Hewlett Packard Enterprise

Solution brief

Check if the document is available in the language of your choice.

HPE PROLIANT SECURE COMPUTING SERVER WITH FORTANIX CONFIDENTIAL COMPUTING MANAGER

Leverage HPE ProLiant and Intel® SGX to run applications securely

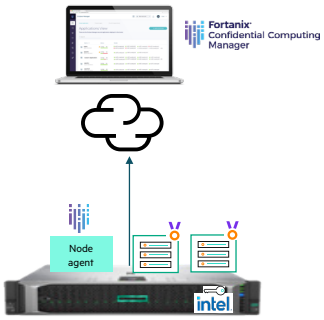

FIGURE 1. HPE server with Fortanix components

Solution overview

- Bring your existing applications to confidential compute environment without rewriting your applications using Fortanix CCM.
- Single-pane-of-glass monitoring and management of secure enclaves and confidential compute nodes with Intel Ice Lake Software Guard Extensions (SGX) processor connected to your most secure HPE ProLiant DL380T server.
- Leverages Intel SGX Technology to run code and data in CPU-hardened enclaves or a trusted execution environment (TEE).
- Remote attestation service allows application node to send an attestation to the platform, which verifies the attestation with the Intel Attestation Service to confirm that the application node is a genuine Intel SGX machine.

Protect applications and data while in use

MAKE YOUR APPLICATIONS CONFIDENTIAL

Overview

Today, data is often encrypted at rest, in Storage, and in transit across the network, but applications and the sensitive data they process are vulnerable to run time. Confidential computing protects data and applications by running them in secure enclaves that isolate the data and code to prevent unauthorized access, even when the compute infrastructure is compromised. While confidential computing is revolutionizing how customers protect their sensitive data, organizations need to simplify the process of creating enclaves, manage security policies, and enable applications to take advantage of confidential computing.

The solution leverages HPE ProLiant DL380T Trusted Supply Chain Server with Intel Ice Lake SGX processors to deliver single pane of glass for managing secure enclaves across the SGX-based confidential compute nodes within the data center.

The solution can help orchestrate critical security policies such as identity verification, data access control, and code attestation for enclaves that are required for confidential computing.

KEY FEATURES

Enclave lifecycle management

The platform manages the entire enclave lifecycle including creation, deployment, monitoring, and auditing. The solution manages confidential computing infrastructure and applications across the environment to provide complete visibility.

Cryptographically enforced policy and auditing

Fortanix manages and enforces security policies including identity verification, data access control, and attestation to help ensure the integrity and confidentiality of data, code, and applications. Using these policies, businesses can implement geo-fencing and compute affinity to support data regulation policies such as GDPR. Fortanix also provides audit logs to easily verify compliance requirements.

Bring your own application support

Fortanix makes it possible to enable existing applications, enclave-native applications, and prepackaged application to run in a secure enclave in minutes. This capability is unique and enables widespread adoption of confidential computing with no development or integration costs.

Code verification

Above all competing methods, Fortanix verifies the identity of code and applications using digital certificates and public key infrastructure (PKI).

HPE trusted supply chain process
Hewlett Packard Enterprise further extends its security capabilities in a server from distribution and shipping, through its complete lifecycle while it is still active. The new features are built on top of the HPE exclusive silicon root of trust security technology, which has been recognized for the ability to reduce risk by insurers in the new Cyber Catalyst program from Marsh program. Hardened security features activated during the manufacturing process offers the following benefits:

- Prevent booting of any compromised OS by using new hardening to connect the server firmware security to the OS by activating the UEFI secure boot
- Reduce attack surface by placing servers in high security mode to verify user authenticity, helping ensure that more than four million lines of firmware code is valid and uncompromised
- Prevent tampering of server firmware and hardware using server configuration lock to verify unauthorized addition of options (NICs, drives) or malicious activity by capturing the inventory or a picture of the server, and its hardware and firmware at the factory to provide protection throughout the supply chain process
- Alert customers with embedded alarm and physical lock if the server has been opened during the supply chain process when an intrusion detection latch, inserted on the server chassis, registers unauthorized opening even if the power is off

Make the right purchase decision. Contact our presales specialists.

Chat **Email** **Call**

Get updates

KEY USE CASES

Secure application development

Fortanix CCM monitors the lifecycle of secure enclaves that run the container applications, which provides unique features such as remote attestation, geo-location enforcement, Digital Right Management (DRM), secret injections, and more. In addition, the platform seamlessly integrates with existing container orchestration technologies, including Kubernetes, Docker Swarm, and OpenShift.

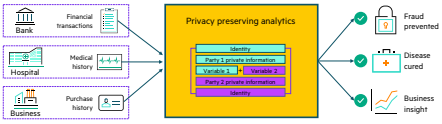

FIGURE 2. Various use cases and desired outputs

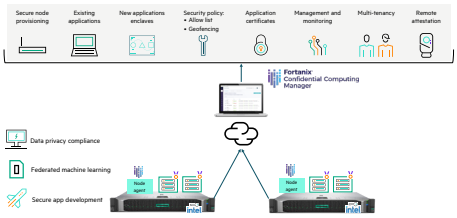

FIGURE 3. Fortanix Confidential Computing Manager

FEDERATED MACHINE LEARNING

Fortanix CCM simplifies and secures the process of sharing private data without exposing it to other parties or violating privacy regulations. Multiple parties contribute encrypted data to a TEE, where the data is combined and analyzed, and then results are output in an encrypted format back to each party with the results of the analytics. Data remains encrypted throughout the entire process, protecting the privacy of the data as it is transferred, during computation and while being stored.

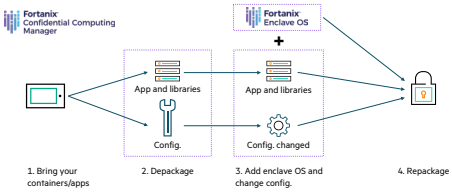

FIGURE 4. Stages of confidential computing

Data privacy compliance

Fortanix CCM can help organizations meet compliance requirements for regulations such as GDPR, the California Consumer Privacy Act (CCPA), and other similar regulations. It also provides fine-grained access controls for the data sets in use in containers. With this new approach, the aggregate data is not exposed outside the secure enclave.

TAKE THE NEXT STEP

Visit hpe.com/security or Fortanix.com for more information.

a50003905ENW, April 2021

Hewlett Packard Enterprise