RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

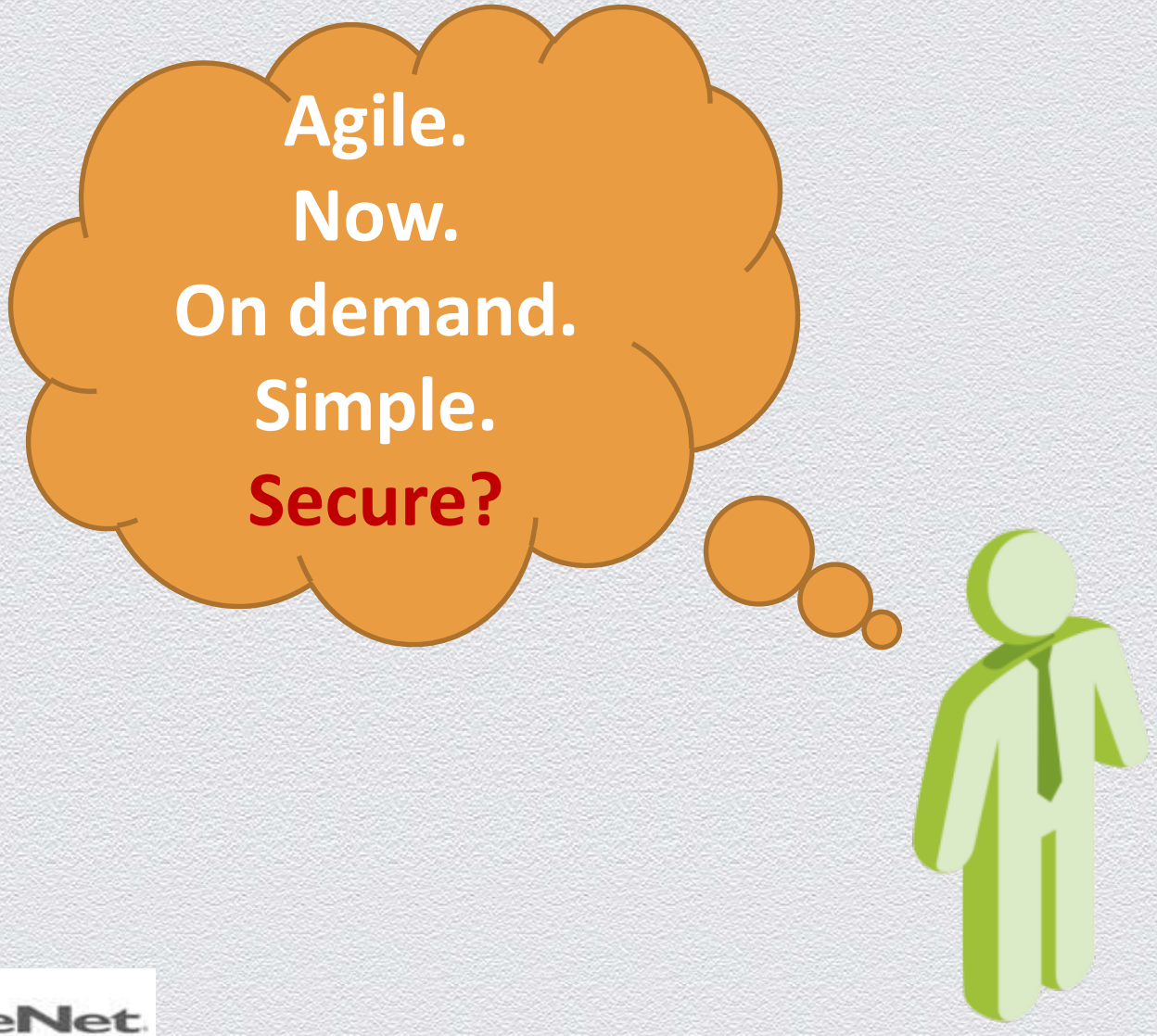
Whose Cloud Is It Anyway? Exploring Data Security, Ownership and Control

SESSION ID: CDS-T11

Sheung-Chi NG

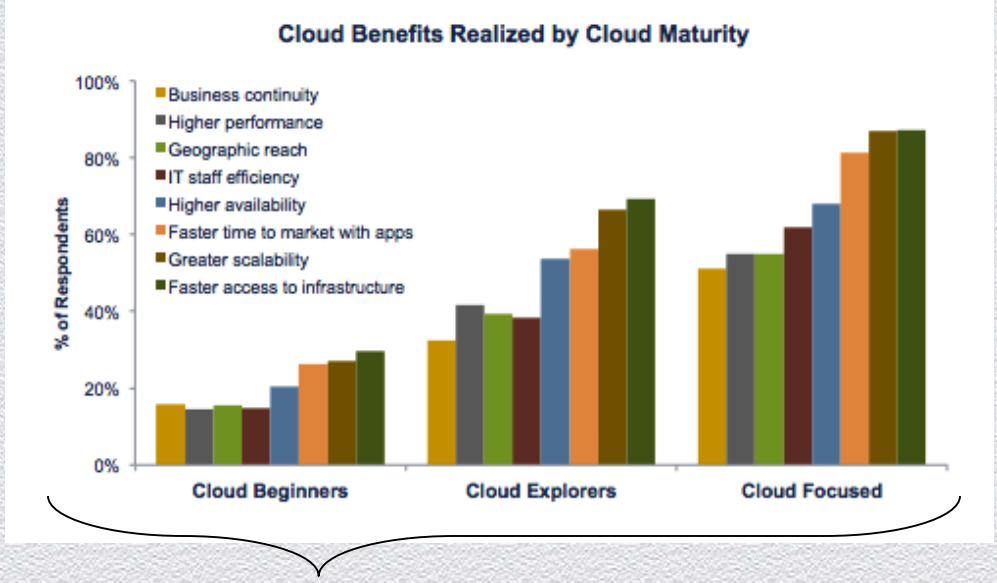
Senior Security Consulting Manager, APAC
SafeNet, Inc.

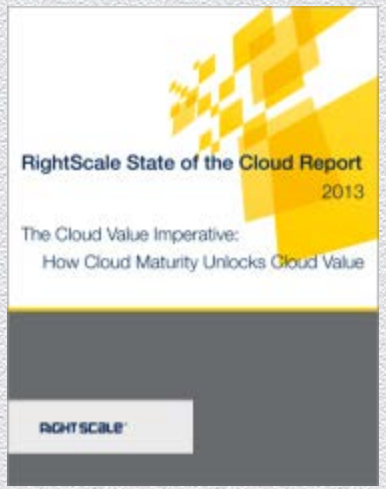
Cloud and Virtualization Are Change the Way IT is Managed and Consumed



Cloud Benefits Are Being Realized…

- 80% of mature cloud adopters are seeing:[1]
  - Faster access to infrastructure
  - Greater Scalability
  - **Faster Time to Market** for Applications
- 50% of cloud users report benefits including:[1]
  - Better application performance
  - **Expanded geographic reach**
  - Increased IT staff efficiency



