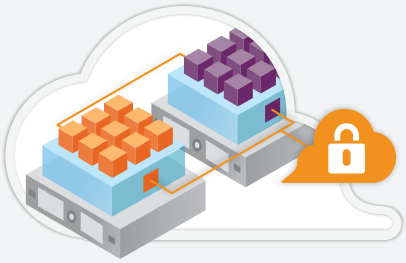
SafeNet | THE DATA PROTECTION COMPANY



Safeguarding Sensitive Data in the Cloud and Virtual Datacenters

A Technical Overview of SafeNet ProtectV

WHITEPAPER

Virtualization in the Enterprise

- 39.4% of servers are virtualized[1]
- By 2018, 86% of all workloads are expected to be running in virtual machines[2]
- The cloud market is expected to grow to $60 billion[3] by the end of 2012

Executive Summary

Although many organizations have made the move to virtualization and cloud service delivery models, there are still significant security challenges these environments present—challenges that many organizations have yet to address. SafeNet ProtectV offers unique capabilities that enable organizations to effectively safeguard sensitive assets in virtual datacenters and cloud environments. This paper details the ProtectV solution, describing the offering's key capabilities, components, and deployment architectures.

Introduction: The Move to Virtualization and the Cloud—and the Security Implications

Compelled by a range of benefits and advantages, organizations of virtually every size and type are adopting virtualization technologies and cloud models. However, in spite of their widespread adoption, virtual and cloud environments present some significant challenges for the security teams tasked with safeguarding sensitive data. Following are a few of the more pressing obstacles:

- **Increased data volumes and mobility.** In virtualized environments, workloads, data repositories, and sensitive data are highly mobile, and frequently being shifted to different virtual and physical resources. In these environments, it is easier than ever to move and copy sensitive data. For example, virtual machines are often routinely backed up, according to proper retention policies. However, given the volume of virtual machines running and the persistent backups of these resources, the locations of sensitive data can increase substantially. Consider that if one virtual machine is backed up every hour, there would be 24 copies of that virtual machine created on a daily basis. This explosive growth in virtual machines and their associated backups all ultimately result in sensitive data residing in many more locations than in years past. This proliferation presents security teams with inherent challenges, increasing the complexity and effort required to secure sensitive assets.
- **Digital data destruction.** Exacerbating matters is the uncertainty that can surround data destruction and retention. With the volume of virtual machine snapshots, it grows increasingly difficult to determine with certainty whether all instances of a sensitive repository are completely and permanently removed from all potential locations. In many cases, when data is deleted, it can be recovered easily. How does an organization make sure that data is securely destroyed?

- **Administrative exposure.** Another potential challenge is posed by the changing dynamics of administration in virtualized environments. Compared to prior computing models, cloud and virtualization ultimately introduce more privileged users and a new class of administrators. Typically, teams of administrators focused on servers, storage, backups, and applications will have some level of access in virtual environments, and quite often security policies and administrative functions are handled independently by each group. Further, companies who use the public cloud will have their data handled by administrators who usually work for the cloud provider, not for the company itself. These administrators must be able to move the data but not be able to view or access it.

ProtectV is a virtual server-based solution, which enables it to adapt to the fluidity of virtual environments.

Introducing SafeNet ProtectV

Today, SafeNet ProtectV enables organizations to leverage the business benefits of virtualization and cloud services, while helping to meet their governance, compliance, and data protection requirements. With ProtectV, organizations can encrypt and secure entire virtualized machines, protecting these assets from theft or exposure. Further, with ProtectV, security teams can encrypt virtual storage, ensuring cloud data is isolated and secured—even in shared, multi-tenant cloud environments. ProtectV can be deployed in public clouds, private clouds, and virtual datacenters.

ProtectV is a virtual server-based solution, which enables it to adapt to the fluidity of virtual environments. At the same time, ProtectV is seamlessly integrated with SafeNet KeySecure, a high availability, appliance-based key management solution that provides a hardened root of trust within the customer's premises. With this combination, the ProtectV solution enables security teams to enjoy these advantages:

- Leverage the deepest, most comprehensive visibility of virtual environments in order to enable effective governance.
- Ensure the highest levels of compliance with all relevant policies and regulatory mandates.
- Apply maximum security and protection to sensitive data assets in virtual environments.

ProtectV: Key Capabilities

Through its integration with KeySecure, ProtectV enables organizations to leverage a hardened appliance for securing keys, policies, and cryptographic processing. At the same time, the solution is efficiently deployed in highly dynamic virtual and cloud environments, so organizations can retain complete control over keys and sensitive assets within their premises—while embracing the opportunities provided by virtualization and cloud delivery models.

