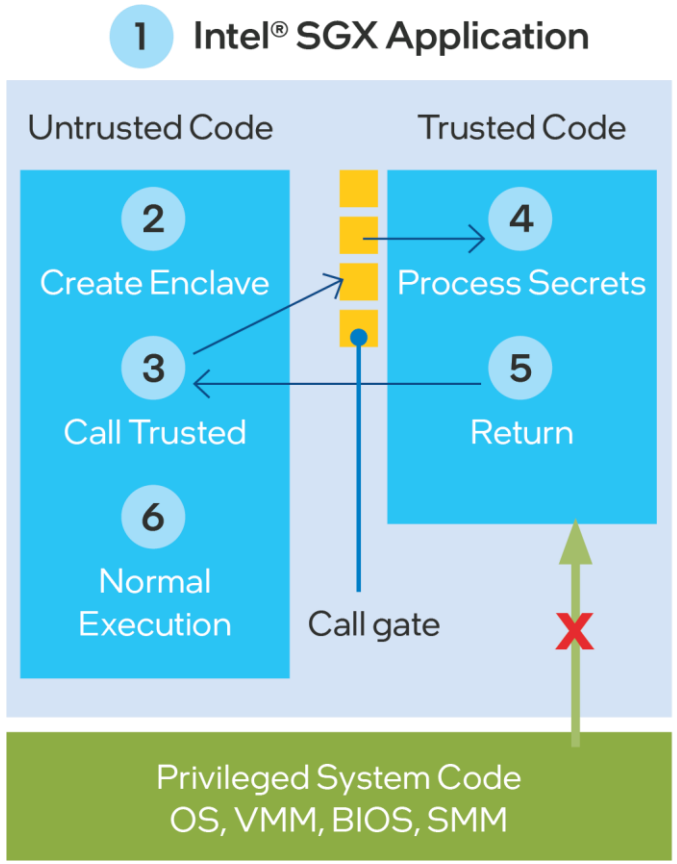


Intel® SGX Enables Confidential Computing

- Intel SGX enclaves are isolated memory spaces that protect trusted data and code
- Hardware protections cannot be overcome by privileged users or software:
  - Without Intel SGX: Data attack surface extends to the entire OS
  - With Intel SGX: Attack surface encompasses only the enclave



Trusted and Untrusted Application Components

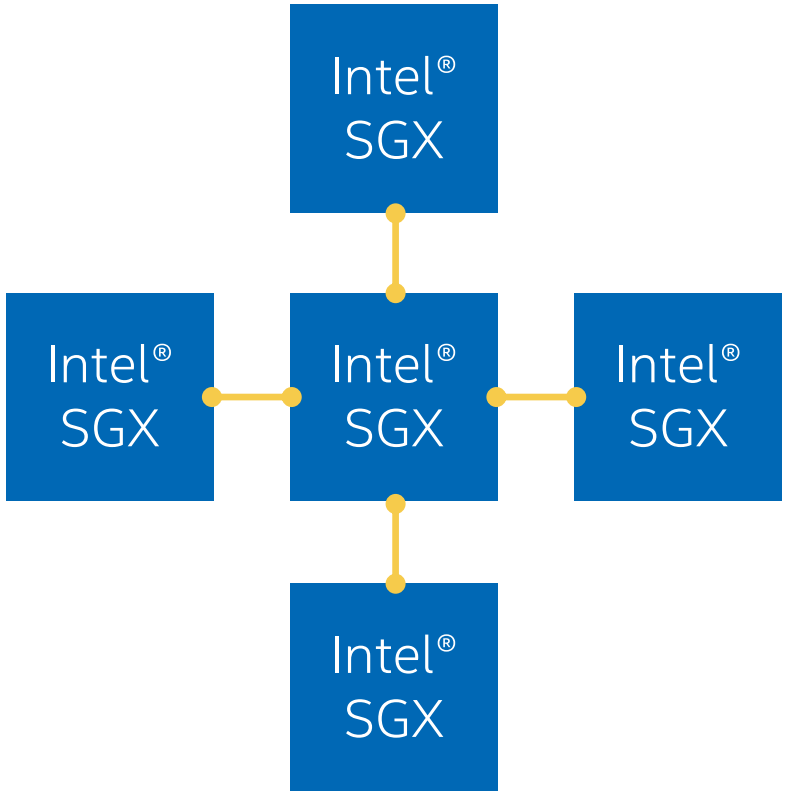


1. App is built with trusted and untrusted parts
2. App runs and creates the enclave, which is placed in trusted memory
3. Trusted function is called, and execution is transitioned to the enclave
4. Enclave sees all process data in the clear; external access to the enclave data is denied
5. Function returns; enclave data remains in trusted memory
6. Normal execution resumes

