White Paper

Confidential Computing

An Ecosystem Solution for Confidential Computing

Anjuna® and HashiCorp enable confidential computing on Red Hat® OpenShift® using Intel® Software Guard Extensions (Intel® SGX). In this architecture, containerized applications isolate secrets such as encryption keys and passwords in hardware-protected memory enclaves.

Table of Contents

Protecting data while in use—as opposed to at rest or in transit—is challenging in part because that data must generally be in an unencrypted state for software to operate on it. Isolating free-text data from other applications and services in the same shared memory space using software measures is limited by definition, because with sufficient privileges, that isolation can always be overcome. Moreover, such measures are poorly suited to protection against system software compromise or insider threats.

Attacks on the software supply chain are a critical emerging cybersecurity challenge that primarily focuses on data in use by exploiting vulnerabilities in tools and code. Research suggests that the number of software supply chain attacks tripled in 2021 compared to the year before,[1] and that organizations of 50,000 seats or more are targeted nearly every week on average.[2]

Resisting these attacks is made more challenging because doing so effectively requires coordinated joint effort between security, development, and operations (DevSecOps) organizations within IT. The rise of DevSecOps in enterprise IT provides that coordination, bringing together all three organizations into a unified team that helps guard against supply chain compromise. Confidential computing supports that effort with an important mechanism to harden the DevSecOps pipeline.

> *Organizations that handle sensitive data such as personally identifiable information (PII), financial data, or health information need to mitigate threats that target the confidentiality and integrity of either the application or the data in system memory.*
>
> – Confidential Computing Consortium[3]

Confidential computing isolates trusted code and trusted data from unauthorized software and users based on a low-level hardware root of trust that extends upward through the solution stack. That root of trust enables a trusted execution environment (TEE), with a low-level hardware foundation that eliminates software dependencies and associated vulnerabilities. The TEE protects the trusted data and code, as well as the integrity of operations performed on it. Unlike software-based measures, the TEE is protected against unauthorized access by users or software, regardless of privilege level.

This paper describes an ecosystem-driven solution for confidential computing based on a hardware root of trust, as illustrated in Figure 1. Intel SGX implements confidential computing with hardware-enforced partitioning of system memory to create enclaves of restricted trusted memory space. Trusted code operates on unencrypted trusted data in enclaves, isolated from unauthorized entities. This silicon functionality is implemented in Intel® Xeon® Scalable processors using a dedicated instruction set, and modifications are typically required to application binaries, designating trusted portions of code to operate in enclaves.

Anjuna Confidential Computing software abstracts away that complexity by enabling any existing software, without modification, to take advantage of Intel SGX enclaves. The work described in this paper implements secret and encryption management based on HashiCorp Vault, running on Intel SGX-capable hardware using the Anjuna platform. The solution runs in containers, using a modified Dockerfile provided by HashiCorp to provide cloud-native operation on Red Hat OpenShift. Following a use case description that describes their combined implementation at the command level and how the solution architecture can be used to harden the DevSecOps pipeline, each of these hardware and software components is described individually.

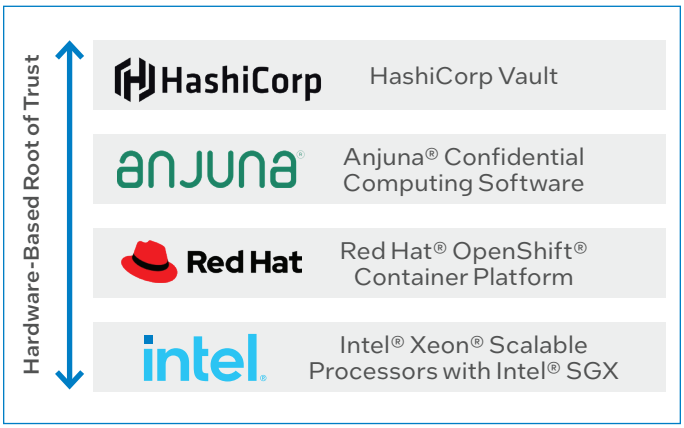

Figure 1. Hardware-based root of trust for confidential computing.

