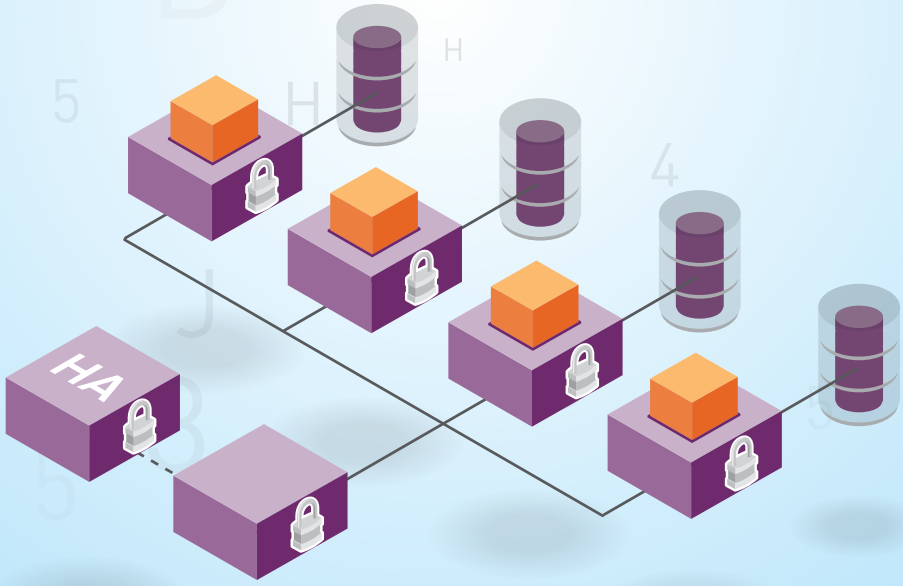
6

ways to enhance security in **AWS**

eBook



SafeNet®

THE DATA PROTECTION COMPANY

Contents

Introduction

Value of the public cloud

Cloud computing is fundamentally transforming the way enterprises, government agencies, and small businesses are managing their data. For many organizations, using elastic, pay-as-you-go cloud services is an attractive, cost-effective way to run business-critical applications and house company data. In fact, it's rare to encounter a company that lacks a desire to migrate from the traditional data center to the cloud.

While every cloud provider brings a different set of benefits to customers, Amazon Web Services has been identified as a leader in cloud infrastructure services by Gartner, with more than five times the compute capacity of its fourteen nearest competitors[1]. With AWS Marketplace, customers have a web-based front end to purchase and deploy cloud-based infrastructure and hundreds of related applications—from both AWS and its partners, such as SafeNet. SafeNet customers who deploy in the AWS cloud report gaining flexibility, redundancy, and availability, while decreasing their data center costs.

1 Source: Gartner, Magic Quadrant for Cloud Infrastructure as a Service, August 19, 2013. 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

Challenges for sensitive data in the cloud

Still, progress to the cloud is most often impeded by the lingering questions companies have surrounding the ability to demonstrate compliance and to illustrate control of sensitive data in cloud environments. For example, there can be challenges to storing sensitive data in the cloud, including credit card numbers, health records, or other personally identifiable information. Illustrating control, security, and compliance for sensitive data has a different set of implementation requirements and challenges when the organization is not the one controlling the entire computing stack.

How do organizations ensure that they can both meet their compliance requirements and keep their sensitive data safe?

How can organizations illustrate control, security, and compliance for sensitive data in 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.

SafeNet, an AWS Advanced Technology Partner, is proud to provide additional security functionality within the AWS cloud.

Security at the heart of AWS infrastructure

In order to support its clients compliance objectives, AWS develops services that are aligned with security best practices, provides appropriate security features in those services, and documents how to use those features. AWS' compliance framework covers FISMA Low, PCI DSS Level 1, ISO 27001, SOC 1/SSAE16, and HIPAA.

The AWS infrastructure features:

- **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 two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted 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.

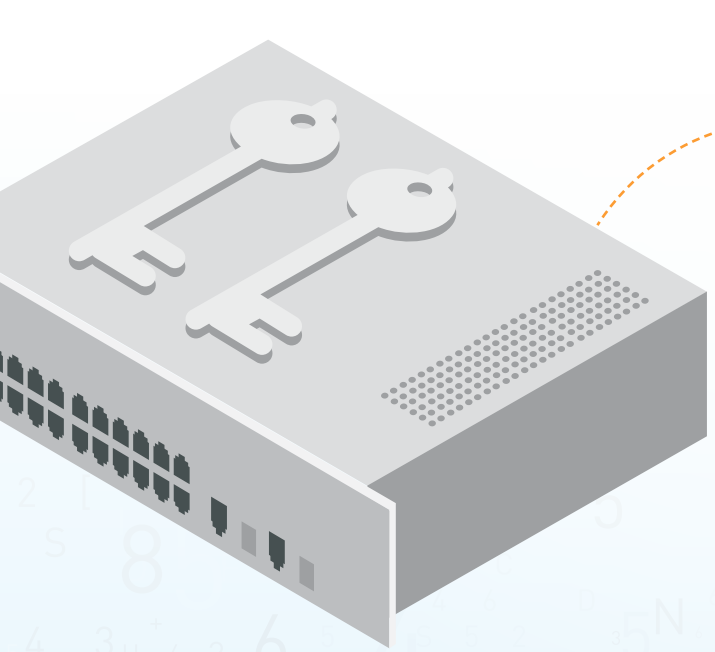
The role of encryption and key management

These challenges can often be addressed through an effective approach to securing data at rest. Experts often recommend encrypting sensitive data and deploying enterprise key management[1] to:

- Isolate regulated and sensitive information
- Separate encryption control and ownership from the cloud provider

This approach delivers separation of duties, as well as centralized monitoring and audit reporting. Not only can organizations demonstrate compliance and pass audits but, most importantly, they can effectively protect sensitive data from specific attacks.

Why are encryption and key management recommended so highly? One reason is that the security mechanisms render the data itself of no value to attackers—unlike other security controls that leave sensitive data in the clear. This data-centric approach means that the computing stack does not have to implement tenant-specific data security policies for the organization to have ownership and control of its data (and to be able to demonstrate to auditors that control is maintained).



