SafeNet | THE DATA PROTECTION COMPANY

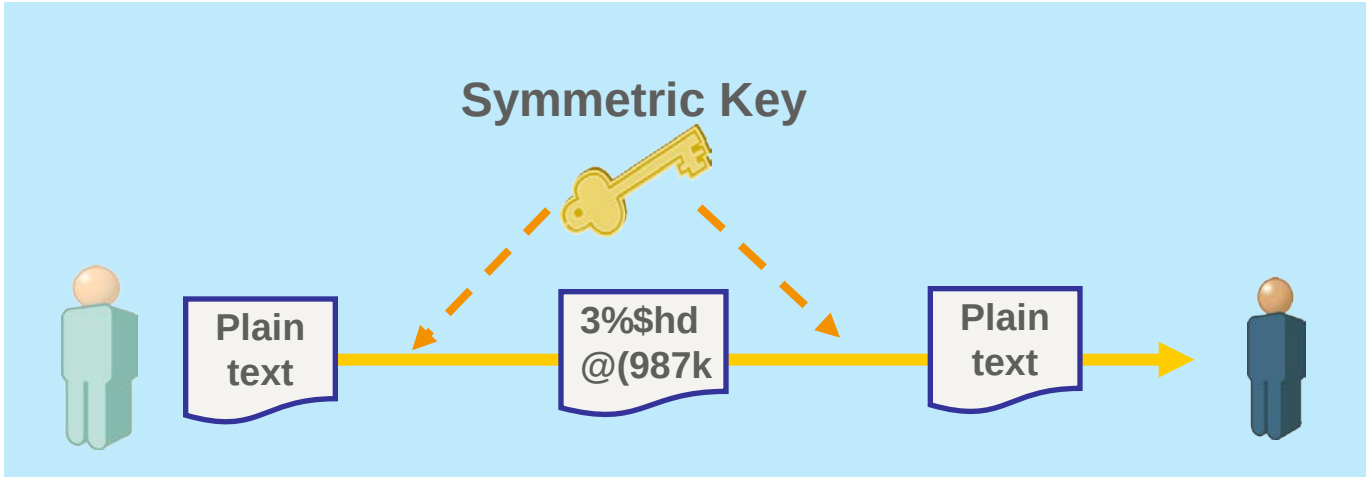
Data Protection:
From PKI to Virtualization & Cloud

Raymond Yeung CISSP, CISA
Senior Regional Director, HK/TW, ASEAN & A/NZ
SafeNet Inc.

Agenda

- What is PKI ? And Value ?
- Traditional PKI Usage
- Cloud Security Challenge
- Solutions

Symmetric Encryption – 1 key



- One key used for both encryption and decryption
- Problem: How to get the one encryption key to both users

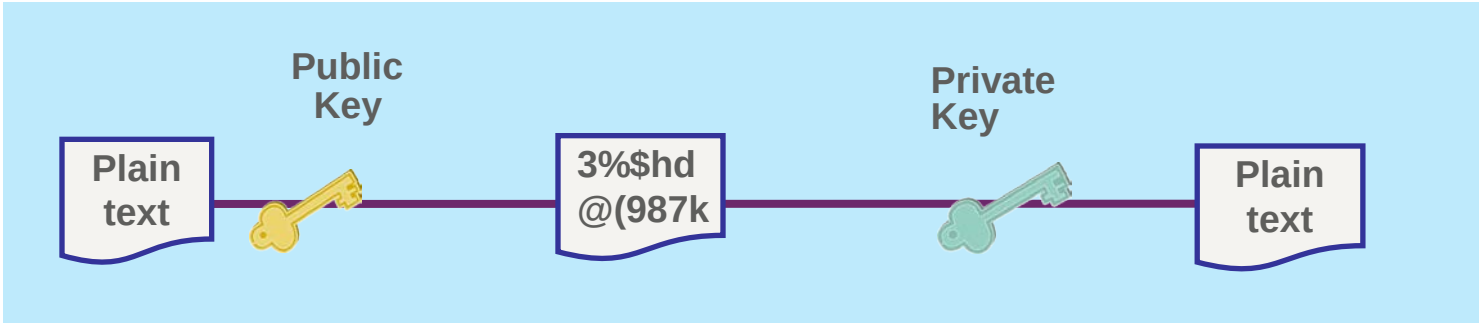
  ….and make sure no one else gets a copy
- Problem: $_nC_2$ keys are needed for n users

