Building Resilience with Disaster Recovery on Cloud

15th October 2020
Agenda

10.00 – 10.10  Webinar Orchestrator e introduzione del concept di DR
Matteo Pontremoli, Director Deloitte

10.10 – 10.25  Deloitte PoV su Resilience e Disaster Recovery
Fabio Battelli, Partner Risk Advisory Deloitte

10.25 – 10.45  Deloitte Cloud Engineering Capabilities su Disaster
Recovery
Barbara Messineo, Consultant Deloitte

10.45 – 11.00  Implementazione DR con AWS, DR da un PoV tecnico e
presentazione dei vari scenari di tempo di ripristino
per diversi casi
Diego Colombatto, AWS Solution architect

11.00  Q&A session
Speakers

Fabio Battelli
Partner Risk Advisory Deloitte

Matteo Pontremoli
Director Deloitte

Barbara Messineo
Consultant – Cloud Engineer

Diego Colombatto
Solution Architect

#BuildResilienceOnCloud
Matteo Pontremoli
Director Deloitte

Matteo Pontremoli is Director at Deloitte Italia with over 25 years of experience in technological and architectural solutions, deep knowledge of enterprise IT and infrastructure and systems migration projects. Within the Cloud practice, he guides the implementation and migration projects and subsequent Cloud operations, architecture solutions, design, implementation and large-scale implementation of IaaS, PaaS and SaaS on the main Cloud providers.
From Disaster Recovery to Business Resilience
Fabio Battelli
Partner Risk Advisory Deloitte

Fabio has been working for over 16 years’ in Consulting field with a specific focus on ICT/Cyber Security where he is well-recognized Trusted Advisor and Subject Matter Expert in critical infrastructure protection (CIP), Security Operations Center (SOC) and Managed Security Services (MSS), Computer Emergency Response Team (CERT), Information Security Risk Management, IT Security Compliance and complex ICT security infrastructure design and deployment.
This new risk landscape is requiring organizations’ to achieve a “Resilience” posture to anticipate and respond effectively to potential unexpected threats.
A solid Business Continuity strategy should identify main threats and related risks that could affect the business operations...

<table>
<thead>
<tr>
<th>Threat Categories</th>
<th>Typical Business Continuity Threats</th>
<th>Business Continuity Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural</td>
<td>Flood, Fire, Earthquake, Heat Wave, Storm</td>
<td></td>
</tr>
<tr>
<td>Social</td>
<td>Hijacking in VIP or Group, Theft (insider/external), Epidemic, Sabotage, Terrorism / Piracy</td>
<td></td>
</tr>
<tr>
<td>Technological</td>
<td>Power Failure, HVAC Failure, ICT outages, Cyber Attack, Supply chain disruption</td>
<td></td>
</tr>
<tr>
<td>Reputational</td>
<td>Sponsor/ 3rd party Scandal, Car Failure, Regulatory Penalties, Large Recall Campaigns, Fake News</td>
<td></td>
</tr>
</tbody>
</table>
“Resilience” is an evolution posture to anticipate and respond effectively to potential unexpected threats.

The Evolution Path from «Backups» to «Resilience»

- **Backups**: Making exact copies of electronic data.
- **Disaster Recovery Plan**: Plan for the recovery of data processing facilities (IT Systems).
- **Contingency Measures & Plan**: Specific Measures & Procedures to follow after operational mishaps.
- **Business Continuity Plan**: Plan for recovering business operations.
- **Business Continuity Management**: Building availability into management processes.
- **Predictive Modeling**: Anticipating the effects of emergencies before they happen.
- **Resilience**: Hardening the enterprise against all foreseeable emergencies.
The Business Continuity Program shall include the preliminary measures to respond to different expected incidents, the procedures to manage incidents and assess the damages, the declaration of state of emergency involving all the components that contribute to service delivery.
Cloud Computing can dramatically change the journey to achieve business resilience...

Organizational Resilience Framework

How should we manage Resilience as we move to the cloud?