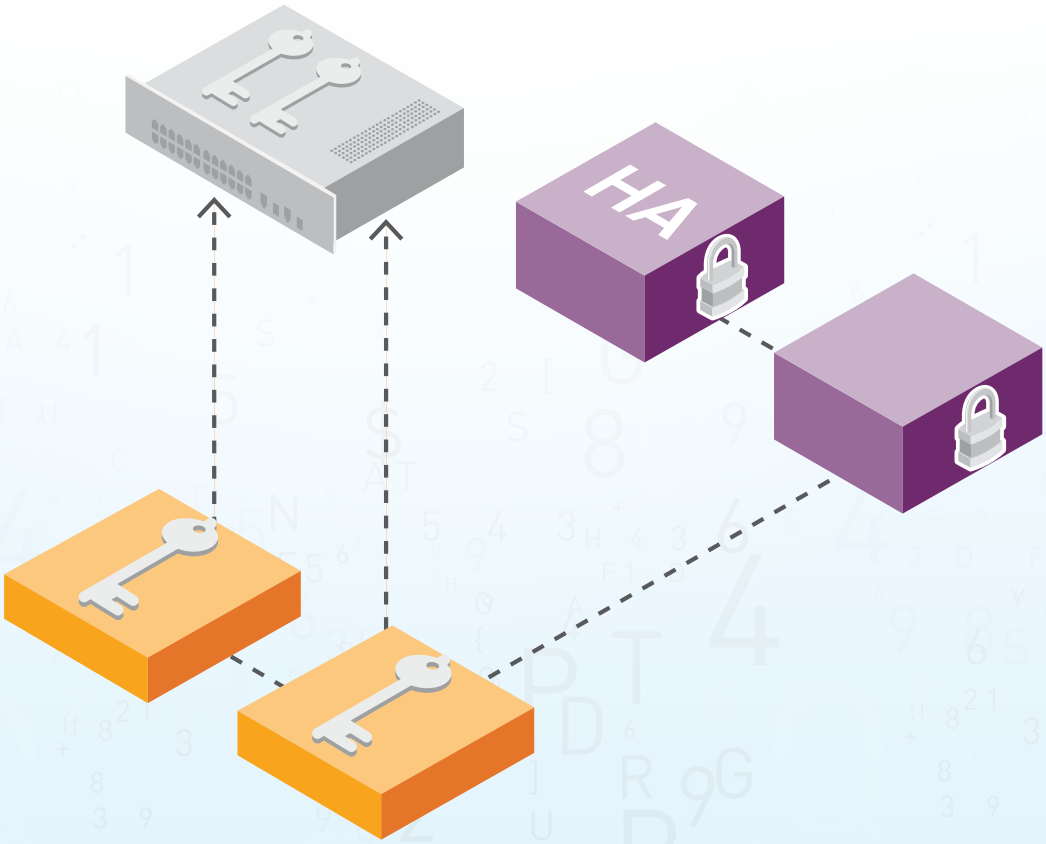
Why are encryption and key management recommended so highly?

1 Recommending organizations include the National Institute of Standards and Technology (Source: NIST, Guide to Storage Encryption Technologies for End User Devices, http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf) and Gartner (Source: Gartner, Simplify Operations and Compliance in the Cloud by Encrypting Sensitive Data, August 15, 2013, retrieved from http://www.gartner.com/document/2574918). 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

Encryption and key management principles

To ensure compliance and effectively secure sensitive data in AWS infrastructure (and other virtualized environments), experts often recommend that organizations employ encryption in the following areas:

- **Instance encryption.** By encrypting virtualized instances, organizations can guard against vulnerabilities inherent in virtualized and cloud environments. For example, it significantly reduces the number of ways users can get sensitive data off virtual images that can be easily moved and copied. It also enables organizations to enforce the separation of duties that compliance mandates require.
- **Field-, column-, and file-level encryption**. Through database- and application-level encryption solutions, organizations can more granularly apply security policies to specific subsets of data. This represents a way to have data secured as it progresses through workflows, and safeguards data when manipulated by processes running within an instance; for example, fields containing sensitive data in a web application.



Encryption and key management principles (continued)

In some organizations that have implemented encryption, key management presents significant challenges. Requirements around key storage, rotation, and deletion can present administrative overhead and cost. Also, in many cases, keys have been stored and managed insecurely; for example, some organizations store their keys in spreadsheets on USB drives. Further, best practices around key rotation haven't been adhered to consistently. 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 that streamline such activities as key rotation and deletion. Finally, 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 begin to centralize the management of cryptographic keys across disparate encryption deployments, which yields benefits in security, administrative efficiency, and compliance.

In addition, key management best practices require a secure 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 is often necessary. Previously, organizations had to store the sensitive data (or the encryption keys protecting the sensitive data) on physical machines in on-premises data centers—which often prevented migrating these applications to the cloud. Today, cryptographic keys can be securely generated, stored, and managed in the cloud, such that they are accessible only by the organization and never by the cloud provider.

Organizations need centralized key management solutions that offer the highest level of security.

Six solutions to **enhance** security

SafeNet offers additional solutions for protecting sensitive data within the AWS platform. This ebook will discuss six solutions that enhance security in AWS infrastructure.

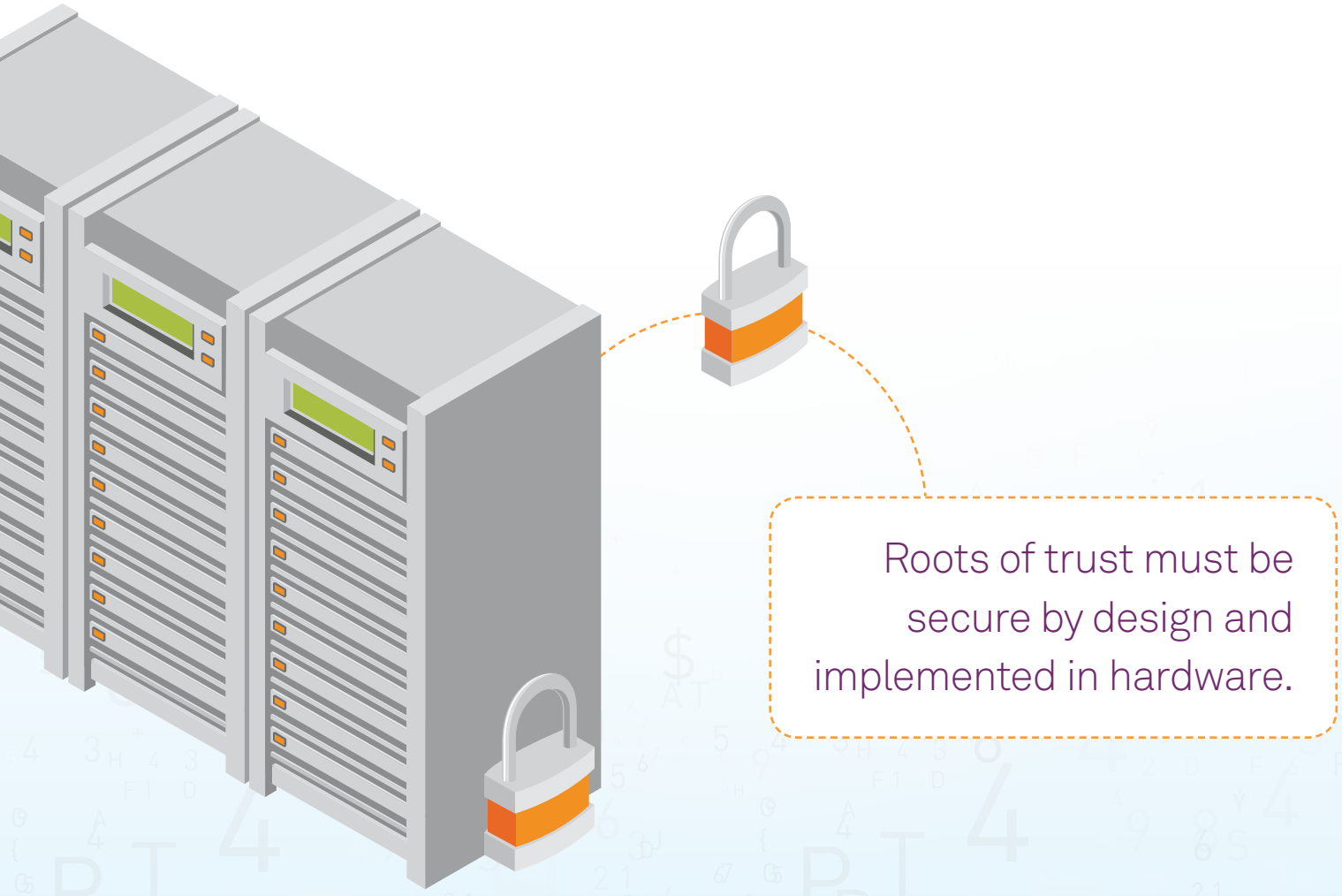
1. Roots of trust
2. Centralized key management
3. Encryption and pre-boot authentication for EC2/EBS
4. Client-side object encryption for S3
5. Storage encryption for AWS Secure Gateway
6. File encryption for EC2 and S3

Roots of trust

Roots of trust, as defined by the Cryptographic Technology Group at the U.S. National Institute of Standards and Technology (NIST)[1], are components that are inherently trusted to perform one or more security-critical functions. Protecting cryptographic keys, performing device authentication, or verifying software are three examples.

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 in implementing hardware-based roots of trust when the cloud is so dependent on virtualization and functionality that is often completely defined by software. SafeNet 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.

1 http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_mobility-roots-of-trust_regenscheid.pdf

AWS CloudHSM

AWS CloudHSM uses SafeNet's Luna SA to provide a "rentable" hardware security module (HSM) service that dedicates a single-tenant appliance located in the AWS cloud for a customer's cryptographic storage needs. From CloudHSM, customers can securely generate, store, and manage the cryptographic keys used for data encryption, such that they are accessible only with explicit authorization by the customer's administrators. They provide a secure foundation to cryptography in the cloud because the keys never leave the appliance. Since all cryptographic operations occur within the HSM and the key never leaves, unauthorized users never have an opportunity to see the information they need to decrypt secured data. CloudHSMs can be provisioned and clustered across multiple Availability-Zones (AZs) and regions to improve availability and performance.

For product details and pricing, visit the **AWS CloudHSM page**.

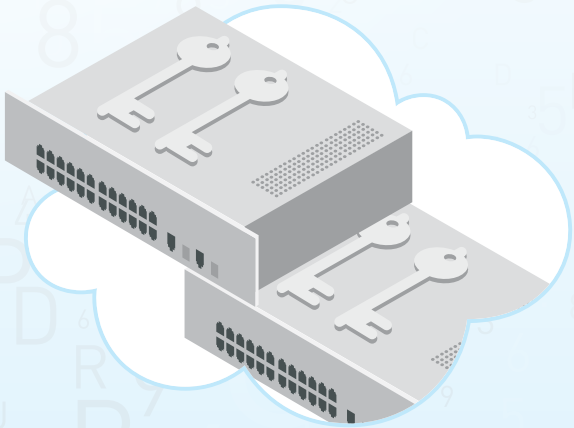
CLICK HERE

amzn.to/1ipyUdC

CloudHSM can be used for:

- Code signing, if you're writing code and storing it in AWS
- A root of trust if you're storing your CA in AWS
- Securing access to proxy layer keys for AWS-based databases

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



Hybrid models and backup options for CloudHSM

Because AWS does not have access to customer keys, customers are strongly encouraged to back up their keys[1]. As an option, customers can back up the contents of up to 20 CloudHSM partitions to a Luna Backup HSM located on their own premises. With the Luna Backup HSM, customers can unplug and lock away the compact USB-connected appliance once their keys are saved. In the event of a CloudHSM's failure or network outage, customers can easily restore their keys from the backup HSM appliance.

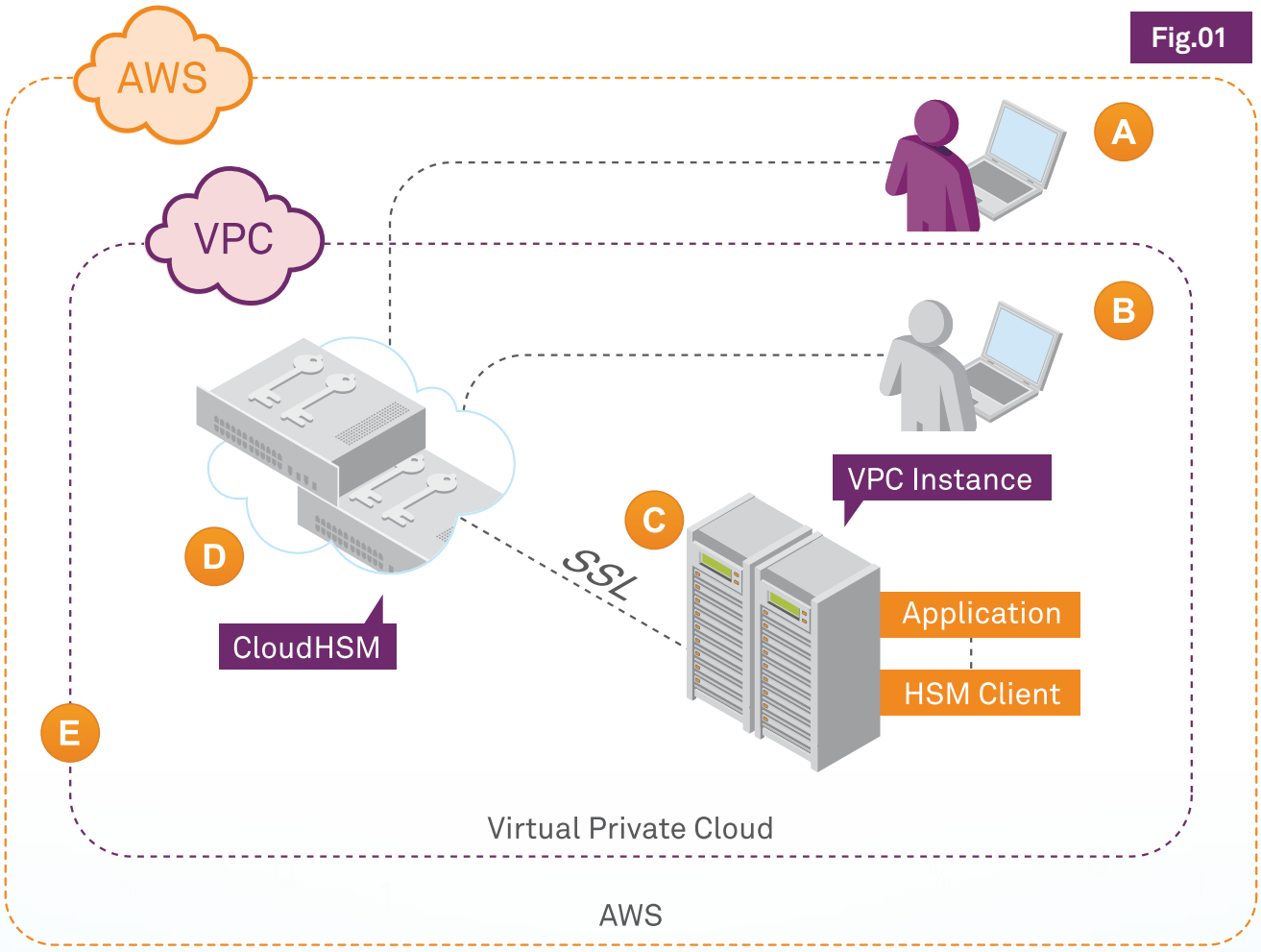
Hybrid implementations that combine CloudHSMs and on-premises SafeNet Luna SA HSMs offer significant elasticity for cryptographic operations, such as certificate validation and signing, document signing, and transaction processing. Organizations that do not normally perform a large number of cryptographic operations on-site can use 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 a CloudHSM's failure, customers can easily restore their keys from a backup HSM appliance.