1 Hardening the DevSecOps Pipeline

Running HashiCorp Vault inside of Intel SGX enclaves provides novel capabilities to harden the DevSecOps pipeline. High-profile software supply chain attacks such as the SolarWinds breach in 2021 demonstrate the common vulnerabilities currently exposed in many DevSecOps pipelines and the potentially destructive impacts they can have. The compromise in the SolarWinds hack injected a malicious Dynamic Link Library into a late stage of the pipeline, which was then signed using the legitimate code-signing certificate before being pushed out in a client update.

Manual security and audit processes for DevSecOps pipelines are common, creating a primary risk vector for software supply chain compromise. The slow pace of these labor-intensive processes can make it difficult to identify pipeline attacks in a timely manner. Using the Anjuna and HashiCorp solution to run applications inside Intel SGX enclaves provides hardware-based proof of software components' integrity, protecting the software supply chain more broadly. This use case extends protection for data at rest throughout the DevSecOps pipeline, as shown in Figure 2:

- **Secure Development Environment.** The local integrated development environment (IDE) is linked to an enclave that helps protect the source management solution (e.g., Git repo) on a central server or cloud system. A secure ledger provides code integrity by means of attested code and binary checkins. This architecture also provides integrity protection by attesting code and binary check-out.
- **Secure Build Environment.** The compiler (e.g., GCC) runs in a container inside an enclave. This topology provides integrity protection by attesting both code input and binary input. A secure ledger adds code integrity by attesting to the binary output.
- **Secure Test Environment.** QA and regression testing are protected inside an enclave, with integrity protection provided by attesting the binary and a secure ledger adding code integrity to the QA results.
- **Secure Release Environment.** The build process is protected inside an enclave, with integrity protection provided by attestation of the build inputs and release versions. A secure ledger adds code integrity.

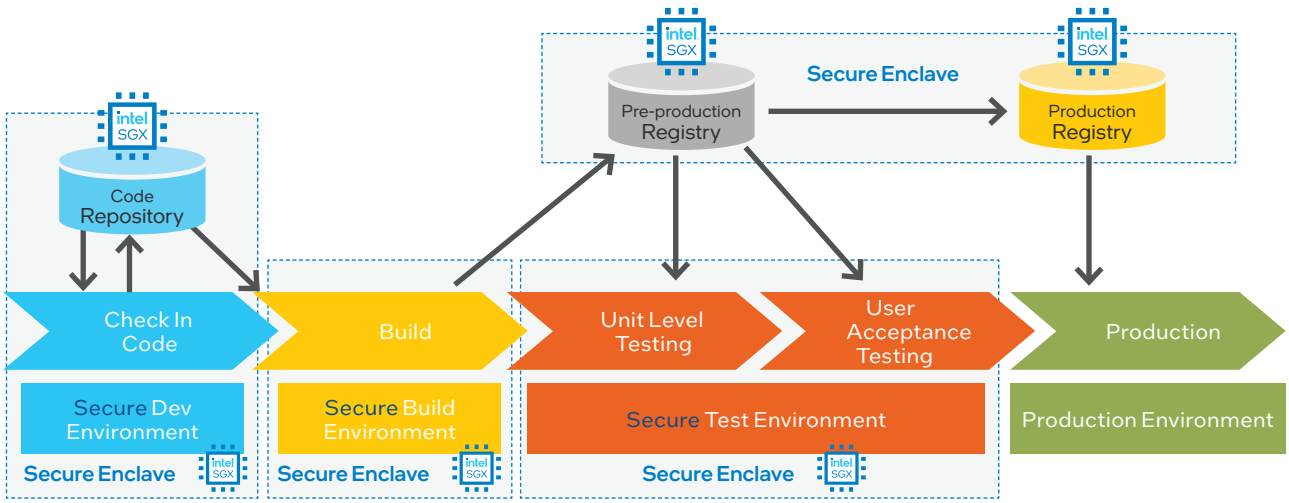

Figure 2. Runtime protections based on Intel® SGX enclaves for hardened DevSecOps.

2 Hardware Enablement for Confidential Computing: Intel SGX

Software-based protections for data are inherently vulnerable to being circumvented by other lower-level or more-privileged software. As a simple illustration, a typical application is unable to shield its data from processes authorized by the OS, hypervisor, pre-boot partition, or a user with root access. From a cyber security perspective, attacks on the OS can compromise everything running on it, effectively extending the attack surface for an individual piece of sensitive data to the entire OS. That state is shown in the "Without Intel SGX" pane of Figure 3.

