WHITE PAPER

Securing Data in Virtualized Data Center and Cloud Environments:

Key criteria for effective protection of virtual workloads

Introduction

Organizations around the world and of every type and size—from smaller start-ups to the Fortune 50, from local municipalities to the largest government agencies—are growing increasingly reliant upon virtualized data centers and cloud services. While the cost advantages and business agility afforded by these models are obvious, so too are the security ramifications.

In this series of white papers Gemalto will review the challenges organizations face as they continue to virtualize their data centers and move other critical aspects of their operations to cloud service providers. In addition, the series will detail key criteria every organization should consider when addressing security and compliance in virtualized and cloud environments and finally introduce the Gemalto SafeNet Identity and Data Protection solution suite that can be deployed to implement a defense-in-depth strategy for data protection. This first paper will focus on the critical issue of protecting virtual workloads containing sensitive and regulated data.

Virtualization and Cloud Environment Challenges

In the physical data center security policies are associated with specific machines but, when organizations are tasked with safeguarding sensitive data, migration to virtualized environments and the cloud present significant challenges including:

- **New privileged users.** The cloud presents fundamental implications when it comes to administrative access. When running in virtual and cloud environments, infrastructures are managed by administrators and privileged users, who may have permissions and controls that extend not only across the infrastructure, but enable them to access VMs, databases, applications, and therefore the sensitive data these systems manage. Privileged users also require higher levels of identity assurance to access shared environments and virtual infrastructure.
- **Erosion of traditional controls.** Historically, security teams in many organizations have relied on security approaches that don't necessarily apply in the cloud. For example, much of the focus of traditional security investments and strategies was directed toward erecting perimeter-based defenses, however, when applications and data reside in a virtual data center or at an external provider's environment, the very concept of the perimeter is less relevant. For example, in virtualized cloud environments, the use of network isolation and hardware-based controls don't ensure protection of virtual machines. If controls are applied to a given physical server, and a virtualized workload moves to a different server, those same controls may not be enforced on another host, and sensitive data may be exposed.
- **Virtual machine mobility.** In cloud environments, virtualized resources are highly dynamic. Virtual machines can be moved, cloned, and archived, which can make enforcement of security policy and auditing difficult and time consuming. Further, in these environments, the virtual resources that house sensitive assets can be cloned and backed using routine automated processes that significantly increase the number of copies of sensitive assets available, and so increase the potential areas of exposure.
- **Databases and applications deployed in virtual environments.** It is even more critical in virtual environments to ensure business need-to-know access to data residing in applications and databases. Deploying encryption in these environments requires granular controls so that only authorized users can access sensitive or regulated data.

- **Maintaining compliance.** When organizations migrate sensitive or regulated data to the cloud, they are still responsible for compliance. To remain compliant with industry standards such as the Payment Card Industry Data Security Standard (PCI DSS) and security and privacy regulations like the Health Insurance Portability and Accountability Act (HIPAA), organizations have to retain control over regulated data and demonstrate to auditors that the required controls are in place at all times.

Securing Virtual Workloads with Gemalto SafeNet ProtectV and SafeNet KeySecure

Gemalto enables organizations to leverage the business benefits of virtualization and cloud services, while addressing their governance, compliance, and data protection requirements. With SafeNet ProtectV, organizations can encrypt and secure entire virtualized machines, consistently enforce security policies, and protect cardholder data from theft or exposure.

SafeNet ProtectV enables organizations to address the specific security and compliance requirements in cloud environments. With SafeNet ProtectV, these organizations can isolate, track and report on VMs containing sensitive data. As a result, they can eliminate costly compensating controls that may be in place for VM protection that complicate audits.

SafeNet ProtectV is deployed with SafeNet KeySecure, a robust key management solution. KeySecure features an optional FIPS 140-2 level 3 validated hardware security module. In addition, SafeNet Virtual KeySecure, a hardened virtual appliance, offers additional flexibility in cloud environements. SafeNet ProtectV and SafeNet KeySecure deliver robust high-availability capabilities that enable organizations to scale deployments in highly dynamic virtual and cloud environments.

Following are more details on these solutions' key capabilities.

Partition Encryption

Policies and regulations often require enterprises to guarantee that, even if a storage node is compromised, sensitive data retained on that node will remain unreadable. To address this requirement, SafeNet ProtectV provides partition encryption, a key mechanism for protection—even when other defenses are breached. This feature offers multiple permissions for controlling disk access to the virtual partition. By using the solution's combination of volume access controls and decryption key rights, security administrators can ensure that only authorized users gain access to encrypted data.