  n =100 users, 4950 keys are needed

  n = 200 users, 19,900 keys are needed

  n = 300 users, 4,455,100 keys are needed

Asymmetric Encryption – 2 keys

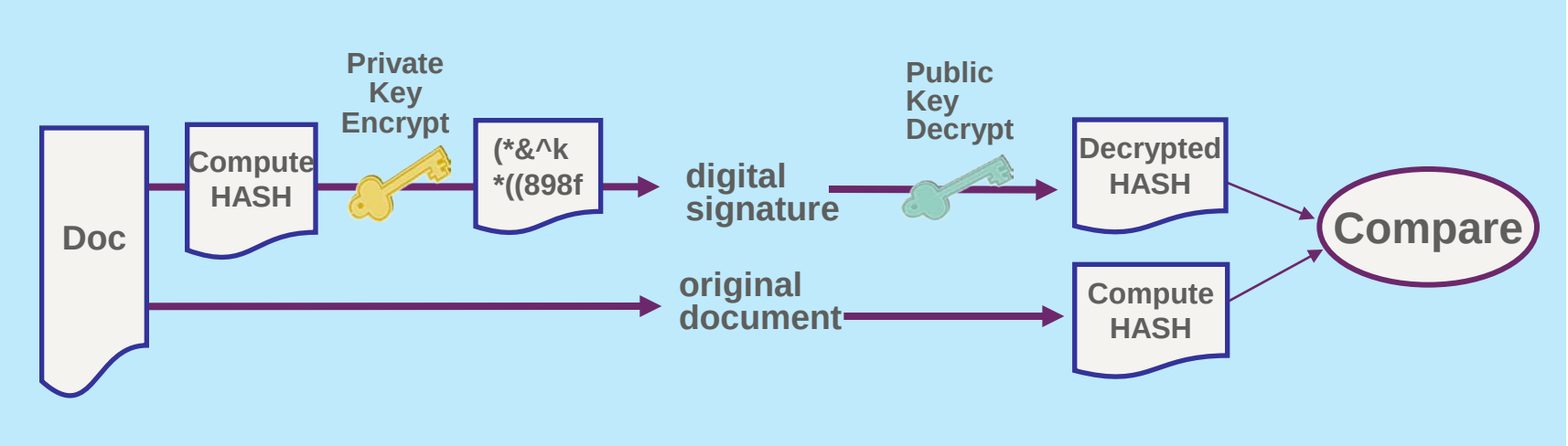


“Public” key - Publish public key in directories etc.

“Private” key - Keep private key “close to your chest”

Encrypt with “Public” key → Decrypt with “Private” key

Digital Signatures



Digital signature is a private key encryption of a HASH e.g. SHA-256

To test a document's authenticity

- Decrypt the signature
- Compare that to a computed HASH of the original document

A digital signature has no effect on the original document

What is a digital identity?

- An asymmetric key pair assigned to a particular individual
  - Implemented using a digital certificate
  - Contains information about you…name etc. plus your public key
  - Certificate is digitally signed by a trusted source e.g. Hongkong Post, VeriSign
  - It's like issuing a digital passport

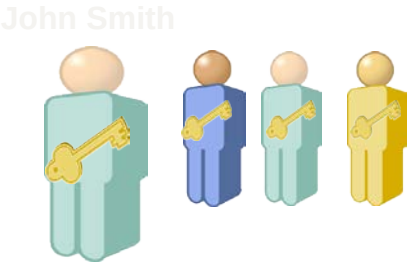
How do you use your digital identity?

- Use your private key to digitally sign documents
- Others verify your signature with the public key on your certificate

What is a PKI? (Public Key Infrastructure)

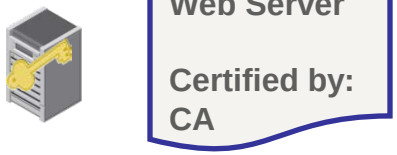
- System to deploy and manage digital identities

Issue digital identities
Revoke digital identities
Publish public keys via directories



Value of PKI

- Create Digital Identity for User/Application/Device/Server in eWorld to achieve

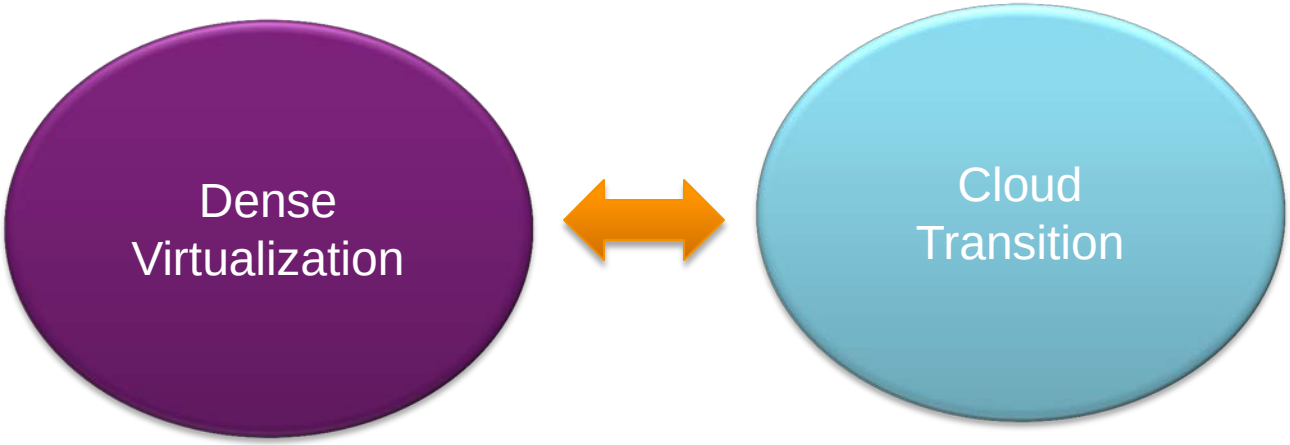


- Confidentiality – Data Encryption
- Integrity - Digital Signature
- Authentication – Digital Signature
- Authorization - Certificate
- Non-repudiation - Digital Signature + Certificate

