Migrating Applications To The Cloud

Security and Compliance Considerations

Norm Barber, Managing Director
UnifyCloud LLC

February 2015
Speaker: Norm Barber
Managing Director, UnifyCloud LLC

- 35-year veteran of the IT industry starting as an IT Director in traditional IT organizations.
- Participated in the transition from distributed processing through client-server to the use of Cloud and mobile.
- Last 15 years focused on Security, Identity & Access Management (S/IAM), and IT Risk Management.
- Currently, Managing Director at UnifyCloud LLC, a Cloud-focused consultancy specializing in S/IAM controls.
- Previously, held management positions with PwC, KPMG, Andersen Worldwide (Partner and Global Services Director for the Security & Privacy practice) and Protiviti (Founding Managing Director and Identity Practice Lead).
- Microsoft’s Strategic Security Advisor for the US Financial Services sector and Principal Program Manager for the Customer & Partner Engineering Group within the Azure Identity & Security Services Division.
- Held CISSP and CISM certifications and served on the Technology Committee of the Institute of Internal Auditors.
- Member of the Cloud Security Alliance (CSA), the Information Systems Audit and Control Association (ISACA), the Information Systems Security Association (ISSA), InfraGard (the private sector and FBI partnership), and U.S. Secret Service Electronic Crimes Task Force.
15-year journey...the Security threat landscape...

Key Threats
- Mainly leveraging social engineering

Key Threats
- 9/11
- Mainly exploiting buffer overflows
- Script kiddies
- Time from patch to exploit: Several weeks

Key Threats
- Zotob (2005)
- Attacks «moving up the stack» (Summer of Office 0-day)
- Rootkits
- Exploitation of Buffer Overflows
- Script Kiddies
- Raise of Phishing
- User running as Admin

Key Threats
- Organized Crime
- Botnets
- Identity Theft
- Conficker (2008)
- Time from patch to exploit: a few days

Key Threats
- Organized Crime, potential state actors
- Sophisticated Targeted Attacks
- Operation Aurora (2009)
- Stuxnet (2010)

Key Threats
- Nation-state attacks; Sony is not an anomaly
- Kinetic Attacks; the Internet of Things (IoT)
- Technology innovations that outpace security
- Data on user-owned mobile devices

Key IT Risks
- Security
- Confidentiality
- Reliability
- Availability

Key IT Risks
- Security
- Confidentiality
- Reliability
- Availability
- Stability
- Speed
New IT all up risks for the Cloud-era...

Stability of Cloud platforms

**Stability** [stuh-bil-i-tee] noun
1. continuance without change; permanence.
2. resistance to change, especially sudden change
New IT all up risks for the Cloud-era...

Speed of Cloud adoption

**Speed** [speed] noun
1. relative rapidity in moving, going, etc.; rate of motion or progress.
2. full, maximum, or optimum rate of motion.

CIOs - “Must go faster!”
UnifyCloud’s Mission

Our Mission is to help our clients deal with the speed of Cloud adoption and the utilization of ever-evolving Cloud-based services.

We focus on the implementation of effective Enterprise-grade S/IAM* controls, creation of Cloud app-development Best Practices, and the migration of apps to the Cloud.

The capabilities we deliver are:

- Native in a CSV’s IaaS / PaaS platforms
- Configurable by the subscriber
- Provided by a 3rd party Cloud service (as needed)
- Delivered by migration / compliance tools

* Security and Identity & Access Management
Key Takeaway:

The magnitude of the migration effort to the Cloud, the complexity of both customized apps and Cloud environments, and the requirement for ongoing app-level monitoring suggests the need for what Gartner calls a “programmable security infrastructure capable of supporting security policy ‘toolchains’.”

Discussion Areas:

• Four Premises associated with Cloud adoption;

• Using technology to address the challenges of these Premises; and

• A case study on lighting up this “toolchain” technology.
Premise #1: Cloud adoption is accelerating around PaaS...