SafeNet ProtectV encrypts the entire data partition in a non-intrusive manner, so there is no need to backup data, reformat the partition prior to encryption, and restore the data after encryption. In addition, SafeNet ProtectV offers a partition recovery feature that allows the resumption of encryption mid-cycle, even after interruption by power outages and other unexpected events.

Key Criteria for Protecting Virtual Workloads

The following are key criteria for protecting virtual workloads in virtual and cloud environments:

- Ensure the entire VM can be encrypted, including OS, swap, and data partitions
- Prevent unauthorized users from starting VMs containing sensitive data, even those that have been moved, cloned, terminated or archived
- Separate administration and access of cryptographic keys from encrypted data
- Maintain ownership of cryptographic keys and retain the ability to delete them in case of a breach (or CSP agreement termination) to render data in VMs unreadable
- Log and report on administrative activities and events associated with VMs containing cardholder data
- Maintain compliance with security standards and regulations

Boot Management

Many VM security and compliance requirements cover the copying and cloning of images within the virtual or cloud environment. SafeNet ProtectV StartGuard provides organizations with critical control over the boot process. As a result, SafeNet ProtectV protects VMs from unauthorized boot, even when they are moved, dormant, offline, or archived.

SafeNet ProtectV enforces boot management controls through a mechanism that coordinates activities between the SafeNet ProtectV manager and its associated SafeNet ProtectV client nodes.

When the SafeNet ProtectV client is installed on a node, a dual-phase boot loader is also installed. This splits the boot process into two separate phases: bootstrapping and networking is separated from loading the operating system (OS). Once this dual-phase loader is installed, the client asks the ProtectV manager for permission to proceed with an OS load. The manager performs this check based on a unique identifier for each node. If that particular node is registered to allow automatic booting, the OS loads normally. If not, the OS remains unloaded until explicit boot permission is granted by a user SafeNet ProtectV management console.

An immediate benefit of dual-phase boot is that it offers protection against data being exposed through intentional or unintentional VM copying and cloning. If a VM is cloned, the resulting unique identifier will not be registered with the SafeNet ProtectV manager, so the second boot phase will be denied. For cases where boot authorization is required, the cloned VM can be registered, either programmatically or with a few mouse clicks.

Group, Role, and User Policy Management

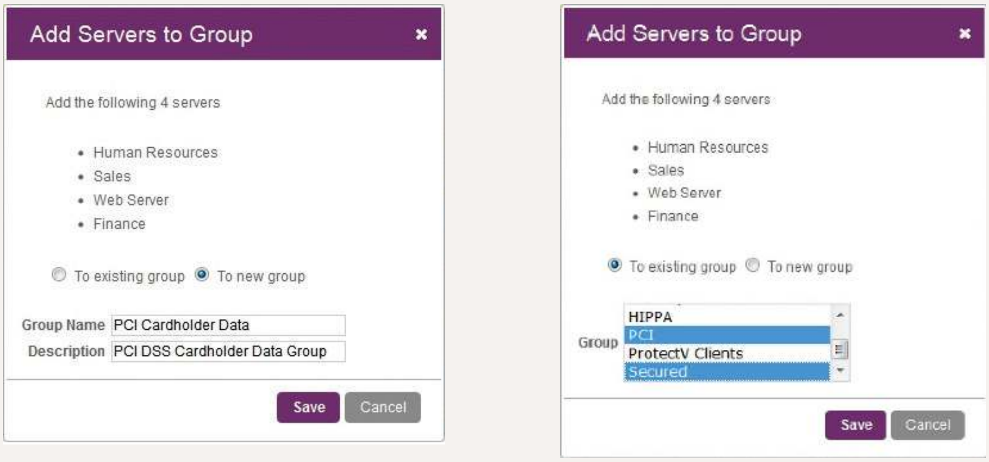
SafeNet ProtectV offers group, role, and user editors that enable auditing and compliance by procedurally enforcing separation of duties and security policies. Following are more details on these editors:

> **Group editor.** SafeNet ProtectV allows administrators to place VMs in one or more groups. Each group has an assigned policy. For example, a policy may require that all volumes contained in a group are encrypted. Also, a group-based policy may grant or deny automatic reboot.

> **Role editor.** SafeNet ProtectV offers an editor for creating, modifying, and deleting roles with detailed controls. Each role consists of a unique set of permissions for dozens of operations, enabling organizations to enforce highly granular administrator roles and separation of duties. SafeNet ProtectV ships with several useful roles predefined, including three distinct administration roles.

> **User editor.** With SafeNet ProtectV, administrators can manage user policies, including assigning names, passwords, and default roles.

Fig. A



Add Servers to Group ×

Add the following 4 servers

- Human Resources
- Sales
- Web Server
- Finance

○ To existing group ● To new group

Group Name: PCI Cardholder Data
Description: PCI DSS Cardholder Data Group

Save | Cancel

Add Servers to Group ×

Add the following 4 servers

- Human Resources
- Sales
- Web Server
- Finance

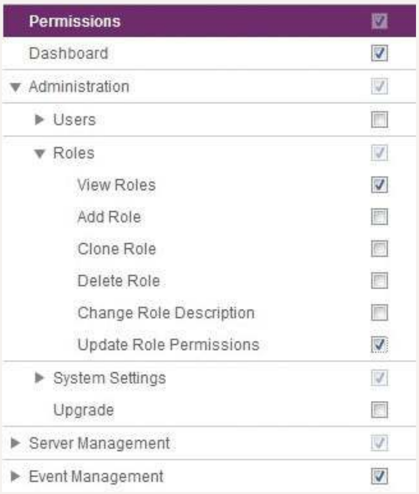
● To existing group ○ To new group

Group: HIPPA / PCI / ProtectV Clients / Secured

Save | Cancel

Fig. A - Through the SafeNet ProtectV console, administrators can assign VMs, create new groups, and also assign a VM to several different groups simultaneously.

Fig. B



Permissions	☑
Dashboard	☑
▼ Administration	☑
▶ Users	□
▼ Roles	☑
View Roles	☑
Add Role	□
Clone Role	□
Delete Role	□
Change Role Description	□
Update Role Permissions	☑
▶ System Settings	☑
Upgrade	□
▶ Server Management	☑
▶ Event Management	☑

Fig. B - SafeNet ProtectV features a sophisticated role editor that enables organizations to enforce separation of duties as required by major security standards

Maintain Compliance: Example PCI DSS v2.0 Cloud Computing Guidelines

PCI DSS Section	Requirement*	SafeNet ProtectV and SafeNet KeySecure Capabilities
Protect Cardholder Data	How are VM images, snapshots, and backups managed to prevent unnecessary capture of sensitive data?	SafeNet ProtectV controls who can start VMs and encryption protects sensitive data captured in backups and snapshots.
	How is data securely deleted [..] and stored images? Will data remnants exist in terminated VMs?	With SafeNet ProtectV, organizations can delete all the a keys associated with data, OSs, and swap partitions. This renders all the sensitive data in the VM unreadable.
	Is all client data securely purged from all CSP systems upon termination of the agreement?	With SafeNet ProtectV, the customer owns the keys, not the CSP. As a result, organizations can delete keys and effectively ensure encrypted assets are purged when a CSP agreement is terminated.
	Where are encryption/decryption processes being performed?	SafeNet ProtectV does encryption "in-place" so data does not have to be sent outside the protected VM to be encrypted or decrypted.
	Where are cryptographic keys stored, and who controls the keys? Are dataencryption keys stored and managed separately from the data they protect?	SafeNet ProtectV and SafeNet KeySecure provide separation of duties between key administration and virtual infrastructure management. Keys are stored separately in a secure vault.
Maintain a Vulnerability Management Program	Are VMs protected from within the VM or from the hypervisor?	SafeNet ProtectV StartGuard offers pre-boot authentication that can control who can launch a VM or provide a challenge/response mechanism for physical systems.

*Information Supplement: PCI DSS Cloud Computing Guidelines, March 2013

**Also see: Addressing PCI DSS in Cloud and Virtual Environments: Protecting Cardholder Data in Virtual Workoads

Conclusion

SafeNet ProtectV and SafeNet KeySecure address many of the requirements for protecting data in virtual workloads and help address many of the compliance requirements faced by organizations.

By encrypting entire virtual workloads and enforcing pre-boot authentication, organizations can take advantage of the flexibility and lower cost operational models provided by virtualization and cloud environments, while still maintaining security and compliance of sensitive data.

Future white papers in this series will cover key criteria and approaches for protecting file, database and application data in virtualized and cloud environments, centralized management and security of encryption keys and establishing higher levels of identity assurance for users and administrators accessing virtual and cloud environments.

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

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM