Secured
Cloud Applications

Security Guide

TRUSTED CLOUD
FABRIC

SafeNet

SafeNet

TRUSTED CLOUD FABRIC

Secured Cloud Applications

SECURITY GUIDE

Benefits:

- **Highly Flexible:** Enables encrypting cloud data in nearly any cloud environment
- **Strong Trust Anchor:** Delivers digital-signing quality trust with FIPS 140-2 level security
- **Highly Agile:** Centralized secure management works across multiple cloud deployments
- **Minimized Costs:** Standards-based interfaces, multiple deployment options, and centralization reduce costs

Introduction: The Promise and Hazards of Moving Applications to the Cloud

For many organizations, the unlimited capacity, ubiquitous accessibility, and near-instant elasticity of cloud-based applications offers tremendous advantages. For example, a retailer who must accommodate the traffic when 70% of their revenue in a single four-week holiday period can use cloud bursting, typically through infrastructure as a service (IaaS), as a cost-effective way to add capacity only during peak periods. Businesses can dramatically scale back the cost and effort to maintain internal processing capacity, while leveraging a pay-as-you-go subscription model.

Yet for all of the possibilities afforded by the cloud, security can present a host of troubling challenges— particularly when these applications interact with critical customer data that must remain secure. How can you secure customer data when the application is in a multi-tenant environment? How do you maintain regulatory and digital signing-level trust in your cloud-based application? And how can this data remain isolated from the cloud provider who has administrative access to the entire infrastructure?

To leverage the strategic benefits of the cloud, organizations need robust and sophisticated security capabilities for guarding against these risks.

SafeNet Solutions for Securing Virtual Applications

SafeNet offers a range of solutions that enable organizations to leverage the business benefits of cloud services, without making any compromises in security. SafeNet solutions offer the right mix of capabilities to allow customers to deploy them in hybrid traditional and cloud-based deployments, and when utilizing multiple cloud providers.

SafeNet offers two solutions for securing virtual applications:

- DataSecure
- Luna SA Hardware Security Modules (HSMs)

DataSecure Specifications

Encryption

- AES, 3DES, DES, RSA (signatures and encryption), RC4, HMAC, SHA-I – SHA512, SEED
- Asymmetric key sizes: 512, 1024, 2048
- Symmetric key sizes: 40, 56, 128, 168, 192, 256

Web and application servers supported

- Oracle, IBM, BEA, IIS, Apache, Sun ONE, JBoss, and more

Databases supporte

- Oracle, Microsoft SQL Server, IBM DB2,Teradata

DataSecure 400 Series

- 100,000+ encryptions/second, less than 100 microseconds latency
- 1U, rack mountable (H: 1.7"; W: 19"; D: 30")

DataSecure 100 Series

- 11,000+ encryptions/second, 250 microseconds latency
- 1U, rack mountable (H: 1.7"; W: 19"; D: 13")

Luna SA Specifications

Encryption

Full Suite B support

- Asymmetric Key with Diffi e-Hellman (1024-4096 bit), RSA (1024-8192 bit) & (PKCS#1 v1.5, OAEP PKCS#1 v2.0), Digital Signing via RSA (1024-8192 bit), DSA (1024 & 2048 bit), (PKCS#1 v1.5) & Symmetric Keys through 3DES (double & triple key lengths), AES, RC2, RC4, RC5, CAST-128. Message Digest is SHA-1, SHA-224, SHA-256, SHA-384 & SHA-512, MD-5 & MAC are HMAC-MD5, HMAC SHA-1, SSL3-MD5-MAC, SSL3- SHA-1-MAC, Elliptic Curve Cryptography (ECC), Korean Algorithms. ECC Brainpool Curves (named & user-defined)

Cryptographic APIs

- PKCS#11, Microsoft CAPI and CNG, JCA/JCE, OpenSSL

Physical Characteristics

Connectivity

- 2x 10/100/1000 Ethernet, CAT5, UTP
- Up to 800 simultaneous NTLS connections
- Luna PED authentication port
- Local serial console port
- Luna Token PC Card reader and/or G5 connection via USB

Dimensions

- 1U rack mount chassis
- 19.0" x 21" x 1.725"

DataSecure for Securing Application Data

DataSecure is an appliance-based platform that offers data encryption and granular access control capabilities that can be applied to virtualized and non-virtualized applications, databases, mainframe environments, and individual files. DataSecure offers:

- Flexible integration with multiple options for integration into databases and/or applications
- Granular encryption options to secure data in your application, with separation of duties to isolate data from application or cloud infrastructure owners
- Highly scalable solution, with enterprise-controlled or performance-optimized cloud-cached keys, and load balancing with geographic redundancy options

Luna SA for Anchoring Trust in the Cloud

The Luna SA 5.0 HSM is the choice for enterprises requiring strong cryptographic security for paper-to-digital initiatives, digital signatures, DNSSEC, hardware key storage, transactional acceleration, certificate signing, code or document signing, bulk key generation, data encryption, and more.

