SEPTEMBER 22, 2016
SANTA CLARA, CA

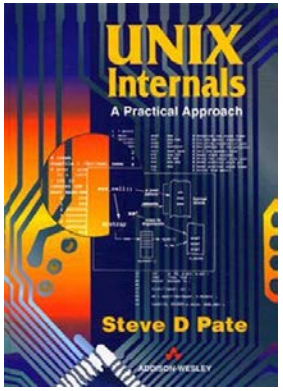
SNIA

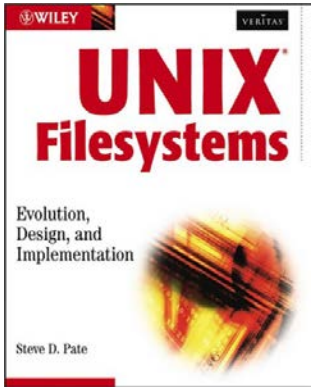
Experiences of Deploying Encryption and Key Management in Private, Public and Hybrid Cloud Environments

Steve Pate
Chief Architect
HyTrust Inc
spate@hytrust.com

Who am I?

- Long background in OS / storage
  - ICL
  - SCO
  - VERITAS
  - Several startups





(*)
- Vormetric CTO
- HighCloud Security CTO and co-founder
- HyTrust Chief Architect

(*) Encryption and Key Management

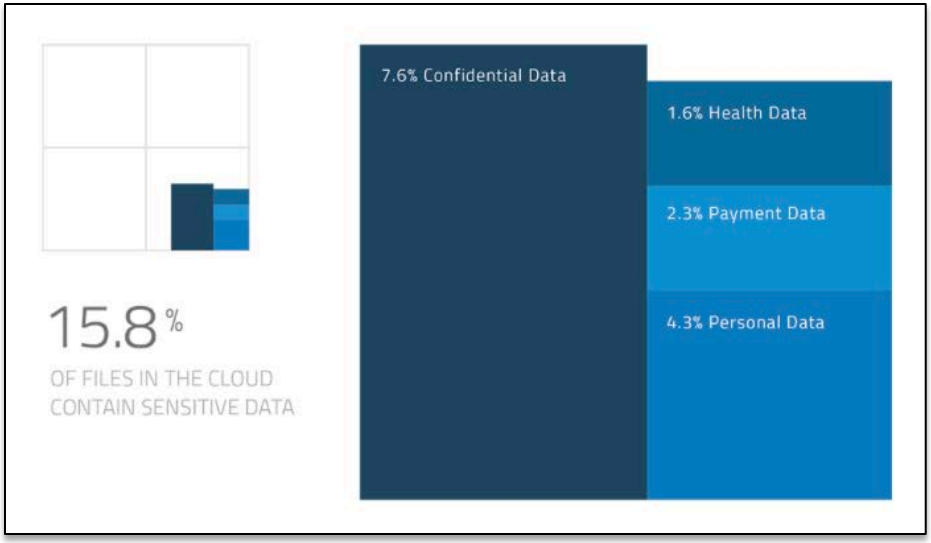
Before the Cloud …

- Why encrypt?
  - Compliance drivers:
    - PCI, HIPAA, IP, government
  - Laptops and other devices (data leaving the building)
- How hard was it?

  "*IT don't just say no. They say hell no!* " – Fortune 500 CISO
  - Physical key management
  - Poor performance
  - Multiple platforms
  - Downtime for initial installation / encryption