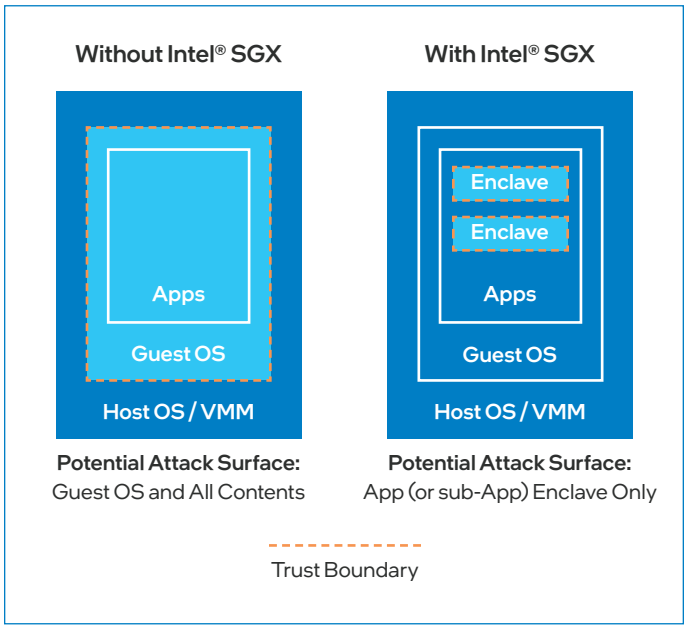

Figure 3. Reduced trust boundary and attack surface with Intel® SGX.

As shown in the "With Intel SGX" pane of Figure 3, Intel SGX memory enclaves isolate data and executing code, using a private memory space that is inaccessible from outside the enclave and the only place where the data is held in an unencrypted state. To access the trusted data held within an enclave, processes must therefore operate within the same enclave as well, which limits the data's attack surface just to the enclave, dramatically simplifying protection. The enclave itself is protected using encryption based on hardware-resident keys that are inaccessible by software.

2.1 Application Architecture: Trusted and Untrusted Components

The primary requirements for application software to make use of Intel SGX are to generate enclaves and designate trusted portions of code that will operate inside of them. Each trusted component is granted access to the trusted memory region that corresponds to a specific enclave that houses trusted data that it consumes, as illustrated in Figure 4. An application can include multiple trusted components, with each granted access to a different enclave (or set of enclaves).

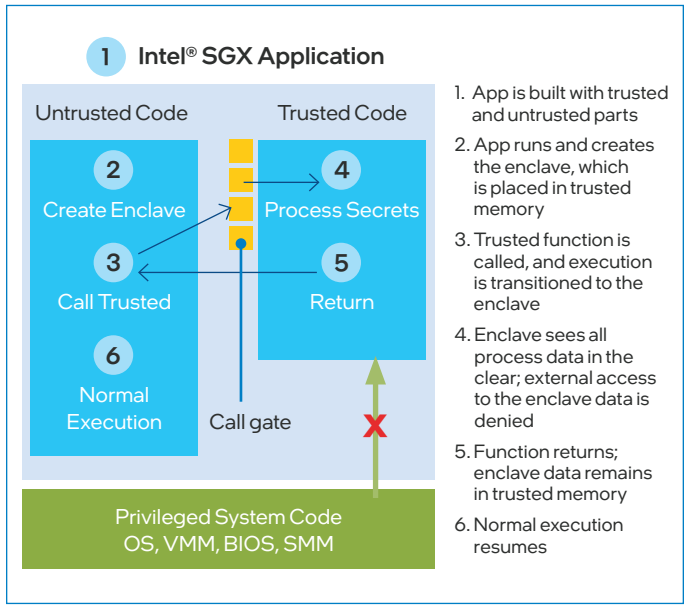

Figure 4. Intel® SGX interaction between trusted and untrusted application components.

The Intel SGX SDK provides the tools for development teams to designate trusted and untrusted portions of applications, provide communication between those portions, and create enclaves for trusted execution using Intel SGX instructions. By default, code is untrusted, meaning that it does not have access to any enclave; that designation includes privileged system software such as the OS, BIOS, firmware, etc. That property enables Intel SGX to use its hardware-based encryption to enforce data isolation against any user, application, or process, regardless of privilege level.