Attestation

Protected Interactions Among Enclaves

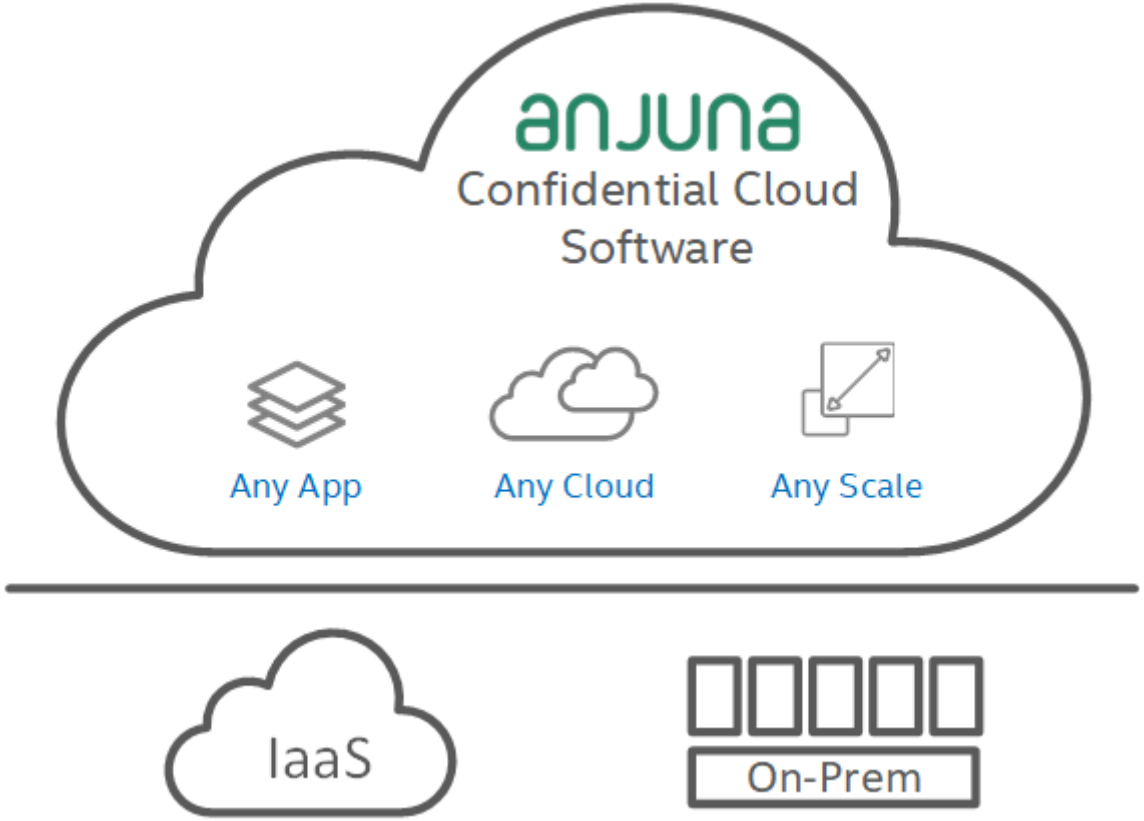
- Intel® Attestation Service communicates between enclaves to verify status:
  - Code is running as built
  - Hardware is Intel® SGX-capable
  - Intel SGX is configured correctly



Anjuna Confidential Cloud Software

Streamlined Workload Isolation

- Run binaries in Intel SGX enclaves, without code changes or recompilation:
  - Any app, on any cloud, at any scale
  - Accelerated time to value
  - Frees up engineering teams to innovate



HashiCorp Vault

Secret and Encryption Management

- Encryption, authentication, and authorization services
- Enables secure storage, management, control, and auditability of secrets