**Platform as a Service (PaaS)** — The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer **does not manage or control** the underlying Cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Examples:
- Application Development, Data, Workflow, etc.
- Security Services (Single Sign-On, Authentication, etc.)
- Database Management
- Directory Services

**Infrastructure as a Service (IaaS)** - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure **but has control over** operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

_NIST Special Publication 800-145_
Beyond IaaS, PaaS will unleash creativity in rethinking scenarios...

- Gartner considers PaaS as “Transformational” over the next 2 to 5 years (as of July 2014).
- PaaS is more than a collection of outsourced infrastructure services that can support legacy apps tweaked for the Cloud.
- PaaS can provide the building blocks for innovative, new scenarios.

Source: Microsoft
Premise #2: Adopting DevOps is happening concurrently...

“When every deployment is done differently, every production environment is a different snowflake. When this occurs, no mastery is ever built in the organization in procedures or configurations.”

Gene Kim; *The Top 11 Things You Need To Know About DevOps*

“How soon? Gartner indicates: “By 2015, 20% of enterprise IT departments that have adopted DevOps principles will extend this vision to incorporate information security up from 2% at year end 2011.”

“...for core components that make up a delivery pipeline, each of the components need to be available as a service, in order to provide a complete ‘DevOps on PaaS’ solution,” *DevOps.com*
DevOps in the Cloud impacts Security processes as well...

“DevOps cannot be successful if security is not an integral part of the vision. We believe a combined philosophy of “DevOpsSec” will become a critical capability for IT departments embracing Cloud operating models to improve security, lower costs, securely embrace new business requirements and protect from advanced threats.”

*DevOpsSec: Creating the Agile Triangle; Gartner*

Gartner Recommendations

- DevOps teams need to evolve into integrated DevOpsSec teams, with security personnel recognized as critical peer members.
- Develop a simplified framework for security policies and processes that complements the agile foundation of DevOps, yet still provides the necessary protection of key enterprise assets.
- Invest in programmable security infrastructure capable of supporting security policy "toolchains," which facilitates speed through automation and flexibility via open APIs.
Premise #3: IT Risk Management is evolving along with the Cloud...

"...by understanding what Cloud is and what it is not and by asking a few key questions of management teams, boards can gain that confidence—in management plans and strategic goals, as well as in the decisions made in response to those plans."

"The potential benefits of Cloud services can be enticing, but with reward comes risk. The enterprise must decide whether the potential risk is within acceptable limits."

"Current and potential Cloud customers must avoid the trap of 'Cloud complacency': assuming that anything that’s as easy to use a Cloud-based service must automatically be secure and reliable. All IT decision makers need to be aware of the degree to which Cloud-using organizations must be responsible for their own security destiny."

Gartner: Hype Cycle for Cloud Security, 2014

Source: ISACA
“Additional Cloud risk has the following main components…”

- Greater dependency on third parties:
  - Increased vulnerabilities in external interfaces
  - Increased risk in aggregated data centers
  - Immaturity of the service providers with the potential for service provider ongoing concern issues
  - Increased reliance on independent assurance processes

- Increased complexity of compliance with laws and regulations:
  - Greater magnitude of privacy risk
  - Transborder flow of personally identifiable information (PII)
  - Affecting contractual compliance

- Reliance on the Internet as the primary conduit to the enterprise’s data introduces:
  - Security issues with a public environment
  - Availability issues of Internet connectivity

- Due to the dynamic nature of cloud computing:
  - The location of the processing facility may change according to load balancing
  - The processing facility may be located across international boundaries
  - Operating facilities may be shared with competitors
  - Legal issues (liability, ownership, etc.) relating to differing laws in hosting countries may put data at risk”
At the end of the day, your Board expects you’ll own IT risk all up...

“Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with Cloud computing... A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.”

**NIST: Guidelines on Security and Privacy in Public Cloud Computing**

Source: Microsoft
Cloud “shared responsibility” models need to be understood...