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

Hybrid models and backup options for CloudHSM

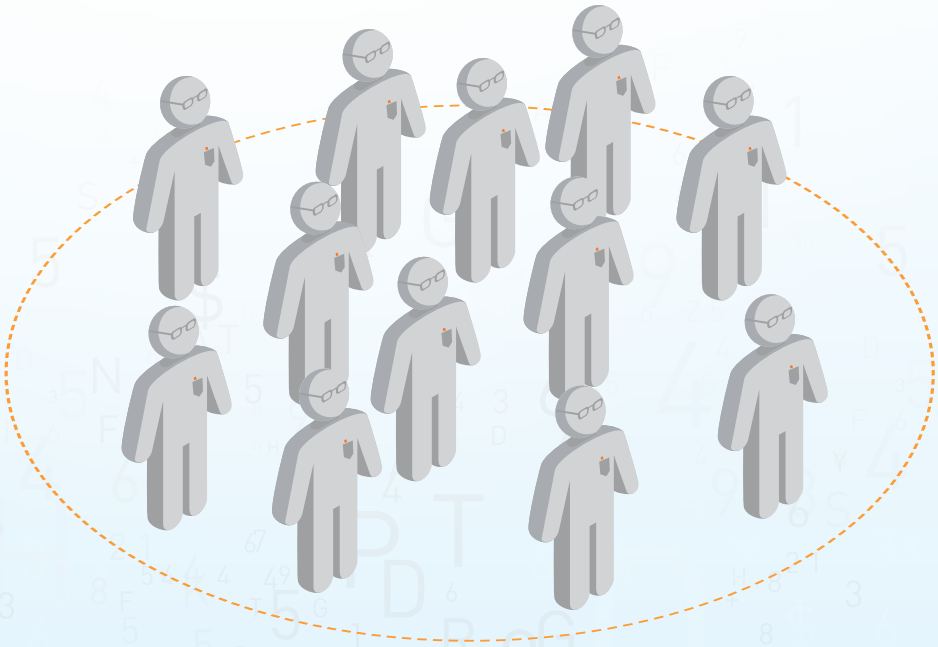
Fig.01



- **A** AWS manages the HSM appliance but does not have access to your 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** CloudHSMs are in your VPC and isolated from other AWS networks

Professional services

SafeNet's consulting and professional services provide support throughout the product's entire lifecycle by helping the customer develop and maintain their security posture. Dedicated HSM consulting teams design the technical implementations, provide project management and development resources, and configure the HSM's security, access, and backup policies. Professional services includes comprehensive, customized multi-day hands-on product training to ensure that the customer is well prepared to manage their enterprise key management (EKM) system once the HSM implementation team finishes with the infrastructure setup.



Customer-premises Luna SA

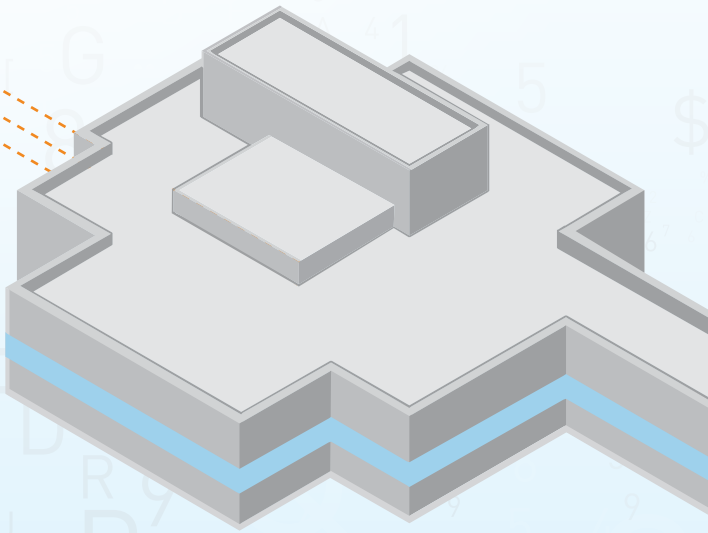
Luna SAs that are deployed on-premises in a customer's data center will still store cryptographic keys and still perform cryptographic operations for applications running and data stored in AWS environments. The appliance's Ethernet connectivity enables flexible deployment and scalability. Built-in TCP/IP support ensures that Luna SA 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 and validated to government standards (for example, Common Criteria EAL 4+ and NIST FIPS 140-2 Level 2) 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 buy Luna SA, **visit SafeNet's Luna SA page**.

