Protecting Sensitive Data in the Cloud

Presented by:
Eric Wolff
Thales e-Security
Topics

• IT Perspectives on Cloud Security
• Tools for Security in the Cloud
• XaaS Encryption/Key Management Strategies
IT Perspectives on Cloud Security
Recent Research

IT Perspectives on Cloud Security

• 2017 Thales Data Threat Report
• Conducted by 451 Research
• Over 1100 IT Executives surveyed
Recent Research

IT Perspectives on Cloud Security

- 2017 Thales Global Encryption Trends
- Conducted by Ponemon Research
- Almost 5000 IT Practitioners surveyed
Recent Research
Breaches Continue

2016: 21% Had a data breach in the last year
2017: 26% Had a data breach in the last year

2016: 61% Previously had a data breach
2017: 68% Previously had a data breach

Tweet along: #Sec360
www.Secure360.org
Recent Research

Encryption Growing as a Solution

Record numbers for companies with an enterprise-wide encryption strategy

Encryption is recognized for protecting data...

Tweet along: #Sec360

www.Secure360.org
Recent Research
Why Encrypt?

- **Compliance** has always been the top driver
- **Information protection** is close to reaching the same level
- Increasing focus on **specific data types**

---

To comply with external privacy or data security regulations and requirement: 55%
To protect enterprise intellectual property: 51%
To protect information against specific, identified threats: 49%
To protect customer personal information: 49%
To limit liability from breaches or inadvertent disclosure: 37%
To reduce the scope of compliance audits: 30%
To comply with internal policies: 19%
To avoid public disclosure after a data breach occurs: 10%
Resources for Cloud Security
Cloud Security Resources

Cloud Security Alliance

• Global, nonprofit

• Building best practices for next generation IT security

• Mission: Become the authoritative source for trust in the cloud
Poll

I have heard of the Cloud Security Alliance
Poll

- I like what CSA does 😊
- I use what CSA creates 😊
- CSA is vendor marketing 😞
Key CSA Resources to Make You Smarter
CSA Security Guidance

- Educational
- Narrative – feels like a book
- Preparation for Cloud Controls Matrix
- Version 4.0 is almost complete
Cloud Controls Matrix

- Cloud services risk management
  - Delineates control ownership
  - Denotes applicability to cloud provider type
  - Anchor for security and compliance posture measurement – use for RFP’s
- Common Language for SLAs
- Maps to global regulations and standards
  - NIST, ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP
- Mapped to Security Guidance
Consensus Assessment Initiative Questionnaire

- Cloud Controls Matrix companion
- Binary questions assess CCM compliance
- Create consistent cloud provider assessment processes
- Enables cloud providers to self-assess security posture
Encryption is recognized for protecting data...
Encryption in the CCM / CAI

• Platform and data-appropriate encryption...shall be required.

• [Encryption] Keys
  • Shall not be stored in the cloud but
  • Shall be maintained by the cloud consumer or trusted key management provider.

• We’re coming back to this in a moment…
White Paper:
Best Practices for Assessing Your Cloud Security Services

vormetric.com/bpaccss

Cloud Control Matrix Requirements Mapped to Vormetric Capabilities
Understanding IaaS, PaaS, and SaaS Encryption and Key Management
## Cloud Classified

### Traditional Cloud Service Providers

<table>
<thead>
<tr>
<th>Type</th>
<th>Encryption</th>
<th>Key Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colo</td>
<td>Bring Your Own</td>
<td>You</td>
</tr>
<tr>
<td>Managed</td>
<td>Many Provide</td>
<td>Cooperative</td>
</tr>
</tbody>
</table>

Encryption and Key Management Generally Easy

---

**IaaS, PaaS, SaaS Providers**

- CenturyLink
- workday
- salesforce
- DOMO
- RACKSPACE
- Microsoft Azure
- Amazon Web Services
- Virtustream
- QTS

---

**Cooperative Key Management**
**Shared Responsibility Model**

**Infrastructure as a Service (IaaS)**
- Customer Responsibility
  - Data
  - Application
  - Runtime
  - Middleware
  - O/S
    - Virtualization
    - Servers
    - Storage
    - Networking
- Provider Responsibility

**Platform as a Service (PaaS)**
- Data
  - Application
  - Runtime
  - Middleware
  - O/S
    - Virtualization
    - Servers
    - Storage
    - Networking

**Software as a Service (SaaS)**
- Data
  - Application
  - Runtime
  - Middleware
  - O/S
    - Virtualization
    - Servers
    - Storage
    - Networking
Poll

- My organization uses SaaS providers
- I am aware of shadow IT in my environment
- My SaaS provider(s) encrypt data at rest
- Why should I care?
If They’re Providing Data-at-Rest Encryption

And they hold the keys
It’s not quite as bad as that!
# Data Protection with Encryption

## Varies by Cloud Model

<table>
<thead>
<tr>
<th>Cloud Model</th>
<th>Encryption Mechanism</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>IaaS</td>
<td>Native, Bring Your Own</td>
<td>If native, seek BYOK, Consider BYOE (Why?)</td>
</tr>
<tr>
<td>PaaS</td>
<td>Native, Some CASB’s provide</td>
<td>If native, seek BYOK, CASB potential limitations</td>
</tr>
<tr>
<td>SaaS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CSA – Cloud Controls Matrix

Let’s go back to Key Management for a sec…

Keys shall not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.
Understanding
Bring Your Own Keys

Your Key Vault
• Protect & manage your keys
• Facilitate compliance with data security regulations
• Many solutions FIPS 140-2 certified

Cloud Key Vault
• Cloud HSMs
• Holds your keys
• Secures your data

Your Data
• Encrypted in the cloud
• Uses your own keys
• You can revoke
• Data in your control
A Hierarchy of SaaS Security

SaaS Vendor 1
Clear Text

Peter Johnson 233 44 255 46
Sally Peterson 418 22 418 31

SaaS Vendor 2
Encrypted with Vendor Keys
mAQ0%oQlP D$0u5Yy&E MX
#U2pEk5!W *4sGmLBY1 1%

SaaS Vendor 3
Encrypted with Customer Keys
mAQ0%oQlP D$0u5Yy&E MX
#U2pEk5!W *4sGmLBY1 1%
BYOK Recommendations

• Study CSA Security Guidance v3
  ▪ Join CSA and contribute to CSA Guidance v4

• When purchasing or re-subscribing to IaaS, PaaS, or SaaS
  ▪ Submit CSA Consensus Assessment Initiative Questionnaire
  ▪ Focus their attention on encryption key management

• Work with a key management or encryption vendor to assist
Questions?
Thank You!