Following are a few of the solution's key capabilities:

- **Flexible integration.** ProtectV offers complete support for automated, highly dynamic virtual environments, which is vital in both ensuring critical security mechanisms are consistently enforced and in streamlining security administration. A ProtectV API is available, which enables flexible integration in cloud and virtual environments. With the API, organizations can configure a range of commands, including setting or retrieving cloud credentials, listing virtual machines secured, starting or stopping virtual machines, and more.
- **Extensibility.** Through its integration with KeySecure and other SafeNet security solutions, ProtectV can support expanded cryptographic services. Consequently, the solution represents an investment that can be leveraged over the long term, even as infrastructures, business objectives, and security requirements evolve.

Even if some administrators requires privileges for moving or managing virtual machines, security teams can still enforce policies so that they can't actually decrypt and access the sensitive data held on those virtual machines.

- **Scalability and high availability.** ProtectV and KeySecure offer support for failover and replication, which enables organizations to ensure the availability and scalability of critical cryptographic processing. Further, with this scalability, organizations can leverage KeySecure across any number of datacenters, cloud deployments, encryption implementations, and regions.
- **Complete visibility and audit trails.** ProtectV provides audit trails for all security operations, so organizations can ensure compliance with relevant policies and mandates, and efficiently demonstrate compliance for auditors.
- **Granular security controls.** With this solution, organizations can realize granular controls over data access. For example, even if some administrators requires privileges for moving or managing virtual machines, security teams can still enforce policies so that they can't actually decrypt and access the sensitive data held on those virtual machines. With ProtectV, security teams can control where and when a virtual machine can be launched, and by whom.

ProtectV Components and Architecture

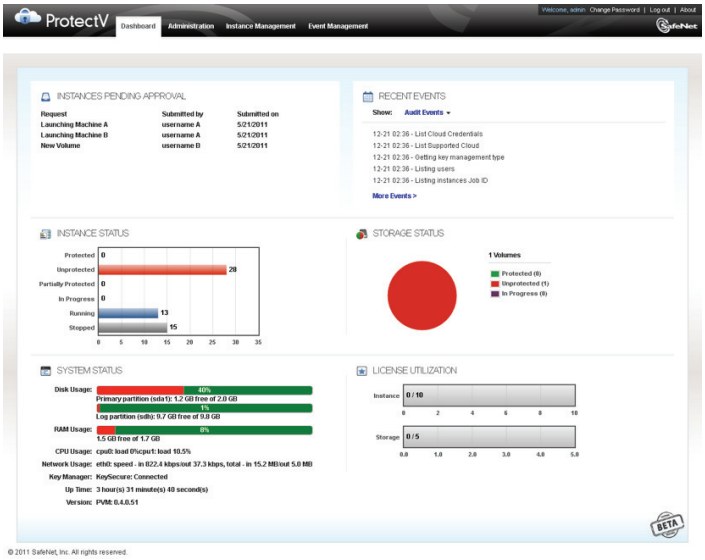
The ProtectV solution features several components, which are seamlessly integrated and enable streamlined deployment. Following is an overview of each component.

ProtectV Clients

- **Where deployed.** ProtectV Clients are deployed in the cloud or virtual environments, where they protect virtual machines.
- **Who accesses.** The virtual machines protected by ProtectV Client are accessed directly by users. ProtectV Client can only be accessed by ProtectV Manager and its administrators.
- **Functionality delivered.** Offering support for Windows and Linux environments, ProtectV Clients enable a range of cryptographic capabilities. These clients enable encryption within both system and volume partitions. Further, they enable encryption that is completely transparent to associated applications. ProtectV Client also is responsible for monitoring security processes.

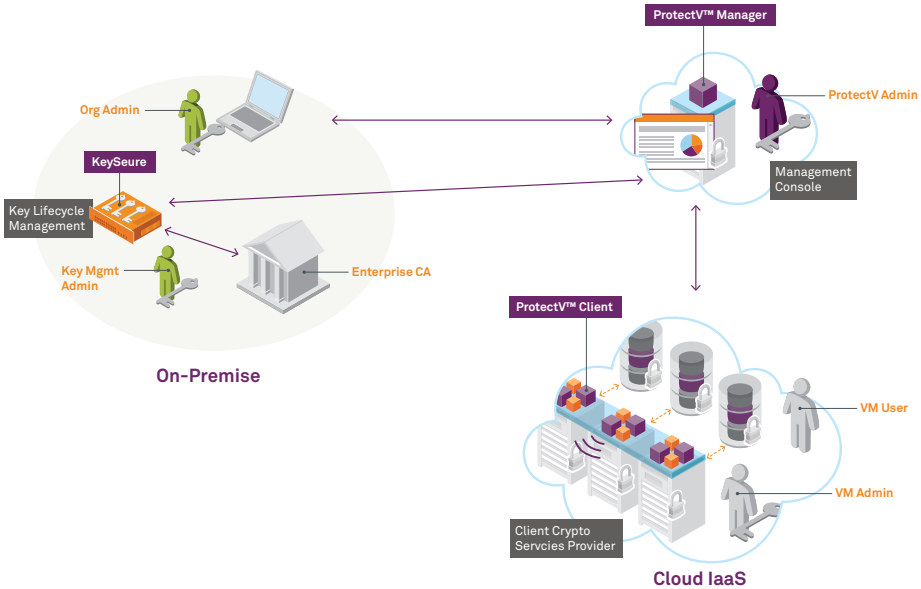
ProtectV Manager

- **Where deployed.** ProtectV Manager is also deployed within the cloud or virtual environment in which encryption is employed. When deployed in Amazon Web Services environments, ProtectV Manager is deployed on a virtual machine that is launched using an AWS Amazon Machine Image (AMI). This component is also deployed on a virtual machine using an ISO image within VMware environments.
- **Who accesses.** Only authorized personnel, such as the ProtectV administrator, the helpdesk administrator, or the owner of the VM, can interact with ProtectV Manager.
- F**unctionality delivered.** ProtectV Manager delivers a central management console that enables administrators to configure, manage, and report on cryptographic activities. ProtectV Manger offers such capabilities as key caching, policy enforcement, and log aggregation. The connection between ProtectV Manager and the ProtectV Clients is secured. The ProtectV Manager also manages the encryption of resources. By centralizing all these capabilities, ProtectV Manager enables security teams to adminster these processes in an efficient, highly scalable manner.



KeySecure

- **Where deployed.** KeySecure is deployed within the customer's premises.
- **Who accesses.** KeySecure is controlled by the key management administrator.
- **Functionality delivered.** KeySecure can be used to manage the lifecycle of all keys and key types, across one or all datacenters as well as private and public cloud deployments. KeySecure stores keys within a hardened appliance that is FIPS 140-2 level 3 compliant, which means it has been certified to the most rigorous standards for its tamper resistance and security safeguards. KeySecure can work directly with the enterprise certificate authority (CA) to ensure trusted digital transactions. By acting as a central facility for all sensitive key activity, and logging and securely storing this information, KeySecure provides a range of capabilities for supporting auditing, reporting, and compliance requirements.



The Importance of Protecting Cryptographic Keys

"As the use of encryption grows and various solutions are deployed, key management becomes exponentially critical and complex. Mismanagement of keys can expose an organization to unnecessary risks."

~Gartner

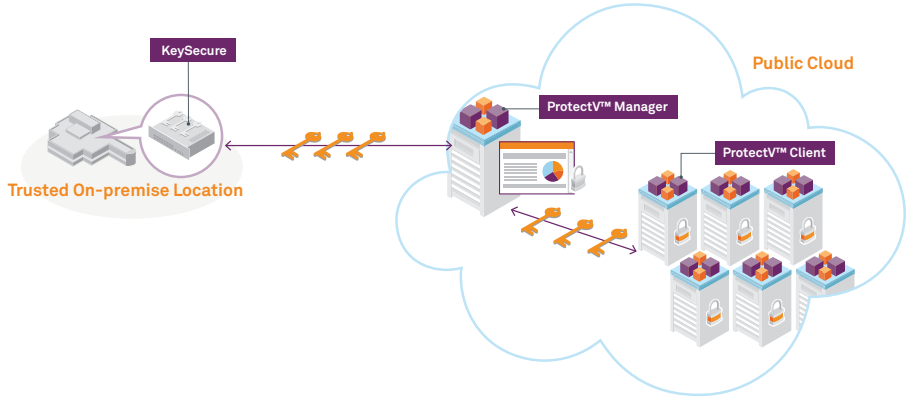
Unparalleled Protection of Cryptographic Keys

