gemalto
security to be free

SafeNet ProtectV™

Ensuring Security and Compliance in the Cloud

SafeNet ProtectV™ provides full disk encryption of virtual machine instances so you can securely run even your most sensitive workloads or any highly regulated data in the cloud. Whether using Amazon Web Services, Microsoft Azure, IBM Cloud, or VMware, SafeNet ProtectV ensures cloud-enabled security.

The industry's first comprehensive high-availability solution for protecting data across virtual and cloud infrastructures, SafeNet ProtectV encrypts entire virtual machine instances and attached storage volumes, keeping your data safe from unauthorized access. In addition, no virtual machine instance can be launched without proper authorization from SafeNet ProtectV StartGuard™ pre-boot authentication.
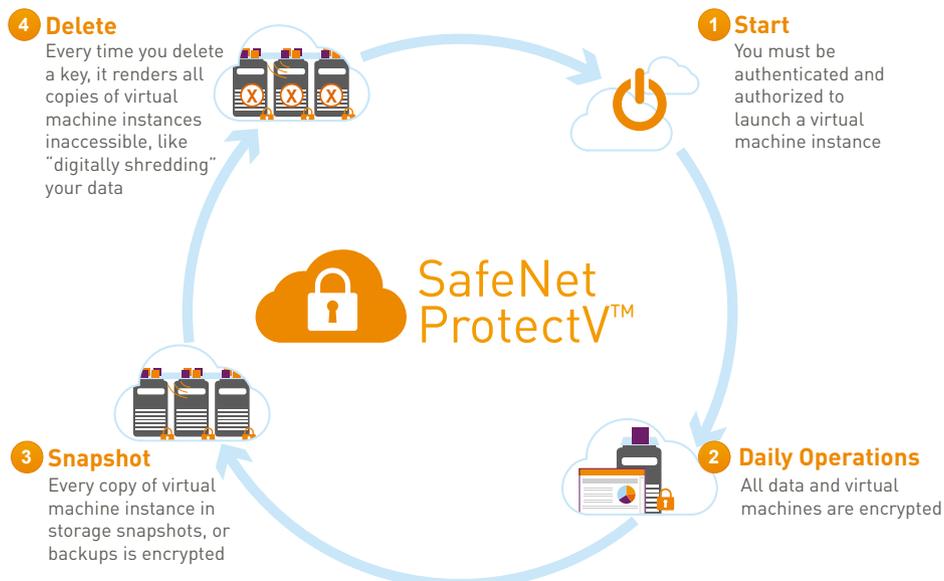
With SafeNet ProtectV's unified encryption and access control, your organization can be safe knowing that you retain access to and control of your encrypted data and keys at all times. In addition, you can enhance your business agility and take advantage of the lower costs inherent in virtual environments.
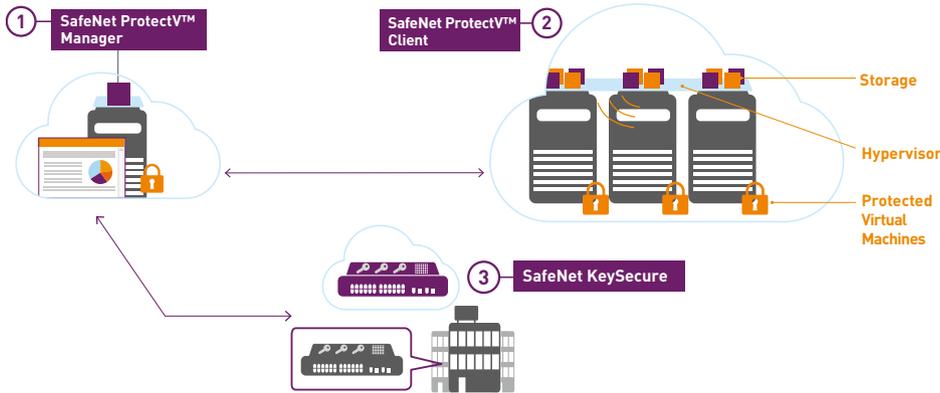
SafeNet ProtectV empowers you to secure your data and prove compliance in cloud-enabled environments

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

Together with SafeNet KeySecure, SafeNet ProtectV provides a highly available encryption solution to address numerous industry security standards and government regulations such as PCI DSS and HIPAA HITECH. Regardless of where your workload resides, you can separate security administration duties, enforce granular controls and establish clear accountability with audit trails and detailed compliance reporting.