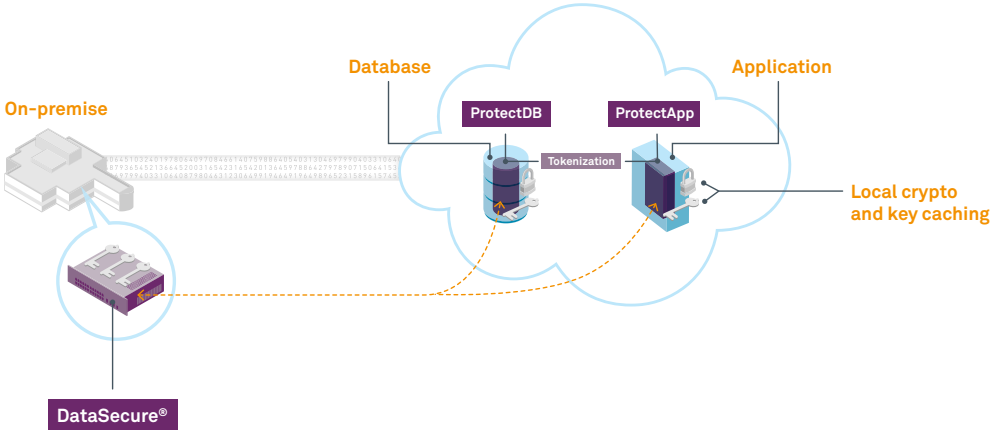
- Trusted security by securing keys in FIPS- and Common Criteria-certified hardware— keys never leave the confines of the hardware appliance
- HSM partitioning delivers significant cost savings— a single HSM can split into a maximum of 20 virtualized HSMs, each with their own access controls and independent key storage

DataSecure Deployment Scenario

When deploying DataSecure, organizations retain full control over cryptography, key management, and policies—all administered through a centralized DataSecure appliance. The following specialized platforms can be deployed in the cloud and managed under DataSecure:

- ProtectDB, which is used to protect cloud-based databases
- ProtectApp, which secures cloud-based applications
- Tokenization Manager, which replaces sensitive data stored in the cloud with tokens

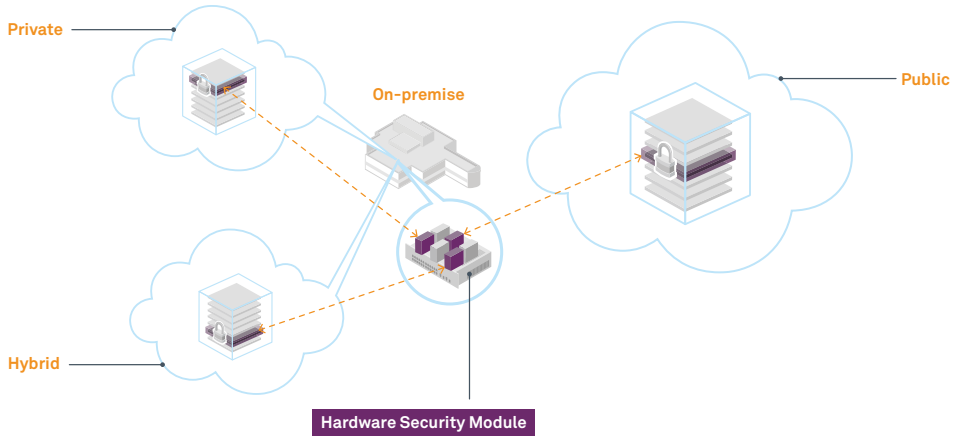
Depending on an organization's business and security needs, one or more of these solutions can be rolled out to the cloud, and centrally governed by the local DataSecure appliance. When requests to decrypt or encrypt sensitive data are submitted to cloud-based applications, they are processed and logged according to the policies configured within DataSecure.



Luna SA Deployment Scenario

With Luna SA HSMs, organizations can move their applications to the cloud while keeping their root-of-trust controlled and secure within the confines of their on-premise HSM. In this approach, keys, cryptography, and policies are all managed within the on-premise HSM. Because both the HSM and the cloud-based resources operate within the same virtual private network, essentially creating a virtual private cloud, organizations encounter minimal interruption due to corporate firewalls, and the like.

The Luna SA's partitioning capabilities can be set for each partition, which can be aligned with a specific application server, and/or specific application or group. This ability enables customers to manage cryptographic keys for the traditional datacenter and external cloud providers in the same platform.



Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected