Adopting Cloud Apps?
Ensuring Data Privacy & Compliance

Varun Badhwar
Vice President of Product Strategy
CipherCloud
Agenda

Cloud Adoption & Migration Challenges
- Introduction to Cloud Computing
- Cloud Security & Privacy Challenges
- Cross Border Laws & Regulations

Emerging Cloud Data Protection Trends
- Top Cloud Data Protection Principles
- Cloud Security - A New Approach
- Addressing Emerging Cloud Threats

Case Studies

Q&A
Introduction
Cloud’s Explosive Growth
Expanding From SMB to Enterprises and Governments

Forecast: Global Public Cloud Market Size, 2011 To 2020

Source: Forrester Research, Inc.
Cloud Computing – Who Controls What?

In traditional IT environments, organizations generally share control over the network with service providers, but for the most part they control the applications, servers, and storage for their IT environments.

In an internal cloud environment, the architecture changes, but not the complexion of control. For public or private (community) cloud offerings the control architecture changes profoundly.
Forrester's clients have consistently rated security as their top concern with cloud computing, ahead of other issues such as performance and availability.

Source: Forrester, 2011

Security still top concern with cloud, despite Amazon outage. Enterprises I speak to are more concerned about security than they are about availability, reliability, or performance.

Source: Gartner, 2011

Security & Compliance Remain the Biggest Barriers to Cloud Adoption

Source: Survey by Marketing Solutions, 2011
The Multi-Tenant, Distributed Delivery Model of Cloud Computing Introduces Further Regulatory Complexities

Q: Are you breaking any regulatory requirements for data privacy when your data "crosses borders"?

A: You could be.
Key Regulatory and Compliance Challenges

• **Localization of Information**: Data may be stored in the cloud without proper customer segregation allowing possible accidental or malicious disclosure to third parties.

• **Individual Rights**: Data may physically reside in a legal jurisdiction where the rights of data subject conflict or may not be protected at all.

• **Data Movement**: The cloud’s loosely defined, uncertain or moving geography means that consumers are faced with increased legal complexity, legal contradictions and uncertainty.

• **Confidentiality**: The cloud facilitates the ability to use/share data across organizations and therefore increases the potential for secondary uses of data that require additional consent or authorization.

• **Breach and Disclosure**: The timely discovery, assessment, and reporting of the breaches from within the cloud are more challenging.

• **Cloud Audit**: It is difficult to audit the data in the cloud, because isolating the scope in a cloud environment is challenging.

• **Data Retention**: Enterprise’s data retention or data archiving requirements may not be met when using cloud due to lack of standardization.
Emerging Cloud Data Protection Trends
Top Cloud Data Protection Principles
Securing sensitive data in the cloud

• Classify your data

• Retain full control over your data in the cloud
  – Cloud providers should not have access to any sensitive customer data

• Do not impact usability or performance

• Standardize on one technology to protect all clouds
  – Salesforce, Amazon, Force.com, Gmail, Workday

• Address all threats in the cloud
  – Encryption, tokenization, malware detection & removal, DLP, auditing & forensics, etc.
Data Classification – A First Step to Cloud Migration

• Decide
  – Which data is ready for storage in the cloud
  – Under which circumstances, and
  – Using which controls

• Enforce
  – Systematic adherence to a sound data classification policy
Retain Full Control Over Data in the Cloud
Encrypt/Tokenize data before it leaves your network

- Preserve data formats & operations
- Retain control of keys

www.privacyassociation.org/symposium
Encryption & Key Ownership

- Implement NIST approved encryption algorithms (e.g. AES)
  - Granular control - field level encryption choice
  - Free-text fields with ability to index and search individual words
- Key ownership
  - Key remains with the customer, never with provider to address external threats
  - Split-keys and dual custody on keys to address internal threats
  - Ability to rotate keys
  - HSM integration
Encryption Based Deployment Layout
Each Server is Completely Stateless & Independent
Tokenization for Cloud Services

- Original data is mapped to randomly generated values (Tokens)
- Mappings stored in local DB
- Tokens have no mathematical relationship with the original data
- Format is preserved – Tokens are structurally similar to original data
Tokenization Based Deployment Layout
Requires Replication Between All Token Servers & Persistent Databases

RTR* - Real Time Replication

www.privacyassociation.org/symposium
## Comparing Encryption & Tokenization

<table>
<thead>
<tr>
<th>Feature</th>
<th>Encryption</th>
<th>Tokenization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Storage</strong></td>
<td>In the cloud - encrypted</td>
<td>On-premises – in a local DB</td>
</tr>
<tr>
<td><strong>Architecture</strong></td>
<td>Stateless – no session information or data stored</td>
<td>Stateful – data is stored in a local database</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>Easy to scale without replication or synchronization</td>
<td>Requires real-time replication of databases</td>
</tr>
<tr>
<td><strong>Distributed Deployment</strong></td>
<td>Easy – the gateways do not need to communicate and exchange data with each other</td>
<td>Hard – the gateways must communicate with each other and exchange data in real-time</td>
</tr>
<tr>
<td><strong>Latency</strong></td>
<td>Near-Zero</td>
<td>Medium-High (dependent on network throughput and deployment architecture)</td>
</tr>
<tr>
<td><strong>Cost Overhead</strong></td>
<td>Low – requires a single virtual server.</td>
<td>High – requires heavy-duty servers, databases for persistent storage, backup and DR services, and heavy administration and maintenance costs.</td>
</tr>
</tbody>
</table>
What’s Right for Your Organization?

