9 ways to enhance security in AWS
eBook
### Contents

#### Data security, encryption, and the cloud

- Value of the public cloud .......................................................... 3
- Securing sensitive data in the cloud ............................................. 4
- Don't just play it safe—keep it safe ............................................. 5
  - Data security in the AWS cloud environment
- The role of encryption and key management ............................. 7
- Not all encryption is created equal ............................................. 8
- Encryption and regulatory compliance ....................................... 9
- Storing data safely in the cloud with customer-owned encryption ............................................. 10
- The importance of secure key management ............................... 11

#### Nine solutions to enhance security

- Roots of trust ........................................................................... 13
  - What are roots of trust?
  - AWS CloudHSM
  - Hybrid models and backup options for AWS CloudHSM
  - Professional services
  - Customer-premises for SafeNet Luna SA HSM
  - Meeting compliance demands with SafeNet solutions
  - Application Integrations
- Key Management Solutions ....................................................... 22
  - SafeNet Virtual KeySecure
  - Using AWS CloudHSM as a root of trust for SafeNet Virtual KeySecure
  - The value of KMIP
- Encryption and pre-boot authentication for EC2 and EBS .............. 26
  - SafeNet ProtectV
- Customer-owned object encryption for Amazon S3 ..................... 28
  - SafeNet ProtectApp with AWS SDKs
- Storage encryption for AWS Storage Gateway ............................ 30
  - SafeNet StorageSecure
- File encryption for EC2 and S3 .................................................. 32
  - SafeNet ProtectFile
- Structured data encryption for EC2 .......................................... 34
  - SafeNet ProtectDB
- Tokenization ............................................................................ 36
  - SafeNet Tokenization
- Strong authentication for AWS WorkSpaces ............................. 38
  - SafeNet Authentication Service for AWS WorkSpaces

#### For more Information

- 37
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 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 five times the compute capacity of its fourteen nearest competitors1 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 SafeNet.

1 Source: Gartner, Magic Quadrant for Cloud Infrastructure as a Service, May 28, 2014. 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 storage offers customers increased flexibility and availability as well as decreased costs, data owners must be able to demonstrate compliance and illustrate control of sensitive information stored in the cloud. As data owners, organizations are often 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 safe the sensitive data stored in cloud environments.
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 SafeNet. As an Advanced Technology Partner, SafeNet 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 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.
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. Customer-owned encryption—combined with strong key management that also is customer-controlled—is what makes encryption a core safety mechanism for protecting data in the cloud.

### AWS and SafeNet Encryption Options for Amazon EC2

<table>
<thead>
<tr>
<th>TYPE OF ENCRYPTION</th>
<th>DEFINITION</th>
<th>NOTES</th>
<th>MEETS SECURITY REQUIREMENTS?</th>
<th>ARE YOU STILL AT RISK?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EBS Server-Side Encryption</td>
<td>Cloud Service Provider (CSP) Encryption with CSP-Managed Keys</td>
<td>AKA Server-Side Encryption (SSE). The CSP is doing both the encryption and the key management. It’s often free or cheap.</td>
<td>No. Customer does not own or control keys or data.</td>
<td>Yes: to rogue administrators, CSP misconfigurations, subpoenas, SSL attacks, and access vulnerabilities.</td>
</tr>
<tr>
<td>Amazon EBS Encryption with AWS Key Management Service (KMS)</td>
<td>CSP Encryption with Customer-Managed Keys</td>
<td>The customer must manage all encryption keys. These keys are often limited for use only within the CSP environment.</td>
<td>No. Customer does not own keys or data.</td>
<td>Yes: to CSP misconfigurations and subpoenas.</td>
</tr>
<tr>
<td>SafeNet ProtectV with KeySecure/Virtual KeySecure (and optional CloudHSM)</td>
<td>Customer-Owned Encryption with Customer-Owned Keys</td>
<td>AKA Client-Side Encryption. The customer can prove ownership of the encryption keys and data— at all times.</td>
<td>Yes. Customer can prove ownership and control of data—at all times.</td>
<td>Unlikely.</td>
</tr>
</tbody>
</table>

---

**Table of Contents >>**
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 management¹ to:

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

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

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.
Storing data safely in the cloud with customer-owned encryption

There are many business benefits of cloud storage. Cloud service providers offer a wide range of products with significant cost savings, accelerated innovation, enhanced agility, and more. Still, many enterprises question how sensitive data can be safely 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 will not only 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 also be able to meet many compliance mandates and security regulations.

