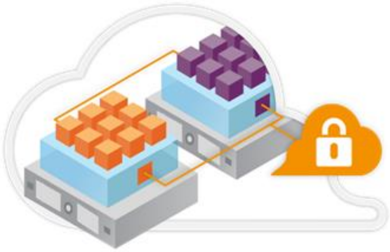
SafeNet THE DATA PROTECTION COMPANY



Encrypt Virtual and Cloud-Based Data Centers with SafeNet ProtectV^{TM}

PRODUCT BRIEF

Why ProtectV?

- **Protection** of sensitive data and intellectual property
- **Compliance** with internal audit and external industry regulations
- **Segregation** of user access across key data types
- **Automation** reduces key management overhead

Security and compliance are often the main barriers preventing organizations from virtualizing and migrating to the cloud. With SafeNet ProtectV, service providers can enable organizations to securely migrate even the most sensitive and highly regulated data to the cloud or virtual data centers – while boosting revenue and decreasing risk as a result.

The industry's first comprehensive high-availability solution for protecting data in all today's environments including, public, private and hybrid cloud models. ProtectV encrypts entire virtual machine instances and attached storage volumes.

When you are providing VMware solutions from a virtual data center, ProtectV ensures that all customer data is encrypted – reducing the risk of data theft and security breaches. Both you and your customers maintain full ownership and control of the data. The solution can also be used to secure cloud-based services that your customers may be using; such as Amazon Web Services' EC2, providing for easy-to-scale capacity, taking advantage of Amazon VPC to run AWS resources in a virtual private network.

Together with SafeNet KeySecure, ProtectV provides a highly available encryption solution to address a myriad of industry security standards and government regulations such as PCI DSS, SOX, and HIPAA HITECH. Regardless of where workloads reside, you can ensure highly-secure segregation of customer data, enforce strict separation of duties between the tenant and provider, and allow customers to manage the data lifecycle while establishing clear accountability with audit trails and detailed compliance reporting.

Deliver Virtual Machine Encryption-as-a-Service

ProtectV's architecture enables quick provisioning of encryption services for tenants, allowing service providers to offer virtual machine encryption as a pay-as-you-go service.

- Seamless incorporation into existing service offerings with programmatic API support that enable automation and orchestration of ProtectV into the provider environment.
- Efficient customer billing with metering API allows you to meter the usageof ProtectV and bill customer accordingly.
- Multiple ProtectV Managers can connect to one KeySecure appliance, making it possible to amortize the cost of each appliance across several customers.

Benefits for You – the Service Provider

- Increase cloud adoption by offering high levels of security
- Enable customers to run more and larger workloads in the cloud
- Help customers meet compliance regulations with secure partitioning functionality for each client and certifications (FIPS,CC,….)
- Ability to up-sell a new solution to existing customers
- Open the door to potential new security market revenues
- Potential to expand security services portfolio
- Increase existing customer penetration
- Ability to up-sell in every new sale engagement
- Differentiation from other IaaS providers

Enable Secure Migration of Sensitive Data to Virtual Data Centers, the Cloud and Shared Environments

ProtectV makes sure virtual machines and storage volumes are as secure as physical servers and storage in the most robust, secure on-premise environment. ProtectV enables the enterprise to control data retrieval and digital shredding, rendering illegitimate or hidden snapshots or copies useless.

- **Complete virtual machine and storage volume encryption:**
  - Encryption of system/OS partitions
  - Encryption of data partitions
  - Encryption of associated snapshots and backups (DR sites, etc.)

Solve Critical Challenges of Security and Control of Data in Virtual Infastructures and the Cloud

The encryption keys used by ProtectV can be either held by the service provider in the data center as part of a managed service offering or can be owned by the customer on an on-premise hardware-based key management solution. ProtectV provides pre-launch authentication and granular access controls to deliver undisputed command and proof of ownership for both data and keys. ProtectV secures virtualized data, preventing unauthorized data exposure or superuser abuse, and helps meet a range of regulations such as PCI and HIPAA HITECH.

- **Pre-launch authentication:** Access to data stored or processed by a protected VM requires explicit user authentication and authorization by ProtectV.

- **Separation of duties:** Role-based encryption polices, together with segregated key management ensure separation of duties between cloud service provider system administrators and the organization's IT administrators, or between different units in the organization's own virtual environment.

Provide Visibility and Proof of Data Governance

Reinforcing control with robust security, ProtectV, provides a single and centralized policy enforcement and audit point enabling data governance relying on explicit authorization and logging of every access event to protected VMs.