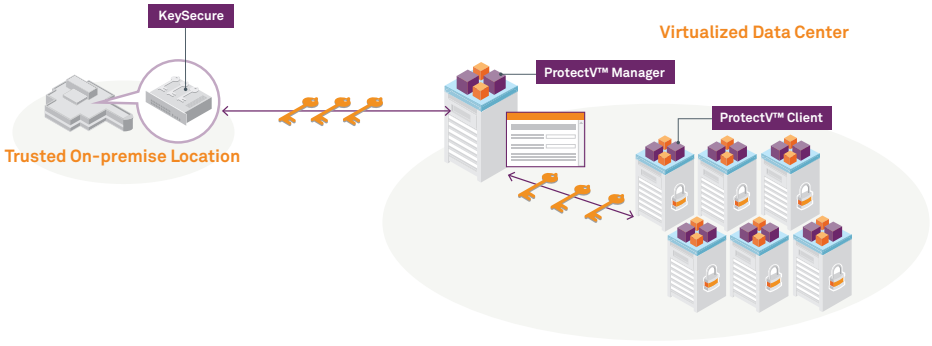
Through its capabilities and deployment architecture, the ProtectV solution ensures that vital cryptographic keys are strongly secured at all times. Following are a few of the solution's key management safeguards:

- **Logical separation.** Cryptographic keys are stored separately from virtual servers. With this logical separation of keys, organizations can ensure keys are fully secured.
- **Obfuscation.** Whether ProtectV Manager is running on a virtual server on premise or in the cloud, keys are obfuscated to ensure key bytes are never exposed to unauthorized use.
- **Granular decryption.** When an authorized user requests access to encrypted resources, cryptographic keys reside on KeySecure to enable decryption. In addition, the virtual machines or instances are never completely decrypted. When a file or other resource is requested by the user, only the specific sector housing that asset is decrypted.
- **Encrypted virtual machines, keys, and snapshots.** ProtectV fully leverages encryption across the infrastructure. The virtual machine that ProtectV Manager runs on is encrypted. Further, the keys stored in the ProtectV Manager database are also encrypted. Finally, snapshots can also be encrypted.
- **Secured key transmissions.** Keys in transit between ProtectV Manager and ProtectV Client are secured via SSL, and can even be further secured through client certified authentication. ProtectV supports both third-party CAs and two-way SSL authentication.

Deployment Scenarios

Whether the ProtectV solution is deployed in a virtual datacenter or if it is deployed to secure sensitive assets in a public cloud environment, organizations start by deploying KeySecure within a trusted location within their premises. ProtectV Manager and ProtectV Clients are deployed either in the virtual datacenter or the public cloud. When deployed, security teams can effectively ensure that all their sensitive assets in the virtual environment are secured.





Deployment Overview

Whether it is being deployed in virtual datacenters or public cloud environments, ProtectV can be implemented in a straightforward and efficient manner.

Following is an overview of the steps required in a typical implementation:

- Set up the cloud service provider environment or virtual datacenter.
- Install and configure KeySecure for ProtectV Manager in a secure on-premise location. Configuration will include such efforts as setting up IP addresses, users, and certificates.
- Take a snapshot of a virtual machine that will be encrypted. This is for backup purposes only; because this virtual machine is not encrypted, administrators are advised to delete this snapshot after the encryption in set.
- Configure ProtectV Manager in the virtual datacenter or cloud environment.
- Connect ProtectV Manager to KeySecure.
- Create users and permissions within ProtectV Manager.
- Install the ProtectV Client on new or existing virtual machines.
- Encrypt partitions using ProtectV Manager.
- Run the encrypted virtual machines.
- Test that the virtual machines are secure. This will typically include the following activities:
    - Start server from the ProtectV Manager console.
    - Log in.
    - Verify read and write permissions.
    - Perform routine functions, such as enabling file sharing, doing a transfer via FTP, or running a database.
    - Shut down or restart the virtual machine.
    - Verify that unauthorized users can't access encrypted virtual machines.

Conclusion

Without effective safeguards in place, virtual datacenters and cloud environments can present a host of risks to sensitive data. With ProtectV, organizations can fully exploit the benefits offered by virtualization and cloud services, and at the same time ensure they have the visibility and control they need to safeguard their sensitive assets at all times.

SafeNet Data Protection

Virtualized 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 virtualized environments and the cloud.

About SafeNet

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet's data-centric approach focuses on the protection of high value information throughout its lifecycle, from the datacenter to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

[1] siliconANGLE, "Quarterly Index: Virtualization Penetration in the U.S. and Europe", Alex Williams, July 21, 2011 http://siliconangle.com/blog/2011/07/21/virtualization-penetration-in-the-u-s-and-western-europe/

[2] Gartner, "Forecast: x86 Server Virtualization, Worldwide, 2008-2018", July 2011

[3] Forrester Research, "10 Cloud Predictions For 2012", Holger Kisker, December 13, 2011 http://blogs.forrester.com/holger_kisker/11-12-13-10_cloud_predictions_for_2012

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