Traditional PKI Usage

- Customer Facing website like Online Banking, Secure Websites
  - SSL Certificate in Web Server
  - End User Certificate in USB-Token or Smart Card
- Critical Application in Gov
  - SSL Certificate in Web Server
  - Application Certificate in Critical Application
- Cross Border Identity Verification
  - Electronic Passport
- Inter-bank financial transactions
  - Server Application for Cross Border financial transaction
- Enterprise security solution

Virtualization & Cloud Mania

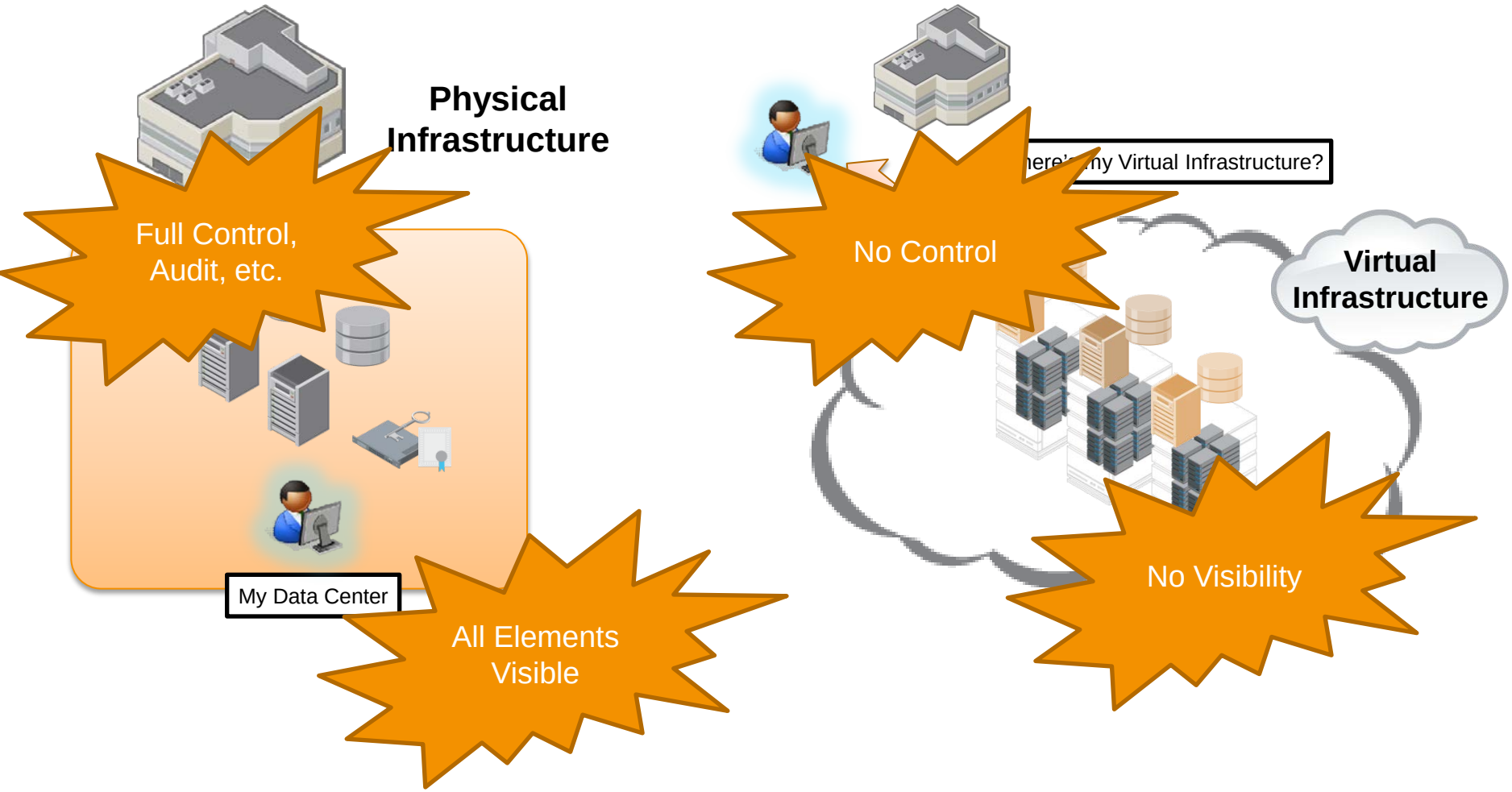


- 39.4% of all servers virtualized
- Average enterprise has 470 virtual servers and 200 are mission critical
- By 2018, 86% of workloads will be running in virtual machines

- 60% of organizations with virtualization have private or public cloud computing in pilot or production
- 70% have VDI in pilot/production

