PRODUCT BRIEF

SafeNet ProtectV™

Ensuring Security and Compliance Across Cloud-Enabled Environments

SafeNet ProtectV™ provides full disk encryption of physical servers, virtual machines, and cloud 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, Microsoft Hyper-V, IBM Bluemix, or VMware, SafeNet ProtectV ensures cloud-enabled security.

The industry's first comprehensive high-availability solution for protecting data across bare metal, virtual and cloud infrastructures, SafeNet ProtectV encrypts entire servers and attached storage volumes, keeping your data safe from unauthorized access. In addition, no SafeNet ProtectV Manager or Client can be launched without proper authorization and authentication from SafeNet ProtectV StartGuard (TM) pre-boot authentication.

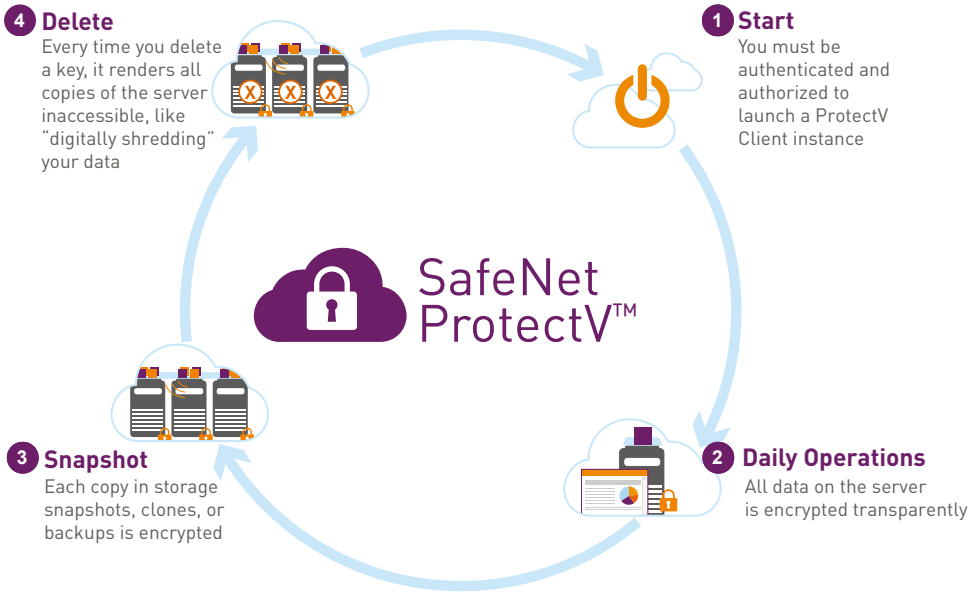
With SafeNet ProtectV's unified encryption, your organization can be safe knowing that you retain access to and control of your encrypted data and keys at all times. In addition, you can enhance your business agility and take advantage of the lower costs inherent in cloud-enabled environments.

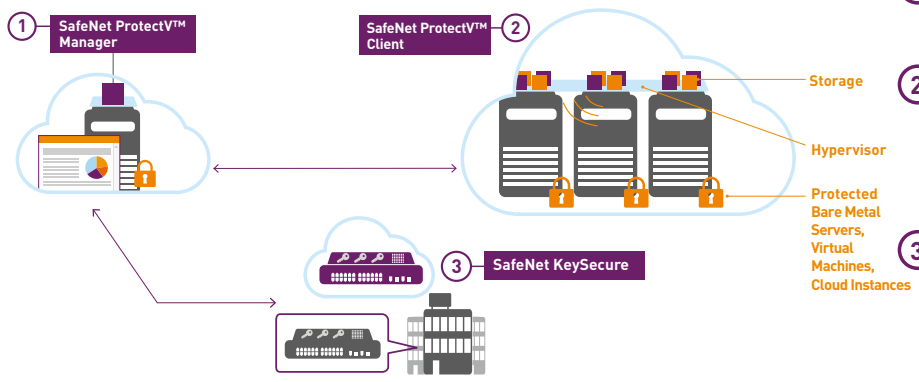
SafeNet ProtectV empowers you to secure your data and prove compliance across cloud-enabled environments

- **Isolate** servers and storage through encryption of operating system (OS) and data partitions
- **Authorize** server launches with SafeNet ProtectV StartGuard™ pre-boot authentication
- **Track** key access to all copies of your data
- **Revoke** key access after terminating an instance 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, GDPR, 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 Data Lifecycle





1 SafeNet ProtectV Manager –
Centralized console for managing encrypted physical, virtual and cloud 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.

Ensure Compliance in the Cloud

> Maintain compliance requirements for regulations such as PCI-DSS, GDPR, and HIPAA across cloud-enabled infrastructure
> Decouple compliance requirements from infrastructure requirements to maximize business agility without compromising regulatory compliance

Protect Your Data in Cloud-Enabled Environments

> Single pane of glass for controlling and monitoring your data across hybrid environments
> Supports Windows and Linux operating systems including XFS
> IBM Bluemix: minimum Private 1 x 2.0 GHz Core
> Microsoft Azure: minimum Standard A2 size
> Provides RESTful APIs and robust CLI commands

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, Hyper-V
> IBM Bluemix: IBM Bare Metal and Bluemix VMs

Minimal System Requirements:
SafeNet ProtectV Manager:
> AWS: m3.medium and larger (for production environments) /1 volume (auto created / 8 GB)
> IBM Bluemix: minimum Private 1 x 2.0 GHz Core
> Microsoft Azure: minimum Standard A2 size
> Microsoft Hyper-V: Ubuntu (Linux 64 bit), 2vCPUs, 4GB memory (minimum), 1 NIC (VMXNET 3), 16GB disk
> VMware: Ubuntu (Linux 64 bit), 2vCPUs, 4GB memory (minimum), 1 NIC (VMXNET 3), 16GB disk

SafeNet ProtectV Client:
> Windows: 256MB RAM, 100MB free disk space
> Linux: 256MB RAM, 100MB free disk space
> AWS Only: Instances should be larger than micro. (t1.micro instances are not supported.)

Client OS Support*
> Microsoft Windows Server
> Microsoft Windows 7
> Amazon Linux
> 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 aws marketplace
Windows Azure Marketplace

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

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free