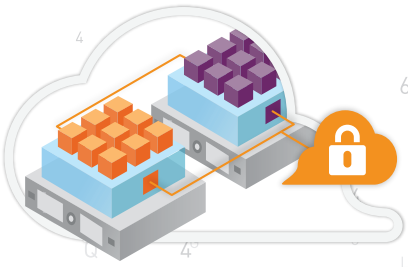
SafeNet | THE DATA PROTECTION COMPANY



ProtectV™

Data Protection for the Cloud

PRODUCT BRIEF

The security risks of virtualization

The structural differences between physical and virtual environments can compromise data integrity, reduce control over user access, compromise compliance, and increase liability.

Broad Distribution of VMs

- Easily replicated through simple snapshots
- Backed up across different datacenters around the globe
- Snapshots and backups are easy to move, copy, or steal without detection

More Privileged Users

- Admins and privileged users often operate independently
- Data co-mingling in multi-tenant environments
- Hard to ensure separation of duties between cloud service provider and organization's superusers

The cloud provides the agility, elasticity, capacity and redundancy required to maintain a competitive advantage in the market. As enterprises move their servers from dedicated physical datacenters to virtual infrastructures or private, hybrid, or multi-tenant public clouds, they enjoy substantial cost and efficiency benefits.

However, this move adds an additional layer of virtualization-specific security challenges. Organizations are being increasingly challenged to ensure robust information security. Even in private clouds and more isolated environments such as virtual datacenters, data is still at risk of exposure.

Introducing SafeNet ProtectV, the industry's first comprehensive high-assurance solution for securing both virtual infrastructure and data, giving organizations the freedom to migrate to virtual and cloud environments while maintaining full ownership, compliance and control of data.

Protect your data in virtual environments and the cloud with ProtectV

Business Benefits	Features
First trusted "lockbox" for protecting Virtual Environments Full encryption of both VMs and storage volumes combined with "tamper-proof" pre-launch authentication ensures complete isolation of data and separation of duties. 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 encryption:** • Enables encryption of entire virtual machines and 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. • Encryption keys are stored on premise, in a high assurance HW based key manager.
Only high-assurance solution for data compliance On-premise, hardware-based key management together with pre-launch authentication and granular access control provide undisputed command and proof of ownership for data and keys. ProtectV secures virtualized data, preventing unauthorized data exposure or super-user abuse, and helps meet a range of regulations such as PCI and HIPAA.	**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.
Visibility and proof of data governance Reinforcing control with robust security, SafeNet 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:** • The only solution that provides an on-premise key management system with the high-assurance FIPS 140-2 level 3 certified KeySecure appliance. Cloud-based key management can also be performed with ProtectV Manager.

vmware PARTNER TECHNOLOGY ALLIANCE

vmware READY

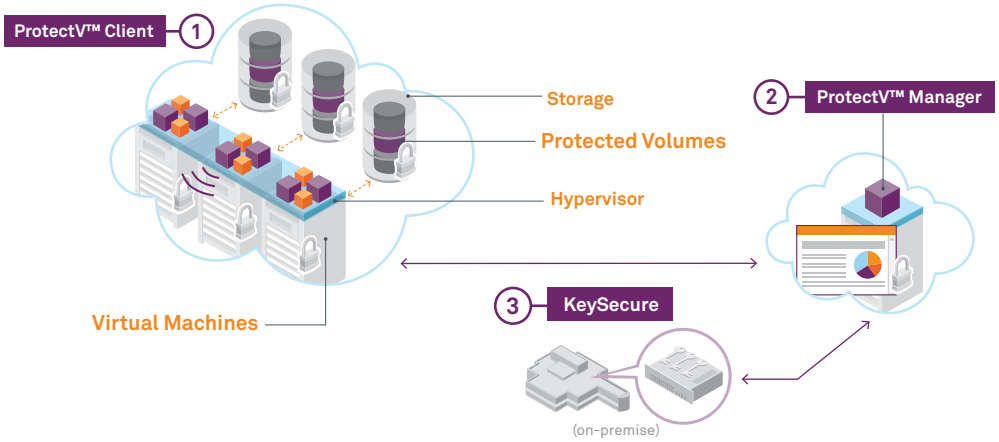
1. Install ProtectV Client on your VMs. Select which servers and storage volumes you want to encrypt and create your policies.

2. ProtectV Manager is a virtual machine that runs as an AWS AMI or as a VM in a VMware environment. Configure ProtectV Manager by creating users and permissions.

3. KeySecure is an optional component for customers interested in higher assurance level. Install KeySecure on-premise as your root of trust for managing the lifecycle for all key types across your data centers, private and public clouds.

ProtectV: How It Works

ProtectV secures regulated data on VMs and storage volumes in virtual datacenters, and public and private clouds.



Technical Specifications

Supported Platforms
- Amazon Web Services EC2
- Amazon VPC
- VMware vCenter

Supported OS
- Microsoft Windows Server 2008 32-bit
- Microsoft Windows Server 2008 R2 64-bit
- Microsoft Windows Server 2003 R2 64-bit
- CentOS Linux 5.5 64-bit
- CentOS Linux 5.6 64-bit
- CentOS Linux 5.6 32-bit
- Red Hat Enterprise Linux (RHEL) 5.6 32- and 64-bit

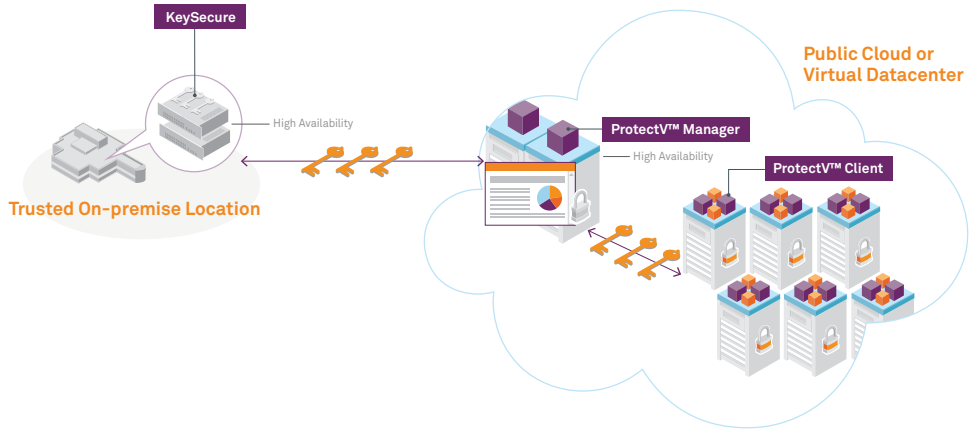
ProtectV Client Supported Browsers
- Internet Explorer 8, 9
- Firefox 4.0.1, 5.0, 6.0
- Google Chrome 12.0 and above

Supported SafeNet Enterprise Key Management Products
- SafeNet KeySecure k460
- SafeNet KeySecure k150
- SafeNet DataSecure i450
- SafeNet DataSecure i150

Deployment Scenarios

Whether data is stored in a virtual environment such as VMware vCenter, or in a public or private cloud such as Amazon Web Services EC2/EBS or Amazon VPC, ProtectV Manager can be easily deployed using pre-defined images. ProtectV is equipped with a user-friendly GUI to manipulate policies, users and roles, and conduct system 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.

Protectv Deployment Scenarios for Virtual Datacenters, Public and Private Clouds



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 organization 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.

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