SafeNet ProtectV Solution for HP CloudSystem

Introduction

By integrating the SafeNet ProtectV solution for HP CloudSystem, HP provides customers the opportunity to leverage virtual data centers, while delivering adaptive security controls and data protection.

HP can offer their customers maximum protection as the data itself is encrypted using the latest technologies in isolated virtual environments. With the data properly isolated, the customer maintains control as to who has access to the data.

Section One: Solution Overview

Overview

The ProtectV solution is built on proven SafeNet technologies, while extending robust security capabilities to the new demands of cloud environments. ProtectV delivers the vital centralized management capabilities that HP can easily automate and allow organizations to practically and effectively deploy encryption across environments with hundreds of virtual machines (VMs), geographically dispersed deployments, and multiple private and public cloud environments. ProtectV uses publicly available SOAP APIs to manage virtual machines, volumes, users, roles, and more.
The Customer Challenge

HP CloudSystem 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 clouds, they enjoy substantial cost and efficiency benefits. However, this move adds specific security challenges around shared pools of compute resources and raises concerns for security, compliance and audit teams, slowing adoption and thus not allowing organizations to reap the cost and operational benefits.

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. In fact, industry experts agree that is not about IF a company’s security systems will be breached, but WHEN. This is even more prevalent in an internet based cloud system environment; making protecting data from unwelcome eyes even more critical.

The structural differences between physical and virtual environments can compromise data integrity, reduce control over user access, compromise compliance, and increase liability. In addition, security risks exist through the broad distribution of virtual machines that can be easily replicated through simple snapshots, are backed-up across different global data centers, and these snapshots and backups are easy to move, copy, or steal without detection. This coupled with more privileged users who operate independently from administrators in a comingled multi-tenant environment; you have a security officer’s biggest nightmare.

ProtectV, offers comprehensive high-assurance solution for securing physical and virtual infrastructure, giving CloudSystem customers the ability to extend encryption and key management services to their internal customers, as well as the ability to securely burst workloads into the public cloud while maintaining full ownership, compliance and control of data.

Advantages for HP CloudSystem

Provide the FIRST trusted “lockbox” for virtual environments
  • Only solution that provides comprehensive encryption of VMs and storage to deliver complete isolation and separation of duties

Provide the ONLY high-assurance solution available for cloud security
  • On-premise, hardware-based key management delivers undisputed control/proof of ownership for data and keys

Provide the DEEPEST visibility into cloud security
  • Delivers a single centralized policy enforcement and audit point
Section 2: Solution Benefits

VM Encryption for HP CloudSystem Delivers

- Encryption of entire VM
- Encryption of associated storage volumes (mapped drives), VM instances (snapshots, backups) and locations (DR sites etc.)
- Even the entire OS partition is protected

Ownership and control of your data

- Pre-launch user authorization to access a VM
- Encryption based separation of duties across virtual and physical environments
- Unified HW based FIPS 140-2 level 3 certified key management to ensure VM ownership

Visibility and proof of data governance

- Unified management - at-a-glance dashboard view and central audit point
- On-premise key management audit for encryption key

ProtectV Benefits

- **Data Isolation**— Eliminate risk of data leakage legal liability, as the customer’s virtual machine and storage volume is completely encrypted and not visible to HP or any other Cloud users. Security teams can logically separate the volumes and virtual machines that hold sensitive data from other areas of the business.

- **Central Management**—Capabilities for bulk deployment and administration, central logging and auditing, key lifecycle management, and integration with virtualization management tools.

- **Separation of Duties**—Enables security teams to separate administrative responsibilities for specific virtual machines and volumes from the cloud super-users who control the larger virtual environment.

- **Cloud Compliance**—Offers the core confidentiality and integrity controls that are key requirements for ensuring compliance with regulatory mandates, including version 2.0 of the Payment Card Industry Data Security Standard (PCI DSS).

- **Strong Pre-launch Authentication**—Features password-based protection at the user level. SSL Web access for virtual machine authentication.

- **Multi-tenant Protection**—Organizations can ensure that, even in shared cloud environments, administrators gain the visibility and controls they need to safeguard sensitive assets.

- **Fully Embrace Cloud Opportunities to Increase Revenue**—Securely allow customers to migrate sensitive assets to the cloud and increase revenue by offering them the only high-assurance data compliance solution for undisputed control and proof of ownership for data and keys.
- **Establish Confidence in Cloud Deployments**—Ensure no users will be able to get to data without proper authorization.

- **Ensure and Demonstrate Compliance**—Maintain the confidentiality and integrity of cloud data.

- **Maximize Control**—Dictate where, when, and how virtual machines and volumes are accessed and run—even across multiple cloud environments.