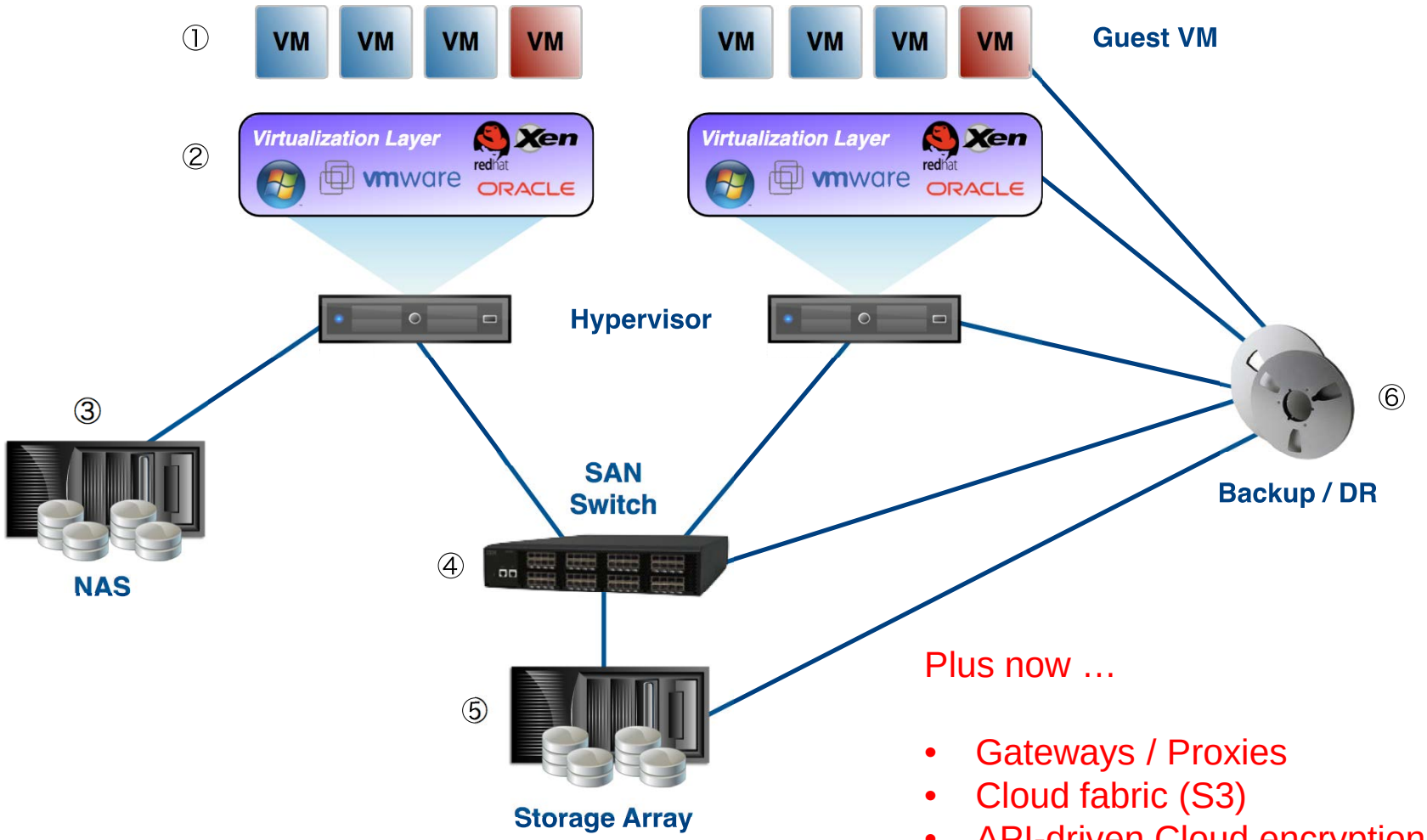
And now, in a post-cloud world

- The data is leaving the building!
- Mistrust is an issue
- Encryption becoming more prevalent
- Cross cloud support is important



Data from SkyHigh Cloud Computing Trends 2016

Who encrypts where?



Plus now …

- Gateways / Proxies
- Cloud fabric (S3)
- API-driven Cloud encryption

Encryption Solutions – Example 1

- VM Encryption:
  - Pros:
    - Encryption travels with the VM
    - Works in physical, virtual and any IaaS platform
  - Cons:
    - Agent running in each VM
    - Usually done above dedup and compression

Encryption Solutions – Example 2

- Hypervisor:
  - Pros:
    - OS guest agnostic
    - No VM agent
  - Cons:
    - Hypervisor-specific
    - Doesn’t work across clouds
    - Backups in the clear

Encryption Solutions – Example 3

- Self Encrypting Drives:
  - Pros:
    - Application / OS / VM agnostic
    - Best for performance
  - Cons:
    - Data coming off the disk is in the clear
    - Key management complex

Key Management

"*Key Management is where encryption projects go to die*"

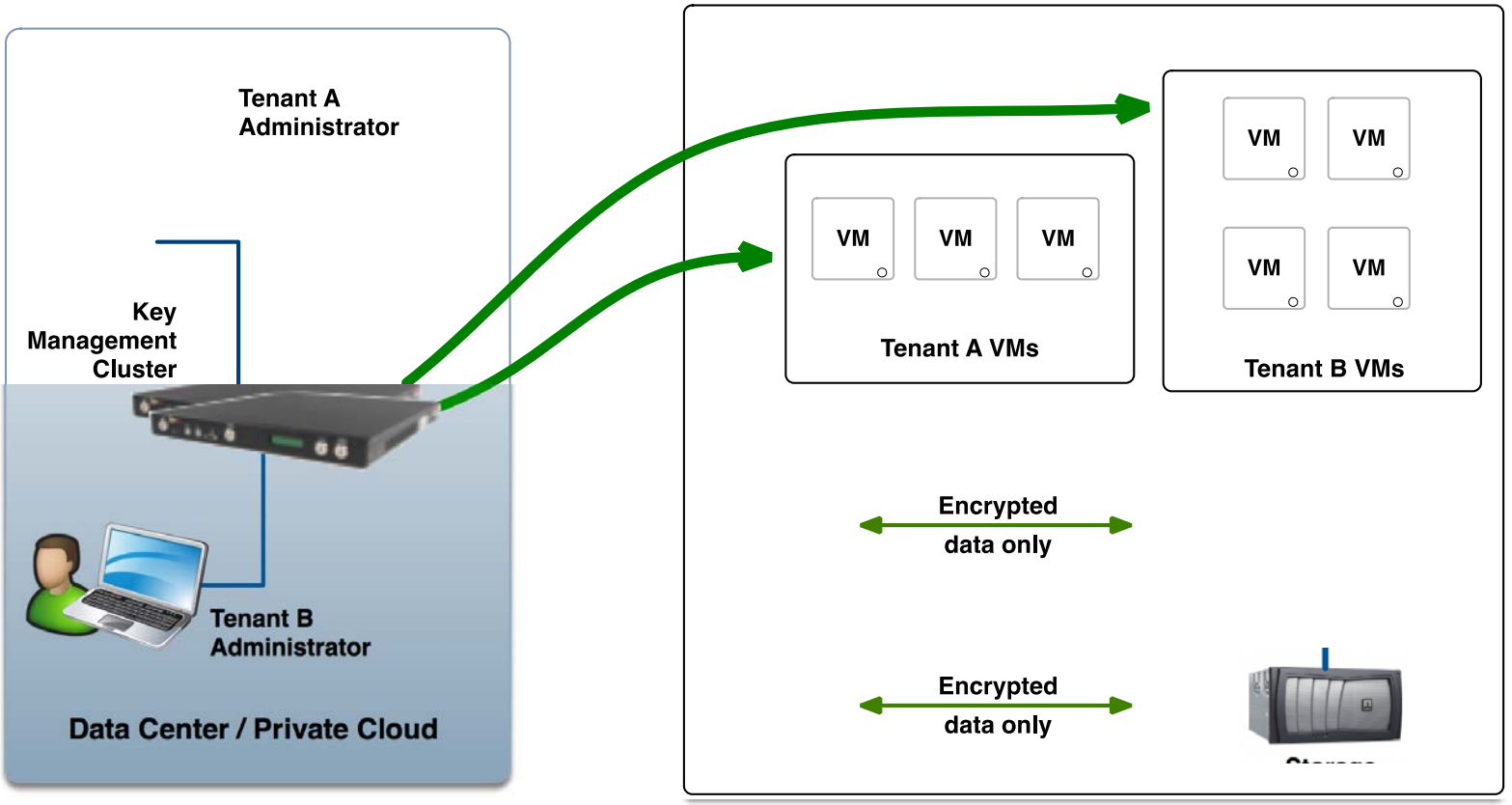
– Wall Street CIO

"*Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system.*"

– Bruce Schneier – Preface to Practical Cryptography:

Key Management Basics

- IaaS with on-premise key management



Key Management Requirements