Three Rules for Encrypting Data Stored in the Cloud

👉 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.

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

👉 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 cost. Additionally, keys often are stored and managed insecurely; for example, some organizations store their keys in spreadsheets on USB drives. 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 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 yields 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 is often 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 SafeNet Key Management Options in AWS

<table>
<thead>
<tr>
<th></th>
<th>Who controls access to key?</th>
<th>FIPS 140-2 validation</th>
<th>Integration with AWS services</th>
<th>Integration outside AWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Key Management Service (KMS)</td>
<td>AWS</td>
<td>No</td>
<td>Amazon S3, Amazon EBS, RedShift, custom applications</td>
<td>Custom applications with keys stored in AWS</td>
</tr>
<tr>
<td>SafeNet Virtual KeySecure in AWS Marketplace</td>
<td>Customer</td>
<td>Level 1</td>
<td>Amazon EC2 instances and EBS volumes with ProtectP; S3 with Protect Ap; KMIP-based endpoints; custom applications; SafeNet key management partner ecosystem: <a href="http://www.safenet-inc.com/partners/technology-partner-search">www.safenet-inc.com/partners/technology-partner-search</a></td>
<td>Yes! Hybrid deployment with Virtual KeySecure for VMWare scenarios and open standards (e.g., KMIP)</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>Customer (in AWS, on an HSM that the customer controls)</td>
<td>Level 2</td>
<td>Redshift, custom applications, SafeNet's HSM partner ecosystem: <a href="http://www.safenet-inc.com/partners/technology-partner-search">www.safenet-inc.com/partners/technology-partner-search</a></td>
<td>Hybrid deployments with customer premise SafeNet Luna SA HSMs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Keys</th>
<th>10</th>
<th>500</th>
<th>1,000</th>
<th>25,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Key Management Service (KMS)</td>
<td>$120/yr**</td>
<td>$6,000/yr**</td>
<td>$12,000/yr**</td>
<td>$300,000/yr**</td>
</tr>
<tr>
<td>SafeNet Virtual KeySecure in AWS Marketplace</td>
<td>$5,472/yr**</td>
<td>$5,472/yr**</td>
<td>$5,472/yr**</td>
<td>$5,472/yr**</td>
</tr>
<tr>
<td>AWS CloudHSM (256-bit AES keys)</td>
<td>$21,481/yr****</td>
<td>$21,481/yr****</td>
<td>$21,481/yr****</td>
<td>$42,962/yr****</td>
</tr>
</tbody>
</table>

*Approximate cost. Usage costs are not included.
**Approximate cost based on annual pricing with reserved instance per KeySecure instance.
***Approximate cost per CloudHSM instance.
SafeNet offers solutions for protecting sensitive data within the AWS platform. This ebook will discuss six solutions that enhance security in AWS infrastructure.

<table>
<thead>
<tr>
<th>Solution</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Roots of trust</td>
<td>13</td>
</tr>
<tr>
<td>2. Key Management Solutions</td>
<td>22</td>
</tr>
<tr>
<td>3. Encryption and pre-boot authentication for EC2 and EBS</td>
<td>26</td>
</tr>
<tr>
<td>4. Customer-owned object encryption for Amazon S3</td>
<td>28</td>
</tr>
<tr>
<td>5. Storage encryption for AWS Storage Gateway</td>
<td>30</td>
</tr>
<tr>
<td>6. File encryption for EC2 and S3</td>
<td>32</td>
</tr>
<tr>
<td>7. Structured data encryption for EC2</td>
<td>34</td>
</tr>
<tr>
<td>8. Tokenization</td>
<td>36</td>
</tr>
<tr>
<td>9. Strong authentication for AWS WorkSpaces</td>
<td>38</td>
</tr>
</tbody>
</table>
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)¹, 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 in implementing hardware-based roots of trust when the cloud is so dependent on the virtualization and functionality that is often completely defined by software. SafeNet and AWS have worked together to address the problem in several important ways.

