



SOLUTION BRIEF

# Securing Sensitive Workloads in the AWS Cloud

## The Business Problem

When organizations are running business-critical applications or storing and accessing sensitive data, they often need rapid access to flexible and low-cost IT resources. Cloud services from Amazon Web Services (AWS) provide the agility, elasticity, capacity, and redundancy required to maintain a competitive advantage in the market. On-demand delivery of these IT resources, with pay-as-you-go pricing, has convinced many organizations to create their servers in or move existing servers to the AWS cloud—with substantial cost and efficiency benefits.

Some applications and data require additional security due to rigorous contractual or regulatory requirements. Until now, companies had to store sensitive data (and/or the encryption keys protecting it) in on-premise data centers. Unfortunately, this either prevented migration of these applications to the AWS cloud or significantly slowed their performance.

## Solution

Today, AWS and Gemalto have teamed up to provide protection for virtual machines, storage volumes, and encryption keys in the AWS cloud that is as secure as physical servers and storage in the most robust, secure on-premise environment.

SafeNet ProtectV and SafeNet Virtual KeySecure from Gemalto and CloudHSM from AWS makes sure your sensitive workloads can migrate to the AWS cloud—no matter what level of security is needed. Best of all, the entire solution stack is available for purchase from AWS.

## The Components

### ProtectV

ProtectV, available on AWS Marketplace, secures your data in the cloud, encrypts entire virtual machine instances and

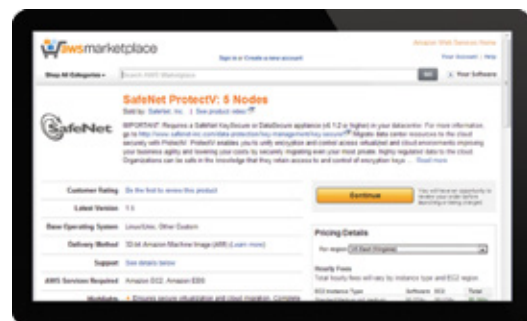
## Key Features

### Complete virtual machine and storage encryption:

- > Enables encryption of entire virtual machines and the storage volumes associated with them
- > No data is written to system partition or storage volume disk without first being encrypted
- > Even data stored in the OS partition is protected
- > Complete encryption and key management solution can be purchased on AWS Marketplace and run completely in the AWS cloud (EC2 or VPC)

### Only high-assurance solution for data compliance in the cloud:

- > Undisputed command and proof of ownership for data and keys
- > Only authorized individuals can launch AMIs
- > Prevents unauthorized data exposure or superuser abuse
- > Helps meet a range of regulations, such as PCI and HIPAA



attached storage volumes, and ensures 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.

## Virtual KeySecure

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

## AWS CloudHSM

SafeNet KeySecure from Gemalto is the only solution to optionally provide a hardware root of trust for encryption keys in support of the AWS CloudHSM service, available directly from AWS. Only your organization has access to the keys stored in CloudHSM—AWS has no ability to view or access the keys. The AWS CloudHSM service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated hardware security module (HSM) appliances within the AWS cloud. The AWS CloudHSM service allows you to protect your encryption keys within HSMs designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you. AWS CloudHSM helps you comply with strict key management requirements without sacrificing application performance.

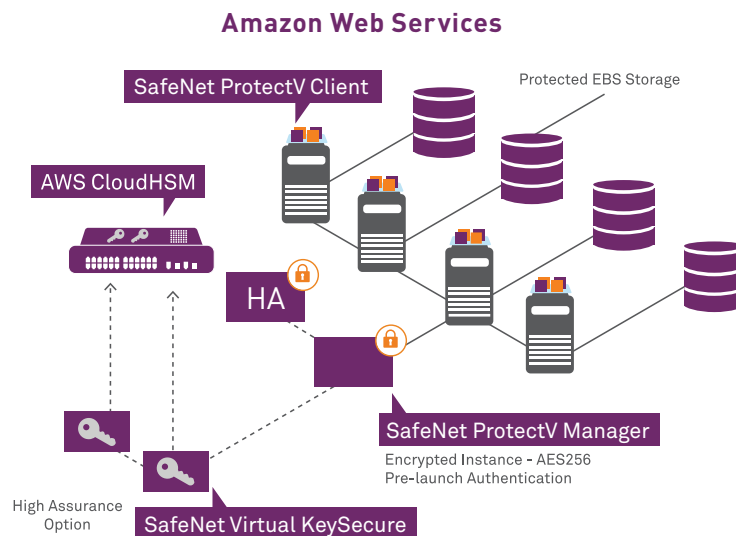
## Key Features

### Enterprise key lifecycle management with government-grade assurance:

- > The only solution that stores encryption keys in a high-assurance hardware-based key vault hosted by AWS
- > Only your organization has access to the keys in CloudHSM— AWS has no ability to view or access

## About Gemalto's SafeNet Identity and Data Protection Solutions

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



**Contact Us:** For all office locations and contact information, please visit [www.safenet-inc.com](http://www.safenet-inc.com)

**Follow Us:** [data-protection.safenet-inc.com](https://data-protection.safenet-inc.com)

[GEMALTO.COM](http://GEMALTO.COM)

**gemalto**  
security to be free