SERVERS WITH INTEL®
XEON® PROCESSORS
RUNTIME ENCRYPTION
CAPSULE* WITH FORTANIX*

Self-Defending Key Management Service with Intel® Software Guard Extensions

Fortanix* Runtime Encryption Capsule* for Intel® SGX

CONTRIBUTORS

Fortanix
Ambuj Kumar
Anand Kashyap

Intel Corporation
Vinay Phegade
Jesse Schrater

INTEL® XEON® E3 V5 PROCESSOR SERIES

TABLE OF CONTENTS

AUDIENCE AND PURPOSE

The audience of this whitepaper includes security architects and technical security leaders considering new and better approaches to help secure their applications in public, hybrid, and multi-cloud deployments by ensuring that there is protection from malicious processes running with higher privileges.

Intel® Software Guard Extensions (Intel® SGX) enables a fundamental change to enterprise security providing hardware-level trustworthy execution of x86 applications. It allows enterprises to help secure sensitive applications independent of the overall security of the infrastructure.

This whitepaper describes a Fortanix* Runtime Encryption Capsule* (REC). REC is a trusted execution environment for workloads to use SGX enclaves for their cryptographic protection from rouge insiders, compromised OS, malware, and other vulnerabilities.

To illustrate use cases for REC, a Self-Defending Key Management Service* (SDKMS) is described. SDKMS enables a cloud-agnostic, cost-effective, self-serviced encryption key management service with competitive cost structure, great performance, verifiable strong security proofs, elasticity, and resiliency for cloud applications.

EXECUTIVE SUMMARY

Enterprises want to migrate to the cloud for cost saving, but security is often a critical concern. Modern enterprises have begun a historic migration of core systems to public, hybrid, and multi-cloud environments. Enterprise IT executives expect that 60% of workload will run in various clouds by 2018 from survey data of 1200 buyers by 451 Research.

According to the largest survey of its kind, the 2016 NorthBridge Future of Cloud Computing survey, security remains the #1 inhibitor of enterprise migration to the cloud.

Enterprises IT is concerned about losing control over security while running in a public cloud. The concerns of enterprises include a dependency on the cloud provider with no clear separation of responsibility between customers and providers. Customers outsource certain tasks, but they retain full responsibility for security of their sensitive workloads. Providers provide their own security to ensure security isolation in multi-tenant contexts where multiple customers may run processes on the same physical hardware but insiders have visibility into customers' applications and data. It's no wonder, therefore, that customers cite privacy and security concerns as a leading obstacle to more rapid and more widespread adoption of cloud migration, particularly to public clouds.

Intel's new Software Guard Extensions (Intel SGX) fundamentally alters the security architecture. Intel SGX enables application code and data isolation even in the presence of a compromised operating system, hypervisor, and privileged administrator. This reduces the attack surface of the applications by several orders of magnitude through per-application isolation based on Intel® hardware-supported encryption.

Fortanix* provides the first commercial implementation of Intel SGX to create Runtime Encryption Capsules* (RECs). REC is a software platform for transparently running applications with Intel SGX protection.

Enterprises seeking hardware-level security for zones of trust have historically been limited to the option of integration with hardware-security module appliances and often cite the resultant key management complexity as a deep pain point. These HSM appliances can be expensive, proprietary, hard to deploy, harder to manage, and are often impossible to scale efficiently. Application integrations are often bespoke, customized jobs; therefore, organizations may be forced to maintain a dedicated staff of specialists to keep up with them for anything large-scale.

INTRODUCTION

Today, elastic scaling and distributed computing are the architectural norm.

Existing key management solutions are not well suited for these architectures, because they offer only limited scalability to small numbers of nodes, and limited high-availability and data recovery.

Further, hardware security modules are one of the last computing resources that are not commonly virtualized or securely time-sliced among multiple tenants or VMs. Therefore, their availability in public cloud is limited and even where available, they break the model, requiring upfront fees, usage floors and other aspects that are fundamentally inconsistent with on-demand scaling and pricing. Thus, it's commonly observed that many organizations requiring secure key management struggle to migrate to public clouds on acceptable technology terms that align with the overall promise of the cloud.