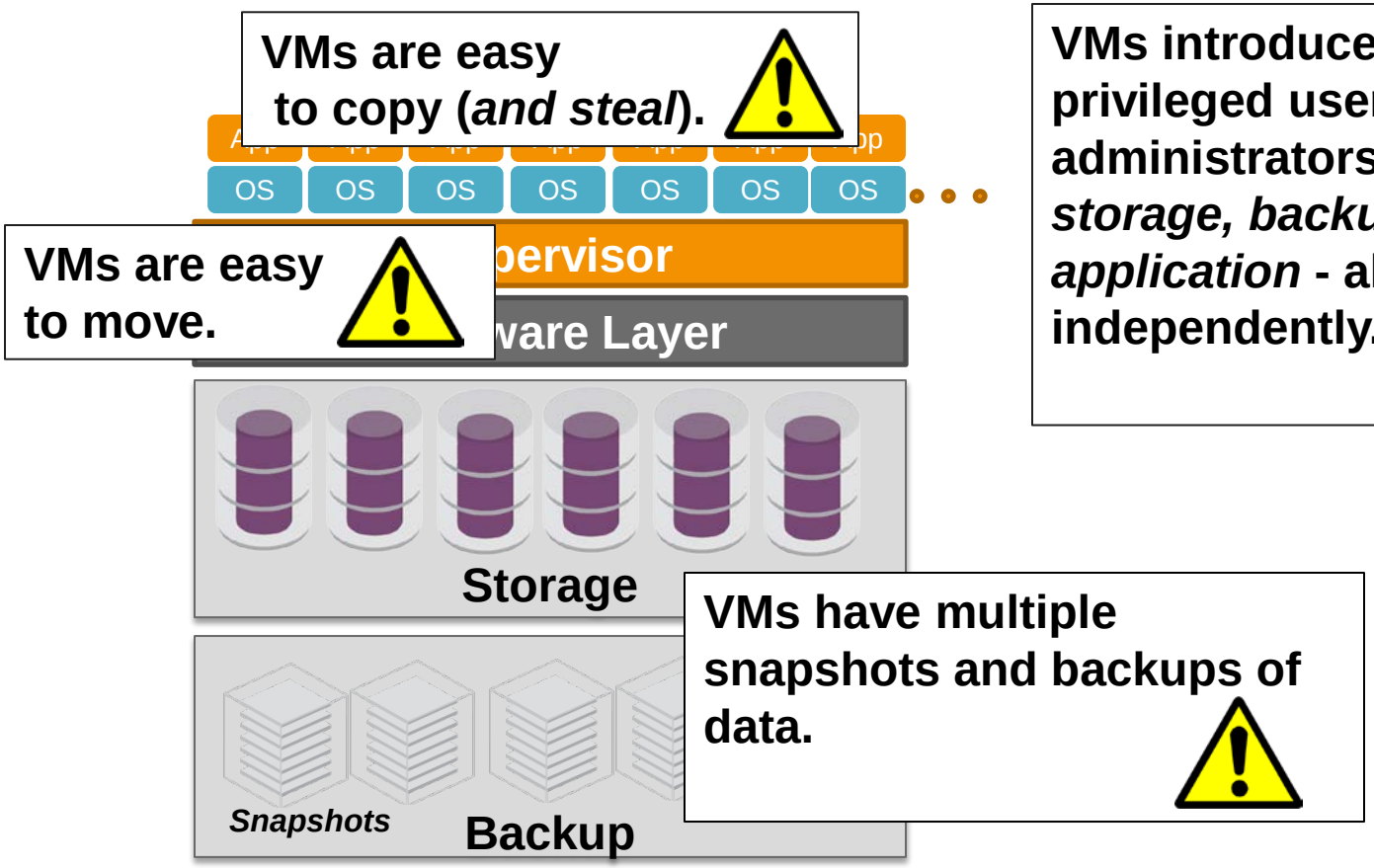
While IT is being pushed towards virtualization…

Virtualized Infrastructure



Data Security Gaps Remain

How secure is my data in a virtualized world?



Contractual Reality

Complete Transfer of Liability or Vague Language

Amazon Web Services™ Customer Agreement

Section 7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, **you acknowledge that you bear sole responsibility for adequate security**, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) **use encryption technology to protect Your Content** from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.

http://aws.amazon.com/agreement/

Salesforce Master Subscription Agreement

8.3. Protection of Your Data. Without limiting the above, **We shall maintain appropriate administrative, physical, and technical safeguards for protection of the security,** confidentiality and integrity of Your Data. We shall not (a) modify Your Data, (b) disclose Your Data except as compelled by law in accordance with Section 8.4 (Compelled Disclosure) or as expressly permitted in writing by You, **or (c) access Your Data except to provide the Services or prevent or address service or technical problems,** or at Your request in connection with customer support matters.