CLICK HERE

bit.ly/1g1Ji9R



Meeting compliance demands

SafeNet offers a range of solutions—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, CJIS, BASEL II, SOX (Sarbanes-Oxley), and GLBA. Whether an organization keeps their data in a virtual machine in an AWS environment or uses AWS S3 to store data, SafeNet can help address the critical requirements of the security regulations, such as:

- **Separation of duties**: Encrypting data and storing encryption keys separately in SafeNet's KeySecure or Virtual KeySecure allows organizations to assign administrative duties to different staff. Infrastructure administrators can maintain their storage or virtual environments without ever having access to clear-text data.
- **Secure key storage:** Luna SA and CloudHSM hardware security modules securely maintain cryptographic materials in FIPS 140-2 Level 3-validated, tamper-proof hardware security modules. These HSMs are available for either permanent on-premises deployments or pay-as-you-go options in the AWS cloud. Keys that are traditionally stored in software with encrypted data are vulnerable to theft and compromise. SafeNet HSMs address these threats with flexible solutions that also fit with an organization's business strategy.
- **Virtualization attacks:** ProtectV encrypts entire virtual instances to ensure that virtual image snapshots and routinely automated backups moved to other host systems are secure from unauthorized access. KeySecure and Virtual KeySecure combine with ProtectV to manage the encryption keys, allowing organizations to maintain strict control over the materials necessary to decrypt their data.

SafeNet solutions allow organizations to demonstrate compliance with the strictest information regulations.

Meeting compliance demands (continued)

- **Audit controls:** 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:** KeySecure and Virtual KeySecure centralize encryption key management from one platform to improve security through streamlined efficiency. SafeNet's solutions 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 control.
- **Data security through encryption and key deletion:** SafeNet StorageSecure, ProtectV, and ProtectApp provides 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 (protected by any SafeNet encryption solution) 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) have several options for database or data-at-rest encryption.

Amazon Redshift

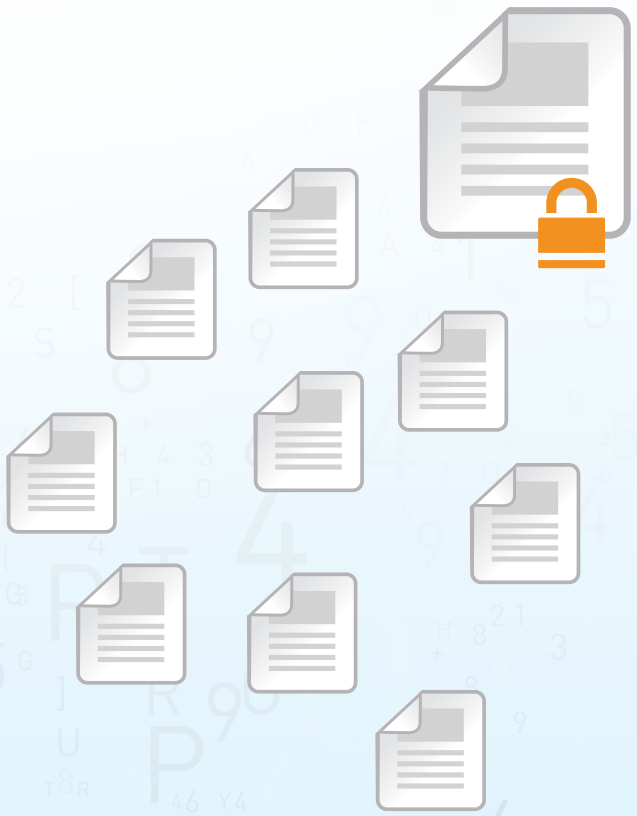
Whether it's for data transport via SSL or for storage encryption, Redshift can keep its cryptographic material in either an on-premises Luna SA HSM or an AWS CloudHSM.

Amazon RDS

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

Luna SA and AWS CloudHSM can integrate with hundreds of third-party products as well. For specifics on integration, please visit SafeNet's HSM interoperability page.

Luna SA 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.



Key management solutions

Virtual KeySecure

Virtual KeySecure for AWS Marketplace centralizes key management for ProtectV-secured virtual instances, as well as other use cases, using a hardened virtual security appliance that runs in the AWS cloud. The combination of Virtual KeySecure and ProtectV enables organizations to unify encryption and control across virtualized and cloud infrastructure, increasing security and compliance for sensitive data residing in AWS EC2 instances. Virtual KeySecure allows organizations to quickly deploy centralized key management in high-availability, clustered configurations. Additionally, Virtual KeySecure ensures that organizations maintain ownership of their encryption keys at all times by hardening the appliance OS and enforcing encryption of the entire virtual appliance.

If you're an AWS customer, Try Virtual KeySecure **FREE for 30 days.**

CLICK HERE

amzn.to/1dpVBJO

Virtual KeySecure can be used for:

- Managing encryption keys and key policy for AWS EC2 deployed workloads encrypted with ProtectV
- Securely storing and managing keys for encrypting many on-premises storage solutions

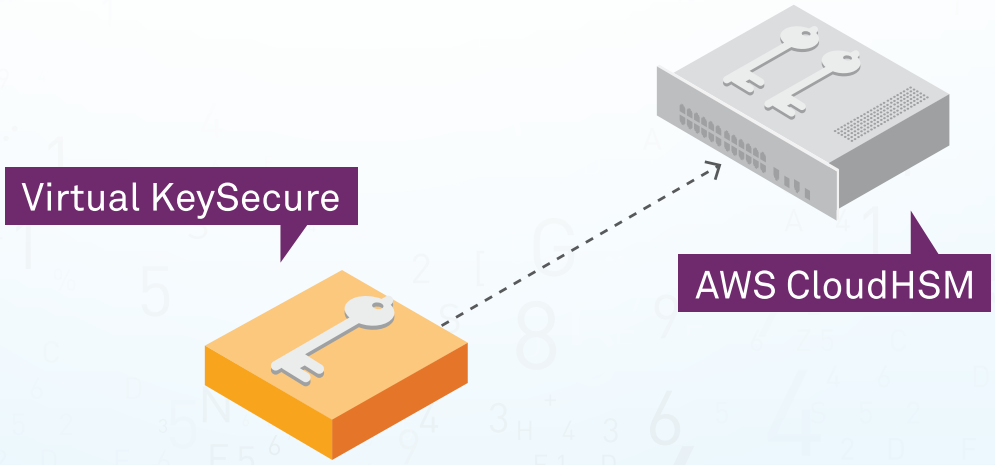
Virtual KeySecure ensures that organizations maintain ownership of their encryption keys at all times.

Using CloudHSM as a root of trust for 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's CloudHSM service, an optional hardware root of trust for encryption keys. AWS customers can easily configure Virtual KeySecure to store master keys in CloudHSM, a Luna SA hardware security module residing in the AWS cloud. The AWS CloudHSM can securely generate, provision, and store cryptographic resources for 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 Virtual KeySecure to store master keys in CloudHSM.



The value of KMIP

Today, many enterprises are suffering from encryption key creep— isolated silos of encryption deployments for various data layers scattered across workgroups, infrastructure elements, and locations. Each encryption silo has its own sets of keys, its own key policies and enforcement mechanisms, and may or may not support managing keys across their lifecycle. As industry analyst group Securosis writes, "The more diverse your keys, the better your security and granularity—but the greater the complexity" for managing all those keys.