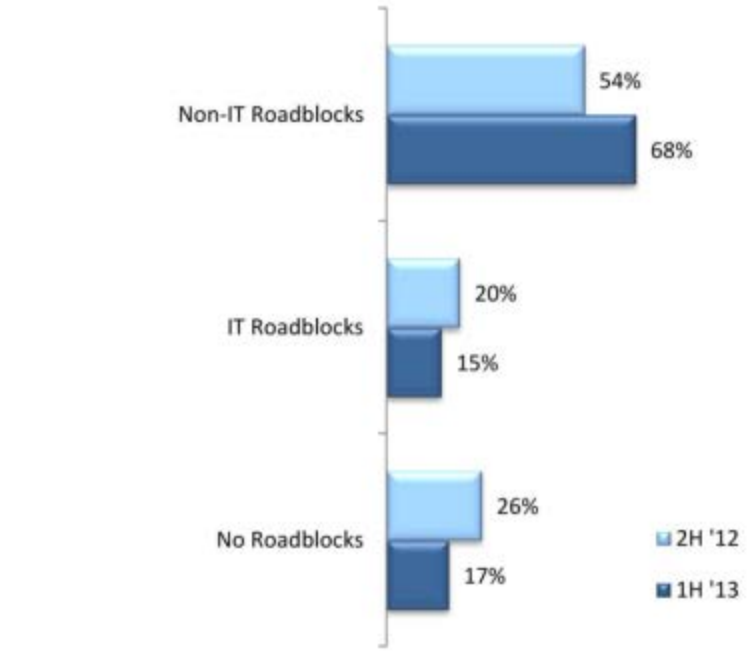


[1] *RightScale State of the Cloud Report 2013*

…But Cloud Benefits Are Driven by Sharing

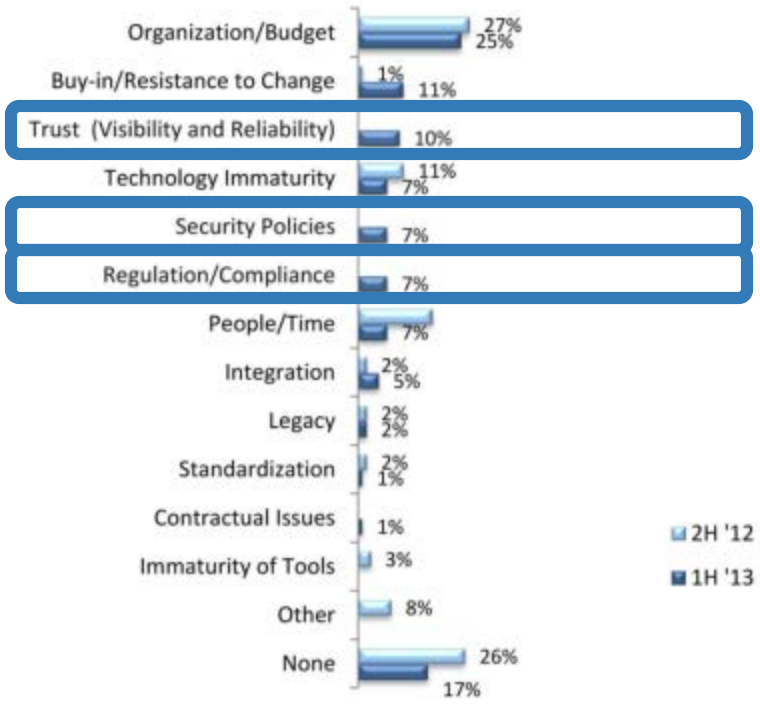
And Security and Compliance Are Not the Biggest Fans of Sharing…

Leading Inhibitors to Cloud Adoption



Are there any roadblocks inhibiting you from reaching the next phase of your cloud computing initiatives?

2H '12, n=100; 1H '13, n=100.



If yes, please explain.

Source: Cloud Computing – Wave 5 | © 2013 451 Research, LLC. www.451research.com

451 TheInfoPro 2013 Cloud Computing Outlook – Cloud Computing Wave 5

Security and Compliance Concerns With Shared Clouds

Data Governance Lack of Visibility	• Can you track all of my data instances? Backups? Snapshots? • Am I aware of government requests/discovery? • Do you knew when data is copied/moved ?
Data Compliance Lack of Data Control	• Who is accessing my data? • Can I illustrate compliance with internal and external mandates? • Is there an audit trail of access 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 or who's lifecycle has expired?

How Do You Maintain Ownership and Control Of Your Information In A Multi-Tenant Environment?

SafeNet

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

Encryption: Un-Sharing in a Shared Environment

Strong encryption with key management is one of the core mechanisms that Cloud Computing systems should use to protect data. While encryption itself doesn't necessarily prevent data loss, safe harbor provisions in laws and regulations treat lost encrypted data as not lost at all. The encryption provides resource protection while key management enables access to protected resources.

- **Cloud Security Alliance**, Security Guidance for Critical Areas of Focus in Cloud Computing

Companies are looking to protect data in the cloud through encryption keys and robust key management. This enables companies to secure data from breaches as well as prevent the cloud provider from accessing the information if they decide to end their relationship with the cloud provider.

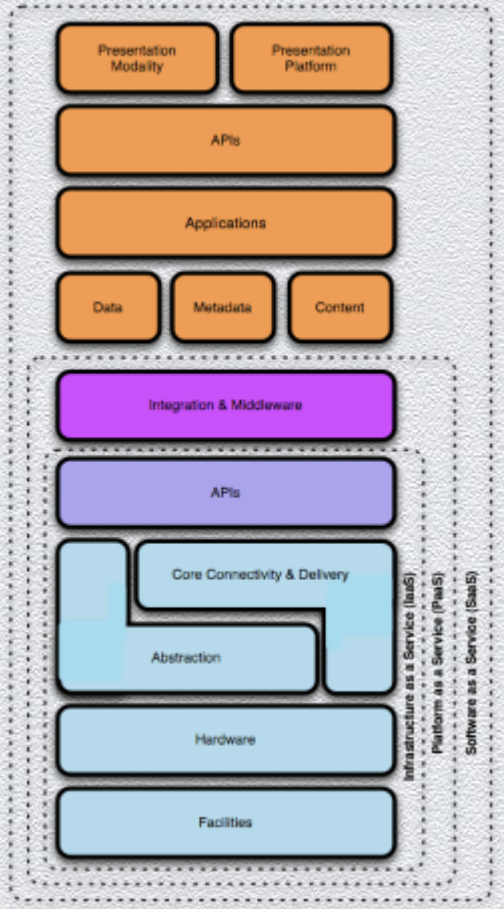
- **Frost and Sullivan**, Michael Suby

Encryption is one of the best ways to secure corporate data in the cloud, but it has to be encryption that the company controls.

- **Forrester Research**, Jonathan Penn

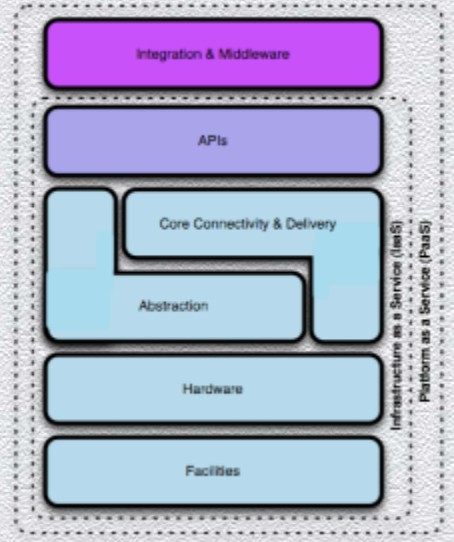
Risk – Control

Salesforce - SaaS

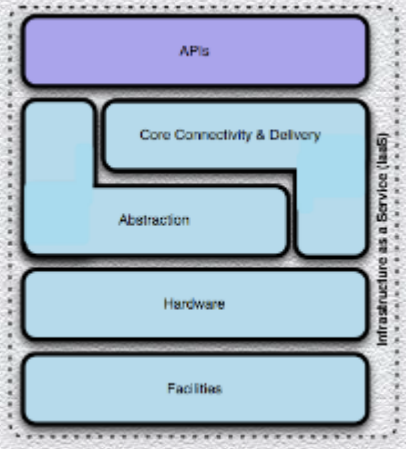


The lower down the stack the Cloud provider stops, the more security **you** are tactically responsible for implementing & managing yourself.