2.2 Attestation: Protected Interactions Among Enclaves

The Intel® Attestation Service enables communication and interaction between Intel SGX enclaves with cryptographic status verification of the trusted execution environment, based on the hardware root of trust. Key attributes of an enclave that are verifiable using attestation include the following:

- **The code is running as-built** in a genuine enclave
- **The hardware is an Intel SGX-capable platform** with all needed microcode updates applied
- **All necessary Intel SGX hardware and software configurations** are made correctly

Attestation may involve enclaves that are hosted on the same platform or on separate platforms. The former case is referred to as "local attestation" and is common, for example, so that multiple components of a single application—each in its own enclave—can work together on shared tasks. Remote attestation, on the other hand, provides confidentiality and integrity assurances for communications between enclaves on separate hosts such as verification between a server application and a remote data source, even over untrusted channels.

Built-In Crypto Acceleration Complements Intel® SGX

Intel® SGX is part of the platform-level approach to securing cloud-native networks that is designed into the 3rd Generation Intel® Xeon® Scalable processor. Among the range of hardware-resident security features that complement Intel® SGX, the platform's built-in hardware-based cryptographic acceleration is of particular note.

To help mitigate the performance impacts of pervasive encryption, the platform provides up to **4.2x higher TLS** encrypted connections per second.[4] **Read more ›**

3 Streamlined Workload Isolation: Anjuna Confidential Computing software

Protecting data in use using Intel SGX enclaves enables computations to be carried out on it without exposing it in the clear. Taking advantage of this capability typically requires modifying applications to designate trusted portions of code that operate inside the enclave. To reduce the associated training and operational requirements on development teams, Anjuna Confidential Computing software provides the ability to run any application in an Intel SGX enclave without requiring any changes to application binaries. That simplification helps accelerate the time to benefit from confidential computing projects, as well as allowing developers to focus on more value-added work.

Anjuna Confidential Computing software is built to operate in any environment where Intel SGX resources are available, including either on-premises or on infrastructure-as-a-service such as Microsoft Azure. It integrates easily with existing tools and workflows, including modernization and transformation initiatives such as DevOps and DevSecOps. The platform is deeply optimized and enabled for Intel architecture, to protect workloads in Intel SGX enclaves augmented with hardware-accelerated encryption and hardware roots of trust, across today's distributed cloud perimeter. It maintains a zero-trust network infrastructure that effectively obscures the presence of secrets as well as providing robust access control. Flexibility benefits of Anjuna Confidential Computing software include the following:

- **Any application.** No code changes or recompilation are needed, extending support transparently to custom, packaged, and legacy applications as well as container platforms including Red Hat® OpenShift®.
- **Any cloud.** Anjuna Confidential Computing software is built for the multi-cloud world, including private and hybrid clouds in conjunction with public ones such as Azure.
- **Any scale.** The platform handles any number of nodes, with minimal performance impact and protection that traverses multiple clouds along with data and applications.

Confidential computing capabilities based on Anjuna Confidential Computing software easily integrate into existing infrastructure and operations. Standard APIs integrate out of the box with existing management systems such as security information and event management (SIEM). The software is deployed on each cloud instance, and it automatically isolates data and code using Intel SGX, including the deployment and operation of HashiCorp Vault in enclaves.

4 Secret and Encryption Management: HashiCorp Vault

Protecting application secrets such as encryption keys, passwords, tokens, certificates, and other sensitive data is the core goal of confidential computing. HashiCorp Vault is a widely adopted secrets management tool that runs encryption, authentication, and authorization services to enable secure storage, management, control, and auditability of secrets. Beyond protecting access, Vault also provides monitoring and governance, making it possible to understand what parties, applications, and services are accessing specific secrets, across platforms.

Key features of Vault include the following:

- **Secure secret storage.** Vault encrypts secret key/value pairs before writing them to storage, providing an added layer of protection beyond protecting the storage itself.
- **Dynamic secrets.** Vault can generate short-lived secrets on demand, such as credentials for a database or S3 storage volume, and automatically revoke them after use.
- **Live data encryption.** Vault can encrypt and decrypt data without storing it, enabling developers to store encrypted data in databases or other conventional data stores without defining encryption schemes.
- **Leasing and renewal.** Vault maintains leases for each secret, to govern automatic revocation of the secret at end-of-lease; built-in APIs provide the mechanism for clients to renew secrets.
- **Built-in secret revocation.** Vault automates revoking sets of secrets, such as all secrets of a given type or that have been accessed by a given user, which is valuable for both key rolling and intrusion response.