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.

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, HP, IBM, Sepaton, CipherCloud, and more are KMIP-compliant. (See SafeNet's KeySecure interoperability page for more information.) And all of these solutions can have their keys securely stored and completely managed by Virtual KeySecure for AWS—no matter where those devices, services, and applications live.

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

Encryption and pre-boot authentication for EC2 and EBS

SafeNet ProtectV

SafeNet ProtectV, available on AWS Marketplace, enables organizations to unify encryption and control across virtualized and cloud environments, improving business agility and lowering costs by securely migrating even the most sensitive, highly regulated data to 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 encrypts entire virtual machine instances and attached storage volumes, while ensuring complete isolation of data and separation of duties. ProtectV also ensures that no virtual machine instance can be launched without proper authorization from 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.

ProtectV encrypts entire virtual machine instances and attached storage volumes.

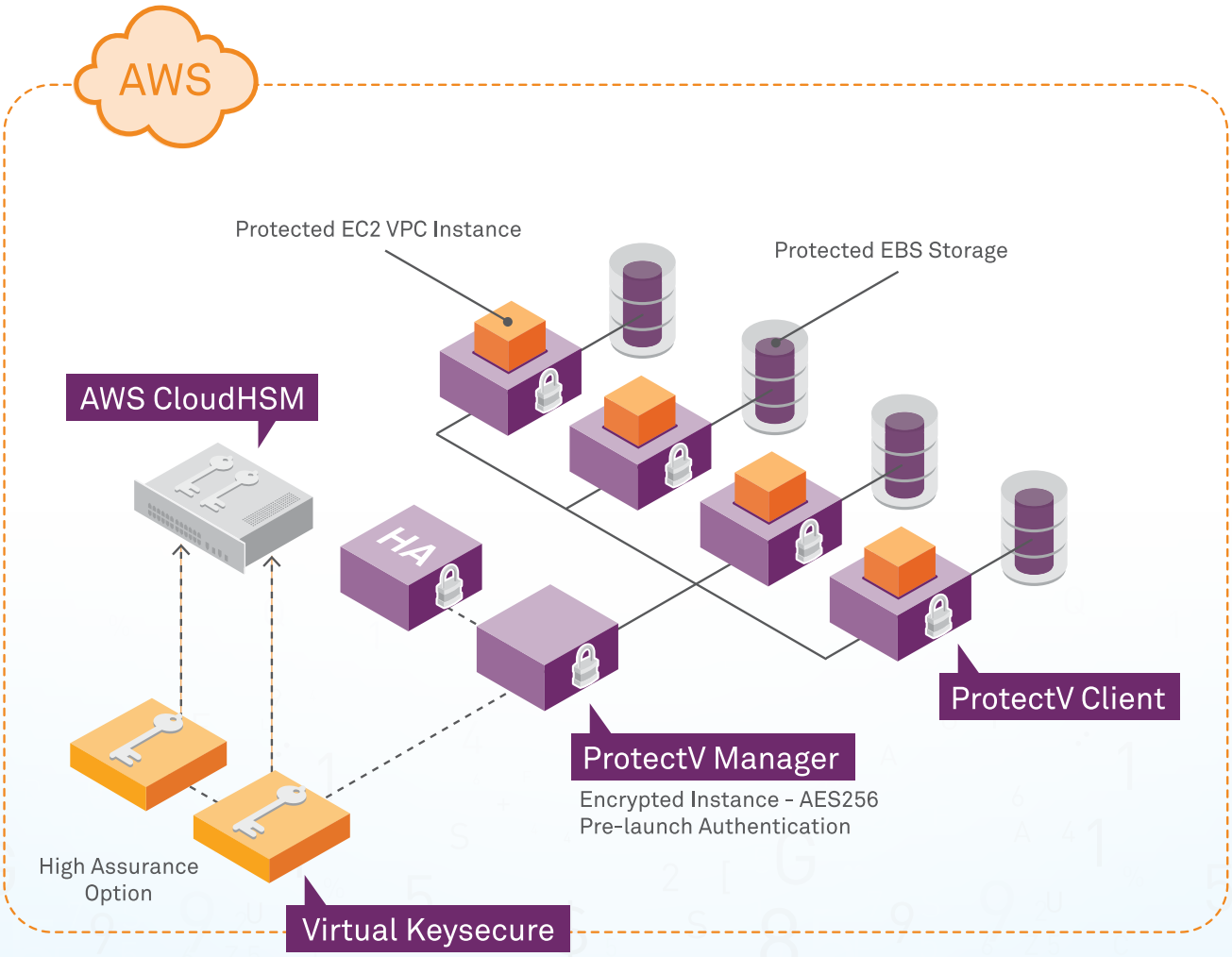
If you're an AWS customer, Try ProtectV **FREE for 30 days:**

- **5 Nodes** amzn.to/1gLPVBZ
- **25 Nodes** amzn.to/LOXgCZ
- **100 Nodes** amzn.to/1ewZeCr

ProtectV can be used for:

- Addressing compliance standards for cloud environments such as the PCI DSS cloud guidance
- Granular role-based control of who can start a virtual instance with pre-boot authentication
- Securing AWS-based instance and storage volume archives, including snapshots and backups
- Protecting sensitive workloads containing directory, intellectual property, payment card, and personally identifiable information

SafeNet ProtectV



Client-side object encryption for Amazon S3

SafeNet ProtectApp with AWS SDKs

SafeNet ProtectApp, when integrated with AWS SDKs, provides customer-controlled client-side object encryption for storage in Amazon's Simple Storage Service (S3). 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. SafeNet KeySecure—either on-premises or as a hardened virtual appliance run in an AWS EC2 environment—work with the SafeNet/AWS encryption client to store the cryptographic keys and offload cryptographic functions in order to encrypt data prior to archiving in S3 without impacting performance.