SafeNet ProtectV Secures the Entire Virtual Machine Instance Lifecycle

4 Delete
Every time you delete a key, it renders all copies of virtual machine instances inaccessible, like "digitally shredding" your data

1 Start
You must be authenticated and authorized to launch a virtual machine instance

3 Snapshot
Every copy of virtual machine instance in storage snapshots, or backups is encrypted

2 Daily Operations
All data and virtual machines are encrypted

SafeNet ProtectV™

1 SafeNet ProtectV Manager – Centralized console for managing encrypted virtual machine instances, security admin profiles, and policies.

2 SafeNet ProtectV Client – Installed on virtual machine instances, or physical servers, the Client enforces pre-boot authentication based on associated ProtectV Manager security policies and encrypts data as it is written to storage.

3 SafeNet KeySecure – Highly available enterprise key management solution to manage the lifecycle for all key types across your data centers, private and public clouds. Delivered as a hardware appliance or as a hardened virtual security appliance that can be deployed on premises or in the cloud.

Protect Your Data in Cloud-Enabled Environments

> Comprehensive data protection and security policy management for virtual and cloud infrastructure

> Single pane of glass for controlling and monitoring your data in the cloud

> Supports Windows and Linux operating systems

Ensure Compliance in the Cloud

> Maintain compliance requirements across cloud-enabled infrastructure

> Decouple compliance requirements from infrastructure requirements to maximize business agility without compromising regulatory compliance

SafeNet Identity and Data Protection Solutions

Cloud-enabled security solutions, like all enterprise security, need to be managed in a layered approach to the information protection lifecycle that combines encryption, access policies, key management, content security, and authentication. These layers need to be integrated into a flexible framework that allows the organization to adapt to the risk it faces, wherever the data resides across the data center, hybrid and cloud environments.

Wherever data resides, Gemalto offers persistent, secured storage for structured and unstructured data. Gemalto provides a practical framework for delivering the trust, security, and compliance enterprises demand when moving data, applications and systems to the virtual environments and the cloud.

To learn more about Gemalto's complete portfolio of SafeNet Identity and Data Protection solutions, please visit our website at www.gemalto.com.

Technical Specs

Cloud Platforms Supported

> Amazon: Amazon EC2, Amazon VPC, Amazon GovCloud

> VMware vSphere

> Microsoft Azure

> IBM Cloud: IBM Bare Metal and SoftLayer VMs

Minimal System Requirements:
SafeNet ProtectV Manager:

> AWS: m3.medium and larger (for production environments) /1 volume (auto created / 8 GB)

> VMware: Ubuntu (Linux 64 bit), 2vCPUs, 4GB memory (minimum), 1 NIC (VMXNET 3), 16GB disk

SafeNet ProtectV Client:

> AWS: m1.small or larger instance, 256MB RAM, 100MB free disk space

> VMware: 256MB RAM, 100MB free disk space

Client OS Support*

> Microsoft Windows Server

> CentOS

> Oracle Linux

> Red Hat Enterprise Linux (RHEL)

> SUSE Linux Enterprise Server (SLES)

> Ubuntu

*Refer to our website or Customer Release Notes for the latest technical specifications and supported versions.

Available now on:

Buy and run on Amazon EC2
awsmarketplace

Windows Azure Marketplace

IBM Cloud

amazon webservices™

Microsoft Azure

vmware®

BLOCK READY

IBM

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

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free