5 Cloud-Native Infrastructure: Red Hat® OpenShift®

Red Hat OpenShift Container Platform is a Kubernetes-based, enterprise-grade software foundation for cloud-native infrastructure, as illustrated in Figure 5. OpenShift enables development teams to adopt application topologies based on containerized microservices, a key requirement for modern approaches such as DevOps and DevSecOps. It automates deployment, management, and maintenance functions to optimize administrator efficiency, with added services such as networking, monitoring, registry, and authentication to further streamline deployments.

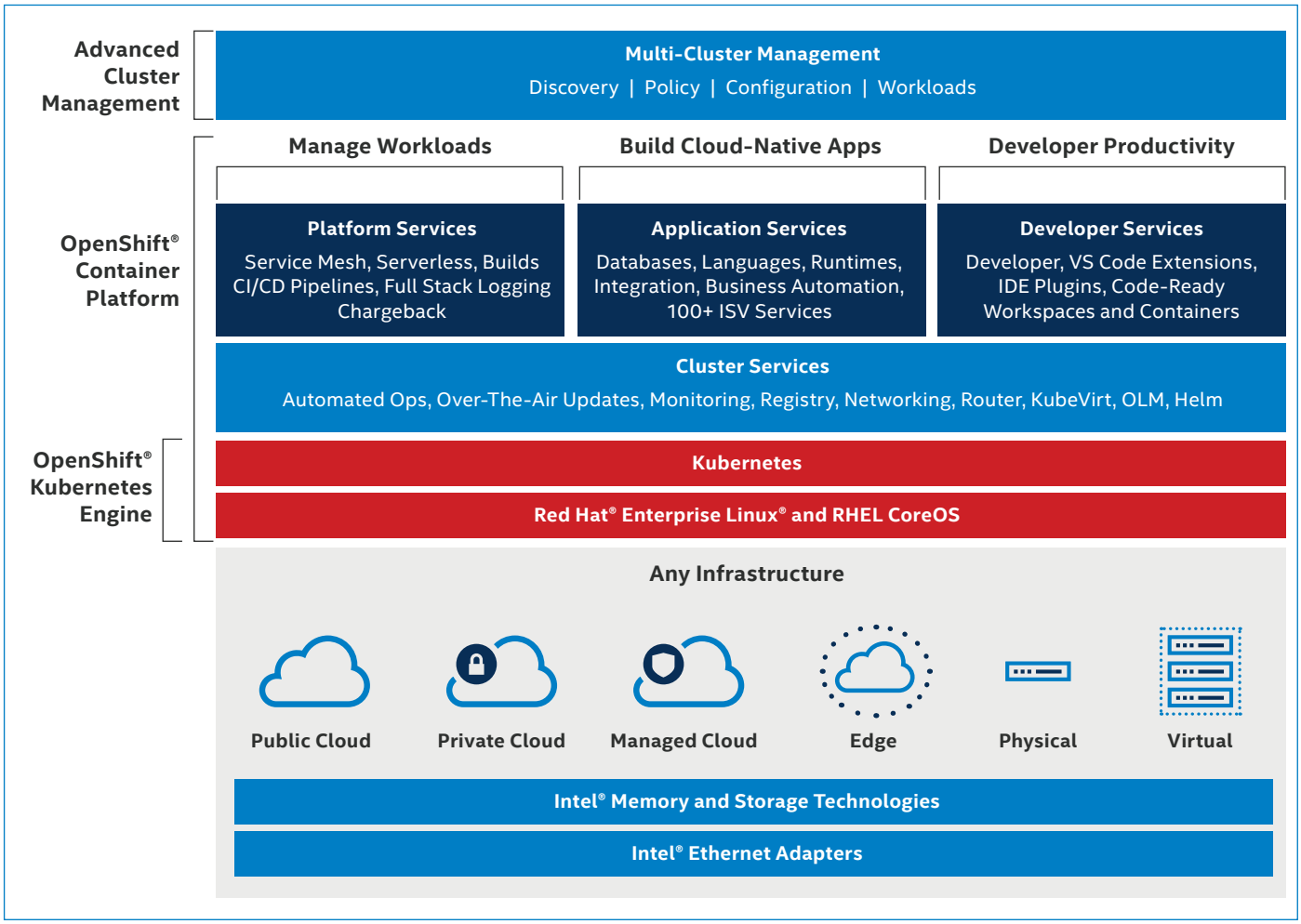

Figure 5. Red Hat® OpenShift®.