**AWS CloudHSM**

AWS CloudHSM uses SafeNet Luna SA 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. CloudHSMs can be deployed in a high-availability configuration across multiple Availability-Zones (AZs) and regions to improve availability and performance.

For product details and pricing, visit the [AWS CLOUDHSM](#) page.

Click Here

**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

With CloudHSM, customers can securely generate, store, and manage cryptographic keys.
Hybrid models and backup options for AWS CloudHSM

Because the AWS CloudHSM does not have access to customer keys, customers are strongly encouraged to back up their keys with an additional appliance. As an option, customers can back up the contents of up to 20 CloudHSM partitions to a SafeNet 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 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 failure of the AWS CloudHSM, 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/
AWS CloudHSM

A. AWS manages the CloudHSM appliances but does not have access to your customer-owned 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 consulting and professional services provide support throughout the product lifecycle by helping customers develop and maintain their security posture. Dedicated HSM consulting teams design the technical implementations; provide project management and development resources; and configure HSM security, access, and backup policies. Professional services includes comprehensive, customized, multi-day, and hands-on product training to ensure that customers are well-prepared to manage their enterprise key management system once the HSM implementation team finishes with the infrastructure setup.
Customer-premises for SafeNet Luna SA HSM

SafeNet Luna SAs 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 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 3) 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 Luna SA, Click Here
SafeNet 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 or 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 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 the data.

- **Secure key storage:** SafeNet Luna SA and CloudHSMs 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.

- **Virtualization attacks:** SafeNet 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 manage the encryption keys and can combine with ProtectV to ensure secure, controlled access to virtual environments.
Meeting compliance demands (continued)

- **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:** KeySecure and Virtual KeySecure centralize encryption key management from one platform to improve security through streamlined efficiency. SafeNet 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, ProtectApp, ProtectDB, ProtectFile, and Tokenization Manager 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) 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 SafeNet Luna SA HSM or an AWS CloudHSM.

Amazon RDS

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, Perspecsys, and others that can store the encryption keys in SafeNet KeySecure or the SafeNet Luna SA HSM (depending on the integration level).

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

Safenet 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.
SafeNet Virtual KeySecure

SafeNet Virtual KeySecure centralizes key management for multiple use cases using a hardened virtual appliance that runs in the AWS Cloud. The combination of Virtual KeySecure and 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.

By encrypting the application and operating systems on the hardened virtual appliance, Virtual KeySecure renders the information tapproof—ensuring protection and control of sensitive data at rest stored or pushed to the AWS Cloud. Virtual KeySecure works alongside SafeNet’s encryption solutions to support a wide variety of use cases that increase security and address compliance mandates. For example, Virtual KeySecure can be deployed with ProtectV to secure sensitive data residing in AWS EC2 instances and AWS EBS volumes or with 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 ProtectV’s capability for cloud bursting and back-up. 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.

If you are an AWS customer, try Virtual KeySecure on AWS Marketplace FREE for 30 days. Click Here
SafeNet Virtual KeySecure can be used to:

- Securely store and manage encryption keys for:
  - AWS EC2 instances with SafeNet ProtectV, ProtectDB, Tokenization Manager, and ProtectFile
  - Amazon EBS volumes with SafeNet ProtectV
  - Amazon S3 with SafeNet ProtectApp and ProtectFile
  - SafeNet Key Management Partner Ecosystem, including storage from NetApp, Dell, IBM, HP, Hitachi, and more
  - Cloud Encryption Gateways
  - KMIP-based endpoints
  - Custom Applications
- Prove customer ownership of encryption keys—no one but the customer has access
  - Ensuring 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 PCI DSS, HIPAA, Sarbanes-Oxley (SOX), and GLBA
  - FIPS 140-2 validation
- Support hybrid and multi-cloud deployments

To learn more about Virtual KeySecure, contact a SafeNet representative.
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 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 SafeNet Virtual KeySecure to store master keys in AWS CloudHSM.
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 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.”

