DATASHEET

Fortanix | ethos technology

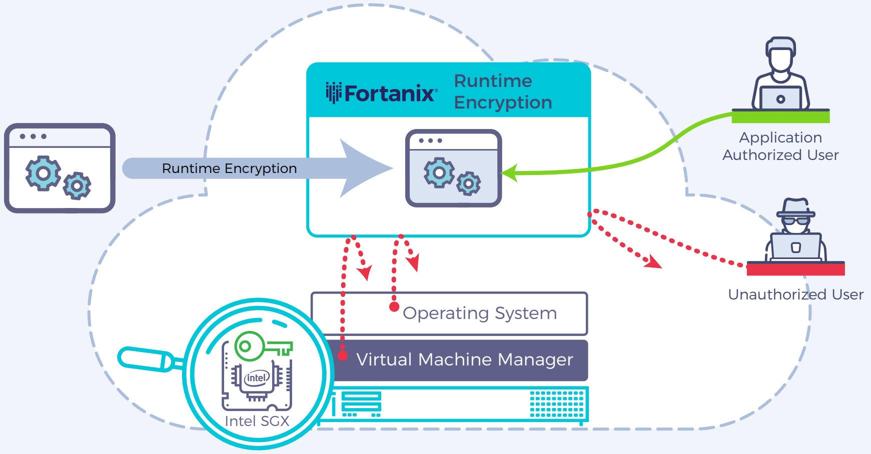
Runtime Encryption™ Platform

Fortanix Runtime Encryption transparently protects your sensitive applications and data in use

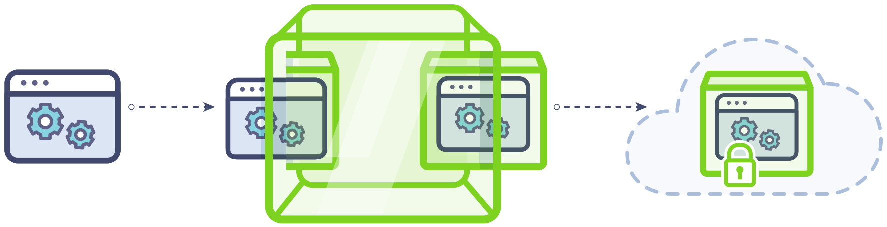
Runtime Encryption overview

Encryption is an effective data protection control, however it's use is currently limited to data at rest and data in motion. When, an application starts to run, it's data in use is vulnerable to a variety of attacks including malicious insiders, root users, credential compromise, OS zero-day, and network intruders.

Runtime Encryption provides deterministic security with runtime memory encryption for applications to protect data in use. Runtime Encryption enables a fundamentally new level of security and privacy allowing organizations with sensitive data to operate in untrusted environments.



Transparently Protect Your Apps



Fortanix Runtime Encryption (RTE) uses Intel® SGX to enable general purpose computation on encrypted data without ever exposing plaintext application code or data to the operating system or any other running process. Therefore even if the infrastructure is compromised or malicious insiders have root passwords, the application remains cryptographically protected.

However, applications do not work out of the box with Intel SGX. Application developers need to rewrite or restructure their application code. Furthermore, developers have limited choice in toolkits and lack the ability to readily create secure distributed applications.

Fortanix RTE includes EnclaveOS™ that is designed to transparently run any application within the trusted execution environment of Intel® SGX. EnclaveOS creates a portable security envelope to run applications in completely protected states without requiring modifications. RTE secures the entire lifecycle of the application.

Deterministic Security

Runtime Encryption provides complete cryptographic protection for your applications. The entire application runs inside a secure execution environment and is protected from OS, root users, hypervisor, any malware or any other process running on the same server, or anyone having physical access to the server. Runtime Encryption ensures that data in use is encrypted and only the protected application can access its data. You can now run highly sensitive applications even on untrusted infrastructure.

Easy to Use

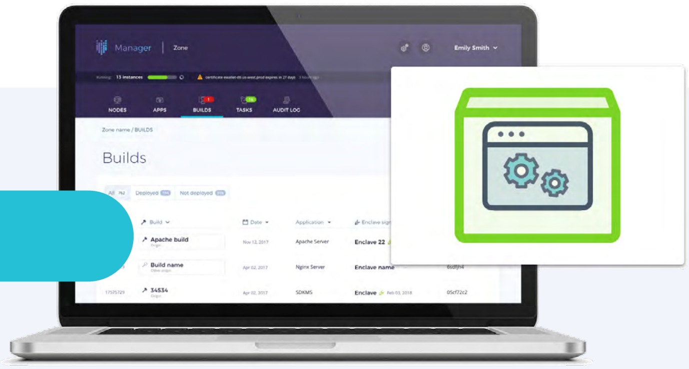
Fortanix EnclaveOS provides a runtime environment that attaches to any application without requiring rewrite or recompile of the application. With Runtime Encryption, you can rapidly build protected application with no application developer burden or learning curve whether you have an existing application or are developing a new application. Runtime Encryption seamlessly supports application development workflows and integrates with orchestration tools like Kubernetes, extending the security benefits to application developers working in an agile environment.

Broad Application Support

Runtime Encryption is purpose-built to protect container-based applications but also supports any x86 application built using a variety of major programming languages. Application developers can readily create secure distributed applications. With support for Python and R, Runtime Encryption can protect sensitive data analysis and machine learnings applications. Commonly used applications such as Databases, Web Servers, Build Servers, Directory Servers and Key Managers are available protected out of the box.

CONTACT FORTANIX
TO SECURE YOUR APPS:

CONTACT



Builds

Build	Date	Application	Enclave sig	
Apache build	Nov 12, 2017	Apache Server	Enclave 22	
Build name	Apr 02, 2017	Nginx Server	Enclave name	6sdfjh4
34534	Apr 02, 2017	SDKMS	Enclave Feb 03, 2018	05cf72c2