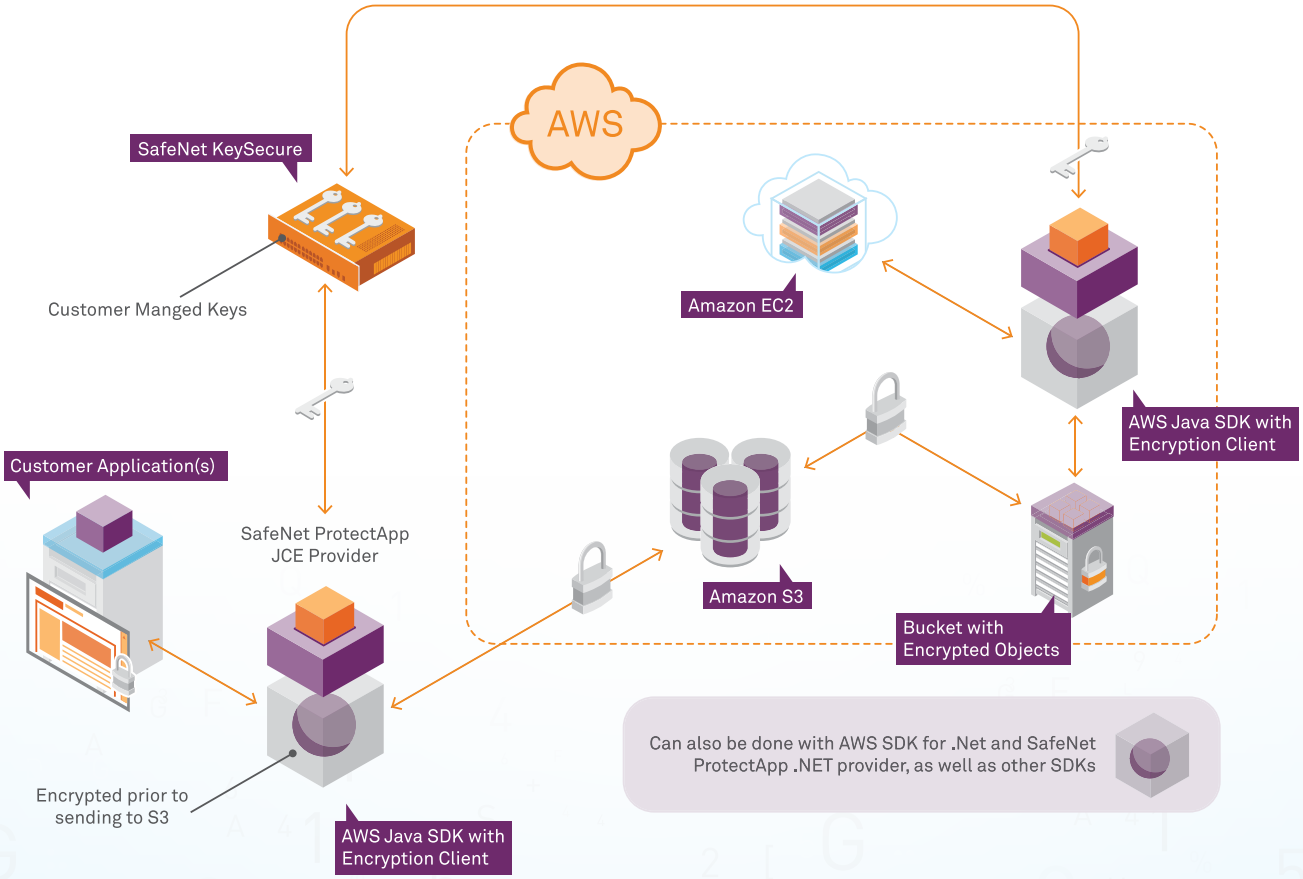
The SafeNet/AWS encryption client gives customers control of their data by encrypting it within the application before it is uploaded to S3. AWS customers can ensure their data will be unreadable by unauthorized users since encryption occurs in the customer's control before AWS storage receives the data and the KeySecure appliance protects the corresponding encryption keys. 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.

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

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 with AWS SDKs



Storage encryption for the AWS Storage Gateway

SafeNet StorageSecure

Today, cloud-based storage services like Amazon S3 present organizations with a compelling opportunity: a way to offload the expense and effort associated with managing storage infrastructure internally while enhancing flexibility and agility. Together with StorageSecure and KeySecure, AWS Storage Gateway enables organizations that manage sensitive data to fully leverage the benefits of Amazon S3 while retaining strict controls over data access.

The AWS Storage Gateway is a service that connects an on-premises software appliance with Amazon's cloud-based Simple Storage Service (Amazon S3), enabling organizations to establish a seamless and secure integration between their on-premises storage environment and Amazon S3. The AWS Storage Gateway empowers organizations to harness the cost savings and agility of cloud storage. SafeNet solutions enhance this AWS offering by encrypting sensitive and regulated data before committing it to cloud storage and providing for centralized key management of encrypted storage on premises and in the cloud.

The solution enables organizations that manage sensitive data to fully leverage the benefits of Amazon S3 while retaining strict controls over data access.

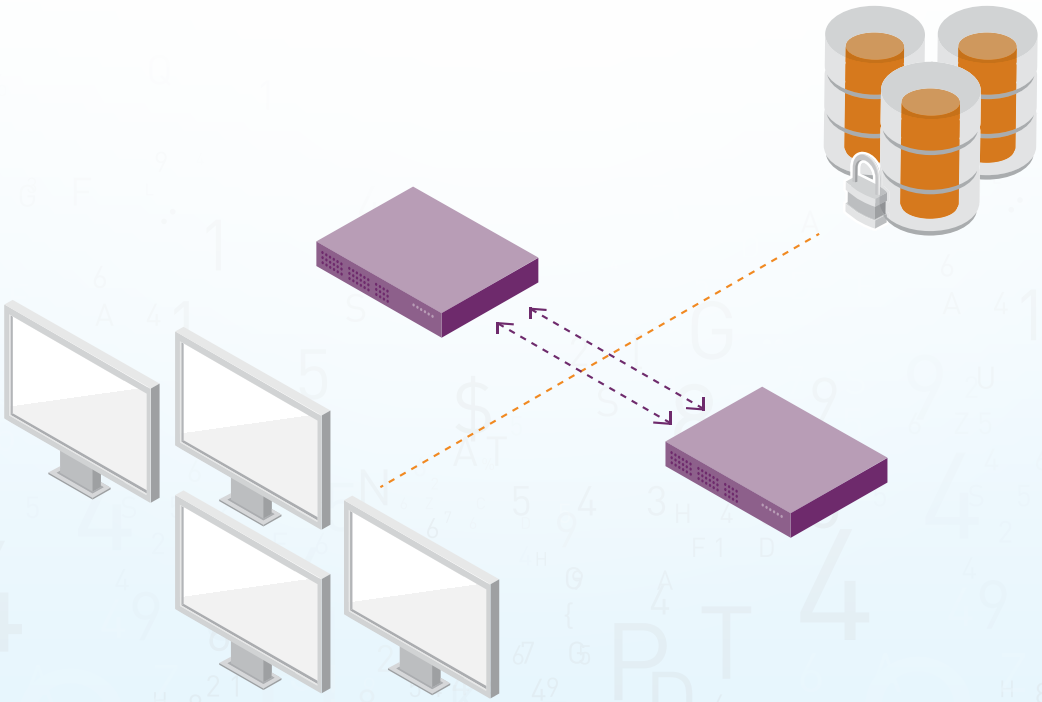
StorageSecure can be used for:

- Enhancing the security and providing granular encryption for AWS Secure Gateway and S3-based backup and archive

SafeNet StorageSecure

StorageSecure is a network encryption appliance that offers optimal protection of data at rest in physical, virtual, and cloud-based storage environments. StorageSecure is a transparent solution that can encrypt sensitive assets before they are saved to Amazon S3 environments. In addition to its iSCSI support, StorageSecure can also be integrated using CIFS, NFS, FTP, TFTP, and HTTP protocols. SafeNet KeySecure works in conjunction with StorageSecure. As a result, StorageSecure can copy encryption keys to KeySecure, providing centralized encryption key management with rich security policies, separation of duties, and audit logging.