http://www.salesforce.com/company/msa.jsp

Cloud Security Challenges

	IaaS	PaaS	SaaS
User ID and Access: Secure Authentication, Authorization, Logging			X
Data Co-Mingling: Multi-tenant data mixing, leakage, ownership			X
Application Vulnerabilities: Exposed vulnerabilities and response			X
Insecure Application APIs: Application injection and tampering			X
Data Leakage: Isolating data		X	X
Platform Vulnerabilities: Exposed vulnerabilities and response		X	X
Insecure Platform APIs: Instance manipulation and tampering		X	X
Data Location/ Residency: Geographic regulatory requirements		X	X
Hypervisor Vulnerabilities: Virtualization vulnerabilities	X	X	X
Data Retention: Secure deletion of data	X	X	X
Application & Service Hijacking: Malicious application usage	X	X	X
Privileged Users: Super-user abuse	X	X	X
Service Outage: Availability	X	X	X
Malicious Insider: Reconnaissance, manipulation, tampering	X	X	X
Logging & Forensics: Incident response, liability limitation	X	X	X
Perimeter/ Network Security: Secure isolation and access	X	X	X
Physical Security: Direct tampering and theft	X	X	X

Fundamental Trust & Liability Issues

- **Data exposure in multi-tenant environments**
- **Separation of duties from cloud provider insiders**
- **Transfer of liability by cloud providers to data owners**

Fundamental New Cloud Risks

- **New hypervisor technologies and architectures**
- **Redefine trust and attestation in cloud environments**

Regulatory Uncertainty in the Cloud

- **Regulations likely to require strong controls in the cloud**

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
- Likely even more critical for cloud-based applications
  - Lower level of trust, invocation of additional regulatory requirements

Authentication Sprawl

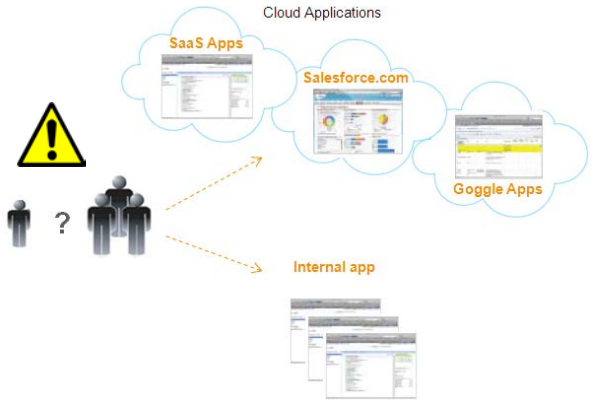
- Separate authentication systems for each cloud provider
  - Operationally un-scalable
  - Typical user password/authentication fatigue and weak passwords