Developed and distributed as open source to foster innovation, OpenShift is hardened, tested, and certified by Red Hat engineers, improving overall security posture. OpenShift also incorporates the hardened Red Hat Enterprise Linux CoreOS, which is designed specifically for running containerized applications.

Multi-cloud-ready by design, OpenShift provides a consistent platform to implement and orchestrate containers across any combination of on-premises, hosted, and public cloud compute nodes, to dynamically provide enterprise services when and where they are needed.

6 Use Case: Anjuna Software Running HashiCorp Vault in an Intel SGX Enclave

This use case demonstrates the steps needed to deploy HashiCorp Vault in an Intel SGX enclave using Anjuna Confidential Computing software in a Red Hat OpenShift cloud-native container environment. It also briefly introduces the applicability of this implementation to hardening the DevSecOps pipeline and software supply chain.

The Anjuna Confidential Computing software simplifies the task of running HashiCorp Vault inside an Intel SGX enclave. Setup and configuration require minor changes to the Dockerfile and **docker-entrypoint.sh** script provided by HashiCorp, as detailed below.

6.1 Modifying the Dockerfile

The process of running HashiCorp Vault inside an enclave begins with modifications to the Dockerfile that HashiCorp provides for creating a Red Hat Universal Base Image (UBI) container for OpenShift. The Dockerfile is available at https://bitbucket.org/anjunasec/partner-hashicorp/src/master/Dockerfile.

6.1.1 Adding the Anjuna Confidential Computing software and Dependencies to the Image

```
RUN wget https://downloads.anjuna.io/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
```

6.1.2 Setting up Anjuna Confidential Computing 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
```

6.2 Modifying the **docker-entrypoint.sh** script

A minor change is also required to the **docker-entrypoint.sh** script provided by HashiCorp at https://github.com/hashicorp/docker-vault/blob/master/ubi/docker-entrypoint.sh.

To run HashiCorp Vault inside an Intel SGX enclave using the Anjuna Confidential Computing software, the second-to-the-last line in the script must be changed from

