gemalto
security to be free

Secure the AWS Cloud with SafeNet Solutions eBook

GEMALTO.COM

Table of Contents

Value of the public cloud

Cloud computing is transforming the way enterprises, government agencies, and small businesses manage their company data. Elastic, public cloud services are enabling agile, cost-effective methods to run business-critical applications and store information. And, while some enterprises aren't yet ready to let go of the traditional on-premises data center, they are exploring and evaluating all of the available options in the exciting, new cloud frontier.

While every cloud provider offers a different set of benefits to customers, Amazon Web Services (AWS) is recognized as a leader in cloud infrastructure services by Gartner, the premier information technology research and advisory firm. AWS has over 10 times the compute capacity of its fourteen nearest competitors[1] and its AWS Marketplace gives customers a web-based front-end to purchase and deploy cloud-based infrastructure—as well as hundreds of related applications—from both AWS and its partners, such as Gemalto.

> Amazon Web Services is recognized as a leader in cloud infrastructure services.

1 Source: Gartner, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, August 3, 2016. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Securing sensitive data in the cloud

While cloud environments offer customers increased flexibility and availability as well as decreased costs, data owners must be able to demonstrate compliance and illustrate control of sensitive information in the cloud. As data owners, organizations often are required to prove that they can meet compliance requirements and keep safe sensitive data stored in cloud environments such as credit card numbers, health records, or other personally identifiable information. The question is: how?

> Organizations are challenged to prove that they can meet compliance requirements and keep the sensitive data stored in cloud environments safe.

Don't just play it safe—keep it safe

While many data owners recognize the need to encrypt their data so that it is unreadable to hackers, they may not be aware that there are encryption features, options, and add-ons that offer different levels of protection. This makes understanding the security scenario—specifically the ownership, management of, and access to encryption keys and how it affects data security—a critical consideration for every enterprise who entrusts its company data to the cloud.

The AWS shared responsibility model

Information security is of paramount importance to AWS customers. Security is a core functional requirement that protects mission-critical information from accidental or deliberate theft, leakage, integrity compromise, and deletion. Under the AWS shared responsibility model, AWS provides a global secure infrastructure and foundation for compute, storage, networking, and database services as well as higher level services.

AWS provides a range of security services and features that AWS customers can use to secure their assets. AWS customers are responsible for protecting the confidentiality, integrity, and availability of their data in the cloud, and for meeting specific business requirements for information protection.

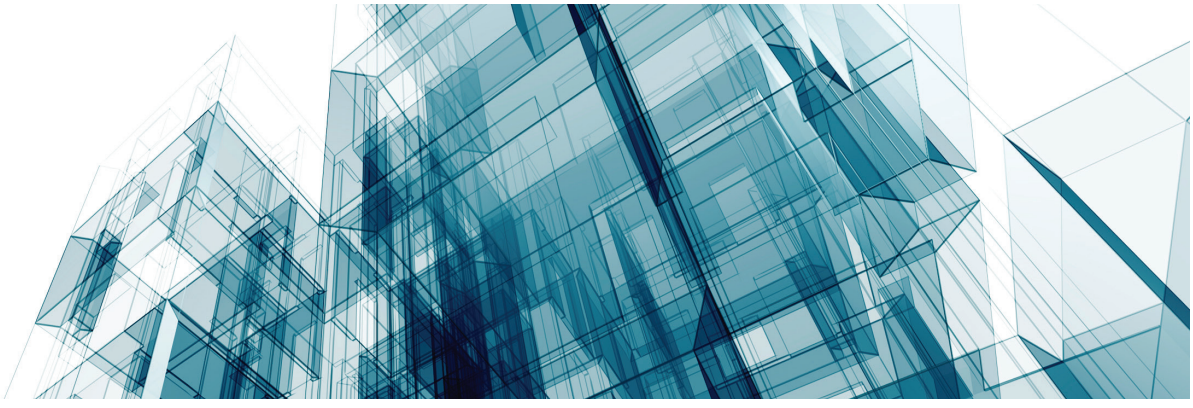
Options for securing assets in the AWS Cloud are available for customers from both AWS and Gemalto. As an Advanced Technology Partner, Gemalto provides security solutions with leading-edge protection to safeguard data stored in the AWS Cloud.

Data security in the AWS Cloud environment

In order to support client compliance objectives, AWS offers services that are aligned with security best practices, appropriate security features within those services, and documents that explain how to use those features. The AWS compliance framework covers FISMA Low and Moderate, PCI DSS Level 1, ISO 27001, SOC 1/SSAE16, and HIPAA. The AWS infrastructure features both **physical** and **logical** security measures.

- **Physical security.** AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass through a minimum of two checkpoints that each require two-factor authentication in order to access data center floors. All visitors and contractors are required to present identification, sign-in, and be escorted and chaperoned by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

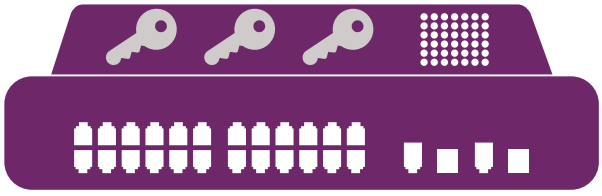
- **Logical security.** This includes such capabilities as disk wiping for both Amazon EBS and instance ephemeral volumes, instance isolation in Amazon EC2 environments, and identity and access management for access to the AWS Console and APIs.



The role of encryption and key management

As data owners, customers alone are responsible for protecting the confidentiality, integrity, and availability of their data in the cloud as well as ensuring that it meets the specific compliance requirements for information protection. Making sure that this data is safe from unauthorized access requires enterprises to consider not only the physical and logical security of the cloud service provider but also **who** is encrypting the data; **when** and **where** the data is being encrypted; and **who** is creating, managing, and accessing the encryption keys.

> Making sure that this data is safe from unauthorized access requires enterprises to consider more than the physical and logical security of the cloud service provider.



Not all encryption is created equal

While encryption often is referred to as the cornerstone of data center security, not all encryption is created equal. For business leaders and IT administrators, understanding the encryption process as it relates to the ownership of and access to company data is crucial to securing it in the cloud. Making sure that encryption and key management—deployed with strong policy-based access controls—are customer controlled is what makes encryption a core safety mechanism for protecting data in the cloud.

The entire SafeNet data protection portfolio deploys with SafeNet KeySecure or SafeNet Virtual KeySecure to keep encryption key ownership firmly in control of the customer and not with the cloud provider. Instead of a "one size fits all" solution, Gemalto offers a portfolio of tools to ensure that customers have the right solution for the challenge they face.

AWS and Gemalto Encryption Options for Amazon EC2

	TYPE OF ENCRYPTION	DEFINITION	NOTES	MEETS SECURITY REQUIREMENTS?	ARE YOU STILL AT RISK?
Amazon EBS Server-Side Encryption	Cloud Service Provider (CSP) Encryption with CSP-Managed Keys.	Encryption performed by the CSP using encryption keys owned and managed by the CSP.	Also known as server-side encryption (SSE); the CSP is doing both the encryption and the key management. It's often free or cheap.	No. Customer does not own or control keys or data.	Yes: to rogue administrators, CSP misconfigurations, subpoenas, SSL attacks, and access vulnerabilities.
Amazon EBS Encryption with AWS Key Management Service (KMS)	CSP Encryption with Customer-Managed Keys.	Encryption performed by the CSP using encryption keys managed by the customer, but owned by the CSP.	The customer must manage all encryption keys. These keys are often limited for use only within the CSP environment.	No. Customer does not own keys or data.	Yes: to CSP misconfigurations and subpoenas.
SafeNet ProtectV with SafeNet KeySecure/ Virtual KeySecure (and optional AWS CloudHSM)	Customer-Owned Encryption with Customer-Owned Keys.	Encryption performed by the customer using encryption keys owned and managed by the customer.	Also known as client-side encryption; the customer can prove ownership of the encryption keys and data–at all times.	Yes. Customer can prove ownership and control of data—at all times.	Unlikely
SafeNet KeySecure/Virtual KeySecure	Customer-owned keys for the following portfolio of customer controlled encryption solutions.	Customer owns and manages their encryption keys either from the cloud or from an on-premises appliance.	Customer can prove ownership of their encryption keys and data at all times.	Yes. Customer can prove ownership and control of data—at all times.	Unlikely
SafeNet ProtectV	Customer controlled virtual machine encryption.	Customer controlled full-disk encryption of virtual machine instances.	Also known as client-side encryption; the customer can prove data ownership at all times.	Yes. Customer can prove ownership and control of data—at all times.	Unlikely
SafeNet ProtectFile	Customer controlled file system-level encryption.	Customer controlled client based encryption of files, folders and network shares.	Also known as client-side encryption; the customer can prove data ownership at all times.	Yes. Customer can prove ownership and control of data—at all times.	Unlikely
SafeNet ProtectApp	Customer controlled application-level encryption with customer owned keys.	Customer controlled API based encryption built directly into applications.	Also known as client-side encryption; the customer can prove data ownership at all times.	Yes. Customer can prove ownership and control of data—at all times.	Unlikely
SafeNet ProtectDB	Customer controlled column-level database encryption.	Customer controlled client based encryption of defined columns in Oracle, IBM DB2 and Microsoft SQL databases.	Also known as client-side encryption; the customer can prove data ownership at all times.	Yes. Customer can prove ownership and control of data—at all times.	Unlikely

Encryption and regulatory compliance

Recognized universally by analysts and experts as an underlying control for cloud data, customer-owned encryption is fundamental to demonstrating regulatory compliance. Experts often recommend encrypting sensitive data and deploying customer-owned key management[2] to

- isolate regulated and sensitive information and
- separate encryption control and ownership from the cloud provider.
- remove systems from audit scope
- ensure data deletion on retired virtual servers

By doing so, organizations can demonstrate compliance and pass audits and, most importantly, protect sensitive data from specific attacks.

2 Recommending organizations include the National Institute of Standards and Technology (Source: NIST, Guide to Storage Encryption Technologies for End User Devices, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf) and Gartner (Source: Gartner, Simplify Operations and Compliance in the Cloud by Protecting Sensitive Data, June 2, 2015). Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Storing data safely in the cloud with customer-owned encryption

There are many business benefits of cloud storage such as significant cost savings, accelerated innovation, enhanced agility, and more. Still, many companies hesitate to bring compliance-regulated or business-sensitive data to the cloud—especially when stealing a virtual machine can be as simple as copying a file. This lack of trust in the cloud is what's preventing customers from gaining the economic and time-to-market advantage that cloud computing has to offer. What can be done to solve this problem? The answer is adding customer-managed encryption and key management to protect data stored in the cloud.