- **Security management across cloud environments:** A unified management platform serves as a central audit point providing an at-a-glance dashboard view of all encrypted and unencrypted virtual machines and storage volumes belonging to the organization.

- **Enterprise key lifecycle management with government grade assurance:** When used with an on-premise key management system, ProtectV delivers high-assurance FIPS 140-2 level 3 certified protection. Cloud-based key management can also be performed with ProtectV Manager.

Technical Specifications

ProtectV Manager can be easily deployed using pre-defined images. Whether data is stored in a virtual data center such as VMware vCenter or a public cloud, such as Amazon Web Services EC2 or Amazon VPC, ProtectV equips users with a user-friendly GUI to manipulate policies, users and roles, system management and monitoring and event management. Moreover, it offers APIs for automation and integration with virtual server provisioning systems and CLIs for scripting and bulk operations for improved agility and rapid provisioning.

Supported Environments:

- VMware vCenter v4 - 5.5
- Amazon Web Services EC2
- Amazon Web Services VPC 9 (Types 3, 4)

Client Servers:

- Windows 2003, 2008, 2012 R2 – Virtual and Physical
- Linux: RHEL, CentOS, Ubuntu and SUSE v10/11

Key Managers:

- KeySecure - k150 (physical/virtual), k460

Minimal System Requirements:

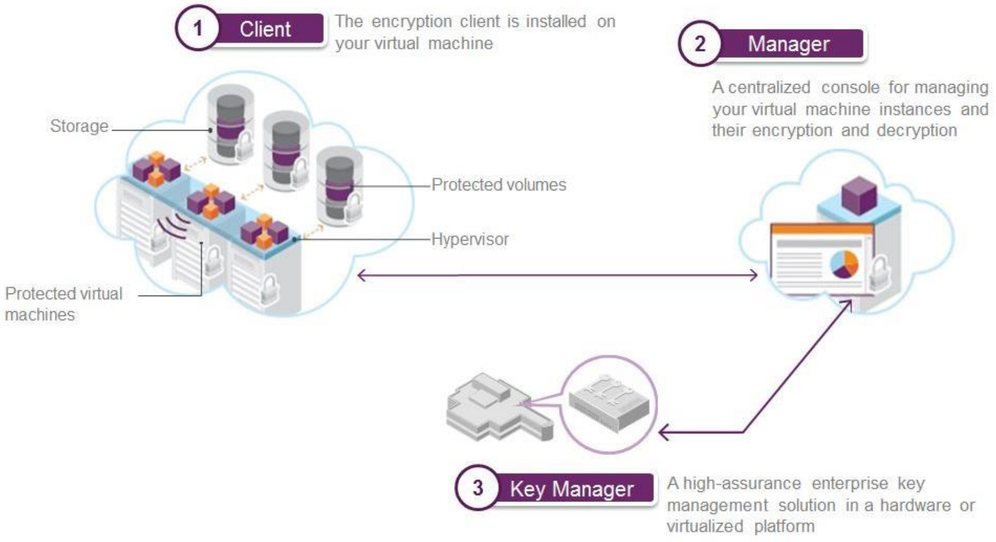
ProtectV Manager:

- VMware: 2 vCPUs, 4GB RAM, Single NIC/ VMXNET3 Ethernet Adaptor, 4 hard drive partitions (8GB 0:0/ 10GB 0:1/ 4GB 0:2/ 5GB 0:3)
- AWS: m1.medium or larger instance/ 2 volumes (auto created/10GB & 15 GB)

ProtectV Client:

- VMware: 256MB RAM, 100MB free disk space
- Amazon Web Services: m1.small or larger instance, 100MB free disk space

ProtectV Solution Components


1 Client
The encryption client is installed on your virtual machine
2 Manager
A centralized console for managing your virtual machine instances and their encryption and decryption
Storage
Protected volumes
Hypervisor
Protected virtual machines
3 Key Manager
A high-assurance enterprise key management solution in a hardware or virtualized platform

Note: SafeNet KeySecure is required.

SafeNet Data Protection

Virtualization and cloud 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 organizations to adapt to the risk it faces.

Wherever data resides, SafeNet offers persistent, secured storage for structured and unstructured data. SafeNet 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 SafeNet's complete portfolio of data protection solutions, please visit our website at **www.safenet-inc.com.**

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: www.safenet-inc.com/connected