Google AppEngine - PaaS

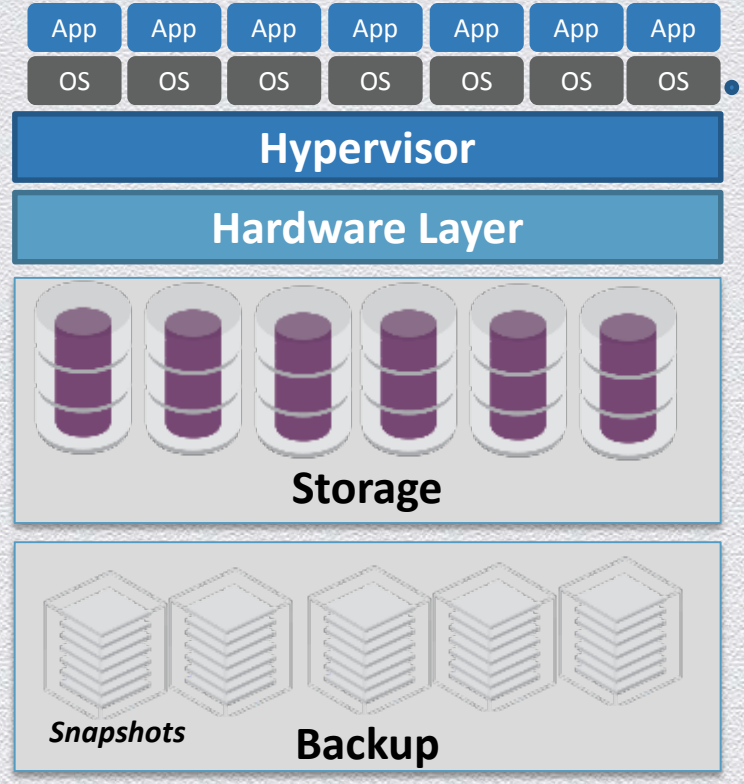


Amazon EC2 - IaaS



Source: Control Quotient: Adaptive Strategies For Gracefully Losing Control (RSA US 2013) by Josh Corman and David Etue. "Stack" by Chris Hoff -> CSA

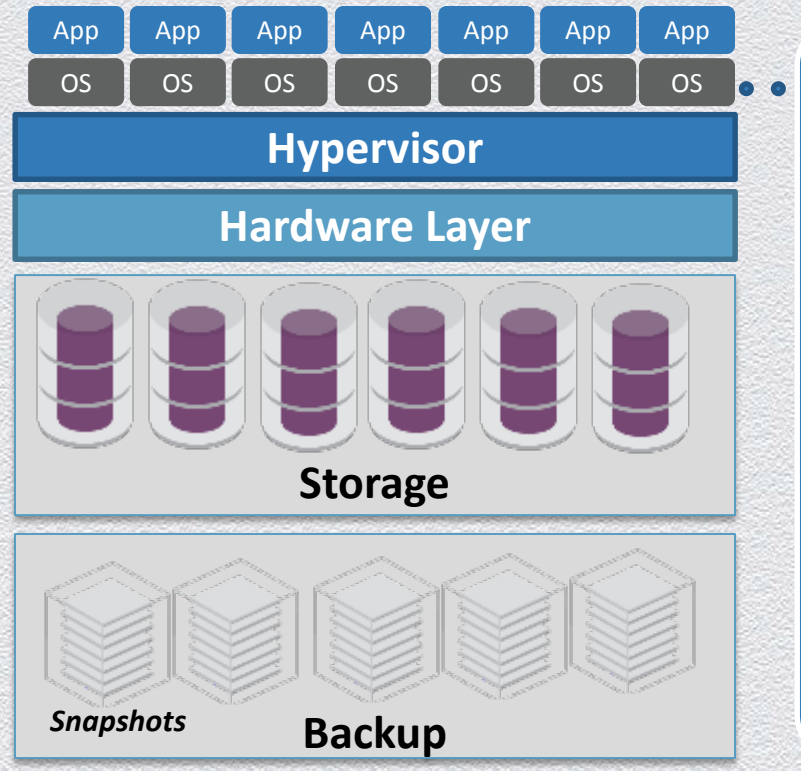
Cloud Data Protection –Data Security, Control & Ownership



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

Cloud Data Protection –Data Security, Control & Ownership



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

Root-of-trust and trusted crypto for virtualized infrastructure

PROBLEM

Loss of Digital Ownership and Control

Secure Digital Signing and PKI in the Cloud

Proving you are you

- Where is root of trust in Digital Signing and PKI when it's all virtual?
- The challenge of attesting to ownership in a virtual world
- Current focus of virtualization research

Maintaining Keys in clouds

- **When your cloud provider handles keys**
  - Appropriate key material
  - Proper lifecycle and policy handling
  - Privileged user abuse

KEY POINTS

- Broad cloud-based platform integration
- Application and data separation
- High performing virtual transactions

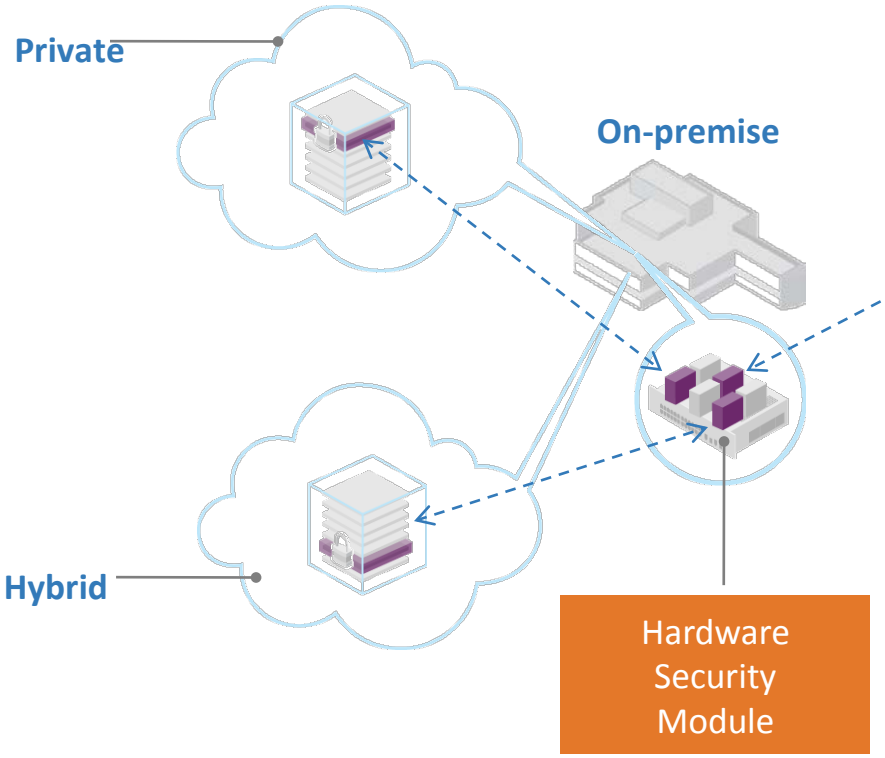
The Cryptography and Entropy Problem

- **Difficult to get true randomness in highly replicated and automated cloud**
- **Flaws in cryptographic functions have huge consequences**
  - September 2010 .NET encrypted cookie problem affects 25% of Internet servers.