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.

https://securosis.com/assets/library/reports/Understanding_and_Selecting_a_Key_Management_Solution.final.pdf
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. 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.

SafeNet ProtectV 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 can be used for:

- 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
- Addressing compliance standards for cloud environments such as PCI DSS, SOX, and HIPAA/HITECH
- Granular role-based control of who can start a virtual instance with pre-boot authentication

Try ProtectV on AWS Marketplace FREE for 30 days.

Click Here

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Click Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
SafeNet ProtectV

To learn more about ProtectV, contact a SafeNet representative.
**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—works 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 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

To learn more about ProtectApp contact a SafeNet representative.
SafeNet StorageSecure

Today, cloud-based storage services like Amazon Simple Storage Service (S3) present organizations with a compelling opportunity to offload the expense and effort associated with managing storage infrastructure internally while enhancing flexibility and agility.

The AWS Storage Gateway is a service that securely connects an on-premises software appliance with Amazon’s cloud-based Amazon S3. Together with SafeNet StorageSecure and SafeNet 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 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 SafeNet 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 protects data at rest

SafeNet 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 SafeNet 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.

To learn more about StorageSecure contact a SafeNet representative.
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 KeySecure and encrypts files that contain sensitive data such as text documents, spreadsheets, bitmap images, databases, and vector drawings. Encryption keys and policies are managed on the KeySecure appliance, improving security and reducing operational overhead. The solution provides a single interface for logging, auditing, and reporting access to protected data and encryption keys. SafeNet ProtectFile also features built-in, automated key rotation and data re-keying, a critical feature for compliance and data protection.

SafeNet 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 they 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 with KeySecure is a highly-scalable solution that works across multiple data centers in the distributed enterprise.
SafeNet ProtectFile

ProtectFile encrypts sensitive data. Data is pushed to S3 using AWS tools.

To learn more about ProtectFile, contact a SafeNet representative.
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. ProtectDB is extremely scalable and works across multiple data centers in distributed enterprises.

Deployed in tandem with SafeNet KeySecure hardware or virtual appliance, ProtectDB offers centralized key and policy management to ensure encrypted data remains secure throughout its lifecycle. The solution provides a single interface for logging, auditing, and reporting access to protected data and encryption keys, a critical feature for compliance and data protection. SafeNet ProtectDB features built-in, automated key rotation and data re-keying, a critical feature for compliance and data protection. The highly-scalable solution 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).

SafeNet ProtectDB can be used to:

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

Application Servers (AWS EC2)

Database Server (AWS EC2)

SafeNet Virtual KeySecure Cluster

ProtectDB provides transparent, column-level encryption

Customer Owned Keys

To learn more about ProtectDB, contact a SafeNet representative.
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. 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
Tokenization

To learn more about Tokenization, contact a SafeNet representative.
SafeNet Authentication Service for AWS WorkSpaces

SafeNet Authentication Service is a cloud-based authentication service that offers multi-factor authentication solutions, protecting identities and ensuring 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.

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.

As a trusted identity provider, SafeNet adds strong authentication to Amazon WorkSpaces offering enterprises the best of cloud-based services for both security and virtual computing.

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 SafeNet representative.
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 SafeNet solutions, customers can safely secure their data in AWS environments by owning their encryption and encryption keys.

SafeNet, a leading global provider of data protection, is an AWS Advanced Technology Partner. 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 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 SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments. SafeNet ProtectV and Virtual KeySecure can be purchased on AWS Marketplace or directly from SafeNet with a bring-your-own-license (BYOL) option.

AWS CloudHSM can be purchased directly from AWS.

More information about SafeNet and the SafeNet products mentioned in this ebook can be found on the SafeNet website: http://www.safenet-inc.com

To contact a SafeNet representative for product information and purchase options, visit http://www.safenet-inc.com/request-information/.

If you are an AWS customer, try Virtual KeySecure on AWS Marketplace FREE for 30 days Click Here

If you are an AWS customer, try ProtectV on AWS Marketplace FREE for 30 days Click Here