RUNTIME ENCRYPTION CAPSULE

Fortanix has created the world's first commercial implementation of a REC using Intel SGX technology.

This enables any application code to run in a hardware-encrypted trusted context created by the Intel® processors—commodity hardware what was previously expensive, proprietary, application-bound hardware security functionality. The application code in REC is isolated from kernel and hypervisor processes. This isolation is enforced by hardware controls provided by Intel SGX.

REC provides runtime and security functionality for execution of the application during its entire lifecycle including provisioning, integration with Intel SGX, runtime attestation, tamper proof guarantees, and communication.

REC ensures that the workload maintains its data confidentiality even when cloud infrastructure is breached or the cloud provider receives a data disclosure request made under the law. Further, the architecture ensures that only the tenant's authorized user shall have access to data. The cloud provider will not have any visibility.

This white paper documents the establishment of a self-service cloud-based Self-Defending Key Management Service (SDKMS) running within a Fortanix REC.

SELF-DEFENDING KEY MANAGEMENT SERVICE

Self-Defending Key Management Service (SDKMS) places a Key Management application service within a Fortanix REC powered by Intel SGX hardware security.

An application running in Fortanix Runtime Encryption Capsule automatically receives security for all communications from SDKMS by transparently encrypting and integrity-checking the system memory, IO accesses, network calls, and other Inter-Process Communications.

SDKMS brings HSM-like security to off-the-shelf Intel datacenter-class computing hardware. Additionally, SDKMS is a true SaaS service, offering on-demand scaling and per-use pricing. Further, consistent with modern software technologies, SDKMS offers capabilities for horizontal scaling, high availability, resiliency, and data recovery.

Built-in load balancing and a REST integration option mean seamless ease of integrating modern enterprise applications with SDKMS.

SDKMS uses SGX crypto protection in Intel® Xeon® CPUs to help protect the customer's keys and data from all external agents, reducing the system complexity greatly by removing reliance on characteristics of the physical boxes. Intel SGX enclaves ensure that Fortanix or any other cloud service provider will have no access to customer's keys or data.

Unlike many hardware security technologies, Intel SGX is architected to help protect generic x86 program code. SDKMS uses Intel SGX not only to help protect the keys and data but also all the application logic for role based access control, account set up, password recovery, etc. The result is significantly improved security for a key management service that offers the elasticity of modern cloud software and the hardware-based security of an HSM appliance, all while drastically reducing initial and ongoing costs.

Fortanix SDKMS is available to enterprises operating in all major public cloud environments and is offered as a SaaS service. It also supports on-premises deployment in private clouds.

CLOUD SECURITY WITH INTEL® SGX

Intel SGX is applicable to any code and data and offers strong isolation against any kind of unwarranted access and modification. Intel SGX enclaves offers security and a trusted environment to provide cryptographic confidentiality and integrity.

Fortanix built SDKMS as the first application to run inside of a Runtime Cryptography Capsule, powered by Intel SGX. This application offers security and a cost-effective key management service to the enterprise cloud ecosystem.

Because Intel SGX is an IA instruction set extension designed for any application, it has much wider applicability. Thus, the Fortanix SDKMS is just one of the many use cases for Intel SGX.

INTEL® SGX OVERVIEW

Intel Software Guard Extensions (Intel SGX), available in 5th generation Intel Xeon processors E3 series, provides protection for the execution environment that significantly reduces the attack surface for applications. Intel SGX offers a set of instructions that applications can use to create a private region of memory that is isolated from all other processes, even those with higher privilege levels. Thus, even if a malware or an insider has access to operating system (OS) root privileges, or if the virtual machine manager (VMM) or BIOS are compromised, the SGX-protected application can still operate with integrity and be able to help protect both its code and data.

ATTACK SURFACE TODAY

Traditionally, x86 architecture follows a hierarchical privilege mode with various software processes operating at different privilege levels. Less privileged software processes have no privacy from processes with more privileges. Figure 1 shows various privilege levels for a typical x86 based system.