SOLUTION

Secure Cloud-Based Identities and Transactions:
Hardware Security Options

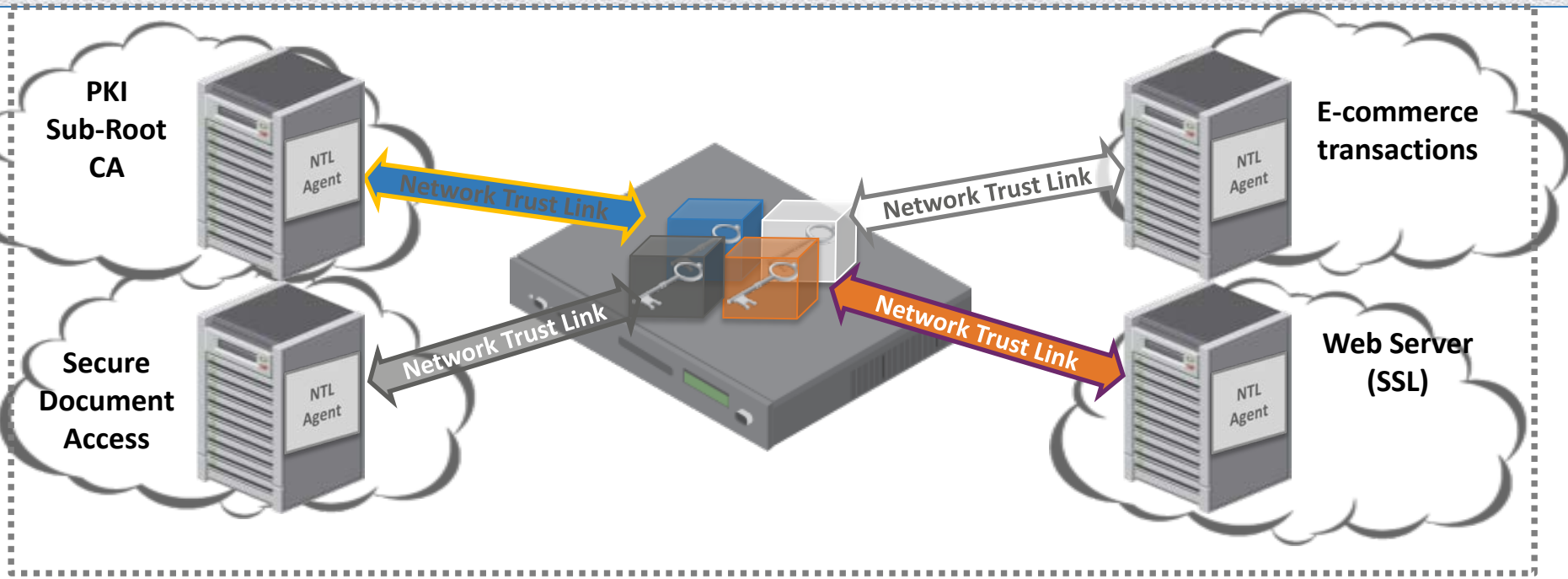
Establish digital ownership and root of trust in virtual environments



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-as-Service



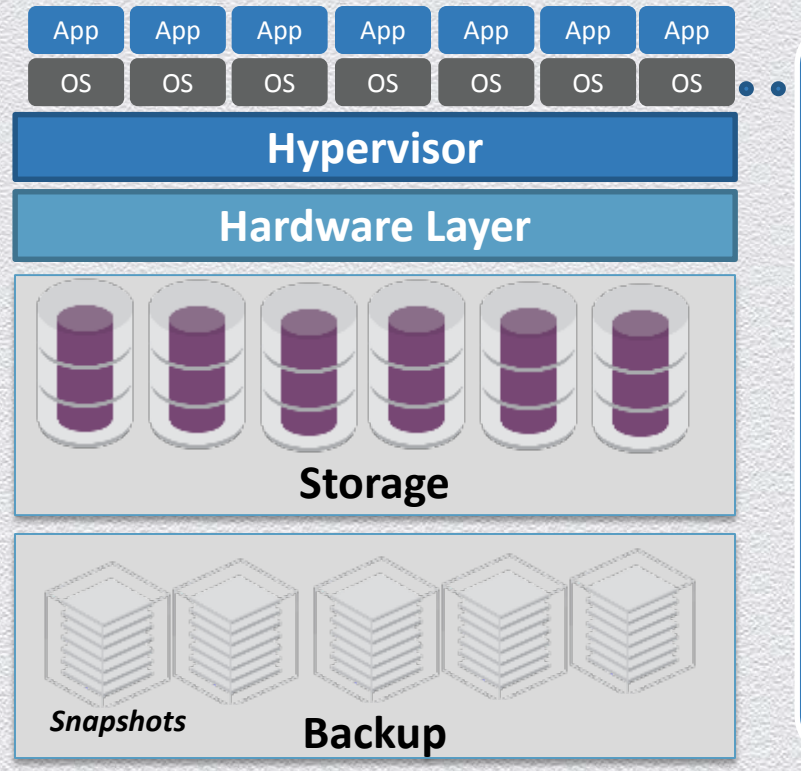
Reduced cost of ownership

- Amortize HSM over multiple applications, organizations, services
- Fewer boxes to buy, install and manage

Centrally managed cryptographic keys

- More secure and simpler to administer
- Keys replicated securely
- Centralized management

Cloud Data Protection –Data Security, Control & Ownership



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

Cryptographic isolation of virtual machines and storage containers

PROBLEM

Securing Uncontrolled Virtual Instances

Achieving compliant isolation and separation of duties in multi-tenant environments

Unlimited Copying of Instances

- **Instances could be copied without awareness**
  - No visibility to instance location, no audit trail
- **Instances used by competitors and malicious users**
- **Enables unlimited brute force attacking**
  - Return to original copy for next iteration of password guessing

Unsecured Container of Confidential Data

- **Identical to lost or stolen laptop, except the instance is often a server**
- **Virtual nature of makes the potential surface area much larger**
  - Not just a single entity lost, potentially unlimited number

