Agenda

- Data Security Challenges
- Top Considerations for Data Centric Security
- Use Case Discussion
  - Rackspace
  - FireHost
  - Amazon Web Services
  - Microsoft Azure
- Q&A
Data is Increasingly More Difficult to Protect

Data Centers
- Physical
- Virtual
- Outsourced

Clouds
- Private, Public, Hybrid
- Multiple vendors

Big Data
- Sources
- Nodes
- Results

Physical Servers
- Local offices and retail locations
- Labs

Copyright 2014 Vormetric, Inc. All rights reserved.
Cloud Security Pain Points

Top Security Concerns With Cloud Computing

- Data Privacy and Security: 41%
- Access and Control: 35%
- Auditing and Compliance: 32%
- Control of Data: 26%
- Security Models/Toolsets: 18%
- Contractual/Legal Issues: 15%
- Internal Issues: 11%
- Network Connection Security: 10%
- Geographical Coverage: 4%


37% Security biggest pain point

73% considered security to be extremely important
Who is Responsible for Security?

ROLE CLARITY

Security ~ You

Security ~ Them

IaaS
Infrastructure as a Service
- APIs
  - Core Connectivity & Delivery
  - Abstraction
  - Hardware
  - Facilities

PaaS
Platform as a Service
- APIs
  - Core Connectivity & Delivery
  - Abstraction
  - Hardware
  - Facilities

SaaS
Software as a Service
- APIs
  - Presentation Modality
  - Presentation Platform
  - Applications
  - Data
  - Metadata
  - Content

Source: Cloud Security Alliance, 2013.

Copyright 2014 Vormetric, Inc. All rights reserved.
Considerations For Data Centric Security Across Cloud, Hybrid and On-Premise

Consolidate key management and policy for lowest TCO

- Single data protection solution for multiple platforms/use cases
  - On-premise and off-premise
  - Multi-IaaS cloud support
  - File and Application Level

Key custodianship with flexible key management

- BYOK
- Know when subpoenaed
- Standards support e.g., KMIP
- Data remanence shredding

Data Access Controls

- Privileged user access policies
- Data residency controls

Security Intelligence

- Know who, what, where, how data is accessed

Copyright 2014 Vormetric, Inc. All rights reserved.
Considerations For Data Centric Security (cont’d): Key & Data Access Policy *On-Premise*

Data Security Manager (Key & Policy Manager) on-premise managed by End User

End User manages Keys and Access Control Policies

Copyright 2014 Vormetric, Inc. All rights reserved.
Considerations For Data Centric Security (cont’d): Key & Data Access Policy *Off-Premise*

- Data Security Manager (Key & Policy Manager) off-premise managed by End User
- End User manages Keys and Access Control Policies
Use Case: Private Top 10 Global Accounting Firm

Use Case/Driver

- Protect Forensic data that includes customer PII
- Ensure that RAX Infrastructure and Server Administrators will not have access to their customer PII

Environment/Deployment Model

- Forensic Application Storing PII information in SQL and Isilon File shares
- Data Security Manager will be deployed in COMPANY Data Center(s)
- COMPANY Infosec will manage keys and policies, controlling access to data

Why Rackspace/Vormetric

- Single solution to protect both structured and unstructured data
- Transparent to Application, SQL DB and RAX hosting infrastructure
- Eliminate CSP Admin risk to data without impacting any IT operations (backup, replication, monitoring etc.)
Use Case: $4.4B Global ISV Targeting Legal, Tax, Accounting, Audit, Healthcare Markets

Use Case/Driver
- Executive/Legal Mandate to protect customer PII

Environment/Deployment Model
- Many Oracle DBs and millions of scanned images with PII
- Data Security Manager deployed in RAX environment

Why Rackspace/Vormetric
- Single platform for protecting structure and unstructured data types
- COMPANY maintains custodianship of keys and data access policies
- RAX manages infrastructure including the Data Security Managers
- Solution integrates seamlessly with hosted backup and other services delivered by RAX
Use Case: Private Healthcare App Service Provider -> Streamlining Life Cycle of Major Surgeries

Use Case/Driver
- HIPAA-HITECH data that needs protecting

Environment/Deployment Model
- MySQL servers running on CentOS with ePHI data
- Data Security Manager hosted within FireHost environment
- COMPANY will manage keys and policies, controlling access to data

Why FireHost/Vormetric
- All-in-cloud solution delivered as part of a broader set of cloud and infrastructure services – single solution provider
- Small fast growing COMPANY – needed cost-effective and easy to manage solution
- Transparent to MySQL/CentOS servers – no application changes needed
- Maintain custodianship of keys and data access policies
Use Case: PegaSystems
Leading CRM/BPM Software Provider

Use Case/Driver

- Enable healthcare CRM/BPM management workloads for AWS
- More than 40 customers migrating workloads into the PegaCloud
- Compliance (HIPAA) and contractual obligation to protect customer data
- Data-across-borderer issues with EU e.g., ensure access is controlled to ‘in country’ company personnel

Environment/Deployment Model

- ~250 instances – mostly Oracle running on CentOS platform
- Data Security Managers deployed on-site in USA, Ireland and Norway and managed by the Pegasystems IT team

Why AWS/Vormetric

- AWS scalability and ease of integration e.g., availability of APIs
- Encryption is transparent to Application/DB and EC2 infrastructure e.g., no changes to application or EC2
- Maintain custodianship of keys and data access policies

Copyright 2014 Vormetric, Inc. All rights reserved.
Market Requirements

Encryption

HIPAA ➔ HITECH ➔ MU

#1

CSA cloud security alliance

Vormetric

Windows Azure
Platform Workload Portability

Private Cloud
(McKesson OneCloud)

Public Cloud
(Microsoft Windows Azure)

Security
(Especially Encryption)
stays relatively constant with moving workloads
Thank you! Questions?

Contact Information:
C.J. Radford
cradford@Vormetric.com
@cjrzd