Because of this approach, a typical application security depends on the integrity of the OS, VMM, or BIOS levels. According to the NIST vulnerability database, in Q4 2016 alone there were about 30 bugs discovered related to privilege escalation[1]. As these bugs get discovered and

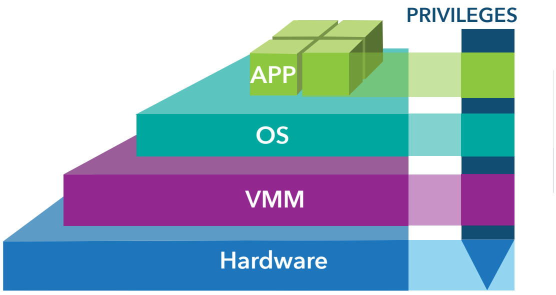


FIGURE 1 – PRIVILEGE LEVELS IN X86 SYSTEMS

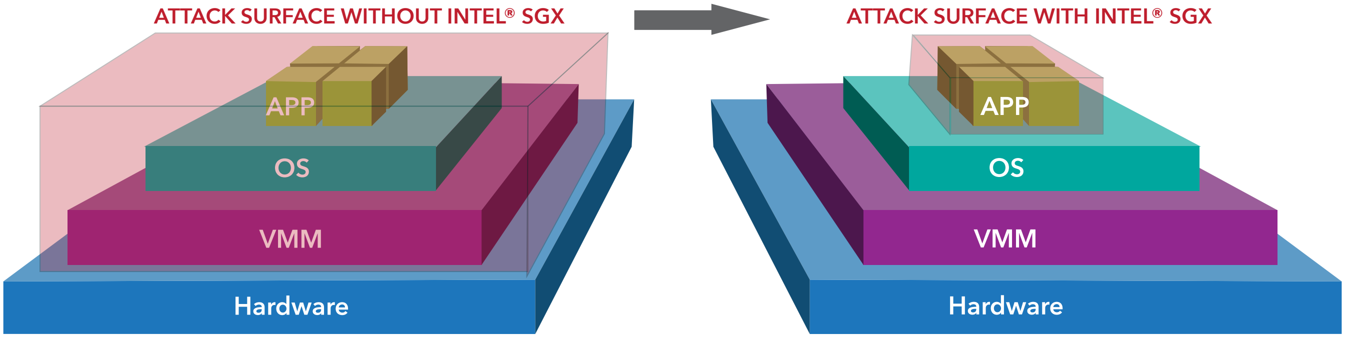

ATTACK SURFACE WITHOUT INTEL® SGX
APP
OS
VMM
Hardware
ATTACK SURFACE WITH INTEL® SGX
APP
OS
VMM
Hardware

FIGURE 2 – REDUCTION OF ATTACK SURFACE WITH INTEL® SGX

patched, IT administrators must find a way to receive, validate, and propagate these patches to live systems, often resulting into a trade-off between business continuity and timely deployment of the security updates.

Moreover, any individual with root credentials for the system can launch a process in kernel mode. A malicious system administrator or a compromised root credential, therefore, can result in severe data breaches even when the system is completely patched with latest fixes. Similarly, there may be multiple latent "zero-day" bugs in the system which are not yet widely discovered. An attacker with knowledge of a zero-day bug can compromise even a completely patched system.

A malicious application running on a server may be able to use a zero-day bug or an unpatched privilege escalation vulnerability to obtain root privilege and then attack other running application. Thus, the attack surface of a conventional application includes all the processes that are running on the same server.

REDUCING ATTACK SURFACE WITH INTEL SGX

Intel SGX enables programmers to create a stand-alone execution environment for applications to run in. An SGX enclave operates with a private region of system memory that is not accessible to any other process, even those running with higher privilege level. Thus, if an application runs inside an SGX enclave, its attack surface is reduced to just itself and excludes all other external processes. Figure 2 shows reduction of the attack surface because of applications running inside the isolated SGX enclave. A typical enterprise application such as MySQL* has about 2.8 million lines of code, while the Linux* kernel by itself has about 17 million lines of code. If one accounts for the VMM and other libraries present on the system, Intel SGX will reduce the attack surface by many orders of magnitude in most cases.

