Secure the AWS Cloud with SafeNet Solutions eBook
# Table of Contents

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 ..........................................................................................6
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
SafeNet Solutions to Secure the AWS Cloud ..........................................................................................13

## Roots of trust

<table>
<thead>
<tr>
<th>What are roots of trust?</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS CloudHSM</td>
<td>15</td>
</tr>
<tr>
<td>Hybrid models and backup options for AWS CloudHSM</td>
<td>16</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>17</td>
</tr>
<tr>
<td>Professional services</td>
<td>18</td>
</tr>
<tr>
<td>Customer-premises SafeNet HSM</td>
<td>19</td>
</tr>
<tr>
<td>Meeting compliance demands with Gemalto solutions</td>
<td>20</td>
</tr>
<tr>
<td>Application Integrations</td>
<td>21</td>
</tr>
</tbody>
</table>

## Key management solutions

<table>
<thead>
<tr>
<th>SafeNet Virtual KeySecure</th>
<th>22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using AWS CloudHSM as a root of trust for SafeNet Virtual KeySecure</td>
<td>24</td>
</tr>
<tr>
<td>Remote Cloud HSM Management with SafeNet Crypto Command Center</td>
<td>25</td>
</tr>
<tr>
<td>The value of KMIP</td>
<td>26</td>
</tr>
</tbody>
</table>

## Encryption and pre-boot authentication for EC2 and EBS

| SafeNet ProtectV | 27 |

## Customer-owned object encryption for Amazon S3

| SafeNet ProtectApp | 29 |

## File encryption for EC2 and S3

| SafeNet ProtectFile | 31 |

## Structured data encryption for EC2

| SafeNet ProtectDB | 33 |

## Tokenization

| SafeNet Tokenization | 35 |

## Strong Authentication for AWS

| SafeNet IDProve for AWS Management Console | 37 |
| SafeNet Authentication Service for AWS WorkSpaces | 38 |

For more information ...........................................................................................................................39
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 Gemalto.

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

---

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 the sensitive data stored in cloud environments safe.
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.

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.
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. Customer-owned encryption—combined with strong key management that is also customer-controlled—is what makes encryption a core safety mechanism for protecting data in the cloud.

AWS and Gemalto 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><strong>Amazon EBS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Server-Side</strong></td>
<td>Encryption performed by the CSP using encryption keys owned and managed by the CSP.</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></td>
</tr>
<tr>
<td><strong>Encryption with AWS Key Management Service (KMS)</strong></td>
<td>Encryption performed by the CSP using encryption keys managed by the customer, but owned by the CSP.</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><strong>SafeNet ProtectIV with KeySecure/Virtual KeySecure (and optional CloudHSM)</strong></td>
<td>Customer-Owned Encryption with Customer-Owned Keys</td>
<td>Encryption performed by the customer using encryption keys owned and managed by the customer.</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>
</tr>
</tbody>
</table>
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.

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://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 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

<table>
<thead>
<tr>
<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>
</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 ProtectIV; S3 with Protect App; 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>
</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>
</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>$4,000/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 Solutions to Secure the AWS Cloud

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

<table>
<thead>
<tr>
<th>Topics</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roots of trust</td>
<td>14</td>
</tr>
<tr>
<td>Key management solutions</td>
<td>22</td>
</tr>
<tr>
<td>Encryption and pre-boot authentication for EC2 and EBS</td>
<td>27</td>
</tr>
<tr>
<td>Customer-owned object encryption for Amazon S3</td>
<td>29</td>
</tr>
<tr>
<td>File Encryption for EC2 and S3</td>
<td>31</td>
</tr>
<tr>
<td>Structured data encryption for EC2</td>
<td>33</td>
</tr>
<tr>
<td>Tokenization</td>
<td>35</td>
</tr>
<tr>
<td>Strong Authentication for AWS</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), 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.

---

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.

**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](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 with an additional appliance. As an option, customers can back up the contents of up to 20 CloudHSM partitions to a SafeNet backup HSM located on their own premises. With the SafeNet 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 SafeNet HSM appliance.

Hybrid implementations that combine 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 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.

4 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, 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 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 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 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 or 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. Infrastructure administrators can maintain their storage or virtual environments without ever having access to the data.

- **Secure key storage:** SafeNet HSM 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. 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 control.

- **Data security through encryption and key deletion:** SafeNet KeySecure, SafeNet ProtectV, SafeNet ProtectApp, SafeNet ProtectDB, SafeNet ProtectFile, and SafeNet 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 and 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 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 HSM (depending on the integration level).

SafeNet HSM 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 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/1dpVBJO
SafeNet Virtual KeySecure can be used to:

- Securely store and manage encryption keys for
  - AWS EC2 instances with SafeNet ProtectV, SafeNet ProtectDB, SafeNet Tokenization Manager, and SafeNet ProtectFile
  - Amazon EBS volumes with SafeNet ProtectV
  - Amazon S3 with SafeNet ProtectApp and SafeNet 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
  - 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 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.

http://www.safenet-inc.com/request-information/
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 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 Cloud HSM Management with SafeNet Crypto Command Center

SafeNet Crypto Command Center remotely administers CloudHSMs hosted on AWS, enabling enterprises and service providers to provide encryption as a service 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.

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.

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

To learn more about SafeNet Crypto Command Center, contact a Gemalto representative. http://www.safenet-inc.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. 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.

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

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

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

To learn more about SafeNet ProtectV, contact a Gemalto representative.

http://www.safenet-inc.com/request-information/
SafeNet ProtectApp

Client-side object encryption for Amazon S3 with 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). 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.

SafeNet KeySecure—either on-premises or as a hardened virtual appliance hosted in the AWS cloud—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 SafeNet 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.

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.
http://www.safenet-inc.com/request-information/
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 datacenters 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

Customer Managed Keys

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

To learn more about SafeNet ProtectFile, contact a Gemalto representative.
http://www.safenet-inc.com/request-information/

SafeNet ProtectFile with SafeNet Virtual KeySecure

Customer Managed Keys

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

To learn more about SafeNet ProtectFile, contact a Gemalto representative.
http://www.safenet-inc.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.

http://www.safenet-inc.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.
http://www.safenet-inc.com/request-information/
SafeNet IDProve for AWS Management Console

Your AWS Management Console and AWS Service APIs are powerful tools that can control many facets of your 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 IDProve 100 (OTP Token)**

The IDProve 100 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 IDProve 700 (OTP Display Card)**

The IDProve 700 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 your 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. [http://www.safenet-inc.com/request-information/](http://www.safenet-inc.com/request-information/)

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 Gemalto representative. http://www.safenet-inc.com/request-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.


> To contact a Gemalto representative for SafeNet product information and purchase options, visit [http://www.safenet-inc.com/request-information/](http://www.safenet-inc.com/request-information/).

> If you are an AWS customer, try SafeNet Virtual KeySecure on AWS Marketplace FREE for 30 days [http://amzn.to/1dpVBJ0](http://amzn.to/1dpVBJ0)

> If you are an AWS customer, try SafeNet ProtectV on AWS Marketplace FREE for 30 days [http://amzn.to/1NX1Bl9](http://amzn.to/1NX1Bl9)
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.