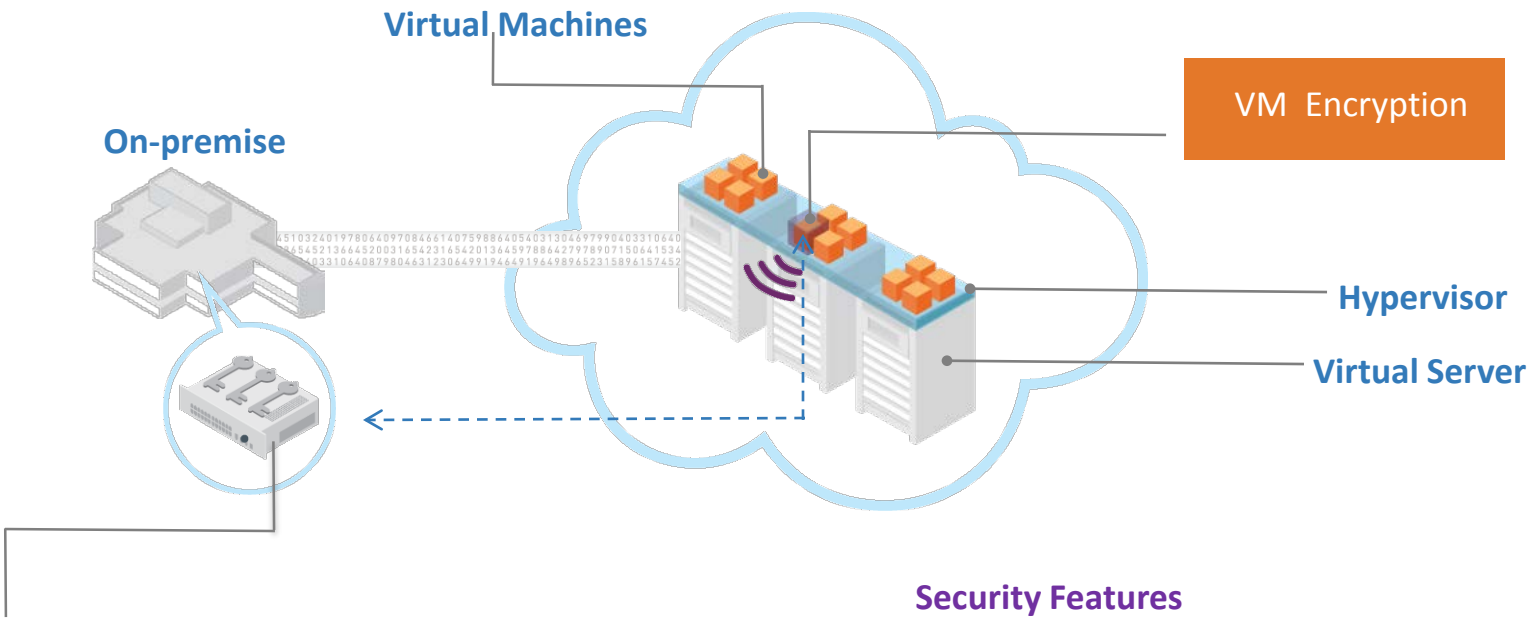
KEY POINTS

- Data Isolation
- Separation of Duties
- Cloud Compliance
- Pre-Launch Authentication
- Multi-Tenant Protection

SOLUTION

Secure Virtual Machines

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



Key Management HW (Supplemental Security Option):

- **Manages encrypted instances**
- **Lifecycle key management**
- **Security policy enforcement**
- **Access control**

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

PROBLEM

Maintain Trust & Control in Virtual Storage Volumes

Loss of ownership in a shared storage environments

Issue of Data Leakage

- **Requires trust in meta-tagging or data isolation strategy of cloud provider**
- **Risks from misconfiguration and cloud administrators**
- **Regulatory evidence of privacy and integrity controls**

Trust and Control Issues

If cloud provider offers encryption:

- **Proper Key Handling**
  - NIST Lifecycle compliance
  - Strength, uniqueness, rotation, etc.
- **NIST approved algorithms**

Administration trust

- **Separation of Duties**

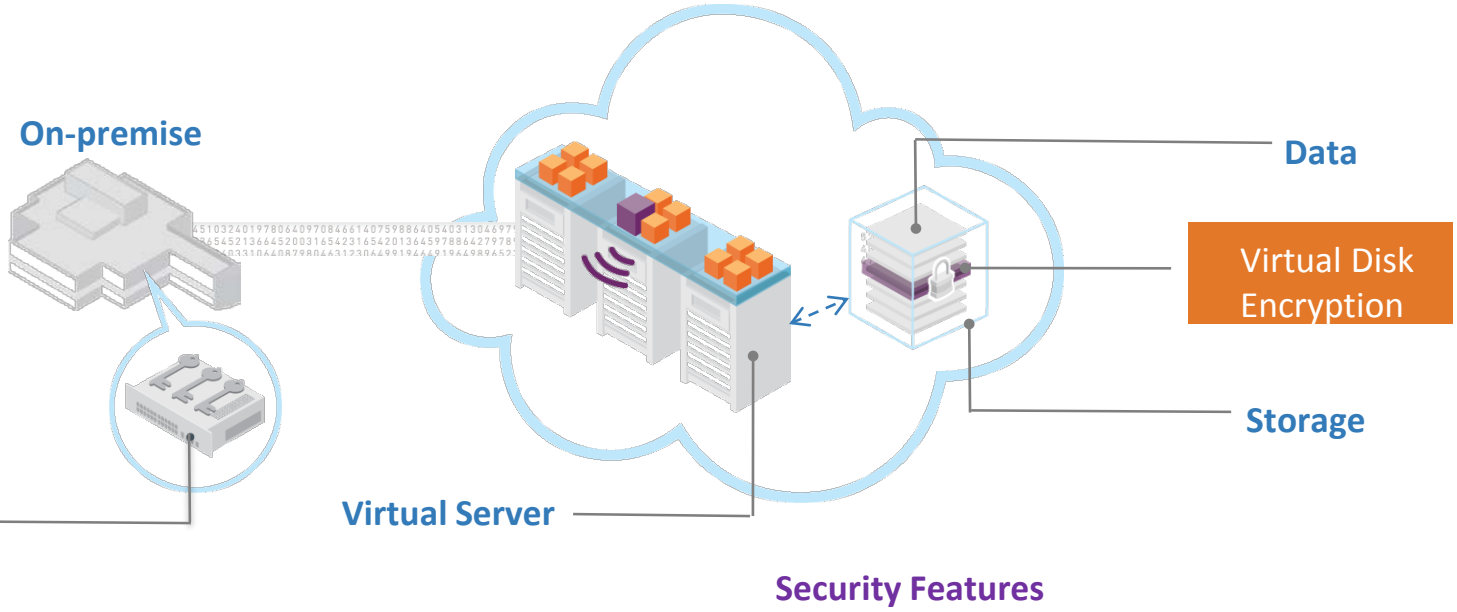
KEY POINTS

- Data Isolation
- Cloud Compliance
- Multi-Tenant Protection

SOLUTION

Secure Virtual Storage

Maintain data privacy in shared storage environments with encrypted data isolation



Key Management HW (Supplemental Security Option):

- **Manages encrypted instances**
- **Lifecycle key management**
- **Security policy enforcement**
- **Access control**