TRANSPARENT MEMORY ENCRYPTION

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

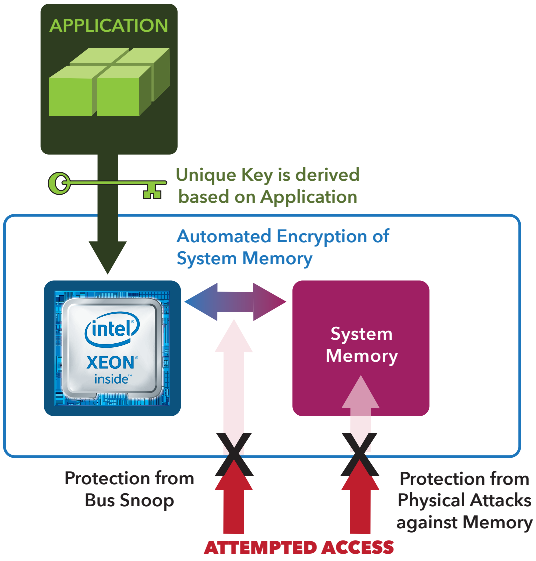

APPLICATION
Unique Key is derived based on Application
Automated Encryption of System Memory
intel XEON inside
System Memory
Protection from Bus Snoop
Protection from Physical Attacks against Memory
ATTEMPTED ACCESS

FIGURE 3 – TRANSPARENT MEMORY ENCRYPTION WITH INTEL® SGX

to access the decrypted memory. Intel SGX also enables greater protection of applications against various powerful attacks including those using memory scraping, ptrace-based tools, and other reverse engineering tools as shown in Figure 3.

REMOTE ATTESTATION

A successful enterprise security mechanism not only protects sensitive applications and data but also provides visibility and control over the assets that are being protected. Intel SGX architecture allows enterprises to measure the applications and associate their cryptographic identities with their deployment. Once Intel SGX protected applications are deployed and running, enterprises can perform a live challenge-response with the applications to ensure they are running as intended. This process of attesting the veracity of remotely-running applications does not require physical proximity with security. It can be done even over untrusted networks and is thus a basis of trust establishment in modern distributed applications running in public or remote clouds.

IMPLEMENTATION OVERVIEW

Fortanix Self-Defending Key Management Service (SDKMS) is a scalable key management service built with Intel CPUs that provides fundamentally more security and resiliency, and that offers pay-per-use pricing for enterprises looking to deploy KMS in the cloud. It uses Intel SGX for protection of sensitive keys from the cloud provider and even Fortanix. An end-to-end key management service and associated sensitive business logic is implemented inside Intel SGX enclaves.

Enterprise administrators can create their primary credential when a business relationship is established with Fortanix. An intuitive portal allows administrators to create multiple security groups and enroll various applications inside these groups. Security groups are isolated from one another and thus an administrator can limit availability of key materials to only the applications that require them. Administrators can add other users and enroll them with an appropriate role such as administrator, team member, or auditor. A secure audit log is maintained for all the privileged actions performed.

Applications can either use standard protocols such as PKCS#11 or KMIP to communicate with SDKMS, or they can use a REST interface for easy integration. In any configuration, the cryptographic capacity of the system is horizontally scalable and completely decoupled from applications.

DESIGN CONSIDERATION

Fortanix Self-Defending Key Management Service is implemented with the following design considerations

- Intel SGX supported systems
- 1GbE and 10GbE networks for optimal scalability

SYSTEM ARCHITECTURE

Figure 4 illustrates the SDKMS scalable architecture. All the nodes in the cluster are identical, built with the system configuration shown in Table 1, and additional nodes can be added to horizontally scale the performance. Using the flexibility offered by x86 architecture, a very robustframework for redundancy and disaster recovery is included.

HARDWARE DESCRIPTION

SYSTEM	PROCESSOR CONFIGURATION	DETAILED CONFIGURATION
N Compute Servers • Ubuntu Linux 16.04 LTS • Intel SGX driver 1.7 • Fortanix REC Software • Fortanix Key Management Software	Intel® Xeon® Processor E3-1585 v5 See processor details at **http://ark.intel.com/products/93742/Intel-Xeon-Processor-E3-1585-v5-8M-Cache-3_50-GHz**	Form Factor: 1U Rack Mount Server Processor: Intel Xeon Processor E3-1230 v5 @3.4GHZ, 1 socket, 4 cores, 8 threads Memory: 64GB DRAM. Storage: 2TB SSD 10Gb Ethernet network