Securing data properly requires that you own—and can prove that you own—your data, from inception to deletion. That means that you—not your cloud provider—must own your encryption and encryption keys. When customer-owned encryption and encryption keys are implemented correctly, your organization not only will be able to secure all of your company assets in the cloud (including data from interactions with customers, vendors, prospects, partners, and more) but also will be able to meet many compliance mandates and security regulations.

Three Rules for Encrypting Data Stored in the Cloud

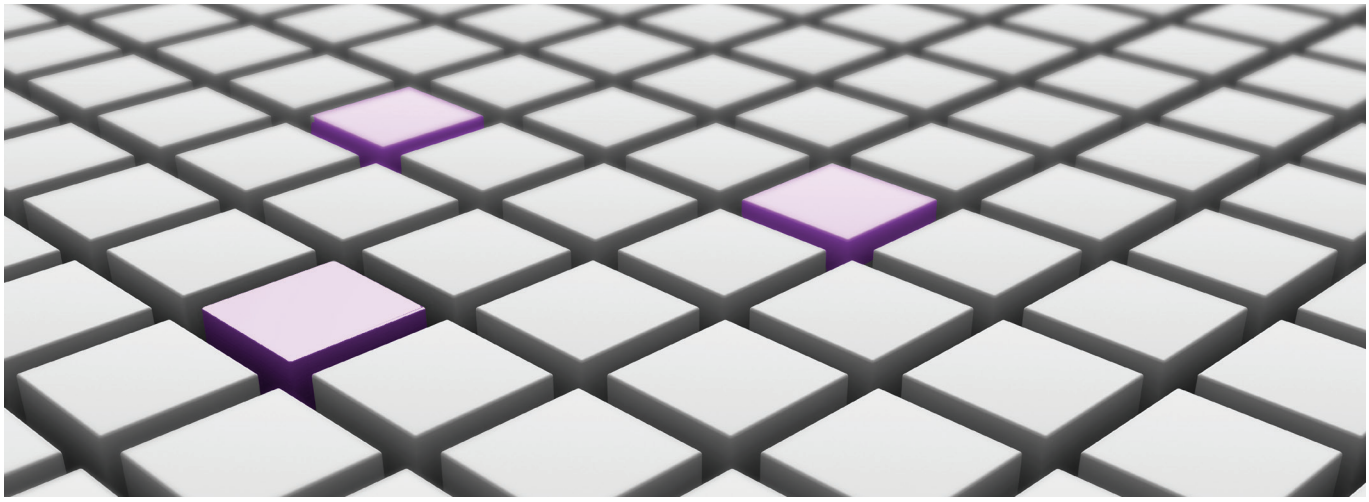
1. Own your encryption so that you—not your cloud provider—can address any and all access requests for the surrender of your company's cloud data.

2. Own and manage the encryption key lifecycle to ensure that your cloud data is always secure.

3. Define and control data access permissions for company personnel, partners, vendors, customers, etc. to prevent unauthorized access to your cloud data.

The importance of secure key management

Key management presents significant challenges for enterprises. Security requirements around key storage, rotation, and deletion can add to administrative overhead and costs. Additionally, keys often are stored and managed insecurely; for example, some organizations store their keys in spreadsheets and on USB drives, in LDAP, or even as flat files on an operating system. Dynamic, virtualized environments only complicate these challenges.



To improve security and administrative efficiency, organizations need centralized key management solutions that offer the highest level of security and streamline activities such as key rotation and deletion. Keys that are customer-owned and managed offer this protection. Organizations should look to work with solutions that adhere to NIST 800-57 key management guidelines and support the OASIS Key Management Interoperability Protocol (KMIP). These standards offer flexibility and broad interoperability; enabling organizations to centralize the management of cryptographic keys across disparate encryption deployments and yielding benefits in security, administrative efficiency, and compliance.

Another key management best practice is to secure a root of trust to store keys. For some applications, hardened virtual security appliances provide an acceptable level of assurance. For applications and data that are subject to rigorous contractual or regulatory requirements, additional protection often is necessary. Cryptographic keys can be securely generated, stored, and managed in the cloud so that they are accessible only by the organization and never by the cloud provider.

Amazon and Gemalto Key Management Options in AWS

	Who controls access to key?	FIPS 140-2 validation	Integration with AWS services	Integration outside AWS
AWS Key Management System (KMS)	AWS	No	Amazon S3, Amazon EBS, RedShift, custom applications	Custom applications with keys stored in AWS
SafeNet Virtual KeySecure in AWS Marketplace	Customer	Level 1	Amazon EC2 Instances and EBS Volumes with SafeNet ProtectV, S3 with SafeNet ProtectApp, Gemalto's key management partner ecosystem https://safenet.gemalto.com/partners/technology-partner-search/ KMIP-based endpoints, Custom Applications	Yes! Hybrid deployment with Virtual KeySecure for VMware scenarios and open standards (e.g., KMIP)
AWS CloudHSM	Customer (in AWS, on an HSM that the customer controls)	Level 2	Redshift, Custom Applications, Gemalto SafeNet HSM partner ecosystem https://safenet.gemalto.com/partners/technology-partner-search/	Hybrid deployments with customer premises SafeNet HSMs

Number of Keys	10	500	1,000	25,000
AWS Key Management Service (KMS)	$120/yr*	$6,000/yr*	$12,000/yr*	$300,000/yr*
SafeNet Virtual KeySecure in AWS Marketplace	$5,462/yr**	$5,462/yr**	$5,462/yr**	$5,462/yr**
AWS CloudHSM (256-bit AES keys)	$21,481/yr***	$21,481/yr***	$21,481/yr***	$42,962/yr***

*Approximate cost. Usage costs are not included.
**Approximate cost based on annual pricing with reserved instance per SafeNet KeySecure instance.
***Approximate cost per CloudHSM instance.

SafeNet Solutions to Secure the AWS Cloud

Learn how SafeNet solutions by Gemalto protect sensitive data in the AWS platform

What are roots of trust?

Roots of trust, as defined by the Cryptographic Technology Group at the U.S. National Institute of Standards and Technology (NIST)[3], are components that are inherently trusted to perform one or more security-critical functions. Three examples are: protecting cryptographic keys, performing device authentication, and verifying software.

These components must be secure by design and, according to NIST, are ideally implemented in or protected by tamper-resistant **hardware**.

In the public cloud, there is a very real challenge to implementing hardware-based roots of trust when the cloud is so dependent on the virtualization and functionality that is often completely defined by software. Gemalto and AWS have worked together to address the problem in several important ways.

> Roots of trust must be secure by design and implemented in hardware.

3 For more information, visit
http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_mobility-roots-of-trust_regenscheid.pdf

AWS CloudHSM

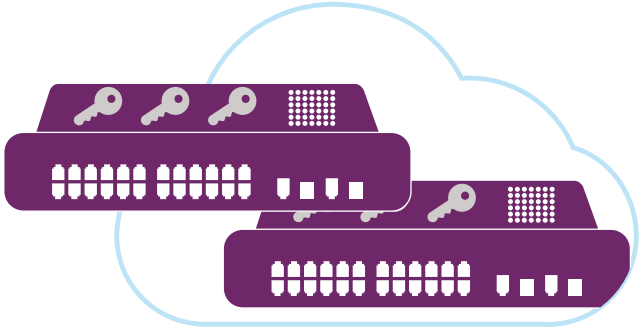
AWS CloudHSM uses SafeNet HSMs from Gemalto to provide a "rentable" hardware security module (HSM) service that dedicates a single-tenant appliance located in the AWS cloud for customer cryptographic storage and processing needs.

AWS CloudHSMs provide a secure foundation for cryptography in the cloud because the keys never leave the intrusion-resistant, tamper-evident appliance. Since all cryptographic operations occur within the HSM, strong access controls prevent unauthorized users from accessing sensitive cryptographic material. AWS CloudHSMs can be deployed in a high-availability configuration across multiple Availability-Zones (AZs) and regions to improve availability and performance.

> With AWS CloudHSM, customers can securely generate, store, and manage cryptographic keys.

AWS CloudHSM can be used for:

- Code signing for code written and stored in AWS
- A root of trust for Certificate Authorities stored in AWS
- Securing access to proxy layer keys for AWS-based databases



For product details and pricing, visit the AWS CLOUDHSM page http://amzn.to/1ipyUdC