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

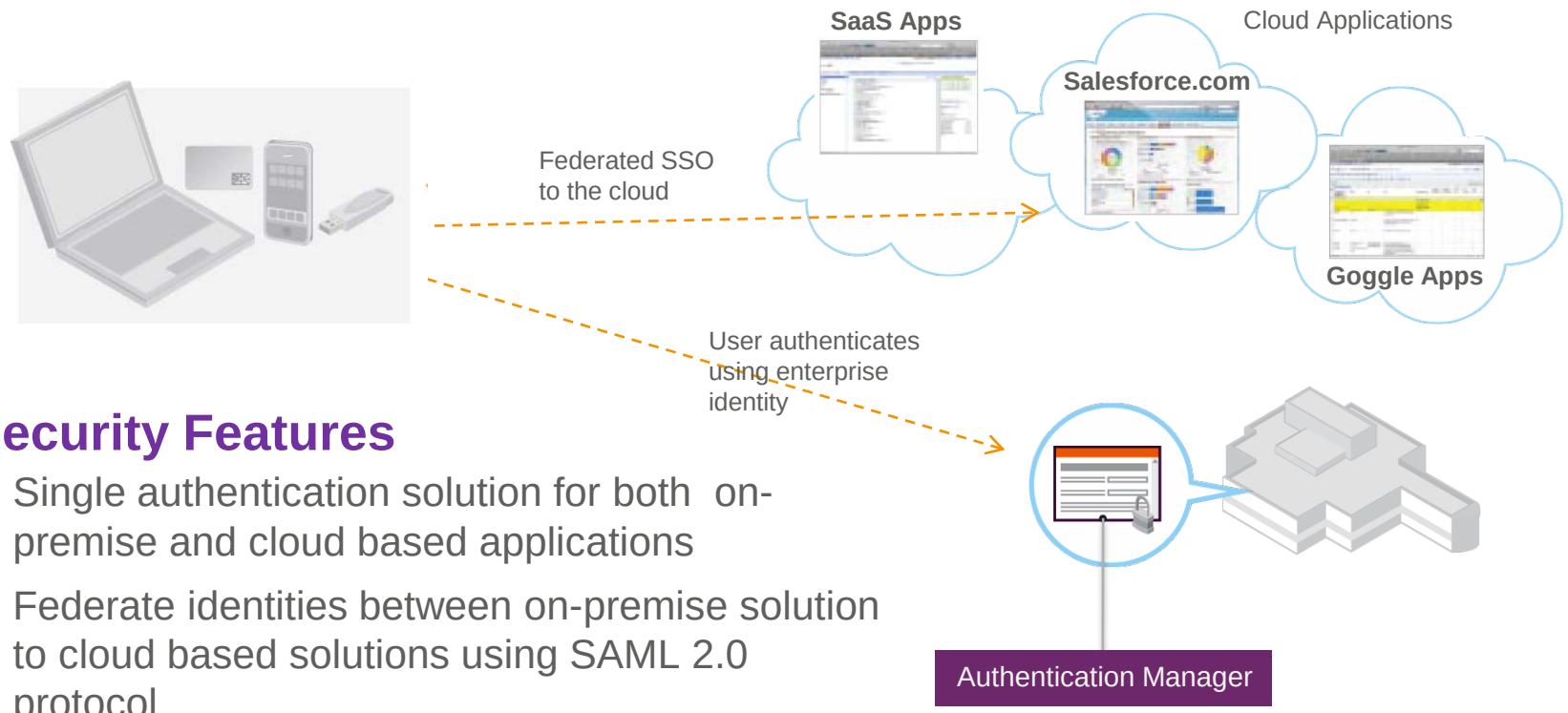
KEY POINTS

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



Secure Access to SaaS: PKI-based 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
- PKI –based Authentication to reduce the hassle for remembering password
- Google Apps and salesForce.com are supported out-of-the-box

Securing Uncontrolled Virtual Instances

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

Unlimited Copying of Instances

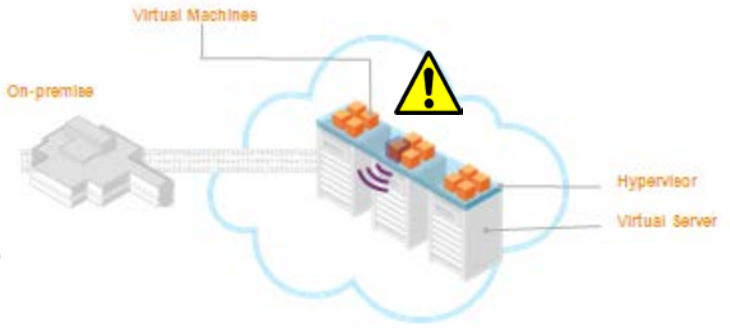
- **Instances could be copied without awareness**
  - No visibility to instance location, no audit trail
- **Instances used by competitors and malicious users**
- **Enables unlimited brute force attacking**
  - Return to original copy for next iteration of password guessing

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 much larger**
  - Not just a single entity lost, potentially unlimited number

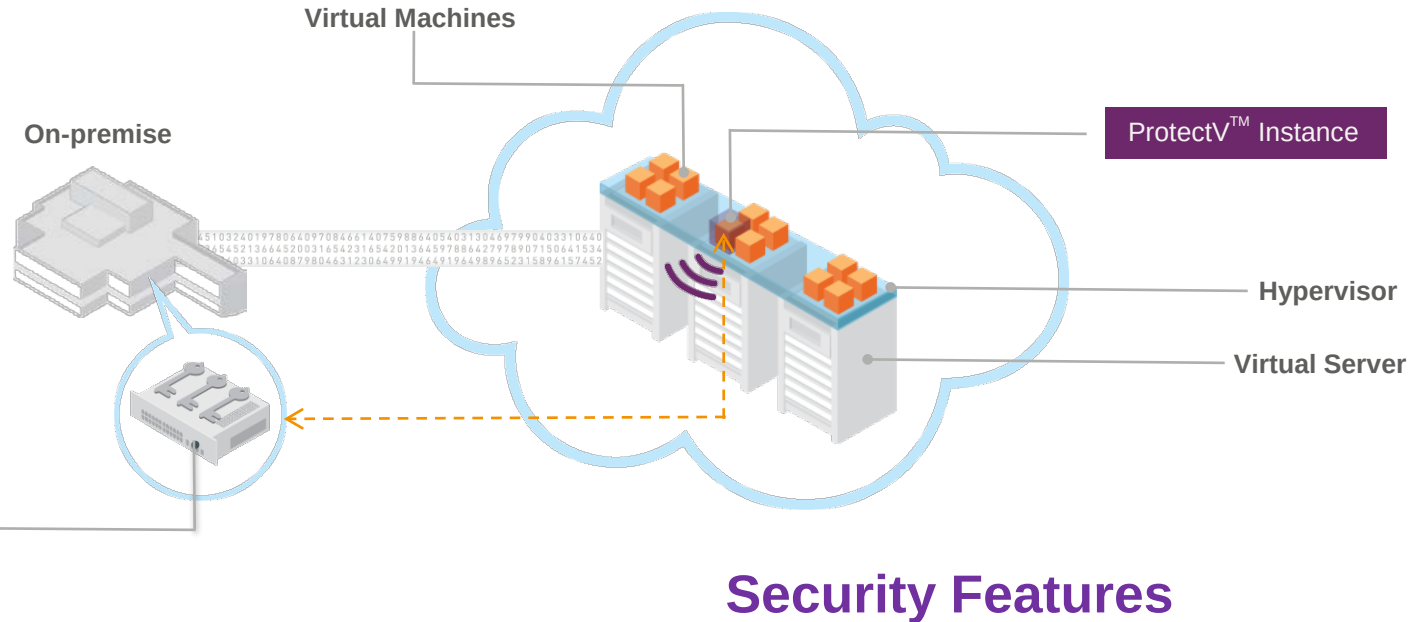
KEY POINTS

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



Secure Virtual Machines: Secure Instance (ProtectV™)