- Simple but secure!
- Highly-available
- Standards adoption (FIPS 140-2, CC, …)
- Support for open standards (e.g. KMIP)
- Fleibility:
  - Virtual and/or physical appliances
  - Integration with HSMs and external KMIP servers
  - On-premise and in the cloud

Simplicity vs Security

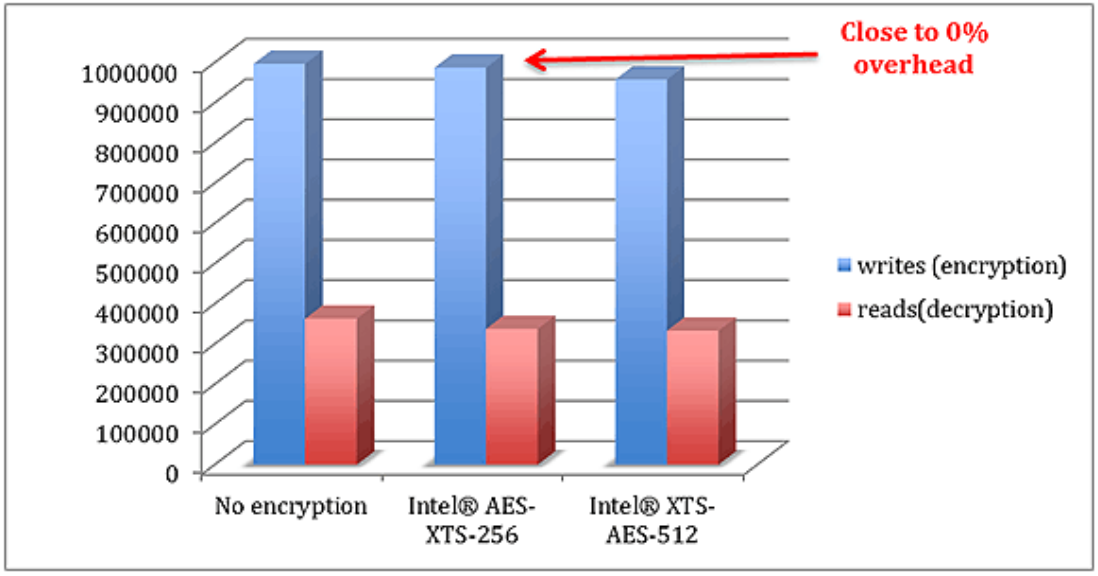
- How registration looked just a few years ago:
  - Download agent
  - Create certification for each install
  - Install and register:
    - Provide certificate
    - Provide IP address(es) of Key Cluster node
    - Add one-time passphrase
  - Authenticate on key server:
    - Repeat one-time passphrase

Simplicity vs Security

- What's changed since then:
  - Zero-touch model
  - Everything API-driven
  - Support for many thousands of endpoints
  - Support for templates / clones / snapshots

Performance

- Encryption used to carry a high overhead
- Intel introduced AES-NI in 2009
- Performance has improved dramatically



https://software.intel.com/en-us/articles/intel-aes-ni-performance-enhancements-hytrust-datacontrol-case-study