When deployed, the AWS Storage Gateway appliance is installed on the customer's premises and is connected to StorageSecure through the iSCSI protocol. StorageSecure connects to the KeySecure appliance, which is used to store cryptographic keys. With StorageSecure connected to the AWS Storage Gateway, security teams can ensure that data is always encrypted before it leaves the organization's facilities for secure storage on Amazon S3. In addition, control of encryption keys never leaves the organization, allowing complete visibility and control over privileged access to the keys and to encrypted data.



File encryption for EC2 instances and S3

SafeNet ProtectFile

SafeNet ProtectFile provides data security with automated file encryption of unstructured data contained in network drives and file servers. ProtectFile is deployed in tandem with SafeNet DataSecure, and encrypts flat files that contain sensitive data, such as text documents, spreadsheets, bitmap images, and vector drawings. Encryption keys and policies are managed on the DataSecure appliance, improving security and reducing operational overhead. The solution combines encryption and access control policies to protect designated folders and files residing on file shares and network drives.

ProtectFile enables data-centric security by rendering files containing sensitive data useless to attackers. As opposed to systems that secure a perimeter or device, ProtectFile secures the data itself, ensuring that files are protected regardless of where files reside or where they are sent.

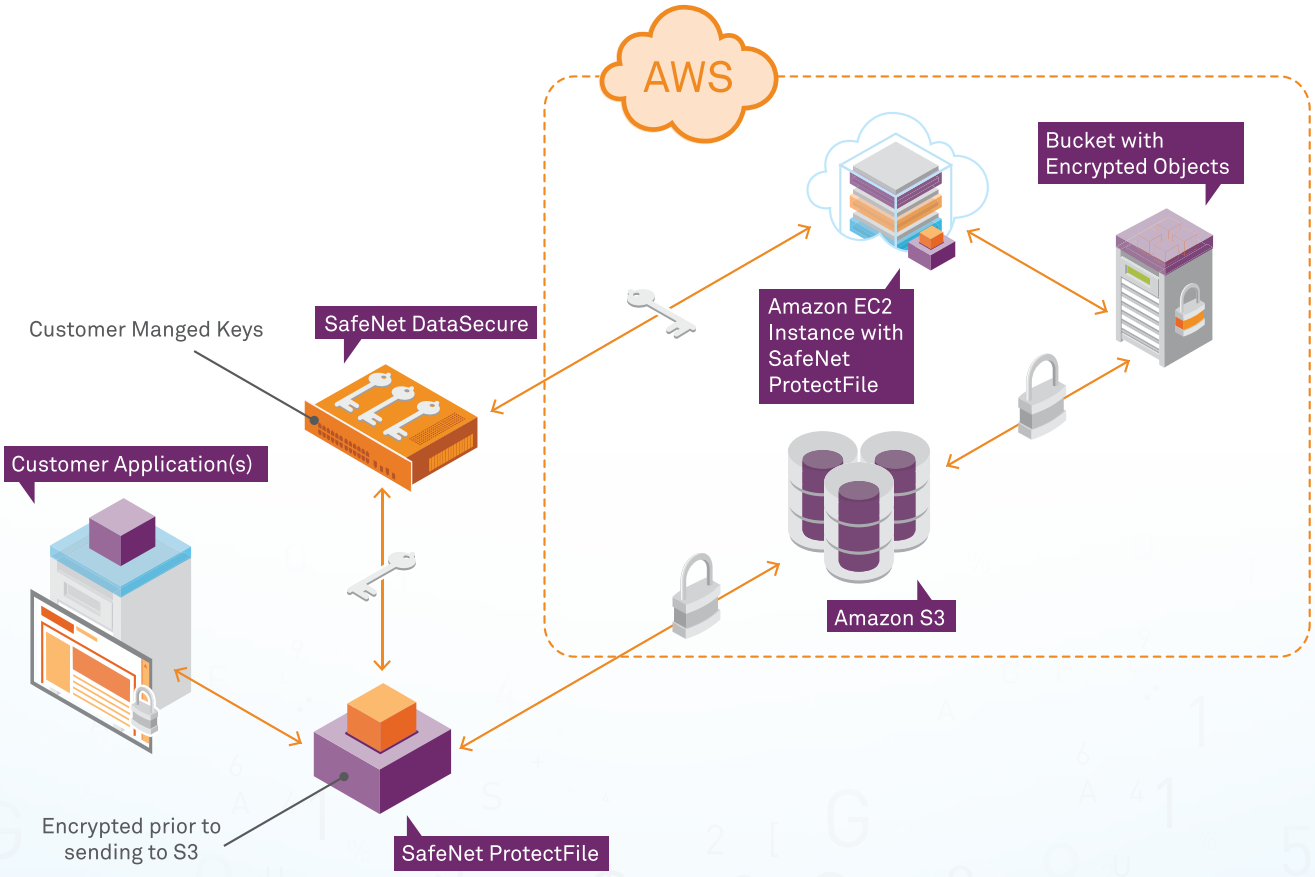
Administrators can set policies to encrypt particular folders and files, granting access only to authorized individuals or groups. When a folder is selected for protection, any file that is deposited in the folder is automatically encrypted.

ProtectFile can be used for:

- Securing sensitive data in a variety of file types
- Assuring that files are encrypted in Amazon EC2, Amazon S3, or on-premises

ProtectFile renders files containing sensitive data useless to attackers.

SafeNet ProtectFile



For more information

Helping to protect the confidentiality, integrity, and availability of customers' systems and data is of the utmost importance to AWS, as is maintaining customer trust and confidence.

SafeNet, a leading global provider of data protection, is an Advanced Technology Partner of AWS. For over 30 years, SafeNet has been securing and protecting the valuable data assets and intellectual property of Fortune 500 global corporations, government agencies, and other organizations.

SafeNet's data-centric approach for information stored in the AWS cloud focuses on the protection of high-value information throughout its lifecycle. Thousands of customers trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

ProtectV and Virtual KeySecure can be found on **AWS Marketplace.**

Try ProtectV **FREE for 30 days**

5 Nodes
amzn.to/1gLPVBZ

25 Nodes
amzn.to/LOXgCZ

100 Nodes
amzn.to/1ewZeCr

Try Virtual KeySecure
FREE for 30 days

CLICK HERE

amzn.to/1dpVBJO

AWS CloudHSM can be **purchased directly from AWS.**

More information about SafeNet and the SafeNet products mentioned in this ebook can be found on **SafeNet's website.**

6 ways to enhance security in **AWS** eBook
Febuary 2014