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



Secure Data Management (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)
- Certificate based authentication options
- Event logging and activation notification

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 mis-configuration and cloud administrators
- Regulatory evidence of privacy and integrity controls

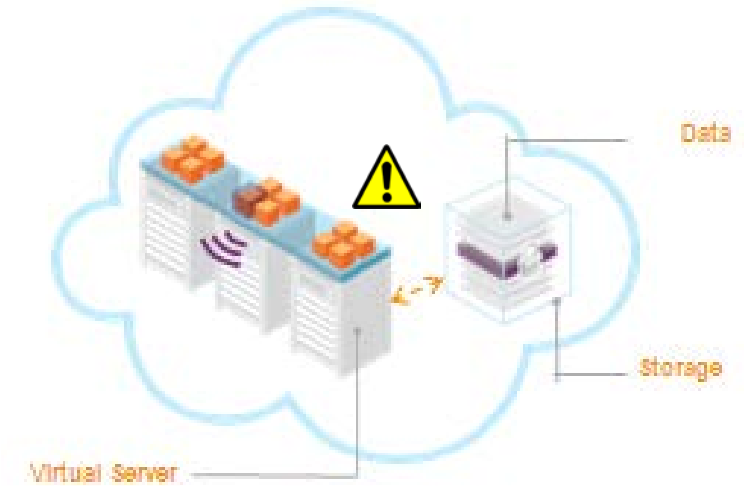
KEY POINTS

- Data Isolation
- Cloud Compliance
- Multi-Tenant Protection

Trust and Control Issues

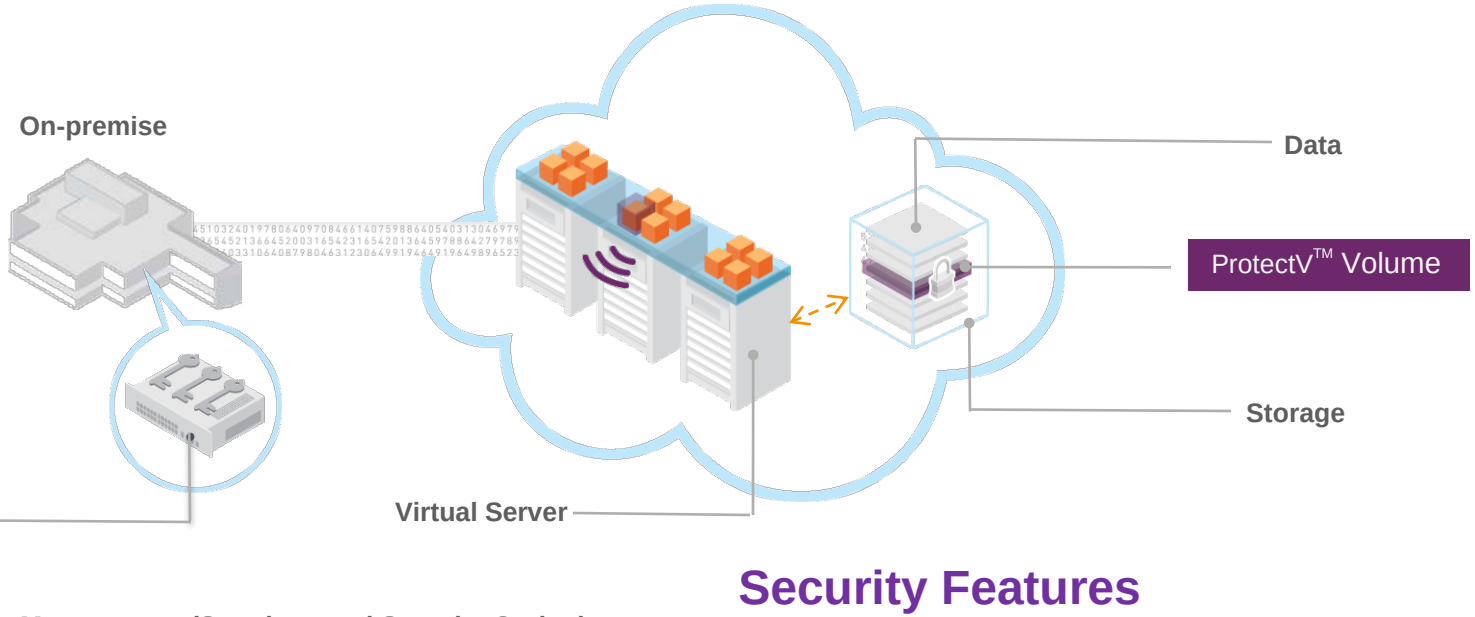
If cloud provider offers encryption:

- Proper Key Handling
  - NIST Lifecycle compliance
  - Strength, uniqueness, rotation, etc.
- NIST approved algorithms
- Administration trust
  - Separation of Duties



Secure Virtual Storage: Secure Volume for Storage Servers

Maintain data privacy in shared storage environments with encrypted data isolation



Secure Data Management (Supplemental Security Option):

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

Security Features

- Multiple cloud storage options:
  - Secure volume for storage servers
  - Common network storage support
  - Customer-based file encryption
- FIPS 140-2 Level 2 Security Certified Solution
- Centralized Policy and NIST 800-57 Key Lifecycle Management