```
exec "$@"
```

to

```
exec anjuna-sgxrun $@
```

6.3 HashiCorp Vault Use Case Implementation

To provide an end-to-end confidential computing platform, the Anjuna Confidential Computing software provides the Anjuna Policy Manager. The Anjuna Policy Manager uses the HashiCorp plug-in architecture to provide access to secrets in HashiCorp Vault, based on attestation from the Intel SGX enclave using the Anjuna Confidential Computing software. Anjuna Policy Manager itself runs inside an Intel SGX enclave, also using the Anjuna Confidential Computing software. The solution creates a policy in Anjuna Policy Manager to provide a secret only to a client running inside an Intel SGX enclave that can provide an attestation quote with a specific MRSIGNER (signing identity) value, and if needed, a specific MRENCLAVE (enclave identity) value.

In the example shown in Figure 6, a signing component runs inside a protected enclave and provides an attestation quote to obtain the signing key. Thus, only a binary that is trusted based on its measurements and signature can access the signing key and use it inside the enclave.

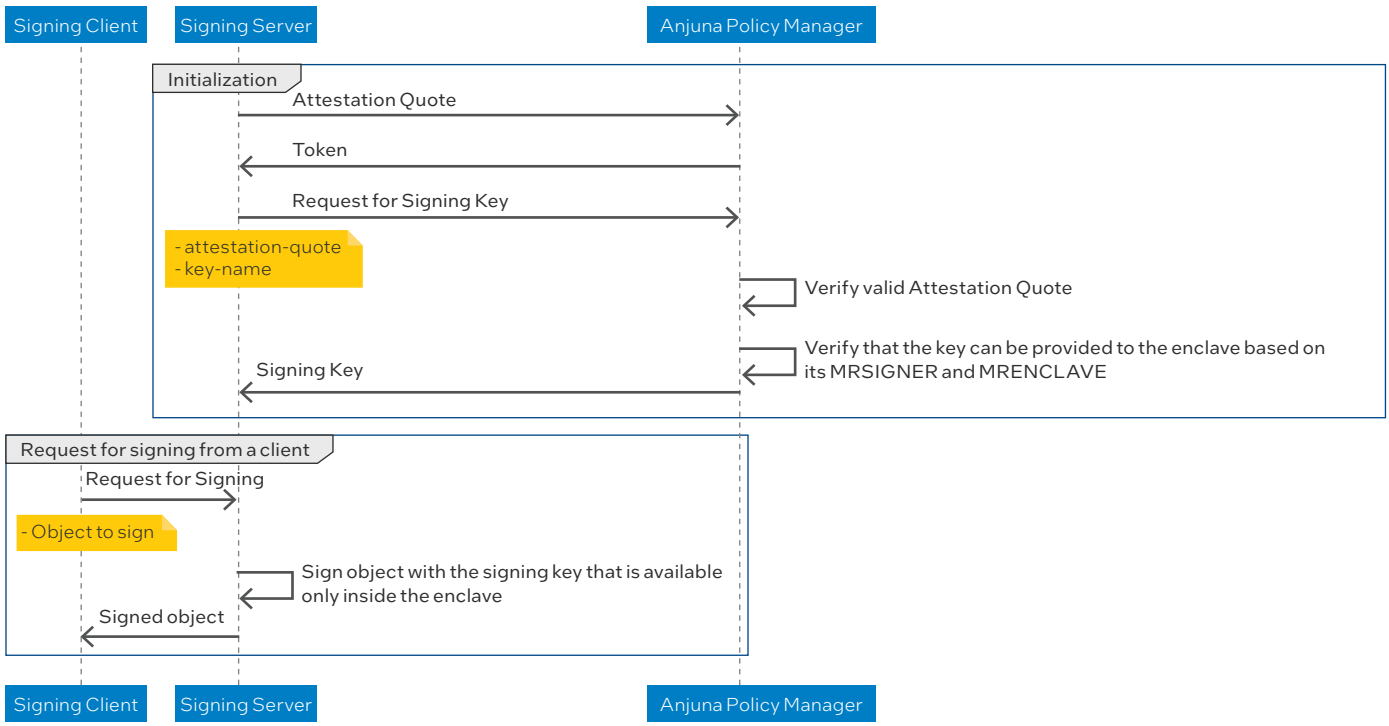

Figure 6. Signing component running inside an Intel® SGX enclave.

7 Conclusion

Confidential computing is a critical enabler for sensitive workloads, protecting data in use with a hardware-based root of trust. Intel SGX provides the silicon-resident foundations for confidential computing, with enclaves of protected memory that house application secrets and the code that acts on them. Anjuna Confidential Computing software streamlines deployment of HashiCorp Vault using Intel SGX enclaves, striving to provide an integrated hardware and software solution to optimize control over application secrets. Cloud-native implementation on Red Hat OpenShift provides a robust automation layer that drives efficiency gains into future-focused initiatives such as DevOps and DevSecOps.

The solution stack described in this paper provides a relatively simple approach to deploying confidential computing services in a multi-cloud environment. This model helps protect consumption of sensitive data, even across distributed networks, and contributes to a future of privacy-protected data-rich computing.

More Information

Intel® SGX: intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html

Anjuna® Confidential Computing software: anjuna.io/product

HashiCorp Vault: hashicorp.com/products/vault

Red Hat® OpenShift®: redhat.com/en/technologies/cloud-computing/openshift

Contributors/Writers:

Anjuna: Ofir Azoulay-Rozanes - ofir@anjuna.io

HashiCorp: Alex Cahn - acahn@hashicorp.com

Intel: Darren Pulsipher darren.w.pulsipher@intel.com; Raghu Moorthy raghu.k.moorthy@intel.com

[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.

[3] Confidential Computing Consortium. https://confidentialcomputing.io/.

[4] See [70], [90], [71], and [69] at 3rd Generation Intel® Xeon® Scalable Processors - 1 - ID:615781 |Performance Index. Testing by Intel as of August 4, 2020. Performance comparisons relative to 2nd Gen Intel® Xeon® Scalable processors using a single buffer algorithm versus multi-buffer algorithms for 3rd Gen Intel Xeon Scalable processors. Results have been estimated based on pre-production tests at iso core count and frequency as of August 2020. Performance gains are shown for individual cryptographic algorithms.

0522/RKM/MESH/349361-001US