- Buildings
- Equipment
- Technology - IT
- Technology - Network
- Human Resources
- Third Parties
FROM DISASTER RECOVERY TO BUSINESS RESILIENCE

...addressing faster and simpler the main business continuity threats

- **Natural Disaster, Fires & Floods**: Hurricanes, recent winter storms, earthquakes, and localized storms
- **Ransomware & Malware**: Malicious software that infects your computer and data computer is locked -- typically by encryption
- **Power outage**: These could impact your own facility or data center, but could also be the cause of third party outages.
- **Self-inflicted outages**: Critical application outages due to human error in implementation or errors not found during testing.
- **Datacenter Outage**: Disruption of service of the entire site
- **Communications outages**: These could be considered third party outages, but since we leverage these for core business processes, losing just this function
- **Network provider**: Third party provider category, but give the criticality of your network access, network issues outside of your control can impact the entire organization.
- **Internet (ISP) outage**: Remote access, and other internet-based work, an internet outage could have a similar impact as a data center outage.
Deloitte’s approach to BCM / DR allow an organization to evaluate credible risks, critical business processes, internal and external dependencies, and the supporting technologies to determine the requirements for recovery.
Combining our strengths, Deloitte Advisory and cloud technologies can help organizations deliver agile and secure “always-on” business capabilities as they develop a cloud adaption framework...

**Resilience Domain**

- Business Continuity Preparedness and Response
- Cyber Resilience
- Incident Response, Emergency Management
- Disaster Recovery

**Deloitte Accelerators**

- **Strategy**
- **Governance**
- **Architecture**
- **Operations**

**Technical Resilience**

- Risk & Compliance
- Incident Response
- Remediaition
- Business Operations

**Cloud Technology**

**Desired End State**

- **Always on**
  Aligns all organizational elements to support zero downtime expectation.

- **Risk sensing**
  Responsive controls designed to align threat mitigation strategies to actual disruptive events.

- **Governance guard rails**
  Configuration management under command of automation eliminates snowflake environments.

- **Confidence in survivability**
  Deliberately induce failure to validate business continuity and the immutability of operations.

- **Agility**
  Protect the cloud with the cloud by dynamically changing the attack surface to absorb attacks and disorient attackers.

- **Reduced dependence on physical data centers**
  Cloud-enabled solutions reduces physical footprint and moves costs from CapEx to OpEx recognition.
...accelerating a cloud-based approach to strengthen an integrated cyber and resiliency strategy

<table>
<thead>
<tr>
<th>Threat Landscape</th>
<th>Business Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who might attack?</td>
<td>Growth/Innovation</td>
</tr>
<tr>
<td>What are they after?</td>
<td>Operational Efficiency</td>
</tr>
<tr>
<td>What tactics will they use?</td>
<td>Risk Management</td>
</tr>
<tr>
<td></td>
<td>Regulatory Compliance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber Cloud Strategy &amp; Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy &amp; roadmap</td>
</tr>
<tr>
<td>Policies &amp; standards</td>
</tr>
<tr>
<td>Training &amp; awareness</td>
</tr>
<tr>
<td>Asset management</td>
</tr>
<tr>
<td>Integration with business and IT processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Foundational Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know Your Assets</td>
</tr>
<tr>
<td>Know Your Data</td>
</tr>
<tr>
<td>Know Your Customers</td>
</tr>
<tr>
<td>Know Your Employees</td>
</tr>
<tr>
<td>Know Your Third Parties</td>
</tr>
<tr>
<td>Know Your Attackers</td>
</tr>
<tr>
<td>Know Your Services/Processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federation, MFA &amp; SSO</td>
</tr>
<tr>
<td>Cloud Roles and Responsibilities</td>
</tr>
<tr>
<td>Privileged access management</td>
</tr>
<tr>
<td>Conditional Access</td>
</tr>
<tr>
<td>Access Certification</td>
</tr>
<tr>
<td>Identity Lifecycle Management</td>
</tr>
<tr>
<td>IAM Governance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy &amp; data protection policy</td>
</tr>
<tr>
<td>Data discovery</td>
</tr>
<tr>
<td>Data loss protection controls</td>
</tr>
<tr>
<td>Granular data access management</td>
</tr>
<tr>
<td>Key Vault deployments</td>
</tr>
<tr>
<td>Key management processes</td>
</tr>
<tr>
<td>Encryption &amp; Tokenization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Architecture Assessment</td>
</tr>
<tr>
<td>DevSecOps &amp; CI/CD</td>
</tr>
<tr>
<td>Secure Development Lifecycle</td>
</tr>
<tr>
<td>SAST/DAST Code Analysis</td>
</tr>
<tr>
<td>PaaS Configuration Standards</td>
</tr>
<tr>
<td>Secure Configuration &amp; Change Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Segmentation</td>
</tr>
<tr>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>IaaS configuration compliance</td>
</tr>
<tr>
<td>Network ACLs</td>
</tr>
<tr>
<td>Secure Connectivity</td>
</tr>
<tr>
<td>Baseline Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligent Threat Protection</td>
</tr>
<tr>
<td>Log Centralization</td>
</tr>
<tr>
<td>SIEM &amp; SOC Integration</td>
</tr>
<tr>
<td>Network Monitoring (IDS/IPS)</td>
</tr>
<tr>
<td>Vulnerability Management</td>
</tr>
<tr>
<td>Endpoint Monitoring</td>
</tr>
</tbody>
</table>