TABLE 1 – HARDWARE CONFIGURATION DETAILS

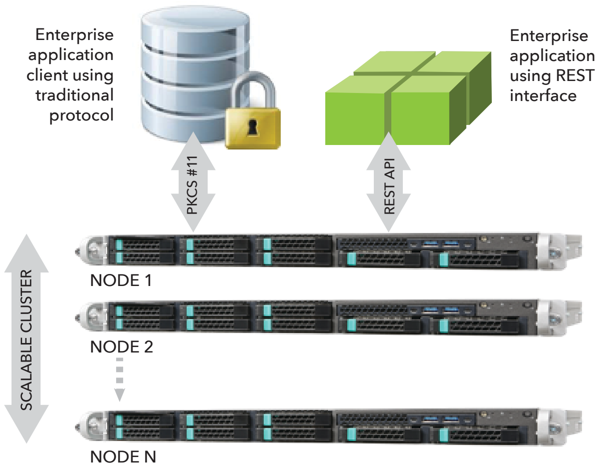

Enterprise application client using traditional protocol
Enterprise application using REST interface
PKCS #11
REST API
SCALABLE CLUSTER
NODE 1
NODE 2
NODE N

FIGURE 4 – KEY MANAGEMENT WITH SCALABLE CLUSTER OF INTEL® SGX SERVERS

As demand increases, businesses can continue adding new machines to the cluster for true horizontal scaling. Each node has access to the entire key space and can be removed for maintenance or hardware upkeep without impacting the operational behavior of the SDKMS.

SDKMS FUNCTIONALITY

The Self-Defending Key Management Service is designed to enable businesses to serve key management needs for all their applications, whether they are operating in public, private, or hybrid cloud.

CRYPTOGRAPHIC OPERATIONS

SDKMS offers a complete implementation of PKCS#11 and KMIP 1.1 protocols. All cryptographic operations including key generation, management, use, and revocation are performed only inside Intel SGX enclave. Intel SGX provides cryptographic protection from any host software.

While PKCS#11 and KMIP are standard interfaces for existing applications, modern cloud applications prefer RESTful interfaces. Unavailability of RESTful interfaces results into increasing complexity at the client side and constant struggle for businesses to cope with their increasing demand. Therefore, SDKMS offers a true REST interface for easy integration with clients and removes much of operational complexities associated with legacy protocols.

ROLE-BASED ACCESS CONTROL

SDKMS supports multiple user roles including regular user, auditor, administrator, etc. All sensitive operations such as enrolling applications, key generation or usage require authentication with SDKMS. Since all access controls are enforced within an Intel SGX enclave, Fortanix or any cloud provider has no access to any of the key material. Similarly, all IT administrators, even with root access to the servers, will not have access to SDKMS unless authorized by SDKMS administrator! This is one of the remarkable security properties of Intel SGX: even physical access to the machine or root privileges cannot be abused to access the sensitive assets.

A secure audit log is maintained for all accesses to SDKMS. Thus, SDKMS administrator and auditors can scrutinize all the users and applications that accessed the SDKMS. A trusted distributed ledger ensures that the audit log cannot be tampered or disabled.

TRUSTED AUTO SCALING

Keeping up with business demands, administrators can keep adding new hardware servers to SDKMS to increase throughput. Using SGX attestation functionality, SDKMS automatically verifies that nodes are operating with the right security posture before enrolling them into the trusted pool of servers.

LIFECYCLE MANAGEMENT

SDKMS provides a robust platform for managing the lifecycle for private cloud solution. Selected SDKMS nodes can be taken offline for maintenance, hardware upgrade or repair, and software update without affecting the overall availability of the system. SDKMS supports security for backup and restore, where the backed-up data remains accessible only to authorized SDKMS nodes without relying on any external, and often vulnerable, manual policy controls.

EASY HARDWARE MAINTENANCE

Each node in SDKMS has visibility into all the key materials, and also has cryptographic knowledge of Role Based Access Control. This enables system administrators to remove any server node from an existing live cluster without affecting the availability of SDKMS. The removed node can be updated or replaced and then added back to the SDKMS cluster with just a few clicks.