The Issues with Virtual Machines

- What is a Virtual Machine?
  - Essentially a set of files
  - Easy to copy
  - Easy to backup
  - Easy to migrate

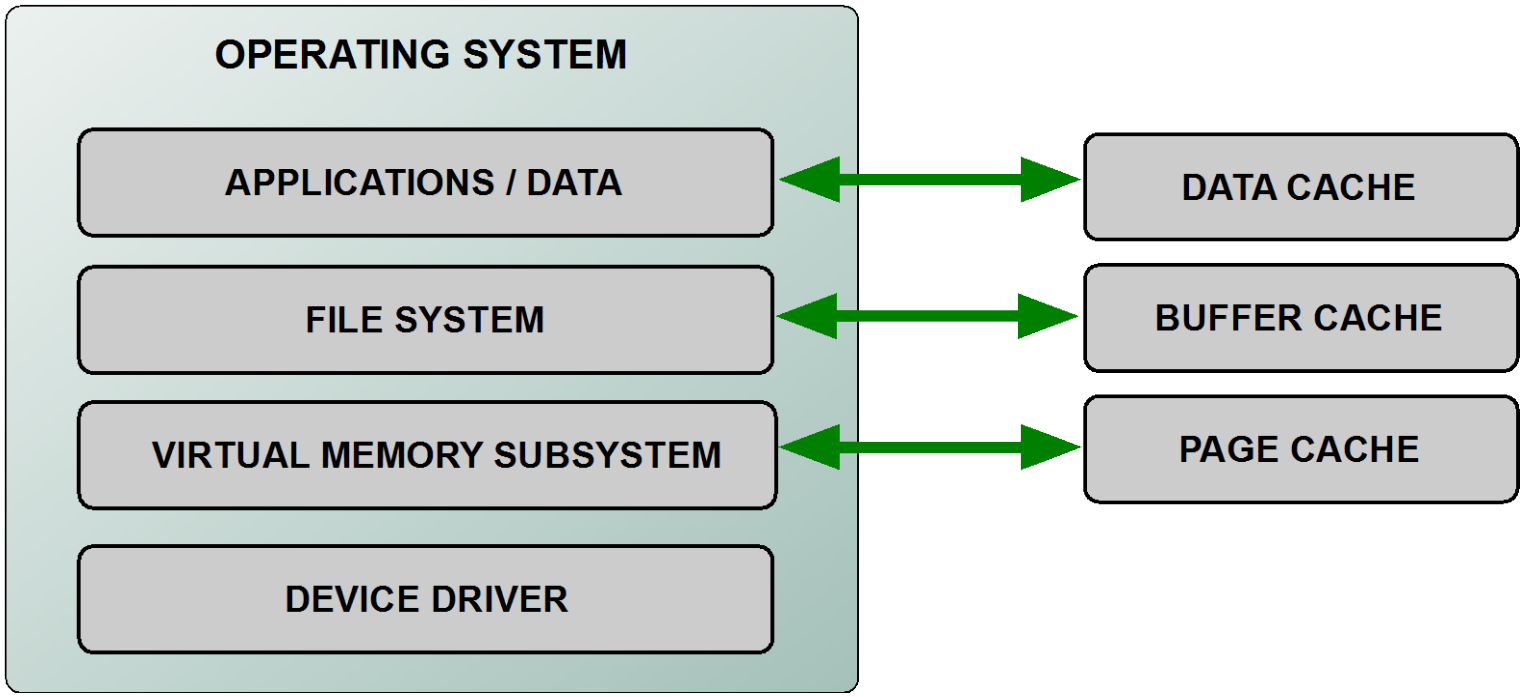
The Issues with Virtual Machines

- But …
  - Snapshot / clone and you have a copy
    - Exposes contents of memory on disk
  - Easy to spin up anywhere
    - Data sovereignty issues
  - Sources of entropy for key generation

One reason why people encrypt everything!