Secure Secret Storage

Encrypted secret key/value pairs

Dynamic Secrets

Short-lived secrets on demand

Live Data Encryption

Encrypt data without storing it

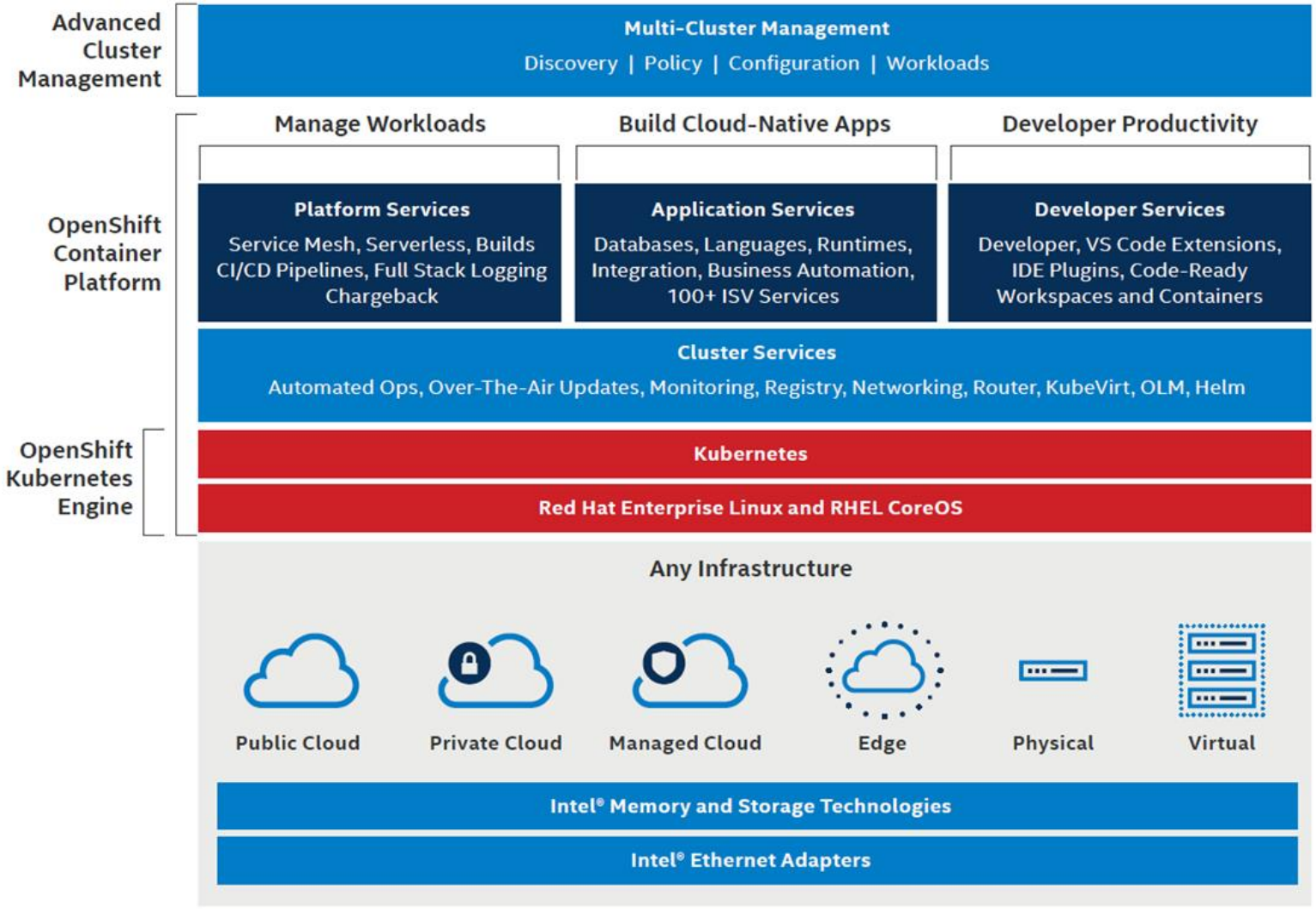
Leasing and Renewal

Automatic secret renewal and revocation

Built-in Secret Revocation

Manual revocation of sets of secrets

Red Hat® OpenShift®: Cloud-Native Infrastructure



Use Case: Anjuna, HashiCorp, and Intel

- **Modify the Dockerfile** from bitbucket.org/anjunasec/partner-hashicorp/src/master/Dockerfile
  - Add Anjuna Confidential Cloud software and dependencies to the image:

```
RUN wget https://s3-us-west-1.amazonaws.com/anjunasecurity.releases/release-1.34/0002/anjuna-
with-deps-rhel-8.tar.gz && tar -zxvf anjuna-with-deps-rhel-8.tar.gz --directory /

 RUN chown -R vault /anjuna && \
     groupadd --gid 1001 sgx_prv && \
     usermod -a -G sgx_prv vault
 RUN mkdir /runtime && chown -R vault /runtime
```