Source: Amazon Web Services

Source: Microsoft
What “managed by customer” means (from a typical SOC* report)...

Controls and reporting as well as configuration oversight excluded from a CSV platform SOC report

- Controls over account / subscription IDs and passwords and access to applications.
- Compliance with applicable laws/regulations.
- Determining and implementing encryption for data.
- Securing certificates used to access applications.
- Selection of access mechanism for data.
- Determining the Services configurations.
- Backup of data to local / Cloud storage.
- Protection of the secrets associated with accounts.
- Implementing interconnectivity between Cloud and on-premises resources.
- Security Development Lifecycle for applications.
- Application QA prior to moving to Cloud production.
- Monitoring the security of applications.
- Reviewing and applying public security and patch updates (IaaS).
- Reporting the incidents and alerts specific to systems and subscriptions.
- Support timely responses with Cloud platform.
- Implementing redundant systems for hot-failover.

* AICPA Service Organization Control (SOC) Reports (Type I and Type II) formerly Statement on Auditing Standards No. 70: Service Organizations (SAS 70)
Premise #4: Moving apps to the Cloud is not once and done...

1. What are the Enterprise standards for PaaS and app-level settings based on Cloud S/IAM policies and best practices?

2. How do we know if LOB apps, once re-factored, or built from the ground up, will be in compliance once deployed?

3. As Cloud environments are evolved by CSVs, apps are enhanced by developers, and/or controls are updated due to emerging threats, how will compliance “drift” be monitored, reported and remediated quickly?

Azure Services...Source: Microsoft
Moving apps to “the Cloud” can seem straightforward....

1 Discover & Assess

- **Discover & Assess** – Create an inventory of applications and workloads that are candidates for Cloud - SaaS (replace), IaaS (lift and shift), PaaS (refactor / rebuild). Sort out the “noise” (agents, drivers, hot fixes). Use criteria such as infrastructure, architecture (32- vs. 64-bit), data compliance requirements, hardware dependency, software EOS, and mission criticality (BCDR).

2 Target & Migrate

- **Target & Migrate** – Determine those apps that have potential SaaS alternatives, that need to be encapsulated to run on IaaS, or can be moved to a more long-term PaaS environment. For PaaS-bound apps, determine the specific PaaS services (Compute, Storage, Network) required, validate at the code level what remediation is required, remediate and test against PaaS standards. Use this same process to validate app readiness for PaaS on new apps developed in the Cloud.

3 Monitor & Report

- **Monitor & Report** – Using a baseline of Enterprise standards for S/IAM and Cloud best practices, monitor and report on app compliance as PaaS environments evolve, apps are changed, and Enterprise standards are updated. Rinse and repeat.
Once moved, apps running on PaaS will experience “drift”...

Main reasons for Drift:

- Devs responsible for LOB apps may:
  - Not have understood fully the S/IAM requirements in the first place,
  - Find guidance too complex to digest, and/or
  - Not have the time / skills to make appropriate changes to meet baseline S/IAM requirements;

- Aggressive, VM-centric, migrations may have swept up LOB apps on those targeted VMs not fully configured or tested for compliance against a S/IAM controls baseline;

- Even with diligence on the part of Devs, over time PaaS environments will evolve as will the associated S/IAM Cloud controls baseline, often in six-month cycles; and

- Manually certifying LOB apps against an ever-evolving S/IAM baseline, will be a time sink and raise questions about thoroughness and accuracy.
Cloud evolution, enhancements and change are inevitable...

**Traditional On-Premises Server Migration**

1. Discover & Assess
2. Target & Migrate
3. Monitor & Report

**Cloud Services Adoption, Provisioning and Deployment**

1. Discover & Assess
2. Target & Migrate
3. Monitor & Report

Cloud Feature PMs - “Start me up!”