Hybrid models and backup options for AWS CloudHSM

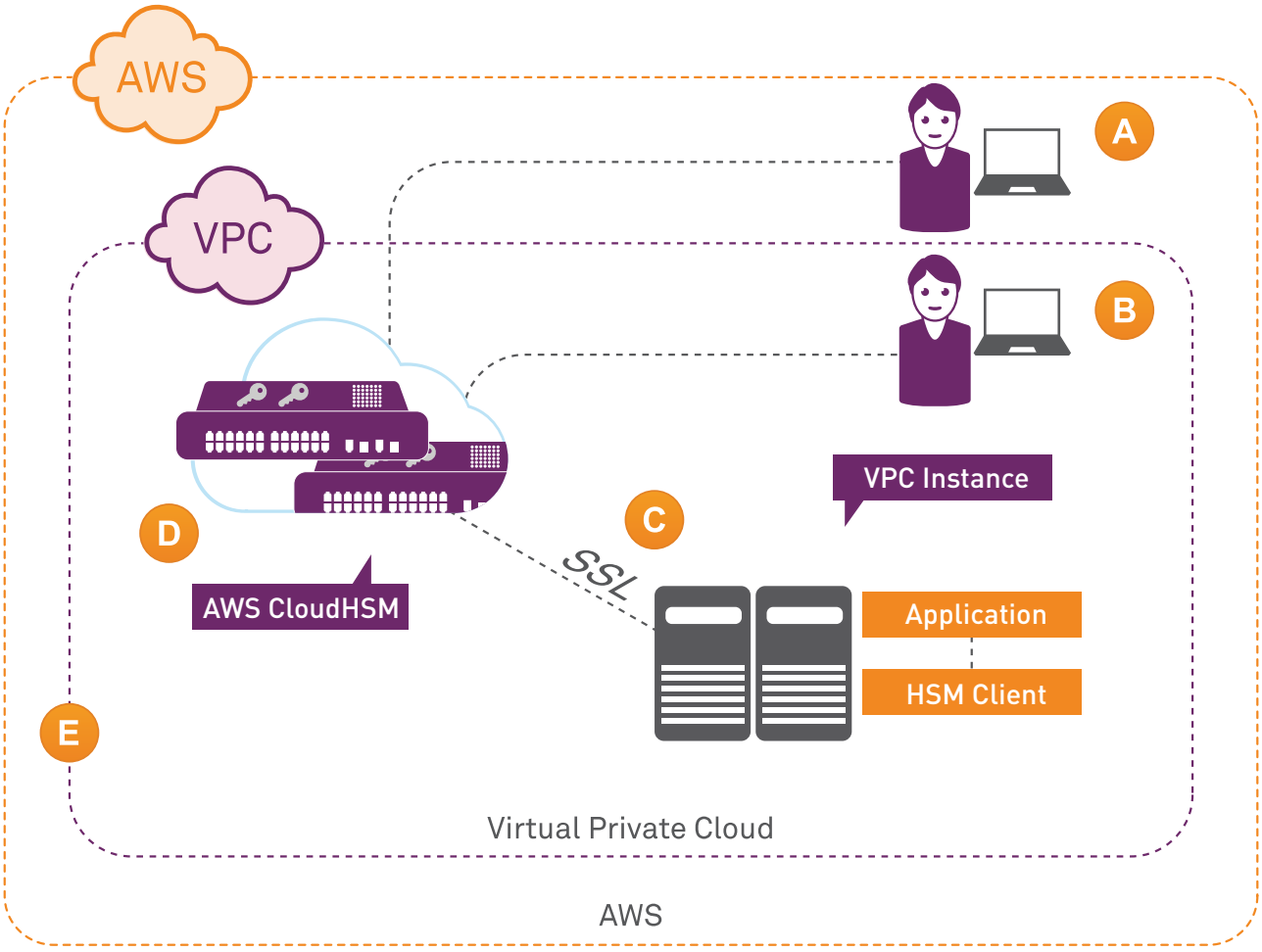
Because AWS does not have access to customer keys stored in AWS CloudHSM, customers are strongly encouraged to back up their keys[4] with an additional appliance. As an option, customers can back up the contents of up to 20 AWS CloudHSM partitions to a backup SafeNet HSM located on their own premises. With the backup SafeNet HSM, customers can unplug and lock away the compact USB-connected appliance once their keys are saved. In the event of a failure or network outage, customers can easily restore their keys from the backup SafeNet HSM appliance.

Hybrid implementations that combine AWS CloudHSMs and on-premises SafeNet HSMs offer significant elasticity for cryptographic operations, such as certificate validation and signing, document signing, and transaction processing. Organizations that do not normally perform a large number of cryptographic operations on-site can use AWS CloudHSMs during periods of increased activity to meet their business needs without making unnecessarily expensive capital investments. The hybrid approach to cryptographic management is an easy, cost-effective solution to these occasional bursts in activity.

> In the event of failure of the AWS CloudHSM, customers can easily restore their keys from a backup SafeNet HSM appliance.

4 For more information, see "Can I back up the contents of a CloudHSM?" at http://aws.amazon.com/cloudhsm/faqs/

AWS CloudHSM



- **A** Although AWS manages the AWS CloudHSM appliance, they do not have access to your encryption keys
- **B** You control and manage your own keys
- **C** Application performance improves (due to close proximity with AWS workloads)
- **D** Secure key storage in tamper-resistant hardware available in multiple regions and AZs
- **E** AWS CloudHSMs are in your VPC and isolated from other AWS networks

Professional services

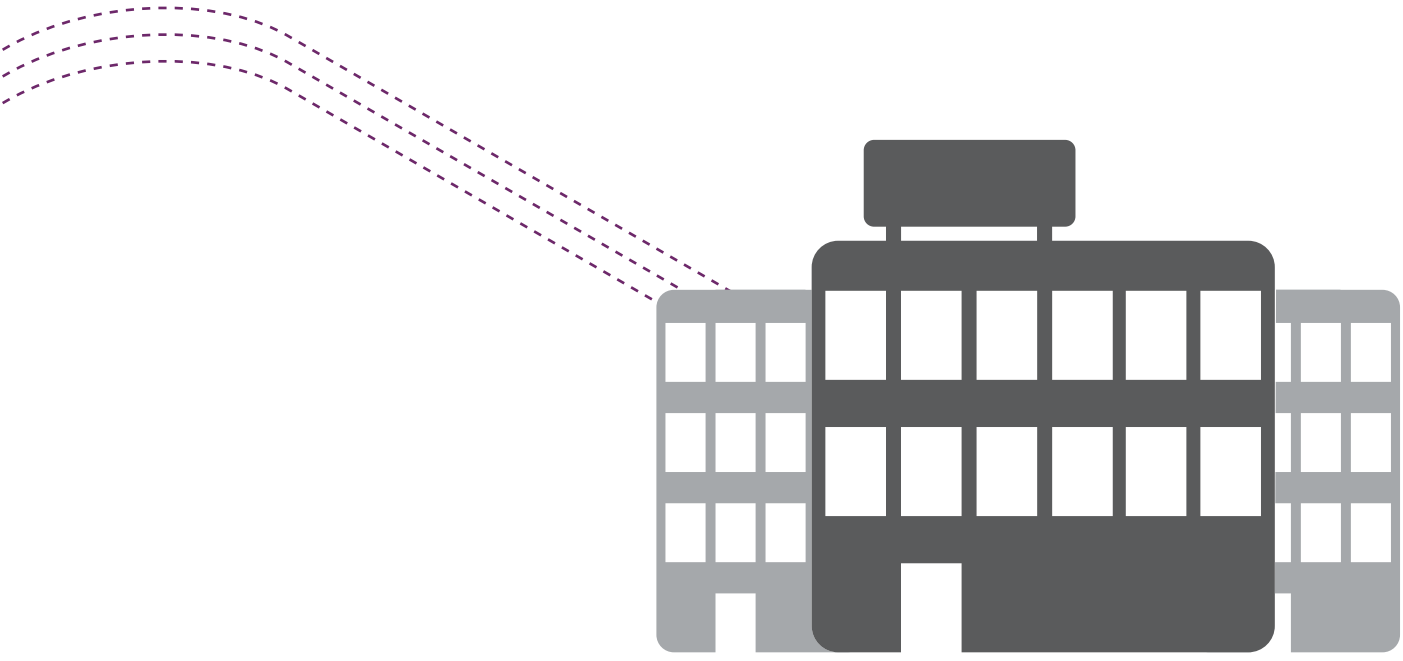
Gemalto consulting and professional services provide support throughout the product lifecycle by helping customers develop and maintain their security posture. Dedicated SafeNet Identity and Data Protection consulting teams design the technical implementations; provide project management and development resources; and configure security, access, and backup policies for HSMs and other Gemalto solutions. Professional services includes comprehensive, customized, multi-day, hands-on product training to ensure that customers are well-prepared to manage their enterprise key management system once the implementation team finishes with the infrastructure setup.

Protect cloud data with an on-premises SafeNet HSM

SafeNet HSMs that are deployed on-premises in a customer data center will store cryptographic keys and perform cryptographic operations for applications running and data stored in AWS environments. Ethernet connectivity of the appliance enables flexible deployment and scalability. Built-in TCP/IP support ensures that the SafeNet HSM installs easily into existing network infrastructures and communicates with other network devices to manage encryption keys, whether they reside on-site or in the cloud.

The tamper-resistant appliances are designed to meet Federal Information Processing Standard (FIPS) 140-2 and Common Criteria EAL4+ standards to provide a maximum level of security. On-premises implementations combine the highest security commercially available, with the confidence that comes when customers maintain full control of their encryption keys in their own data center to establish a solid root of trust for all of their cryptographic operations.

For specifications, product details, and instructions on how to purchase SafeNet HSM http://bit.ly/1g1Ji9R



Meeting compliance demands with Gemalto solutions

The SafeNet product line from Gemalto offers a range of solutions for use in AWS environments—from virtual security appliances to tamper-proof hardware appliances—that allow organizations to demonstrate compliance with the strictest information regulations, such as PCI DSS, HIPAA/HITECH, FISMA, SOX (Sarbanes-Oxley), and GLBA. Following are the compliance issues and the SafeNet products that address them.

- **Ownership of encryption and encryption keys:** With SafeNet KeySecure and SafeNet Virtual KeySecure, customers own both their encryption and their encryption keys. It gives them the flexibility to manage the key lifecycle from creation to rotation to deletion.

- **Separation of duties:** Encrypting data and storing encryption keys separately in SafeNet KeySecure or SafeNet Virtual KeySecure allows organizations to assign administrative duties to different staff. This feature allows infrastructure administrators to maintain the storage or virtual environment without ever having access to the data.

- **Secure key storage:** SafeNet HSM and AWS CloudHSMs securely maintain cryptographic materials in FIPS 140-2 Level 2, tamper-proof hardware security modules. These HSMs are available for either permanent on-premises deployments or as a pay-as-you-go service in the AWS cloud.

- **Virtualization attacks:** SafeNet ProtectV encrypts entire virtual instances to ensure that virtual image snapshots and routinely automated backups that are moved to other host systems are secure from unauthorized access. SafeNet KeySecure and SafeNet Virtual KeySecure manage the encryption keys and can combine with SafeNet ProtectV to ensure secure, controlled access to virtual environments.

- **Audit controls:** SafeNet ProtectV maintains audit controls of all actions pertaining to all copies of data. Organizations will know exactly who commits actions to protected instances for comprehensive reporting.

- **Centralized key management:** SafeNet KeySecure and SafeNet Virtual KeySecure centralize encryption key management from one platform to improve security through streamlined efficiency. These solutions from Gemalto place encryption and key management control squarely in the hands of the customer so third-party administrators do not have access to the data in the environments that they manage.

- **Data security through encryption and key deletion:** SafeNet KeySecure, SafeNet ProtectV, SafeNet ProtectApp, SafeNet ProtectDB, SafeNet ProtectFile, SafeNet Tokenization, and SafeNet High Speed Encryptors provide solutions for security and compliance—in virtual and traditional scenarios—through data encryption. In the event of a breach or change of data ownership, organizations can permanently delete the relevant encryption keys so data that is protected by any SafeNet encryption solution and stored in ciphertext remains unreadable. Through key deletion, organizations ensure that data is both secured at the highest level possible and that they are meeting their compliance requirements.

