Secure Data in the Cloud by – Strong Cryptographic Encryption, Virtual Machine Protection and Authentication Services

Sheung-Chi NG
Security Consulting Manager, APAC
Sheungchi.Ng@safenet-inc.com
May 2013
Data Security Gaps Remain

How secure is my data in a virtualized world?

VMs are easy to copy (and steal).

VMs are easy to move.

VMs introduces a new class of privileged users and administrators - server, storage, backup, and application - all operating independently.

VMs have multiple snapshots and backups of data.
Challenges in Virtualized & Cloud Environments

**Data Governance**
Lack of Visibility

- Do I know where all my data instances are?
- Can I trace every legitimate replication/copy/instantiation event of my data?
- Can I trace unauthorized copying of my data?

**Data Compliance**
Lack of Data Control

- Who is accessing my data?
- Can I enforce an effective access control policy?
- Can I present a trusted audit trail of all access events to my data?

**Data Protection**
Risk of Breach and Data Loss

- Are all my data instances secure?
- Can I assure only authorized access to my data?
- Can I “pull the plug” on data that’s at risk of exposure?
Encryption enables

Governance / Compliance
- Know about every access event
- Location agnostic
- Non repudiation and attestation

Ownership and Control
- Set effective access policies
- Separation of duties
- Data shredding

Data Security
- Prevent leaks or unauthorized access
- Data isolation
- Sprawl resistant
Just ask the market....

- “In the future, you will encrypt data — both in motion and at rest — by default. This **data-centric approach to security is a much more effective way to keep up with determined cybercriminals.**”

- “Over the next few years, expect to see the adoption of other ways to protect and control data... **The most promising technology is the use of encryption for intellectual property.**”

- “Encryption is becoming a **fundamental technology for protecting data in the cloud.**”

- “As a general rule, **cybercriminals cannot sell encrypted data** in the open markets on the invisible Internet; **encrypted data has no value**, thus destroying malicious actors’ primary incentive to steal it.”
Virtualized Data Security in Action

- Root-of-trust and trusted crypto for virtualized infrastructure
- Cryptographic isolation of virtual machines and storage containers
- Storage encryption for Virtual Storage, CIFS, NFS, and iSCSI

- Hypervisor
- Hardware Layer
- Storage
- Snapshots
- Backup

Strong authentication to virtualized infrastructure
Virtualized Data Security in Action

- Root-of-trust and trusted crypto for virtualized infrastructure
- Cryptographic isolation of virtual machines and storage containers
- Storage encryption for Virtual Storage, CIFS, NFS, and iSCSI

Hypervisor

Hardware Layer

Storage

Snapshots

Backup

Strong authentication to virtualized infrastructure
Secure Cloud-Based Identities and Transactions: SafeNet Hardware Security Options

Establish digital ownership and root of trust in virtual environments

**Security Features**
- Anchored root of trust for digital identities and transactions
- FIPS 140-2 Level 2 security Certified Solution
- Multi-host partitioning 20 – 100 per HSM
- Virtual platform support (Xen/Hyper-V/ESX-i)
- 3rd party partner application support, and integration guides on virtual platforms
- Broad cloud-based platform integration
- Application and data separation
- High performing virtual transactions
Crypto Hypervisor In a Cloud Infrastructure

Enterprise

HSM

Data Secure Link

HSM Client

Cloud Provider

Bound HSM Client

Virtual HSM

Granular Secure Link

Multiple Instances

Partition Sharing

Dedicated Partition

Secure Hardware Key Storage for 20 Partitions

HSM HA Group

VM A

Par #1

Par #2

Par #3

Par #4

Par #5

Par #6

Par #7

Par #8

Par #9

Par #10

Par #11

Par #12

Par #13

Par #14

Par #15

Par #16

Par #17

Par #18

Par #19

Par #20

HSM

HSM Client

SafeNet
Virtualized Data Security in Action

**Hypervisor**

- App
- App
- App
- App
- App
- App
- App
- App

**Hardware Layer**

- OS
- OS
- OS
- OS
- OS
- OS
- OS
- OS

**Storage**

- Snapshots

**Root-of-trust and trusted crypto for virtualized infrastructure**

**Cryptographic isolation of virtual machines and storage containers**

**Storage encryption for Virtual Storage, CIFS, NFS, and iSCSI**

Strong authentication to virtualized infrastructure
Secure Virtual Machines: SafeNet ProtectV™ Instance

Control virtual machines in the cloud with secure instance encryption and authentication

**Security Features**

- FIPS level pre-launch instance encryption
- Secure login interface (HTTPS)
- Password, one time password, and certificate based authentication options
- Event logging and activation notification

**SafeNet DataSecure** (Supplemental Security Option):
- Manages encrypted instances
- Lifecycle key management
- Security policy enforcement
- Access control
Secure Virtual Storage: SafeNet ProtectV™ Volume

Maintain data privacy in shared storage environments with encrypted data isolation

SOLUTION

Security Features

> Multiple cloud storage options:
  > ProtectV™ Volume for storage servers
  > NetApp storage support
  > ProtectFile customer-based encryption
> FIPS 140-2 Level 2 Security Certified Solution
> Centralized Policy and NIST 800-57 Key Lifecycle Management

SafeNet DataSecure (Supplemental Security Option):
- Manages encrypted instances
- Lifecycle key management
- Security policy enforcement
- Access control

On-premise

Virtual Server

Data

ProtectV™ Instance

Storage

THE DATA PROTECTION COMPANY
ProtectV and Scaling in Large Environments

Managing ProtectV instances across the cloud

SafeNet KeySecure (on Premise)
- Centralizes key management for persistence and flexibility
- Secure key creation and storage
- Key archiving and shredding
- Easy integration with ProtectV Manager

SafeNet ProtectV Manager
- Provides centralized management
- Supports either customer premise or cloud deployments
- Manages and coordinates ProtectV Security
- Open APIs to cloud management

On Premise

Cloud APIs and Web Services
- Authentication Automation
- Bulk operations

Protected Volumes
Protected VMs

FIPS 140-2 L3

ProtectV Client

ProtectV Manager
Virtualized Data Security in Action

- **Hypervisor**
  - Storage
  - Snapshots
  - Backup

- **Hardware Layer**

- **Strong authentication to virtualized infrastructure**

- **Root-of-trust and trusted crypto for virtualized infrastructure**

- **Cryptographic isolation of virtual machines and storage containers**

- **Storage encryption for Virtual Storage, CIFS, NFS, and iSCSI**
Secure Virtual Share: SafeNet StorageSecure™

Isolates data in Multi-tenant environments

Health Solutions

Pharmaceutical Solutions

Patient Relationship

Medical-Surgical

NAS, CIFS, iSCSI

Storage Secure

Isolated Data

Storage Head

Shares
Virtualized Data Security in Action

- **Hypervisor**
  - App
  - App
  - App
  - App
  - App
  - App
  - App

- **Storage**
  - OS
  - OS
  - OS
  - OS
  - OS
  - OS
  - OS

- **Snapshots**
  - Backup

- **Root-of-trust and trusted crypto** for virtualized infrastructure

- **Cryptographic isolation of virtual machines and storage containers**

- **Storage encryption for Virtual Storage, CIFS, NFS, and iSCSI**
Secure Access to SaaS: SafeNet Multi-Factor Authentication

Protect access to cloud-based applications via centrally managed authentication

Security Features

> Single authentication solution for both on-premise and cloud-based applications
> Federate identities between on-premise solution to cloud-based solutions using SAML 2.0 protocol
> Solution is form-factor agnostic: support for HW OTP tokens, SW solutions and Out of Band
> Google Apps and salesForce.com are supported out-of-the-box

User authenticates using enterprise identity

Federated SSO to the cloud
Securing VDI Images with Strong Authentication and Encryption

- MobilePASS
- CBA
- OTP

MobilePASS

- MobilePASS
- CBA
- OTP

RADIUS Server (not required for CBA)

SafeNet Authentication (On Premise or Cloud)

Encrypted Storage of VDI Images
- ProtectV for VMware Virtual Storage
- StorageSecure for NAS/SAN
Customer: AXXXXX – The largest cloud service provider

1. Device registration request

2. Get encrypted key

3. Send encrypted key to Proxy server

4. Decrypt request sent to HSM

5. HSM decrypts registration key

Video Viewing Device (ie; TV, Xbox)

Device Key DB

Video Content Server

Decryption Proxy Server

SFNT HSMs @ AXXXXX sites globally
Customer: FXXX MXXX - Property loan

- **Need?**
  - FXXX MXXX hosts borrower or loan servicer information along with credit scores and other personal information. They plan to move their information to AWS cloud (cost savings). Their security team will not allow any server on the cloud unless the personal information on databases hosted in public cloud is protected (i.e. encrypted).

- **Why are they interested in ProtectV?**
  - Unique AWS solution
  - Key Management on premise
  - Encrypting the entire VM
  - AWS Referral

- **Environment?**
  - AWS VPC Public Cloud
  - Handful of servers
  - Want to encrypt everything that goes into the cloud
Customer: One of the largest oil & energy companies

- **Need?**
  - On a constant basis, customer is leveraging satellites and a fleet of ships to gather intelligence on petroleum deposits (i.e. ‘where to drill’). The images and data gathered represent a core business asset—so safeguarding this information is critical. The security team within XXXXX was eager to leverage encryption to institute granular security controls over the data stored in its data center.

- **Why are they interested in Storage Encryption in NAS?**
  - Key Management
  - Easy to use
  - Transparent and separate of duty
  - High performance

- **Environment?**
  - NAS Storage environment
  - Terabyte of data generated each hour
Customer : TXX - Logistics company

- No infrastructure deployed to TXX Express premises
- Resilient cloud based service allowing for easy re-use of the service globally
- Low per user per month token cost allowing for integration with the remote access service, offering an integrated and robust solution
  - Cost the same as old remote access solution but offers,
    - Strong authentication as standard
    - More flexible access options
- Flexible form factors allowing easier deployment and acceptance of the technology
- Lower TCO of the existing Authentication solution
- **Time to provision a user down from 5 days to 30 minutes**
SafeNet Solutions for Virtualized Architectures

Root-of-trust and trusted crypto

Isolation of virtual machines

Virtual Machine

Application

Guest OS

Compute

CPU

Virtual Compute

Virtual Network

Storage

NAS / SAN

Physical Network

Database As-A-Service

Network

Strong Authentication

Storage Encryption

Management
Thank You

Sheung-Chi NG
Security Consulting Manager, APAC
Sheungchi.Ng@safenet-inc.com
May 2013