COST EFFECTIVENESS

Intel SGX provides the cryptographic isolation that has in the past required expensive appliances. The entire SDKMS operates on Intel® Xeon processor based CPUs without requiring any dedicated cryptographic accelerators. This enables enterprises to deploy HSM-grade security while paying economical per-use SaaS cloud pricing or employing widely available servers in an on-premises deployment.

FORTANIX SDKMS SAAS CLOUD

Fortanix offers SDKMS as SaaS for the customers who want a self-service security for key management system without maintaining hardware systems. The service is as secure as on-premises operations, and offers businesses a per-use pricing and on-demand scaling benefits of cloud SaaS.

Security Attributes

Fortanix SDKMS has attractive security attributes for even the most security-conscious customers:

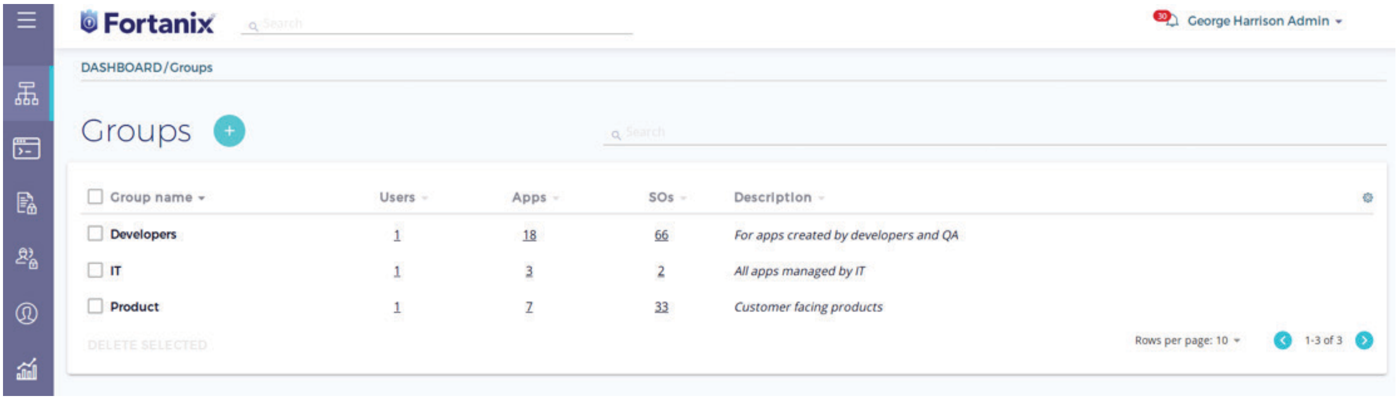
- Confidentiality of all the key material, audit log, data assets is assured independent of the overall security of the infrastructure
- Only the authorized users of the customer have access to its data. All the customer's data is cryptographically shielded from Fortanix

Thus, while many cloud providers use procedural controls, Fortanix uses Intel SGX to keep itself outside the trust boundary. Therefore, Fortanix is able to provide a much higher assurance level – cryptographic protection – for the privacy of customer's data.

FORTANIX SDKMS PRIVATE CLOUD SOLUTION

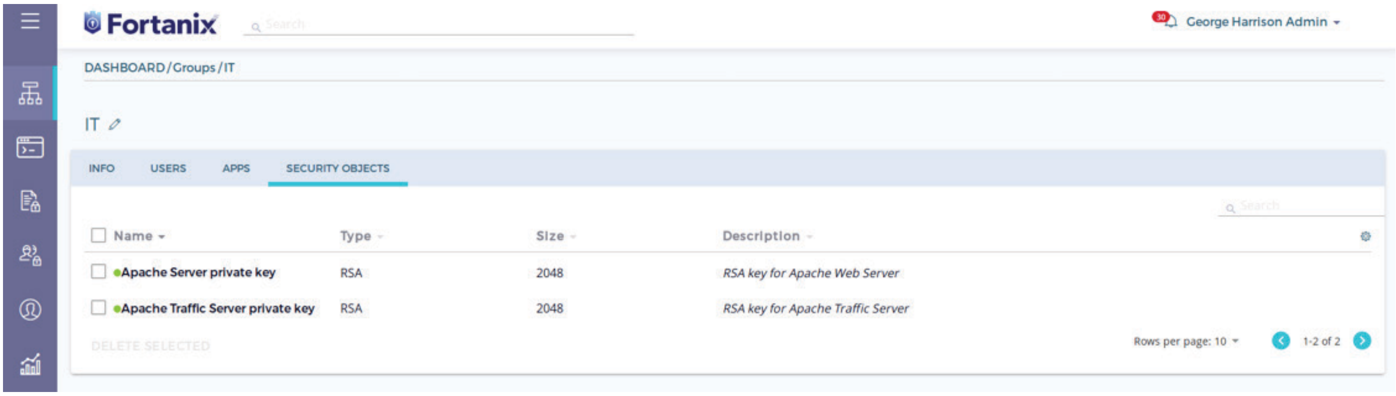
Fortanix SDKMS is installed and configured to use in the following 3 easy steps:

1. **Installation:** SDKMS can be installed as a distributed cluster on nodes running a modern Linux distribution. After installing the first node in the cluster, new nodes are added only after they have been attested by the Intel Attestation Service confirming that they are running the right version of the SDKMS software on Intel SGX hardware. A single IP address is configured to be used as a gateway to the SDKMS service.
2. **Configuration:** Once SDKMS has been installed, an administrator can configure the user account. SDKMS provides integration with customer's SSO, and supports role based access control. An administrator can configure sharing of security objects and keys by creating groups of users and applications, and configure policies for access control.
3. **Usage:** SDKMS users can add applications to the system which can use the key management service using the REST API or the PKCS#11 interface. Every application that is added to the system is provided with an API key to access the system and request for key management and cryptographic operations. Figure 5 shows how new groups are added while Figure 6 shows all the security objects in a group.
4. **Monitoring and Troubleshooting:** SDKMS provides a rich interface to monitor usage, alerts, and various statistics related to the system. See Figure 7 for typical dashboard. A system administrator can use this interface to quickly identify problems and reconfigure the system if needed.



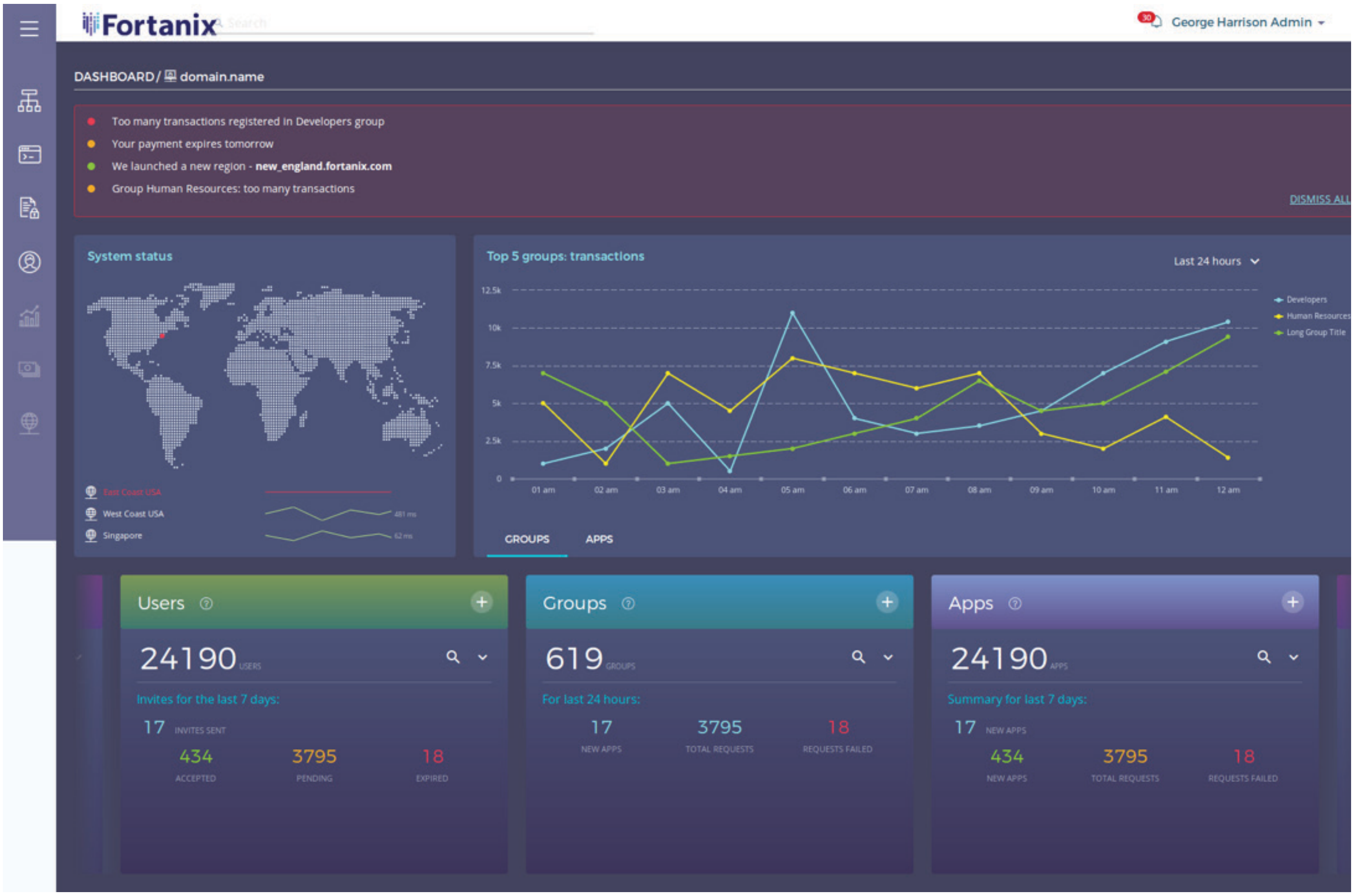
□ Group name	Users	Apps	SOs	Description
□ Developers	1	18	66	*For apps created by developers and QA*
□ IT	1	3	2	*All apps managed by IT*
□ Product	1	7	33	*Customer facing products*

FIGURE 5 – ADDING NEW GROUPS IN SDKMS



Name	Type	Size	Description
Apache Server private key	RSA	2048	*RSA key for Apache Web Server*
Apache Traffic Server private key	RSA	2048	*RSA key for Apache Traffic Server*

FIGURE 6 – SDKMS SECURITY OBJECTS



- Too many transactions registered in Developers group
- Your payment expires tomorrow
- We launched a new region - **new_england.fortanix.com**
- Group Human Resources: too many transactions

Users

24190 USERS

Invites for the last 7 days:

17 INVITES SENT

434 ACCEPTED · 3795 PENDING · 18 EXPIRED

Groups

619 GROUPS

For last 24 hours:

17 NEW APPS · 3795 TOTAL REQUESTS · 18 REQUESTS FAILED

Apps

24190 APPS

Summary for last 7 days:

17 NEW APPS

434 NEW APPS · 3795 TOTAL REQUESTS · 18 REQUESTS FAILED

FIGURE 7 – SDKMS DASHBOARD

SUMMARY

Intel SGX enables new security architectures in x86 computation. Its use allows applications to provide data confidentiality and execution integrity even in the presence of a malicious root user, compromised operating system, and other advanced threats. Fortanix Self-Defending Key Management Service is the first commercially available key management service built entirely using Intel SGX based servers without any cryptographic accelerators.

Fortanix SDKMS is available to enterprises as on-premises software and allows a rapid deployment with RESTful APIs in addition to legacy protocols such as PKCS#11. Fortanix SDKMS offers enterprises HSM-grade security with pay per-use pricing that offers true horizontal scaling and strong access control and audit visibility.

SDKMS is just one of the early use cases possible with the powerful security properties of Intel SGX. Fortanix and Intel will continue working on bringing even more powerful enterprise security products using Intel SGX.

You may try Fortanix SDKMS today or learn more at www.fortanix.com.

LINKS

Read more about Fortanix

http://www.fortanix.com/assets/SGXwhitepaper

Discover more about Intel® SGX

https://software.intel.com/en-us/sgx

0-day bugs

https://web.nvd.nist.gov/view/vuln/search-results?query=privilege+escalation+&search_type=last3months&cves=on

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at **https://software.intel.com/en-us/sgx**

Intel, the Intel logo, Xeon and Phi are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others.