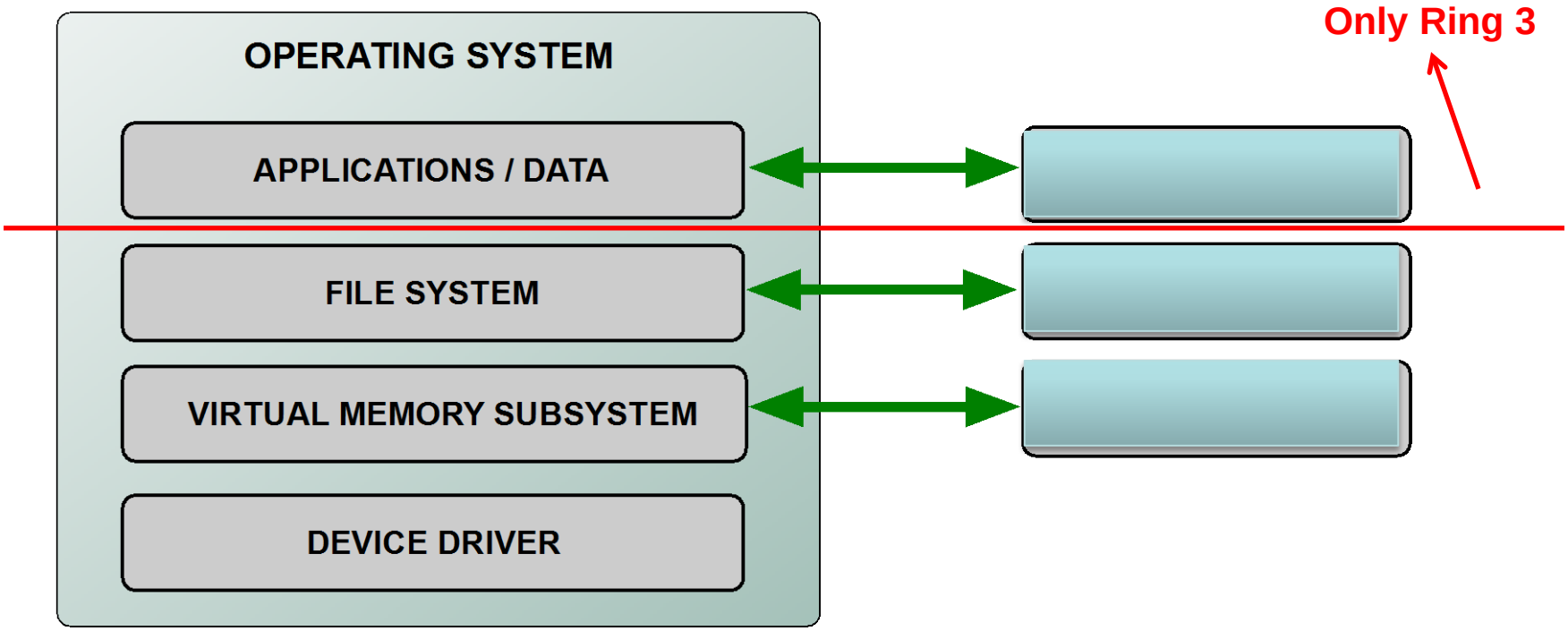
The Memory Problem!

- Snapshot a VM and you expose data



The Memory Problem!

- Intel SGX partly solves this but …



What does the Future Hold?

- More encryption for sure
  - Recall only 15.8% of data in the cloud is sensitive
    - This will increase dramatically
  - Data breaches come with heavy penalties
- Flexible key management:
  - Some proprietary APIs
  - More KMIP
  - Better interoperability
- International standards

Thank you!

Download this presentation and others from SNIA's Data Storage Security Summit at:
http://www.snia.org/dss-summit