Security Features

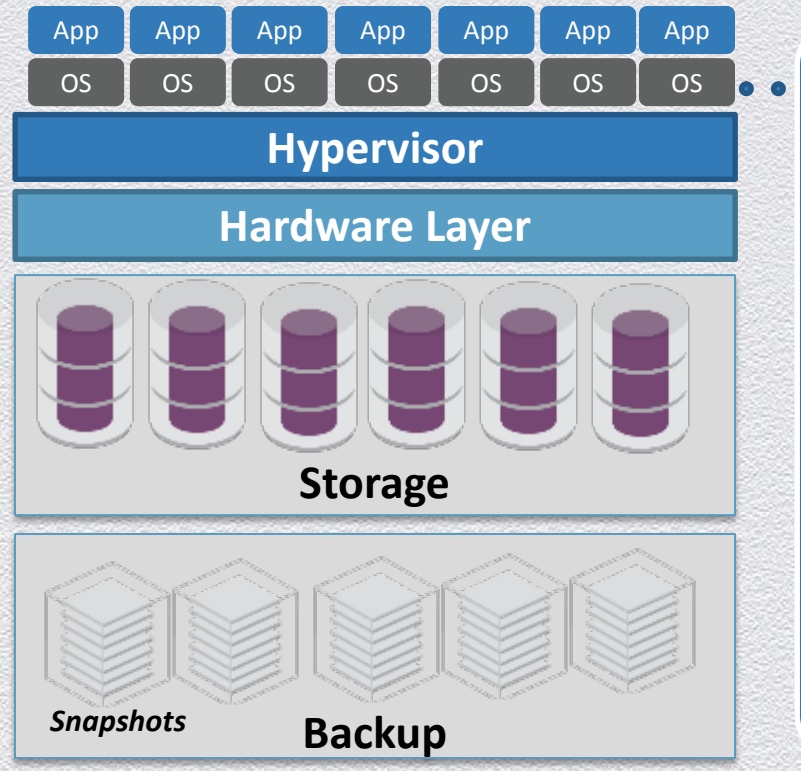
> Multiple cloud storage options:

> Encrypting volume for storage servers

> FIPS 140-2 Level 2 Security Certified Solution

> Centralized Policy and NIST 800-57 Key Lifecycle Management

Cloud Data Protection –Data Security, Control & Ownership



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

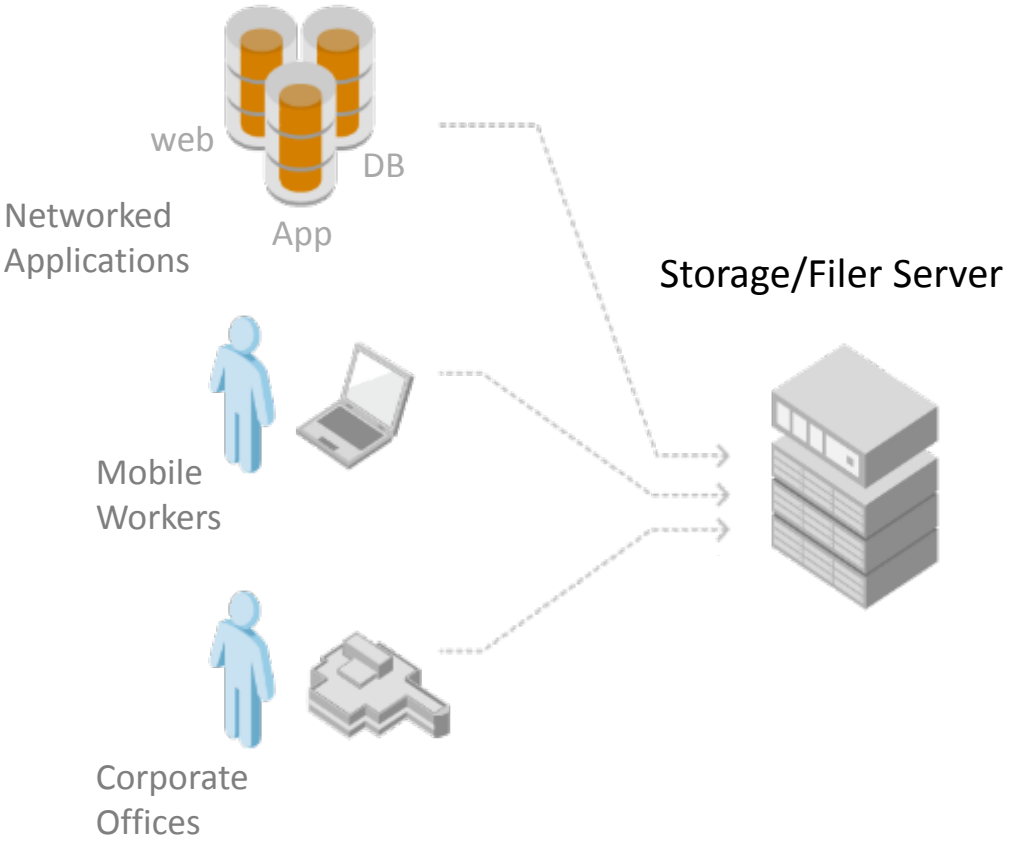
Storage encryption for Virtual Storage, CIFS, NFS, and IP-SAN

SafeNet

PROBLEM

Securing Uncontrolled Shared Storage

Achieving compliant isolation and separation of duties in multi-tenant environments



