Cloud Data Security and the Insider Threat...

Sol Cates
CSO
@solcates
scates@vormetric.com

Copyright 2014 Vormetric, Inc. All rights reserved.
A bit about me

- InfoSec for ~ 18 years
- Currently have 4 jobs
  - Infrastructure
  - Product Strategy
  - Security Practitioner
  - Evangelist/Consultant/Shoulder
Where’s the Perimeter
IT is Being Challenged To Embrace The Cloud

“By 2018 ... 25% of corporate data traffic will bypass traditional perimeter security defenses - up from 4% today.”

Gartner
November 2013

Public Cloud Growth is 5X that of the IT industry as a whole.
Cloud Heightens The Need to Protect Data
Private, Public, Hybrid Cloud and Big Data

Most Cloud Computing Is Under The Radar In Enterprises, Survey Shows

Walgreens has been ordered to pay $1.44 m

It will be mainstream at
multiple business units,
divisions or departments
in my organization.

It will be mainstream at
one business unit,
division or department
in my organization.

We'll still be
experimenting with
it, it won't be in main-
stream production.

It will finally
after the hype
dies down.

Not sure
Why start protecting your data?

- **Data is exploding**
  - Volume
  - Variety
  - Velocity

- **Reasons for encryption multiplying**
  - Regulations – PCI, HIPPA, Breach Disclosure
  - Contractual Obligation
  - Risk Reduction
  - Breaches

- **FACT: Data can’t protect itself**
New Frontier, Pioneers, and Challenges

Cloud
- Many types of clouds
  - IaaS, SaaS, PaaS, BPaaS, etc...
- Many Providers
  - Some large fish, and lots of little fish
- What’s their security philosophy?
- Who owns the data?
- Who is exposed to it?

Big Data
- So much data, so little governance
- Has not concept of a data type or classification
- Is the data in your repository regulated or classified?
- Does your organization want to utilize different data sets, that traditionally can’t be mixed?
Understanding Cloud Architectures

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

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

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

Source: Cloud Security Alliance, 2013.
Encryption has moved
From a Tax to a Business Enabler

- Cloud and Big Data Are Enablers of Business
- Security Remains the #1 Concern as data moves outside the perimeter
- Cost of encryption no longer a tax on the business, now viewed as an enabler of cost savings and competitive advantage

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%

Q. What are the top cloud computing-related security problems that affect your organization? Please describe up to three. N=94.
IT’s Dirty Little Secret
Insiders gone wild...

- A rogue contractor was able to compromise international surveillance programs.
- He didn’t do anything ground breaking.
- He had administrative rights in the data center.
  - He was given admin rights as part of his job function.
  - He leveraged the inherent flaw in the system, of superuser access to data.
VORMETRIC
2014 INSIDER THREAT REPORT
EUROPEAN EDITION

537 IT DECISION MAKERS
France, Germany and the United Kingdom

80% Enterprises (€250M +)

Research conducted by Ovum on behalf of Vormetric, March 2014.
Telephone interviews with IT and Security Managers
ORGANIZATIONS DO NOT FEEL SAFE

Only 9% Feel safe

TOP 3 REASONS THEY ARE INSECURE

40% Meeting Compliance Requirements
30% Requirements or expectations from customers
30% Advanced Persistent Threats (APTs)
**HOW ARE ENTERPRISES RESPONDING TO THE THREAT?**

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using data encryption</td>
<td>68%</td>
</tr>
<tr>
<td>Increasing budget</td>
<td>66%</td>
</tr>
<tr>
<td>Constantly monitoring data access</td>
<td>49%</td>
</tr>
</tbody>
</table>

Europe feels less vulnerable than the US

- 25% feel vulnerable to insider threats in Europe
- 39% are concerned with abuse of privileged user access rights in Europe
- 47% feel vulnerable to insider threats in the US
- 63% are concerned with abuse of privileged user access rights in the US
Information Technology’s Dirty Little Secret

30

100

1
Information Technology’s Dirty Little Secret

30+ Years super users have been managing our servers, their configurations, and data.

100% Super users have 100% access to all data in the systems they manage.

1 It only takes 1 compromised/rogue user to cause havoc.
Establishing Some Terms

- **Privileged User**
  - Employees who use data and systems as part of their jobs
  - Executives who have more access than they should
  - Administrators who are the governors of the systems

- **Super User**
  - Account that leverages the ring-0 privilege
  - Examples: root, administrator, SYSTEM

- **Ring-0**
  - The kernel process who has complete access to all resources

http://en.wikipedia.org/wiki/Protection_ring
What is the issue?

- Superusers control the system, packages, patches, and data permissions.
- The nature of the superuser is that they have full access to data accessible by the system.
- If a superuser is compromised or goes rogue, the impact can be severe, as they can destroy, steal, and manipulate.
Traditional Controls for Super Users

- **Monitoring**
  - OS Level auditing, keystroke logging, etc...

- **Privileged Account Management**
  - Checkout account with single usage password

- **Policy based elevation**
  - Tools that allow a user to elevate to the superuser on a per command basis. sudo, powerbroker, etc...
  - They are good for saying **who** can do **what** as root. But does not control **what** root can do.

None of these controls stop the superuser…
Just how one becomes the superuser
# World-Class Brands Rely on the Vormetric Data Security Platform

## Global Customers
- Over 1,400 customers
- 17 of the Fortune 25

## Most Security Conscious Brands
- Largest financial institutions
- Largest retail companies
- Major manufacturers
- Third party business service providers
- Government agencies

## Cloud Service Providers Trust Vormetric

<table>
<thead>
<tr>
<th>IBM</th>
<th>Cloud Managed Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>rockspace</td>
<td></td>
</tr>
<tr>
<td>CenturyLink</td>
<td></td>
</tr>
<tr>
<td>Firehost</td>
<td>Secure Cloud Hosting</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>Partner Network</td>
</tr>
<tr>
<td>Google Cloud Platform</td>
<td></td>
</tr>
</tbody>
</table>

## OEM Partners
- IBM
- Symantec

---

> With Vormetric, people have no idea it’s even running. Vormetric Encryption also saved us at least nine months of application rewrite effort, and its installation was one of the easiest we’ve ever experienced.

— Karl Mudra, CIO
Delta Dental of Missouri
Vormetric Data Security Platform
Solves inefficiencies of point product solutions
Questions?

Sol Cates
CSO
@solcates
scates@vormetric.com