Application integrations

Amazon Redshift and Amazon Relational Database Service (RDS) for Oracle Database can be configured to store master keys in an on-premises SafeNet HSM or AWS CloudHSM instances.

Using on-premises SafeNet HSM or AWS CloudHSM to store Amazon Redshift Encryption Keys

When using Amazon Redshift's optional built-in encryption capabilities for securing data in transit via SSL or using hardware-accelerated AES-256 to secure data at rest, Amazon Redshift customers can use their own on-premises SafeNet HSM or AWS CloudHSM to store and manage their encryption keys.

Using SafeNet KeySecure, SafeNet HSM or AWS CloudHSM to store Amazon RDS Oracle TDE Keys

RDS customers can encrypt the entire database using Oracle on Amazon RDS Transparent Disk Encryption (TDE) and Native Network Encryption (NNE) features and store the keys in the AWS native tools. RDS customers can also opt for more granular field- and column-level encryption with products from partners such as CipherCloud, Blue Coat, and others that can store the encryption keys in SafeNet KeySecure or the SafeNet HSM (depending on the integration level).

Other application integrations

SafeNet HSM and AWS CloudHSM can integrate with hundreds of third-party products. For specifics on integration, please visit the SafeNet HSM interoperability page.

SafeNet HSM and AWS CloudHSM also integrate with a large number of cryptographic protocols and APIs such as PKCS#11, CAPI (Microsoft CryptoAPI 2.0), CNG (Microsoft Cryptography API: Next Generation), JCA (Java Cryptographic Architecture), and OpenSSL.

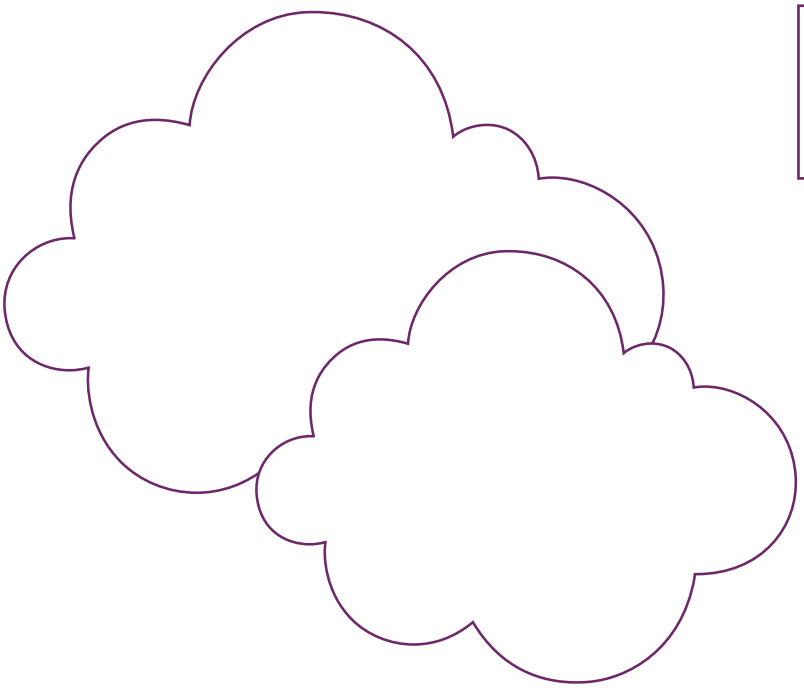
SafeNet Virtual KeySecure

SafeNet Virtual KeySecure, available in the AWS Marketplace, centralizes key management for multiple use cases using a hardened virtual appliance that runs in the AWS Cloud.

By encrypting the application and operating systems on the hardened virtual appliance, SafeNet Virtual KeySecure renders the information tapproof—ensuring protection and control of sensitive data at rest stored or pushed to the AWS Cloud. SafeNet Virtual KeySecure works alongside other SafeNet encryption products to support a wide variety of use cases that increase security and address compliance mandates. The combination of SafeNet Virtual KeySecure and SafeNet ProtectV enables organizations to unify encryption and key management, provide visibility and proof of data governance, manage entire VM lifecycles, and allow customer control and ownership of their data. For example, SafeNet Virtual KeySecure can be deployed with SafeNet ProtectV to secure sensitive data residing in AWS EC2 instances and AWS EBS volumes or with SafeNet ProtectApp to secure data stored in Amazon S3.

SafeNet Virtual KeySecure allows organizations to quickly deploy centralized key management in clustered configurations to ensure key availability. It provides load balancing for high-performance applications as well as support to SafeNet ProtectV's capability for cloud bursting and back-up. SafeNet Virtual KeySecure's ability to separate encryption keys from AWS and other AWS tenants ensures that customers maintain ownership of their encryption keys at all times. Without this, customers cannot prove ownership of their data, resulting in security and compliance gaps. The solution is FIPS 140-2 Level 1 validated and optionally supports a hardware root of trust for encrypting keys supporting Amazon's CloudHSM service.

SafeNet Virtual KeySecure also supports cloud and hybrid deployment options for VMware scenarios and a variety of encryption products supporting OASIS Key Management Interoperability Protocol (KMIP) standard.



Try SafeNet Virtual KeySecure on AWS Marketplace FREE for 30 days.
http://amzn.to/2fSjW7Q

SafeNet Virtual KeySecure can be used to:

Securely store and manage encryption keys for

- AWS EC2 instances with SafeNet ProtectV, SafeNet ProtectDB, SafeNet Tokenization and SafeNet ProtectFile
- Amazon EBS volumes with SafeNet ProtectV
- Amazon S3 with SafeNet ProtectApp and SafeNet ProtectFile
- Cloud Encryption Gateways
- KMIP-based Endpoints
- Custom Applications
- Direct Connect supported by SafeNet High Speed Encryptors
- SafeNet Key Management Partner Ecosystem, including storage from NetApp, Dell, IBM, HPE, Hitachi, and more

Prove customer ownership of encryption keys; no one but the customer has access

- Ensures that all requests to access encrypted data, including subpoena requests, must be directed to the customer who retains key ownership—tapproofing

Support a variety of asymmetric and symmetric algorithms

Delete encryption keys

Export encryption keys outside of the AWS environment

Address compliance with information regulations, such as GDPR, PCI DSS, HIPAA, Sarbanes-Oxley (SOX), and GLBA

- FIPS 140-2 validation

Support hybrid and multi-cloud deployments

To learn more about SafeNet Virtual KeySecure, contact a Gemalto representative.
https://safenet.gemalto.com/request-information

SafeNet Virtual KeySecure for NetApp Cloud ONTAP

SafeNet Virtual KeySecure for NetApp Cloud ONTAP is a hardened, 64-bit, virtual security appliance that provides centralized key management and data access policies for NetApp Cloud ONTAP. SafeNet key management simplifies the operational challenges of managing encryption keys, making sure keys are secure and information is always available to authorized users across your NetApp Cloud ONTAP environment. SafeNet Virtual KeySecure maintains data confidentiality on NetApp Cloud ONTAP through efficient centralized key management and by enforcing customized security policies surrounding data access. This combination of a modern storage infrastructure and SafeNet key management delivers the peace of mind that your data and its encryption keys are protected against unauthorized access, while simultaneously making the most efficient use of your storage investments. SafeNet Virtual KeySecure centralizes all key management activities, including key signing, role-based administration, quorum control, backup and distribution of encryption keys, and an optional hardware root of trust using SafeNet HSMs or Amazon CloudHSM service. Meeting compliance mandates in the cloud is greatly simplified through verifiable and auditable enterprise key management—all keys, certificates, and passwords are securely managed; key ownership is clearly defined; and key lifecycle management is logged to provide a non-repudiative audit trail.

Highlights:

- **Centralizes and simplifies** key management activities, including key signing, role-based administration, quorum control, and the backup and distribution of encryption keys enterprise-wide for your NetApp Cloud ONTAP environment.
- **Leverage shared resources** while securing data by business policy to segregate data for multiple departments, business units, or customers.
- **Built-in auditing, logging, and alerting functions** facilitate regulatory compliance in your NetApp ONTAP environment with a non-repudiative audit trail.

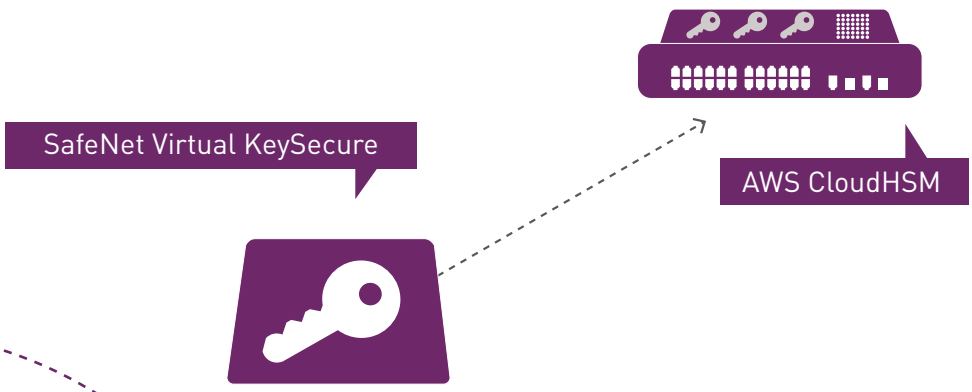
Try it free for 30-days
in the AWS Marketplace
http://amzn.to/2gbl1Z6

Using AWS CloudHSM as a root of trust for SafeNet Virtual KeySecure

While storing the master key in a hardened virtual appliance is appropriate for some assurance requirements, other customers may require a tamper-resistant hardware root of trust protecting critical encryption keys that are subject to strict contractual or regulatory requirements.

SafeNet Virtual KeySecure supports AWS CloudHSM service, an optional hardware root of trust for encryption keys. AWS customers can easily configure SafeNet Virtual KeySecure to store master keys in AWS CloudHSM (a SafeNet HSM residing in the AWS cloud). The AWS CloudHSM can securely generate, provision, and store cryptographic resources for SafeNet Virtual KeySecure and other keys used to encrypt and sign sensitive and regulated data on Amazon EC2 without giving processes direct access to encryption keys.

> AWS customers can easily configure SafeNet Virtual KeySecure to store master keys in AWS CloudHSM.