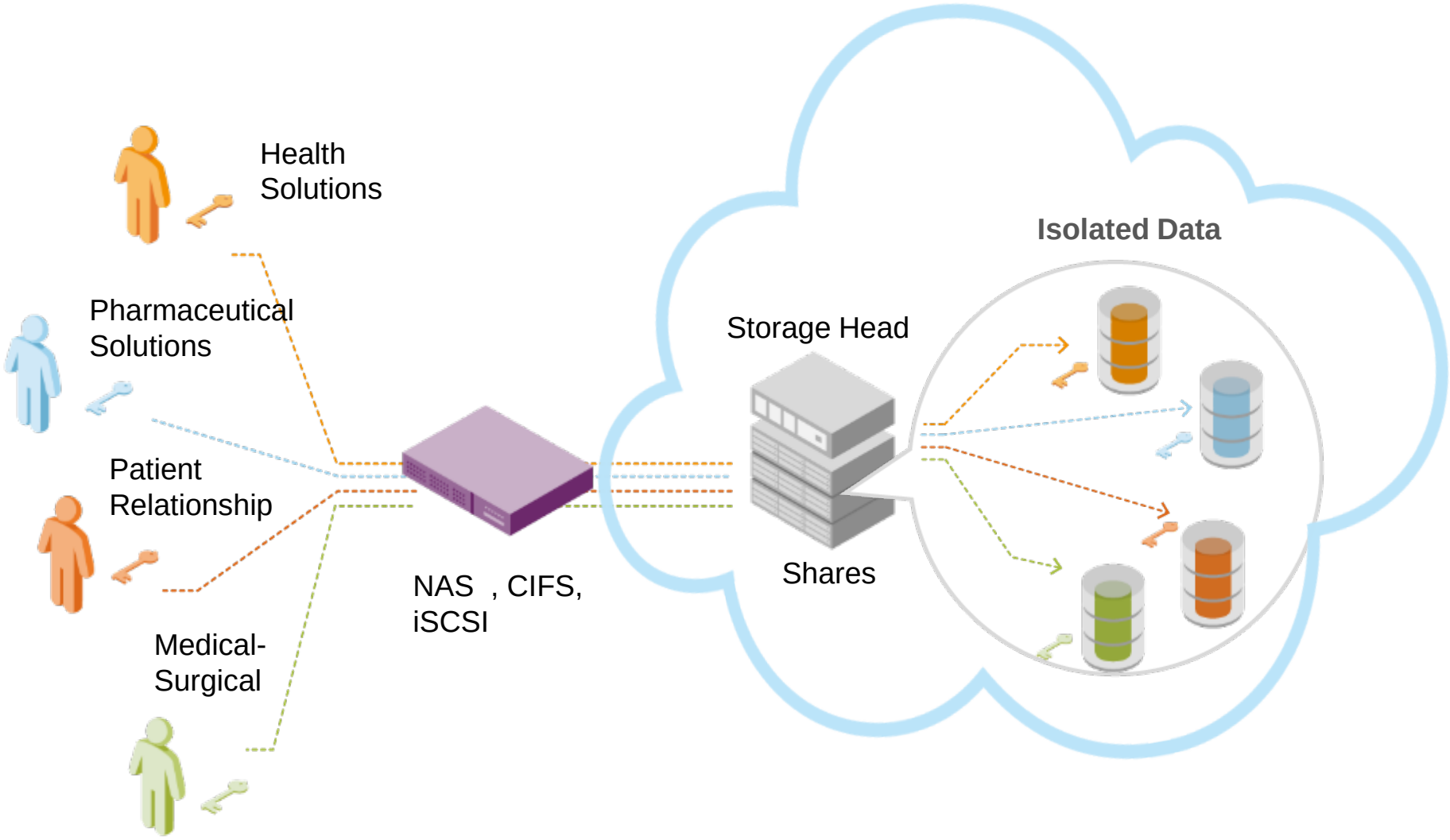
KEY POINTS

- Data Isolation
- Separation of Duties
- Cloud Compliance
- Multi-Tenant Protection

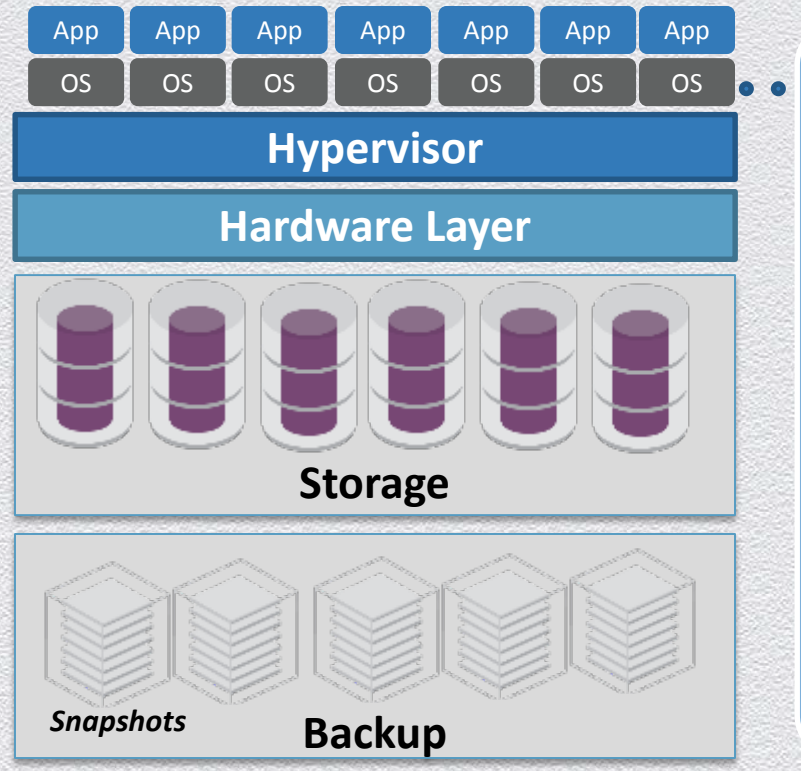
- **No encryption**
  - Everyone can see and manipulate all data files
  - Anyone who manages data can access it
  - Only secure when drive is powered off
  - No separation of duties or data isolation

Secure Virtual Share

Isolates data in Multi-tenant environments



Cloud Data Protection –Data Security, Control & Ownership



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

Strong authentication to virtualized infrastructure

PROBLEM

Controlling Access to SaaS and Cloud Applications

Keeping data secure when you don't own the system

Enforcing Authentication Strategy in the Cloud

- **Multi-Factor authentication required for any apps**
  - Cloud or Physical (Any devices "BYOD")
- **Likely even more critical for cloud-based applications**
  - Lower level of trust, invocation of additional regulatory requirements

Authentication Sprawl

- **Separate authentication systems for each cloud provider**
  - Operationally un-scalable
  - Typical user password/authentication fatigue and weak passwords

Preserving Flexibility

- **Likely to use multiple cloud providers simultaneously**
- **Desire rapid re-provisioning to try new services**
- **Preserve options in chaotic cloud market**
  - The cloud market will consolidate- not if, but when

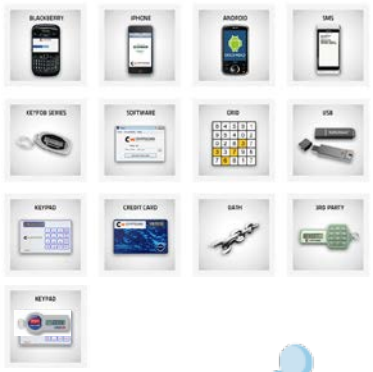
KEY POINTS

- Single Sign On Access
- Federated Identities
- Seamless Integration
- Rapid Provisioning

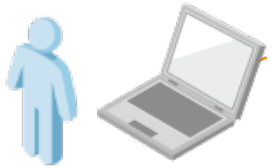
SOLUTION

Secure Access to SaaS

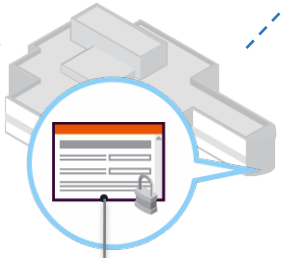
Protect access to cloud-based applications via centrally managed authentication