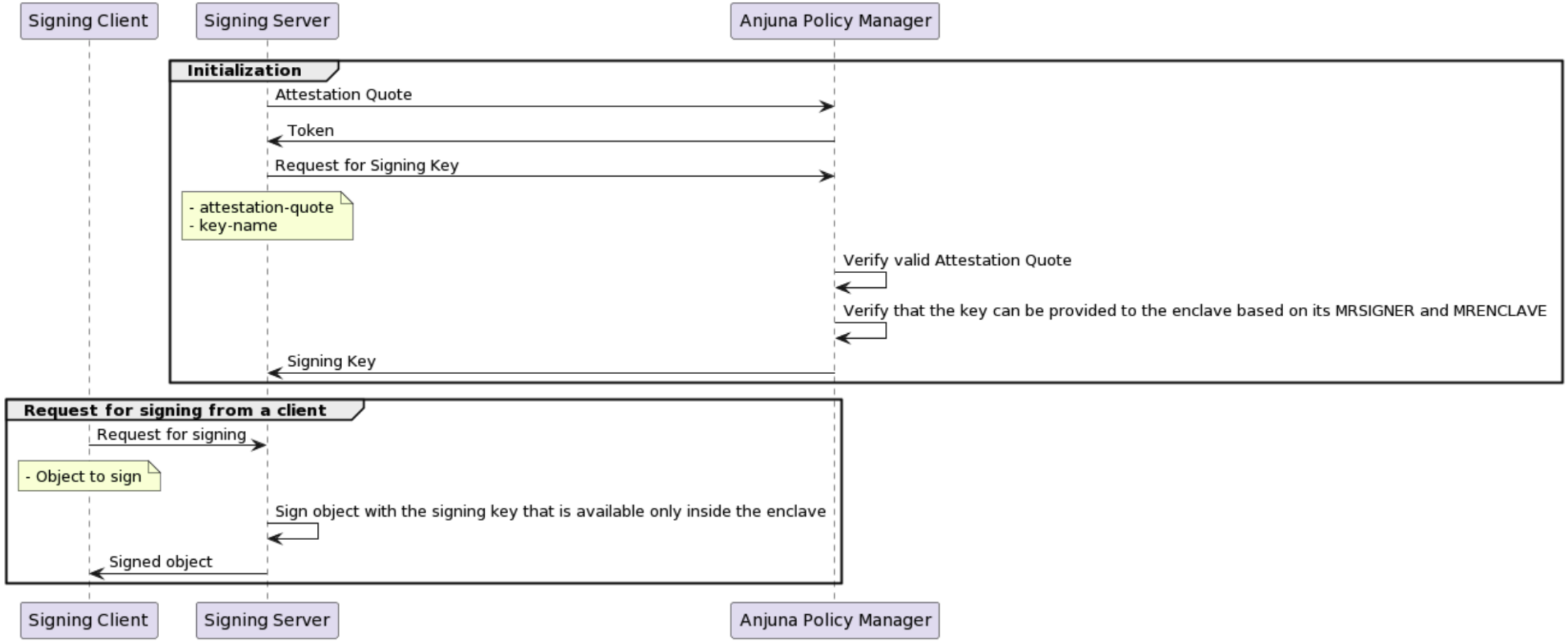
  - Set up Anjuna Confidential Cloud software environment variables:

```
WORKDIR /runtime
ENV PATH="/anjuna/bin:/anjuna/tools:${PATH}"
ENV ANJUNA_DIR=/anjuna/
ENV ANJUNA_BIN_DIR=/anjuna/bin
ENV SGX_SIGNER_KEY=/anjuna/signing/enclave-key.pem
ENV AZDCAP_DEBUG_LOG_LEVEL=error
```

- Modify the script at github.com/hashicorp/docker-vault/blob/master/ubi/docker-entrypoint.sh
  - To run HashiCorp Vault inside an Intel SGX enclave using the Anjuna Confidential Cloud Software, the second-to-the-last line in the script must be changed:

```
exec "$@"  ⟶  exec anjuna-sgxrun $@
```

HashiCorp Vault Use Case Implementation



Further Information

- Intel® SGX: intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html
- Anjuna Confidential Cloud Software: anjuna.io/product
- HashiCorp Vault: hashicorp.com/products/vault
- Red Hat® OpenShift®: redhat.com/en/technologies/cloud-computing/openshift

Legal Disclaimers

Performance varies by use, configuration and other factors. Learn more at www.intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for configuration details. No product or component can be absolutely secure.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.


intel