Remote AWS CloudHSM management with SafeNet Crypto Command Center

SafeNet Crypto Command Center remotely administers AWS CloudHSMs, enabling enterprises and service providers to provide an encryption-as-a-service offering to their internal and external customers. SafeNet Crypto Command Center lets organizations take full advantage of the benefits of virtualization including easy access and reduced total cost of ownership without compromising security or compliance.

SafeNet Crypto Command Center is the market's first true crypto hypervisor, enabling enterprises and service providers to manage one to thousands of AWS CloudHSMs from one central location. Easily provision crypto services by partitioning AWS CloudHSMs in a manner that makes a single appliance behave as if it is many appliances with cryptographic keys kept secure from the other partitions. The result is a single AWS CloudHSM appliance, or a device pool of appliances, that can serve many lines of business and applications at once. Additionally, the rightful key owner retains control of the keys—even in multi-tenant environments—through role separation and crypto isolation for administrators and owners.

Try SafeNet Crypto Command Center for FREE with a Freemium license from Gemalto. http://bit.ly/1LrUsHx

SafeNet Crypto Command Center can be used for:

- **Improved Security:** Standardization through crypto recipes and automation eradicates the risk of non-compliance and ensures security even in heavily regulated industries.
- **Efficiency:** Centralized management of cloud crypto resources eliminates encryption islands. Automation, scalability, and delegation of responsibilities to non-crypto experts reduces costs and shortens time to market when implementing cloud encryption solutions.
- **Simplicity:** Crypto service templates remove cloud complexity and empower more users to use crypto in the enterprise.
- **Improved Quality:** High Availability (HA) ensures business continuity and consistent service levels.

To learn more about SafeNet Crypto Command Center, contact a Gemalto representative. https://safenet.gemalto.com/request-information

The value of KMIP

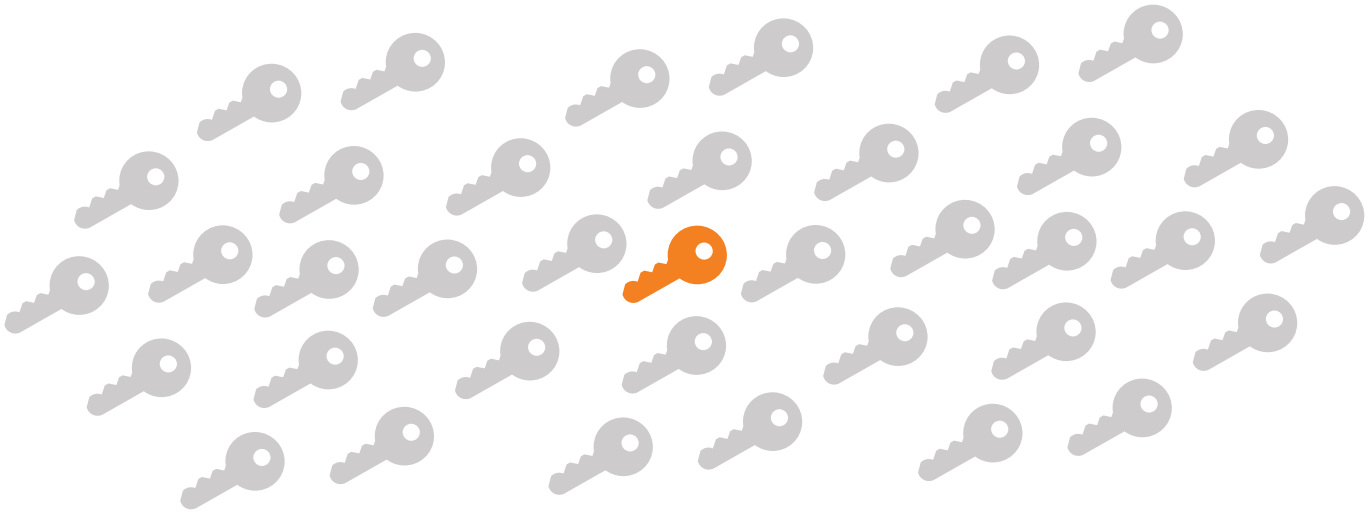
Today, many enterprises have isolated silos of encryption deployments for various data layers scattered across workgroups, infrastructure elements, and locations. Each encryption silo has its own set of keys, its own key policies and enforcement mechanisms, and may or may not support managing keys across their lifecycle.

Without centralized key management, the time and costs required to manage encryption keys can be overwhelming. However, the Key Management Interoperability Protocol (KMIP) provides a way to address this challenge. KMIP is a standard protocol that allows heterogeneous cryptographic environments and key managers to communicate without custom integration. This reduces not only the operational costs for enterprise key management but also the time and effort involved in the integration.

> Managing encryption keys can be overwhelming, but KMIP addresses this challenge.

With KMIP, any supporting environment—self-encrypting hard drives, tape drives, databases, applications, and encryption SDKs—can use the KMIP protocol to communicate with any KMIP-compliant key manager.

Today, many encrypted solutions from NetApp, Hitachi Data Systems, HPE, IBM, Sepaton, CipherCloud, and more are KMIP-compliant. (See the SafeNet KeySecure Interoperability Overview for more information.) And, all of these solutions can have their keys securely stored and completely managed by SafeNet Virtual KeySecure for AWS—no matter where those devices, services, and applications live.



SafeNet ProtectV

Virtual machine encryption for Amazon EC2 and EBS with SafeNet ProtectV

Available on AWS Marketplace, SafeNet ProtectV encrypts entire virtual machine instances and attached storage volumes while ensuring complete isolation of data and separation of duties. SafeNet ProtectV also ensures that no virtual machine instance can be launched without proper authorization from SafeNet ProtectV StartGuard™ pre-boot authentication. In addition, all of the data in archives, including snapshots and backups, are encrypted. The copies and snapshots of virtual machine instances are tracked and are impossible to instantiate without authorized access.

SafeNet ProtectV enables organizations to unify encryption and control across virtual and cloud-enabled environments, improving business agility and lowering costs by ensuring you can run even the most sensitive, highly regulated data in the cloud. Organizations choose between several levels of assurance and deployment modes for centralized key management, and retain access to and control of encryption keys at all times.

SafeNet ProtectV provides security and compliance across virtual and cloud-enabled infrastructure to secure sensitive workloads in the cloud, store confidential data and comply with regulations in controlled industries

- **Isolate** virtual machines and storage through encryption of OS and data partitions
- **Authorize** virtual machine launches with ProtectV StartGuard™ pre-boot authentication
- **Track key access** to all copies of your data
- **Revoke key access** after terminating an instance or in the event of a breach

SafeNet ProtectV encrypts entire virtual machine instances and attached storage volumes.

SafeNet ProtectV can be used for:

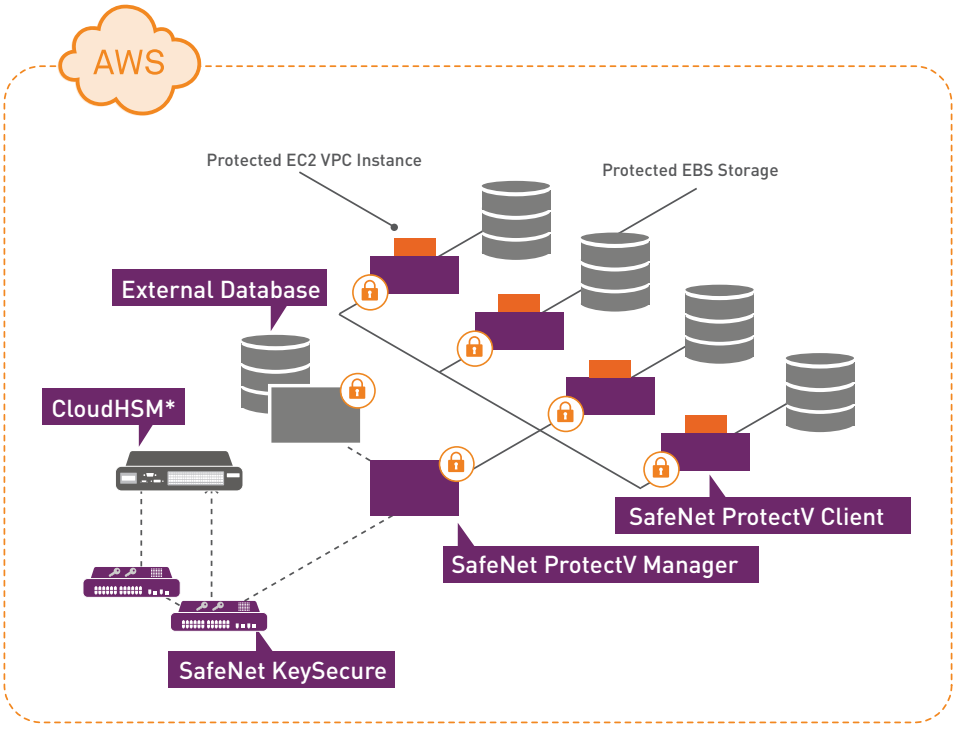
- Securing leading cloud service providers such as AWS with instance and storage volume archives, including snapshots and backups
- Protecting sensitive workloads containing directory, intellectual property, payment card, and personally identifiable information
- Addressing compliance standards for cloud environments such as GDPR, PCI DSS, SOX, and HIPAA/HITECH

Try SafeNet ProtectV on AWS Marketplace FREE for 30 days. http://amzn.to/1NX1Bl9

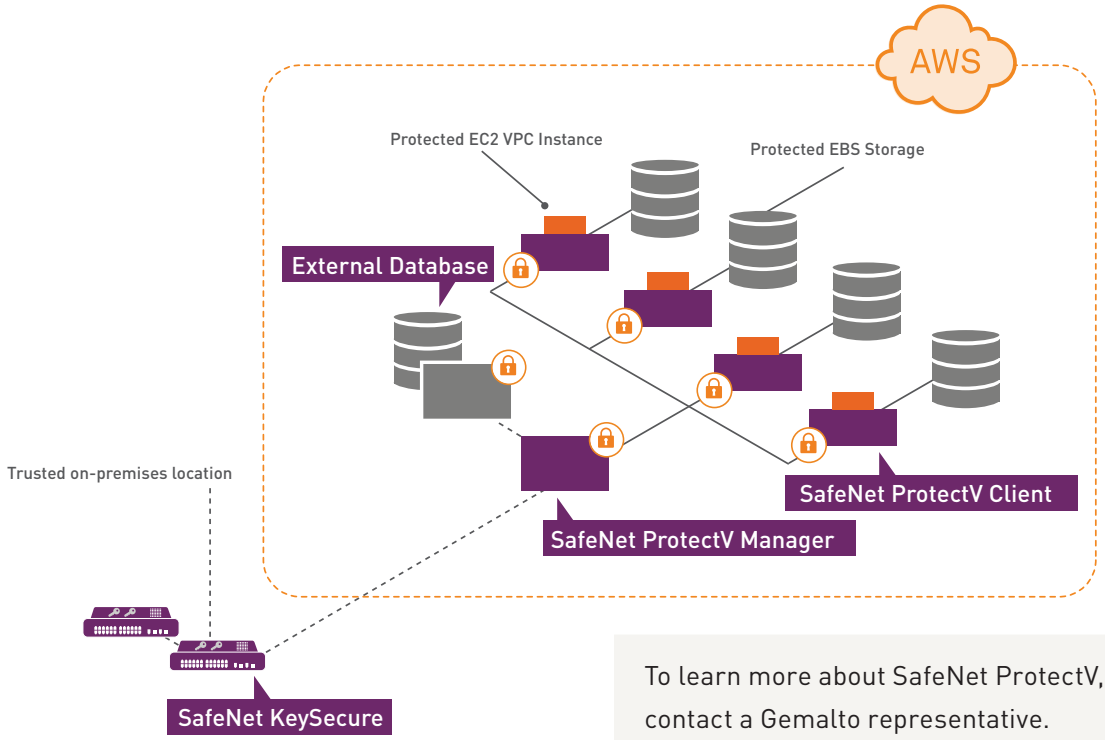
- 5 Nodes http://amzn.to/2g8YXiH
- 25 Nodes http://amzn.to/2ezd0N7
- 100 Nodes http://amzn.to/2gbgvKa

Return to Table of Contents

SafeNet ProtectV



*Also Supports SafeNet HSM on-premises



To learn more about SafeNet ProtectV, contact a Gemalto representative.
https://safenet.gemalto.com/request-information

SafeNet ProtectApp

SafeNet ProtectApp, when integrated with AWS SDKs, provides customer-controlled client-side object encryption for storage in Amazon's Simple Storage Service (S3). SafeNet ProtectApp's Java API and AWS SDK for Java interoperate to form an encryption client that provides keys as input to applications in order to encrypt an object before loading it to storage. For customers running applications on AWS EC2 instances, SafeNet ProtectApp integrates directly into the application with its own APIs.

SafeNet KeySecure—either on-premises or as a hardened virtual appliance hosted in the AWS cloud— stores the cryptographic keys and can offload cryptographic functions in order to encrypt data prior to archiving in S3 without impacting performance.

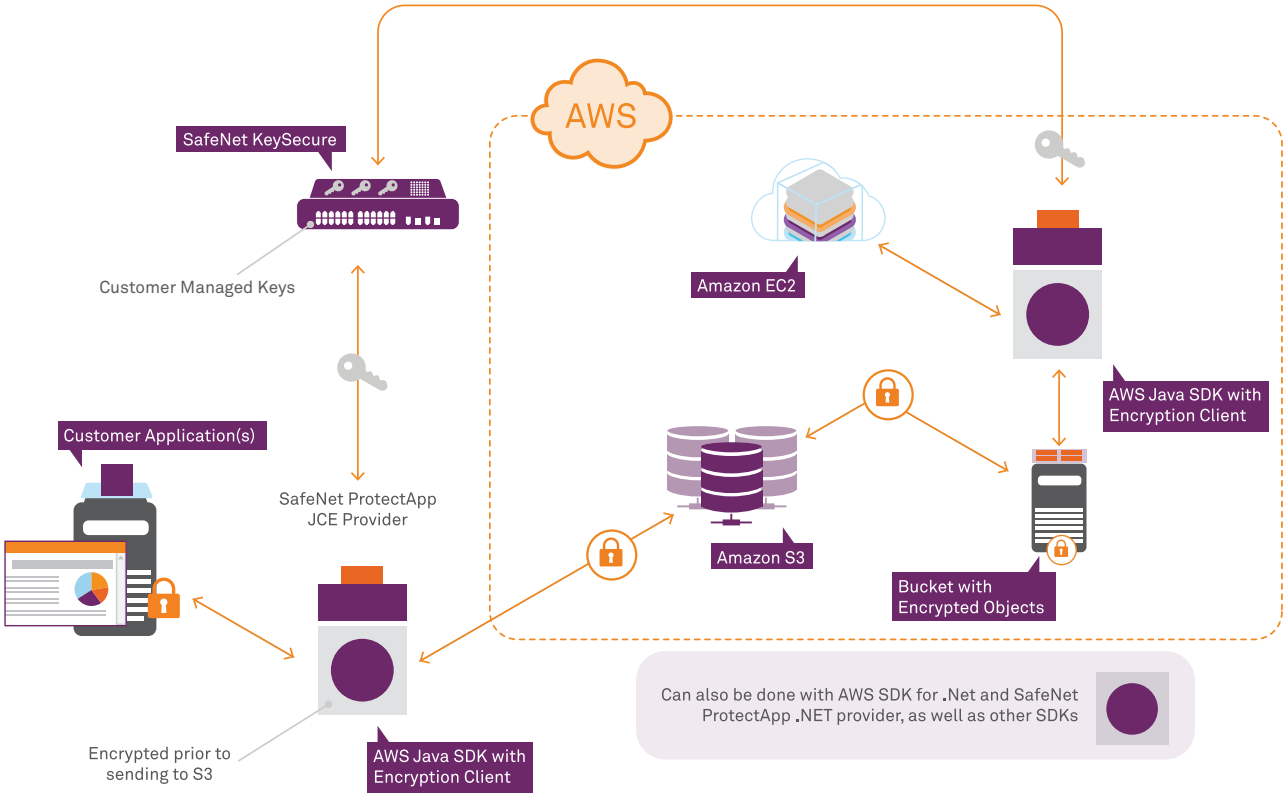
The SafeNet/AWS integration gives customers control of their data by encrypting it within the application and securing it before it is uploaded to S3 or as it is used on and off the EC2 instance. AWS customers can ensure their data will be unreadable by unauthorized users since encryption occurs in the customer's control and is managed by the customer using SafeNet KeySecure. In this setup, AWS administrators can manage the storage environment but never have access to cleartext data nor the keys to render the data as cleartext.

SafeNet ProtectApp with AWS SDKs can be used for:

- Securing data for applications running in Amazon EC2, Amazon S3, and on-premises
- Making sure the cloud provider never has access to unencrypted application data

> SafeNet ProtectApp provides customer controlled client-side object encryption for Amazon S3.

SafeNet ProtectApp with AWS SDKs



To learn more about SafeNet ProtectApp, contact a Gemalto representative.
https://safenet.gemalto.com/request-information

SafeNet ProtectFile

File Encryption in AWS EC2 and S3 with SafeNet ProtectFile

With SafeNet ProtectFile, organizations can apply transparent and automated file encryption to data in Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3) environments. The solution can also be leveraged to securely transfer encrypted data between an on-premises datacenter and Amazon S3. SafeNet ProtectFile encrypts unstructured, sensitive data on servers (such as credit card numbers, personal information, logs, passwords, configurations, and more) in a broad range of files including word processing documents, spreadsheets, images, database files, exports, archives, and backups, as well as data in Hadoop implementations. SafeNet ProtectFile features granular access controls to ensure only authorized users or processes can view protected data, including the ability to prevent rogue administrators from impersonating another user with access to sensitive data. A complete, enterprise-ready encryption solution, SafeNet ProtectFile provides built-in, automated key rotation and data re-keying, comprehensive logging and auditing, remote, silent installation scripts for automated deployment, and requires no changes to an organization's existing AWS environment.

SafeNet ProtectFile is deployed in tandem with SafeNet KeySecure or SafeNet Virtual KeySecure for centralized key and policy management. Administrators can set policies to encrypt particular folders and files, granting access only to authorized individuals or groups. Once a folder is selected for protection, any file deposited in the folder is automatically encrypted and will be rendered useless in the event of unauthorized access or a breach.

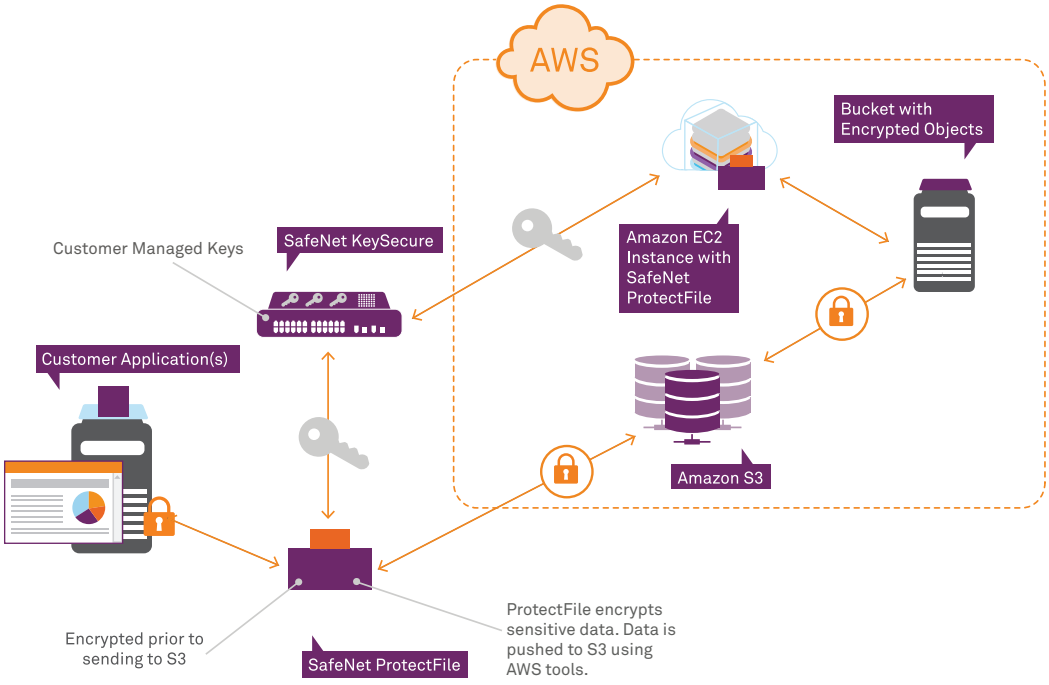
As a highly-scalable data protection solution, SafeNet ProtectFile and SafeNet KeySecure work across multiple data centers in the distributed enterprise. It can also extend protection to a number of popular AWS integrations including SQL databases (i.e., MySQL, PostgreSQL, MS SQL Server, Oracle), NoSQL databases (i.e., MongoDB and Cassandra), and Chef configuration management tool.