Federated SSO to the cloud



User authenticates using enterprise identity

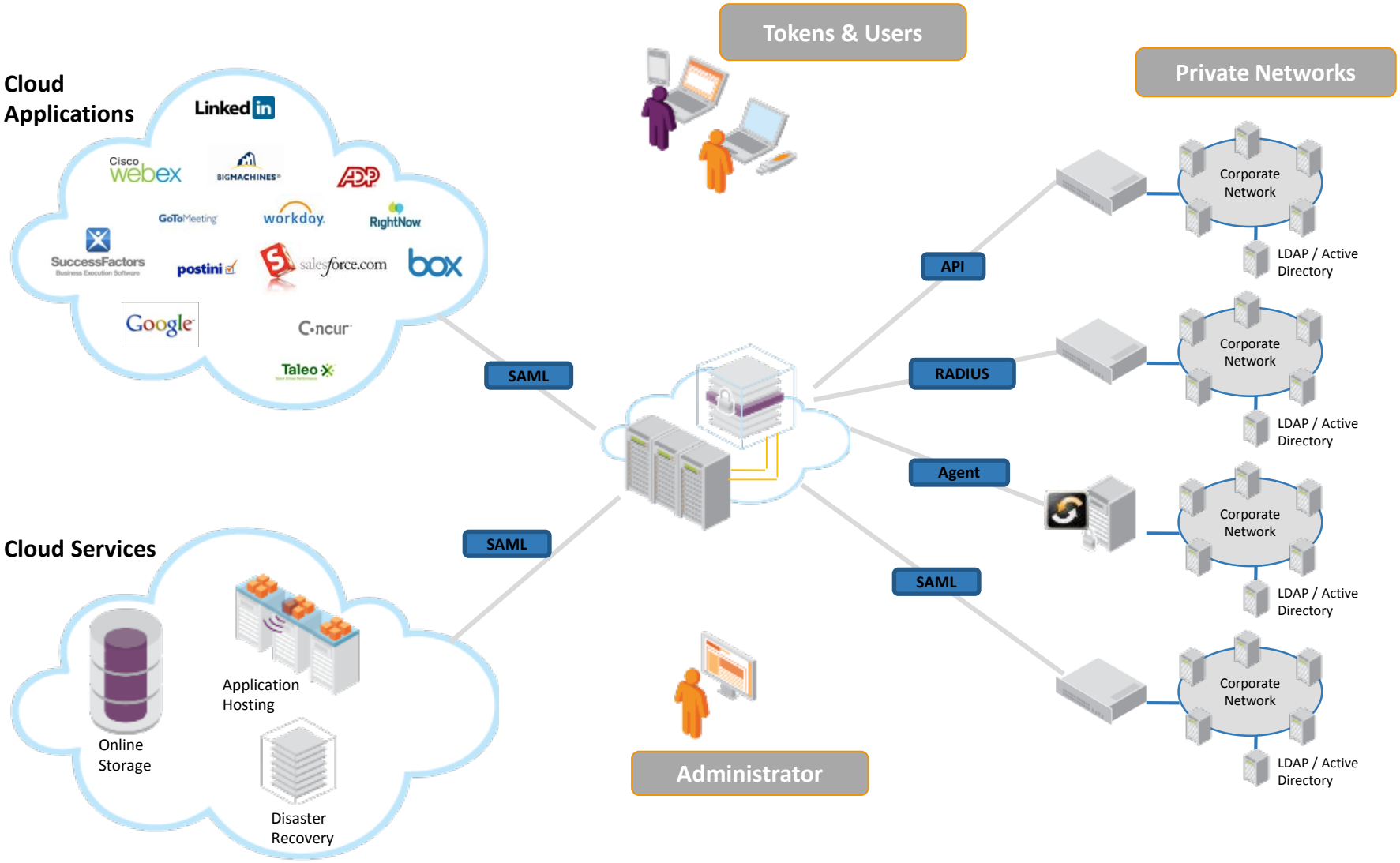


On-Premise Authentication Server

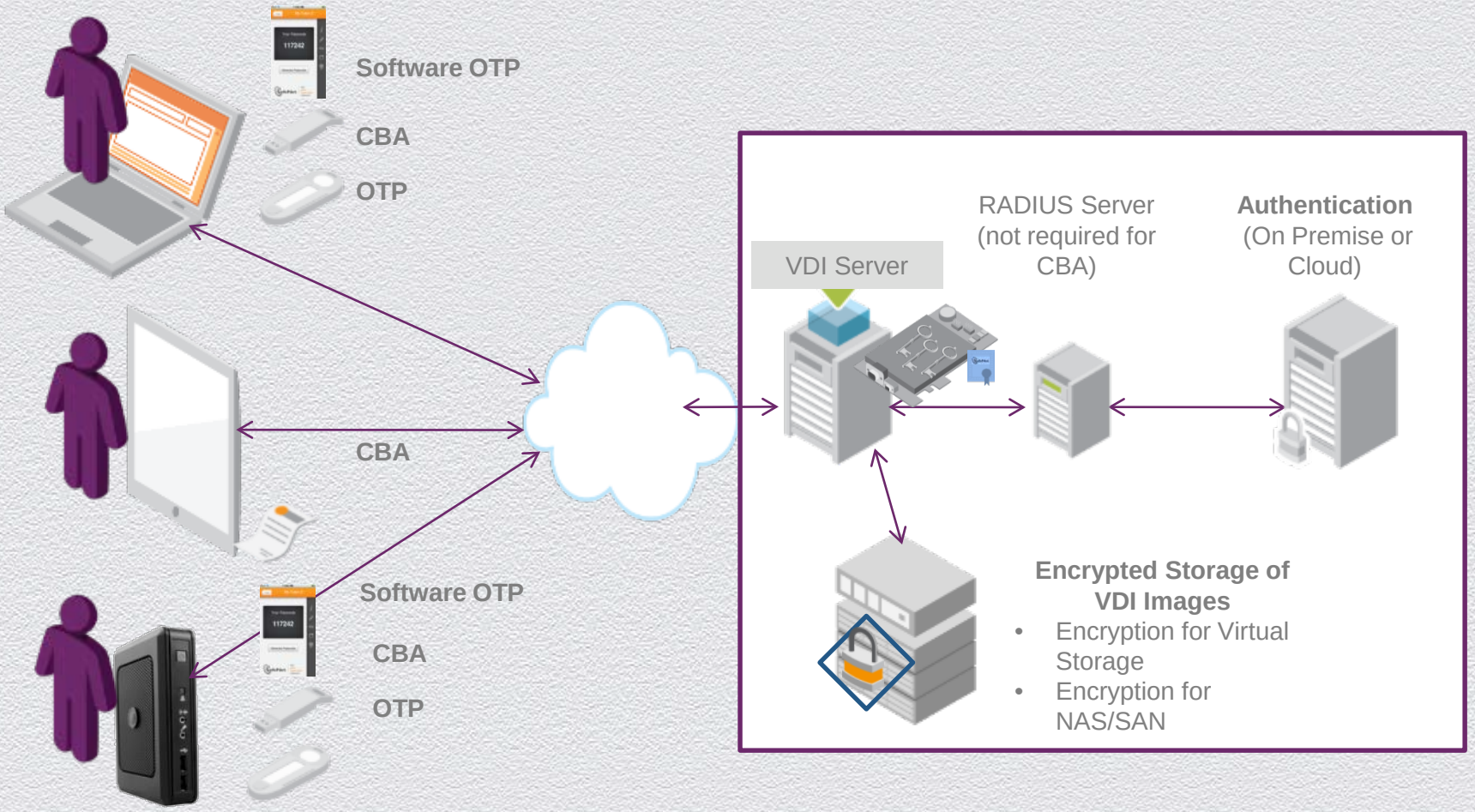
Security Features

- 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

Protect Everything: Networks, Applications and Authentication as a Service



Securing VDI Images with Strong Authentication and Encryption



SafeNet

#RSAC

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Encryption: Un-Sharing in a Shared Environment

Strong encryption with key management is one of the core mechanisms that Cloud Computing systems should use to protect data. While encryption itself doesn't necessarily prevent data loss, safe harbor provisions in laws and regulations treat lost encrypted data as not lost at all. The encryption provides resource protection while key management enables access to protected resources.

- **Cloud Security Alliance**, Security Guidance for Critical Areas of Focus in Cloud Computing

Companies are looking to protect data in the cloud through encryption keys and robust key management. This enables companies to secure data from breaches as well as prevent the cloud provider from accessing the information if they decide to end their relationship with the cloud provider.

- **Frost and Sullivan**, Michael Suby

Encryption is one of the best ways to secure corporate data in the cloud, but it has to be encryption that the company controls.

- **Forrester Research**, Jonathan Penn