Fortanix®

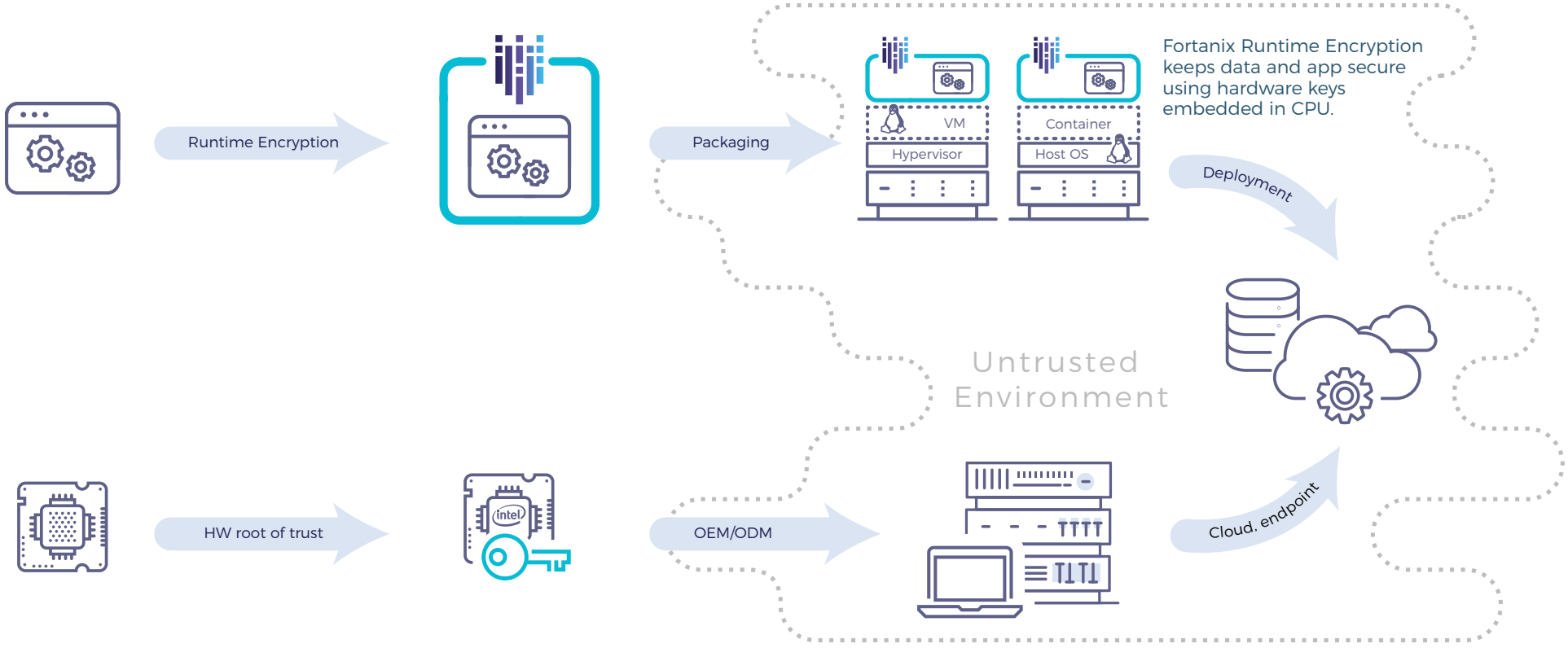
Runtime Encryption — a new paradigm in security

Technology Brief: Fortanix Underlying Technology

Fortanix Runtime Encryption (FRE) technology enables applications to process and work with encrypted data, without the possibility of exposing plain-text code or data to the operating system or any other running process – including any form of malicious attack. FRE is built using the Intel® SGX technology, available in Intel® CPUs, and makes data and applications used inside Intel® SGX enclaves inaccessible to the cloud service provider, as well as Fortanix itself.

The implications of the ability to provide complete, easy-to-implement encryption of the execution environment of any application or data are immense, and so are the particular use-cases, detailed in separate solution briefs.

This technology brief describes the fundamentals of Intel® SGX technology and Fortanix Runtime Encryption.



info@fortanix.com | +1 (628) 400 2043 | 444 Castro St #702 Mountain View, CA 94041

Fortanix

About Intel® SGX (Software Guard Extensions)

- Intel® SGX technology provides protection for the execution environment that significantly reduces the attack surface for applications.
- Intel® embeds encryption key in CPU during manufacturing (5th gen and on), and provides a set of instructions that applications can use to create a private region of memory (aka enclave) that is isolated from all other processes, even those with higher privilege levels (root users).
- Once an application runs inside an Intel® SGX enclave, all the system memory that is allocated to it is transparently and automatically encrypted by the CPU core. Moreover, the key used to encrypt memory resides in CPU hardware. Therefore, if an attacker tries to snoop the system memory by reading directly form system memory, it will not be able to access the decrypted memory. SGX also protects against memory replay attacks.
- This provides hardware-level-security for the applications and workloads running on an SGX-enabled machine.

The challenge building apps to run with SGX:

- In order to protect application with SGX, the application's code must be altered and Intel's SGX SDK must be used. This effort is app-specific (e.g. for each app, the developer needs to partition it into trusted and untrusted parts and build using Intel SDK)
- SGX SDK provides low level primitives to build standalone C/C++ apps, but doesn't provide libraries, tools, and support to build more complex apps (e.g., distributed apps, apps written in other languages such as Java, web services, etc.).
- This results in severe limitations of the use, implementation and scalability of SGX.

info@fortanix.com | +1 (628) 400 2043
444 Castro St #702 Mountain View, CA 94041

Fortanix Runtime Encryption (FRE)

- **FRE is an abstraction layer** that is easily installed on every generic hardware, enabling any **unmodified** app to run in a hardware-encrypted trusted context created by Intel® SGX CPU.
- In order to enjoy full SGX protection, all that's required is to **simply install the app** (plain binary) on top of FRE.
- **FRE supports any type of app**: Native, container, VM, etc. written in any programming language.
- **FRE uses the SGX key** in CPU to encrypt app's runtime, creating a trusted environment (enclave) even in an untrusted environment — an independent hardware-enforced footprint to keep the app secure.
- **The app is secure wherever it is deployed**: No root users, IT personnel, Cloud Service Providers, nation states, etc. have any access or visibility into FRE's protected data. Only the tenant's authorized user can access the data.
- **FRE secures the app's entire lifecycle** — Provisioning, integration with Intel® SGX, runtime attestation, tamper proof guarantees, and communication. Trust management is maintained across distributed SGX enclaves. The app maintains its data confidentiality even when cloud infrastructure is breached or the cloud provider receives a data disclosure request made under the law.
- **FRE's broad-platform approach enables multiple use-cases** such as Self defending KMS + HSM and database encryption, as well as out-of-the-box ability to scale, cluster, serve hybrid and distributed environments and more.