- **Supported Encryption Algorithm**—AES-256

---

**Section 3: Solution Architecture: How it Works**

Administrator installs Protect V client on the VMs requiring full VM encryption. ProtectV makes fully encrypting the VM efficient, fast and automated. Through policies created in ProtectV Manager only authorized users are allowed to launch the VM. During daily operations, all data and VMs remain encrypted—every copy of the VM in storage or backup is encrypted. Every time the key is deleted, it “digitally sheds” the data, rendering all copies of VMs inaccessible.

---

**Secures the Entire HP CloudSystem Lifecycle**

1. **Power On**
   - Every day that you power on HP CloudSystem-HP Blades, ProtectV makes it efficient, fast, and automated

2. **Start**
   - You must be authenticated and authorized to launch a VM

3. **Daily Operations**
   - All data and VMs are encrypted

4. **Snapshot**
   - Every copy of VM in storage or backup is encrypted

5. **Delete**
   - Every time you delete a key, it “digitally shreds” the data, rendering all copies of VMs inaccessible
ProtectV: How it works

ProtectV secures regulated data on VMs and storage volumes in HP Cloud System Matrix.

1. ProtectV Manager (PVM)
   ProtectV Manager is a virtual machine that runs as a VM in a VMware environment. It is deployed and managed by the HP Orchestration back plane.

2. ProtectV Client (PVC)
   ProtectV client software is automatically installed with each VM that is deployed from the HP Orchestration. It allows the VM to send/receive encryption/decryption messages to and from the PVM.

3. KeySecure
   A Virtual Appliance to securely manage and store the encryption keys. It is deployed and managed by the HP Orchestration back plane. This can optionally be installed on customer premise to allow the customer to fully take ownership of the keys.

Deployment Scenario: HP CloudSystem

Trusted on-premise location

HP CloudSystem

HP BladeSystem & ProtectV Client

Section 4: Demonstration of Solution
Included in Demonstration

SafeNet is proud to offer current and future HP CloudSystem customers the ability to test drive ProtectV.

After registering on the HP AllianceOne Marketplace, a customer will be given access to a pre-installed ProtectV environment. They will remote desktop to the HP CloudSystem server where they will have the opportunity to explore the three main components that make up ProtectV; ProtectV Client, ProtectV Manager and KeySecure.

All of the components that make up ProtectV have been virtualized to run in an HP CloudSystem environment. This allows customers to have a completely virtualized environment while still allowing full volume encryption of all virtualized disks.

A guide will be provided to the customers after successfully connecting into the HP CloudSystem remote desktop session. This guide will walk them through:

1) How to install ProtectV Client software on each VM
2) How to set policies for administrator rights to each VM
3) How to initiate encryption and decryption in the VM
4) How to manage the keys used for encrypting and decrypting volumes of data

Customer Demonstration Process

From a workflow perspective, the customers from start to finish will perform the following:

1. **Register**: Initiate registration with HP AllianceOne Marketplace
2. **Connect**: Customer is provided connection details to HP CloudSystem servers via RDP.
3. **Install and Configure**: Customer will have ProtectV and KeySecure fully installed and configured for them to test drive.
4. **Test Drive**: Customer will walk through a series of test case scenarios which will help guide them to obtaining a full understanding of the features and benefits of using ProtectV. Including:

   **Pre-boot Authentication**: Each Virtual Machine which is encrypted with ProtectV will have a pre-boot authorization boot-loader installed. This allows ProtectV to fully encrypt the VM including the Operating System partition.

   **Client Software**: Each virtual machine will have client software installed. This client software allows the ProtectV Manager to communicate with each VM to signal operations such as encryption/decryption messages. This client software can either be
manually installed within the operating system, or can be installed as part of a VM template.

Pre-boot Loader - When a virtual machine boots, it reaches the pre-boot loader, which waits for a key to be provided to decrypt the Virtual Machine. The ProtectV client software and ProtectV Manager, negotiate a secure communications channel. Once this is established, a key is retrieved from the Key Secure virtual appliance.
Boot ProtectV Manager - An administrator can now boot the VM from the ProtectV Manager.

Encrypt Partitions - The administrator can now choose to encrypt partitions which are discovered from the HP CloudSystem environment. Simply clicking Encrypt Partition will start the encryption process. This encryption process can happen while the VM is being used to eliminate any downtime during encryption.
ProtectV Management Console - The ProtectV manager console, provides an overview to an administrator of the current state of all VM’s currently being managed within the HP CloudSystem environment.

Section 5: Contact Information

Pete Catalanello
Phone: 510.326.3423
Email: pete.catalanello@safenet-inc.com