When to Apply Encryption

- Data security, privacy or residency concerns are primary drivers
- Need to scale across thousands of users, with millions of records and multiple geographies
- Performance is a key consideration
- Budgets for infrastructure, administration and on-going maintenance are tight

When to Apply Tokenization

- Scale of deployment is limited to a few hundred users, thousands of records and a single geography
- In return for on-premise data storage, you are willing to compromise on performance
- Budgets for infrastructure, administration and on-going maintenance are a non-issue
Unified Policies Across All Clouds

Multiple Key Management
Inconsistent Policies
One Gateway for Each Cloud

Single Key Management
Unified Policies
Single Gateway across All Clouds
Address Emerging Cloud Threats in Real-Time

- **Cloud Data Protection**
  - Encryption, Key Ownership
  - Tokenization, Masking
- **Cloud Malware Detection**
- **Cloud Audit**
- **Identity & Access Control**

[Diagram showing data privacy, security, compliance, and data residency with icons for cloud data encryption, cloud malware detection, data tokenization, and cloud audit.]

[Image with website URL: www.privacyassociation.org/symposium]
Case Studies
## Industry Examples

<table>
<thead>
<tr>
<th>Organization</th>
<th>Pain-points Addressed</th>
<th>Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Democratic Party of Canada</td>
<td>24M Canadian voters identities in the US cloud</td>
<td>R</td>
</tr>
<tr>
<td>Multi-National Investment Bank</td>
<td>Migrate to SaaS to collaborate on highly sensitive M&amp;A information</td>
<td>P, S</td>
</tr>
<tr>
<td>F100 Health Insurance</td>
<td>Patient information and radiology files going to cloud</td>
<td>P, C</td>
</tr>
<tr>
<td>F100 Technology</td>
<td>Federal restrictions on access to defense customer information (ITAR)</td>
<td>C</td>
</tr>
<tr>
<td>Costa Rican Banks</td>
<td>Financial applications in the cloud</td>
<td>P, C</td>
</tr>
<tr>
<td>Major US Bank</td>
<td>Migrating apps (sensitive data) to cloud from current 6,000 users to 20,000+</td>
<td>R, S</td>
</tr>
<tr>
<td>Major Australian Bank</td>
<td>Regulators require information to reside within jurisdiction</td>
<td>R</td>
</tr>
</tbody>
</table>

data Residency: R  
data Privacy: P  
Compliance: C  
Security: S
Case Study: Top Canadian Bank

• Overview:
  – Investment Banking group interested in adopting a cloud application, but security and compliance groups concerned about leakage of confidential M&A data

• Challenge:
  – Cloud application did not sufficiently meet their organizational security requirements around data separation, encryption and key management

• Solution:
  – Cloud encryption gateway has allowed the Bank to secure sensitive data using highly secure encryption schemes without having to share the encryption keys with the cloud provider
  – The Bank has integrated the gateway with their existing enterprise key management solution and given them the ability to rotate keys at regular intervals

• Benefit:
  – The Bank is planning to extend its usage of the cloud app by purchasing hundreds of additional licenses for the Capital Markets group
Case Study: New Democratic Party

- **Overview:**
  - NDP holds records of all Canadian voters (over 24 million), which it was looking to manage in Salesforce

- **Challenge:**
  - Deployment stalled for over a year due to data-residency and privacy concerns (U.S. Patriot Act)
  - Salesforce’s database-level encryption broke critical functionality such as search, sorting and reporting

- **Solution:**
  - Deployed a cloud encryption and tokenization solution within a couple of weeks that addressed all NDP requirements – preservation of native Salesforce functionality, seamless integration with AppExchange apps including Informatica Cloud, no visible latency, and ability to integrate with Apex code

- **Benefit:**
  - NDP was able to migrate 24M records to Salesforce before the election deadline
Case Study: Top 5 US Bank

• Overview:
  – Mortgage division wanted to leverage a cloud solution to implement a loan applications portal
  – Customers have the ability to upload relevant documents (e.g. W2, paystubs, etc.)

• Challenge:
  – Existing malware solution is unable to scan documents in the cloud
  – All customer data must be stored in an encrypted format

• Solution:
  – Implemented a cloud malware detection engine that scans documents on-the-fly as they are uploaded by customers in the portal. Infected documents are blocked
  – If no malware is detected, the files are encrypted and stored in the cloud

• Benefit:
  – The Bank was able to comply with the internal security requirements that were preventing them from migrating the portal into the cloud
Summary

• Eliminate privacy & security concerns with cloud stored data
  – Satisfy compliance & residency requirements for customer-sensitive data
  – US Patriot Act, Canadian PIPEDA, EU Data Protection Directive

• Protect customer-sensitive data against emerging cloud threats
  – Minimize data loss from security breaches (e.g. Epsilon, Dropbox)
  – Data Breach cost estimated at $214 per customer record *
  – Protect reputation

• Accelerate cloud adoption and value realization
  – Significant cost savings in migrating on-premise apps to public cloud