SafeNet ProtectFile can be used for:

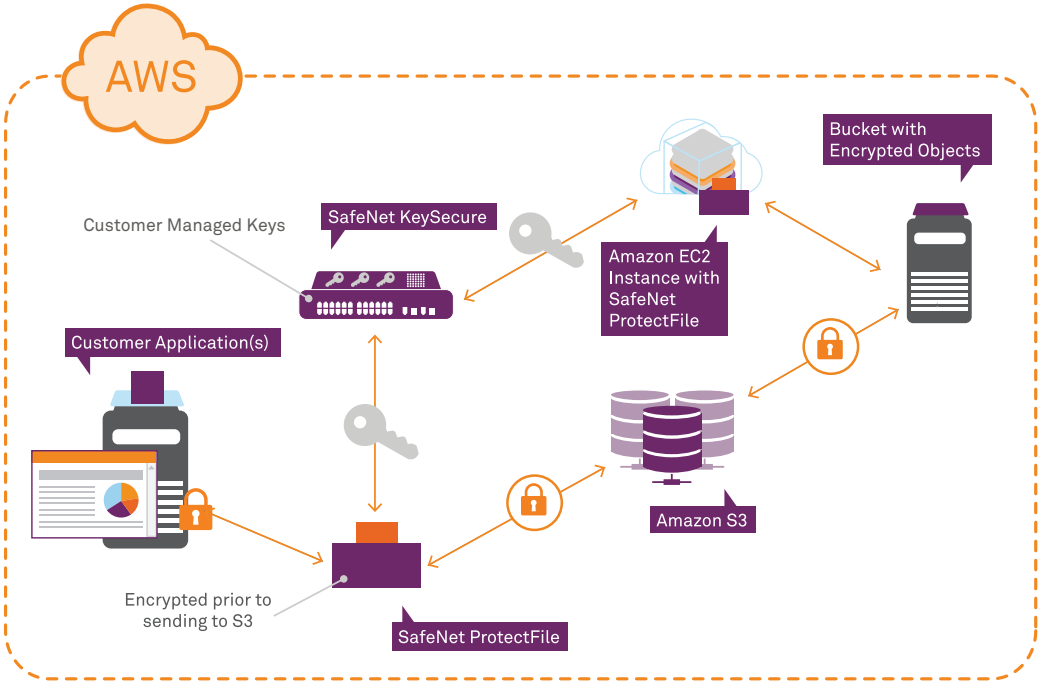
- Assuring that files are encrypted in Amazon EC2, Amazon S3, or on-premises
- Securely transferring encrypted data between an on-premises datacenter and Amazon S3

> With SafeNet ProtectFile, organizations can apply transparent and automated file encryption to data in Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3) environments.

SafeNet ProtectFile with SafeNet KeySecure



SafeNet ProtectFile with SafeNet Virtual KeySecure



To learn more about SafeNet ProtectFile, contact a Gemalto representative.
https://safenet.gemalto.com/request-information

SafeNet ProtectDB

Column-level database encryption in Amazon EC2 and S3 with SafeNet ProtectDB

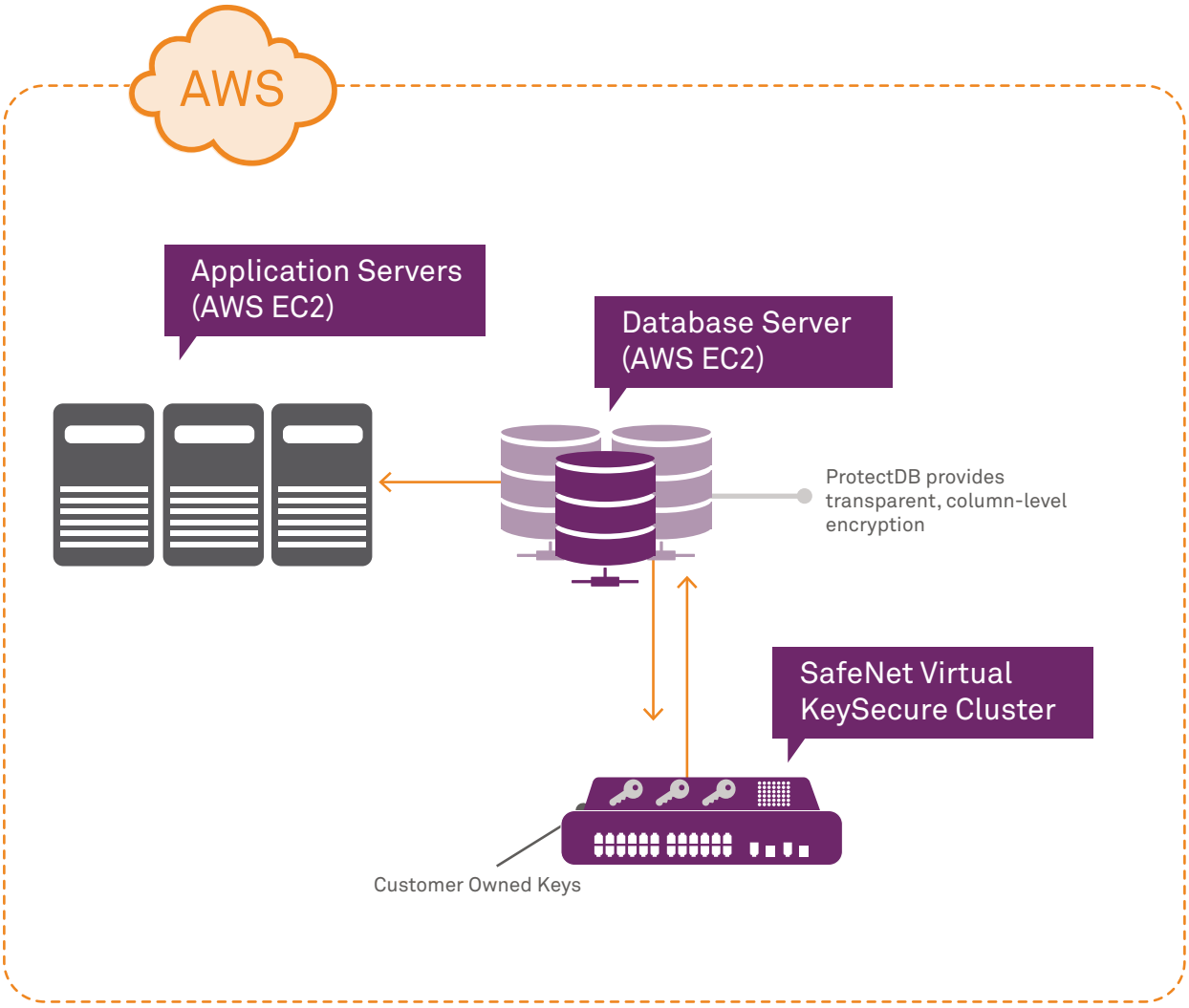
From credit card information, patient data, and social security numbers to customer email addresses—the most valuable information and assets of an enterprise reside in databases. When migrating that data to AWS EC2, SafeNet ProtectDB provides transparent column-level encryption of structured data residing in databases. The solution enables large amounts of sensitive data to be moved in and out of the data stores rapidly by efficiently encrypting and decrypting specific fields in databases that may contain millions of records. SafeNet ProtectDB is extremely scalable and works across multiple data centers in distributed enterprises.

Deployed in tandem with SafeNet KeySecure hardware or virtual appliance, SafeNet ProtectDB offers centralized key and policy management to ensure encrypted data remains secure throughout its lifecycle. The solution also features granular access controls to ensure only authorized users or processes can view protected data, built-in key rotation and data re-keying, and comprehensive logging and auditing—critical features for compliance and overall data protection. Safenet ProtectDB is highly-scalable and enables isolation of sensitive data in a shared infrastructure, separation of duties, and improved compliance with a variety of regulations including, but not limited to, credit card numbers for Payment Card Industry Data Security Standard (PCI DSS) and protected health information (PHI) for the Health Insurance Portability and Accountability Act (HIPAA).

SafeNet ProtectDB can be used to:

- Secure sensitive data at the column level in databases
- Assure column-level data encryption in Amazon EC2 instances, Amazon S3, or on-premises

SafeNet ProtectDB



To learn more about SafeNet ProtectDB, contact a Gemalto representative.
https://safenet.gemalto.com/request-information

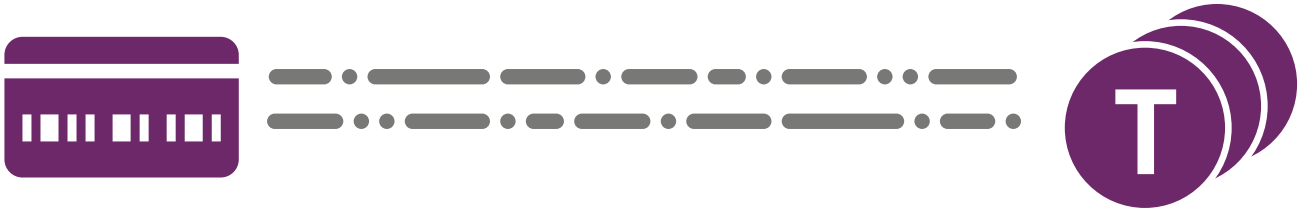
SafeNet Tokenization

SafeNet Tokenization protects sensitive data (primary account numbers, social security numbers, phone numbers, passwords, email addresses, etc.) by replacing it with a unique token that is stored, processed or transmitted in place of the clear data. Using Format Preserving Tokenization (FPT), SafeNet Tokenization preserves the length and format of the sensitive data. SafeNet Tokenization is also flexible in its ability to support a variety of token formats, such as last four, first six, custom formats, and regular expression. The solution utilizes Web APIs for easy deployment, requires no changes to existing databases and applications, and is extremely scalable across multiple data centers in the distributed enterprise.