When “Drift” is unmanaged

© UnifyCloud LLC All rights reserved
These four Premises argue for technology as a way to cope...

1. Cloud adoption is accelerating around PaaS...
2. Adopting DevOps is happening concurrently...
3. IT Risk Management is evolving along with the Cloud...
4. Moving apps to the Cloud is not once and done...

Technology that can provide both guidance and governance while evolving at Cloud-speed as platforms evolve, apps change, and IT Risk Management / threat models adapt. This technology should have four components:

- App Discovery and Migration Target Assessment
- Controls & Settings Knowledgebase / Repository
- App Cloud Readiness Assessment, Remediation, and Test
- Compliance Monitoring and Reporting
Tooling to support the app migration roadmap to PaaS...

1. Discover & Assess
2. Target & Migrate
3. Monitor & Report
Migrating Applications To The Cloud

Case Study
Client’s charter: Create a Dev-centric, self-service solution to...

- Move LBI and MBI LOB apps* to Azure PaaS in an efficient and highly leveraged way (i.e., is NOT dependent only on development resources);
- Assure those moved LOB apps are compliant with our S/IAM controls and preferred Enterprise PaaS settings in the first place;
- Allow for the evolution of S/IAM controls and PaaS settings so that the baseline for migration and operations are consistent; and
- Monitor LoB app compliance over time providing for fast and efficient remediation when the inevitable “drift” happens.

*Data Classification: Low Business Impact (LBI) and Medium Business Impact (MBI)
App assessment was detailed and prescriptive...

Typical app patterns
- Web-based
- Websites
- Mobile

- 30+ Azure Services
- >200 Data Points
- >300 Settings
Included the “As Is” app architecture... as well as the “To-Be”...

But we only have 1 database for this app.

No, actually you access 9 databases.
Azure Validator Recommendations

Application Name: MS Plancast
Application ID: ICTO-2037

- No of Projects: 19
- No of Files Scanned: 666
- No of Lines: 522
- Scan Date: 03/02/2015

Total Recommendations: 1315
- Application & Platform Design: 38
- Network & Availability: 4
- Storage: 1270
- Security: 3

Estimate Effort Sizing:

<table>
<thead>
<tr>
<th></th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1211</td>
<td>99</td>
<td>5</td>
</tr>
</tbody>
</table>

Impact:
- Mandatory: 100.0%
- Optional: 0.0%

Azure Readiness (#Files: 666)
- Azure Ready: 85.0%
- Need Changes: 14.0%
IT Risk Management Professionals Call To Action

• Understand the unique End of Service risks associated with Windows Server 2003 (7/15) and SQL Server 2005 (4/16) regarding applications built on those platforms:
  ▫ Upgrade applications to run on-premises on Windows / SQL with more current versions;
  ▫ Retire older applications and look for SaaS solutions as replacements;
  ▫ Encapsulate the older, unsupported applications and “lift and shift” to IaaS; and
  ▫ Refactor / rebuild mission critical applications into “modern applications” to run on PaaS.

• Understand the importance of Security, Identity Management and Compliance all-up in a Hybrid IT environment. A CSV’s SOC report (or other risk assessment) is necessary, but not sufficient;

• Prepare to operate your IT Risk Management program at “Cloud Speed”. Recognize that threats, platform features, and modern apps will constantly evolve and you must manage “drift”; and

• Evaluate risk management tools that have been designed to operate in the Cloud and take into consideration the ever changing nature of Hybrid IT and its frequently updated IT control structure.
Summary:

- Four challenges can make migration slow, tedious and complex:
  - Cloud adoption is accelerating around PaaS...
  - Adopting DevOps is happening concurrently...
  - IT Risk Management is evolving along with the Cloud...
  - Migrating apps to the Cloud is not once and done...
- Technology can address these challenges.
- UnifyCloud LLC has developed this technology.
Migrating Applications To The Cloud

Norm Barber, Managing Director
normb@unifycloud.com

Questions?