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

Maintaining Keys in clouds

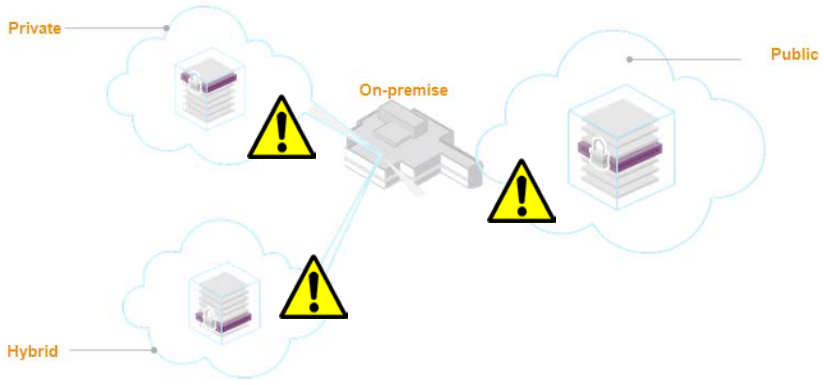
- **When your cloud provider handles keys**
  - Appropriate key material
  - Proper lifecycle and policy handling
  - Privileged user abuse

The Cryptography and Entropy Problem

- Difficult to get true randomness in highly replicated and automated cloud
- Flaws in cryptographic functions have huge consequences

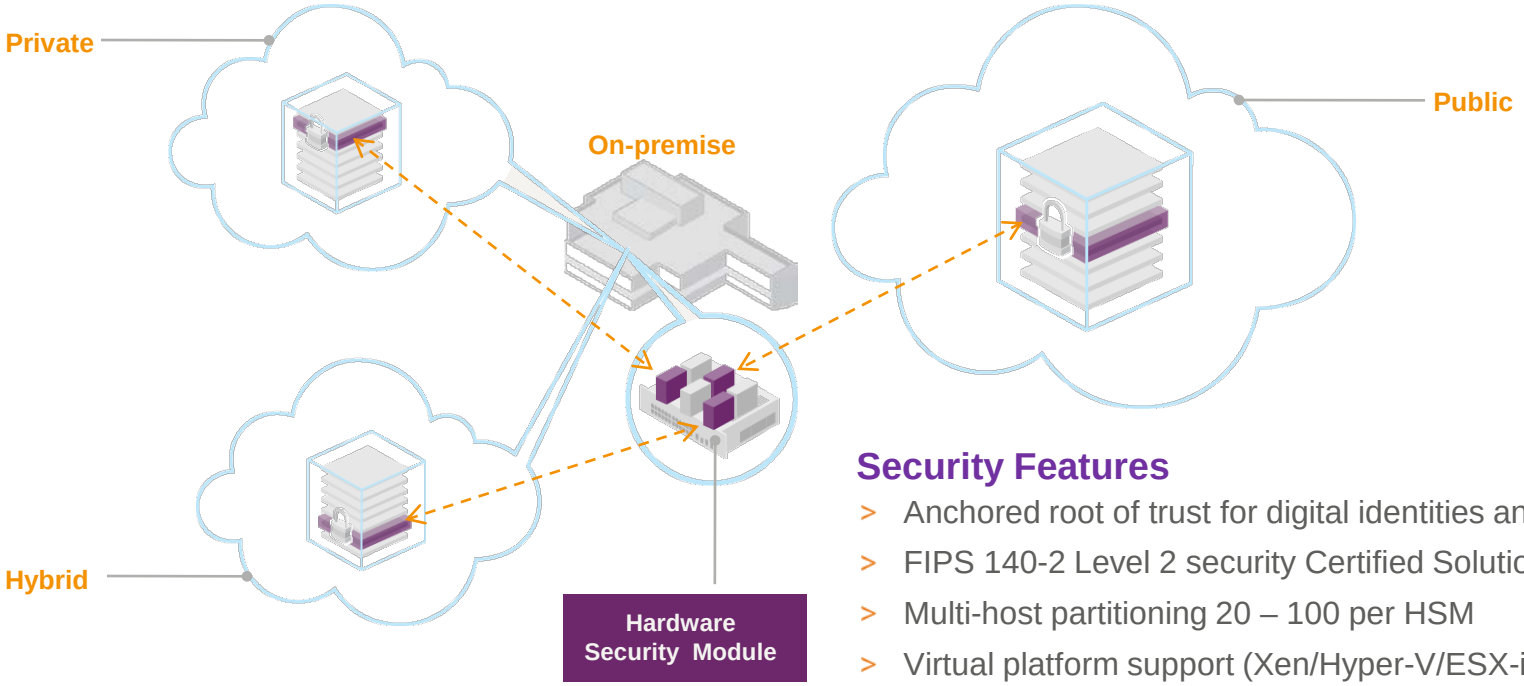
KEY POINTS

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



Secure Cloud-Based Identities and Transactions: Hardware Security Modules (HSM)

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

SafeNet | THE DATA PROTECTION COMPANY

Thank You!

SafeNet Inc.

www.safenet-inc.com