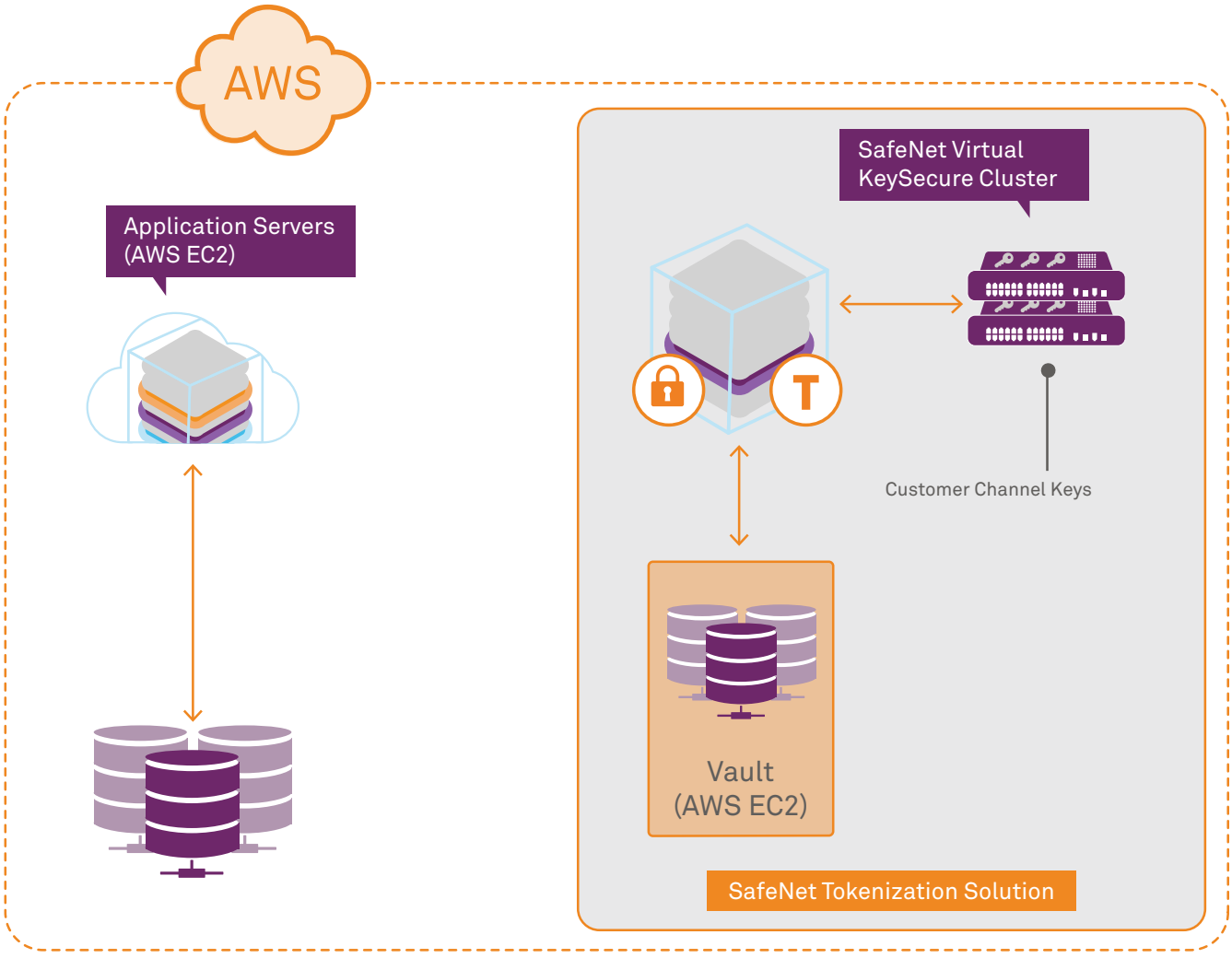
Deployed with SafeNet KeySecure hardware or virtual appliance for centralized key and policy management, SafeNet Tokenization provides a single, centralized interface for logging, auditing, and reporting access to protected data, keys, and tokens. SafeNet Tokenization also features built-in, automated key rotation and data re-keying, a critical feature for compliance and data protection. Compliant with PCI Tokenization Guidelines and VISA Tokenization Best Practices, Tokenization is an ideal solution for organizations with high compliance costs as it significantly reduces regulatory scope, facilitates the annual audit process, and results in reduced total cost of ownership.

SafeNet Tokenization can be used to:

- Protect sensitive data stored on-premises or Amazon EC2 instances by replacing it with a surrogate value that preserves the length and format of the data
- Reduce PCI-DSS Audit scope and ultimately operational costs



SafeNet Tokenization



To learn more about SafeNet Tokenization, contact a Gemalto representative.
https://safenet.gemalto.com/request-information

Securing Data in Motion Across AWS Networks with SafeNet High Speed Encryptors

SafeNet High Speed Encryptors (HSE) enable secure cloud connectivity across AWS infrastructure such as AWS Direct Connect. SafeNet HSEs provide proven high-assurance Layer 2 network security for an organizations' sensitive data, real-time video and voice, as it moves across virtual and physical networks, between data centers, to the last mile, and up to the cloud and back again.

Ensure secure, encrypted communications to and from AWS with SafeNet High Speed Encryptors and AWS Direct Connect in the partner or customer cage or via Layer 2 connections.

High-assurance data in motion encryption

Trusted security

Protecting Fortune 500 customers across financial institutions, telcos and other commercial organizations

Certified FIPS 140-2 L3, Common Criteria, NATO, UC APL, CAPS

Maximum network performance

> Near-zero overhead

> Microsecond latency

Scalable and simple

> "Set and forget" management

> Low total cost of ownership

High-assurance vulnerability protection

> True end-to-end, authenticated encryption

> State-of-the-art client side key management

To learn more about Safenet High Speed Encryptors, contact a Gemalto representative https://safenet.gemalto.com/request-information

SafeNet IDProve for AWS Management Console

The AWS Management Console and AWS Service APIs are powerful tools that can control many facets of the AWS infrastructure. Logging into those services with just a username and password doesn't provide organizations with the confidence that those users are who they say they are—and for many companies, their AWS infrastructure is too valuable not to provide an additional layer of identity validation.

SafeNet Display Card

The SafeNet Display Card is a secure, time-based OTP password token that offers strong protection for your AWS Management Console using two-factor authentication. With the touch of a button, this unconnected device generates a one-time password (OTP). When used in combination with a valid username, the authentication server validates the code and access is granted to the appropriate network resources.

SafeNet Display Card

The SafeNet Display Card is a secure, event-based OTP password display card that offers strong protection using two-factor authentication. The remote OTP display card features a button-activated digital display password that, when combined with a valid username, provides strong authentication for the AWS Management Console.

Strong Authentication at Your Fingertips

- Hand-held device with single button
- No PIN needed
- Secure remote access
- Zero footprint; no required software on end-user devices

To learn more about SafeNet IDProve products, contact a Gemalto representative. https://safenet.gemalto.com/request-information

To purchase SafeNet IDProve products, visit the Gemalto webstore. http://bit.ly/1WlYiVQ

SafeNet Authentication Service for AWS WorkSpaces

AWS WorkSpaces and SafeNet Authentication: Secure Virtual Computing

Amazon WorkSpaces is a managed desktop computing service in the cloud. It allows customers to access and easily provision cloud-based desktops with the device of their choice.

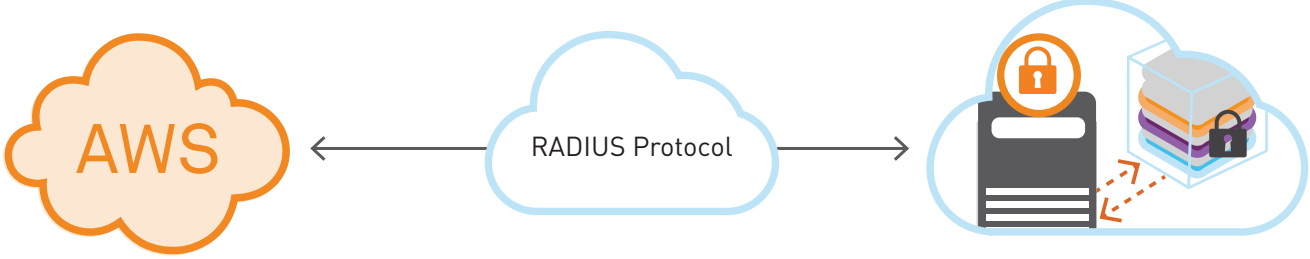
SafeNet Authentication Service is a cloud-based authentication service that offers multi-factor authentication solutions that protect identities and ensure that individuals accessing Amazon WorkSpaces are who they claim to be.

SafeNet Authentication Service, combined with Amazon WorkSpaces, offer enterprises a best-in-class virtual desktop system with strong authentication.

Next-Generation Authentication from SafeNet

- Reduce the risk of unauthorized access to sensitive corporate resources.
- Reduce IT management overhead through automated user and token lifecycle administration.
- Enforce consistent access policies throughout your IT ecosystem—VPNs, SaaS applications, web portals, and on-premises applications.
- Have a single point of management for defining and managing access controls to all resources.
- Increase user convenience with federated login, extending enterprise identities to the cloud.

To learn more about SafeNet Authentication Service, contact a Gemalto representative.
https://safenet.gemalto.com/request-information



For More Information

Helping to protect the confidentiality, integrity, and availability of customer systems and data, as well as maintaining customer trust and confidence, is of utmost importance to AWS. With Gemalto's SafeNet Identity and Data Protection solutions, customers can safely secure their data in AWS environments by owning their encryption and encryption keys.

Gemalto, a leading global provider of data protection, is an AWS Advanced Technology Partner and uses a data-centric approach for information stored in the AWS cloud focusing on the protection of high-value information throughout its lifecycle. Thousands of customers trust Gemalto to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments. SafeNet ProtectV and SafeNet Virtual KeySecure can be purchased on AWS Marketplace or directly from Gemalto with a bring-your-own-license (BYOL) option. AWS CloudHSM can be purchased directly from AWS.

- More information about Gemalto and the SafeNet products mentioned in this eBook can be found on the SafeNet website: http://www.safenet.gemalto.com
- To contact a Gemalto representative for SafeNet product information and purchase options, visit https://safenet.gemalto.com/request-information
- If you are an AWS customer, try SafeNet Virtual KeySecure on AWS Marketplace FREE for 30 days http://amzn.to/2g8ZK2U
- If you are an AWS customer, try SafeNet ProtectV on AWS Marketplace FREE for 30 days http://amzn.to/2g91f18

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments and data – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com
Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free