**Deloitte Cloud Cyber and Resilience Framework**

**Input**

**Leading Practices**
- Recognized information security leader
- Project/engagement experience
- Published industry research (CIS)
- Azure/AWS/GCP security best practices

**Industry Standards**
- ISO 27001/2
- NIST Cybersecurity Framework
- Cloud Controls Matrix CSA

**Cloud Cyber Risk Domains**

**Response**
- Response Planning
- Communications
- Disaster Recovery Planning
- Data Backup/Recovery Strategy
- Incident/Change Management
- Orchestration Playbooks
Customize with Deloitte your own Disaster Recovery on AWS
Speakers

Barbara Messineo
Consultant – Cloud Engineer

Barbara has more than 3 years of experience in several international projects where she covered each phase of the cloud migration journey.

Experienced in AWS Cloud Migration and Disaster Recovery project in the field of safety-critical systems.

Responsible for the analysis of the architecture, the identification of all potential failure modes and definition of safety approaches.
Deloitte named the worldwide leader in Public Cloud Infrastructure Professional and Managed Services by Gartner.\(^1\)

Deloitte named a worldwide leader in Business Consulting Services based on capability and strategy by IDC.\(^2\)

Deloitte named a leader in Cloud Professional Services by IDC.\(^3\)

Deloitte named a strong performer in Application Modernization And Migration by Forrester.\(^4\)

Deloitte named a global leader in Cloud Consulting based on capabilities by ALM Intelligence.\(^5\)

---

1 Source: Gartner, Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide, Chee Eng, Scot MacLellan, Ross Winser, Brandon Medford, 4 May 2020
4 Source: Forrester Research, The Forrester Wave™: Application Modernization And Migration Services, Q3 2019; By Bill Martorelli with Christopher Voce, Julia Caldwell, Matthew Flug, Diane Lynch, July 16, 2019
5 Source: ALM Intelligence; Cloud Consulting 2016; ALM Intelligence estimates © 2016 ALM Media Properties, LLC. Reproduced under license

---

1 Source: Gartner, Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide, Chee Eng, Scot MacLellan, Ross Winser, Brandon Medford, 4 May 2020
4 Source: Forrester Research, The Forrester Wave™: Application Modernization And Migration Services, Q3 2019; By Bill Martorelli with Christopher Voce, Julia Caldwell, Matthew Flug, Diane Lynch, July 16, 2019
5 Source: ALM Intelligence; Cloud Consulting 2016; ALM Intelligence estimates © 2016 ALM Media Properties, LLC. Reproduced under license
## Why choose Deloitte for your Cloud DR Solution

Deloitte is uniquely positioned to help our clients be successful in the definition of DR Plan

### Experienced Team

**Breadth of Cloud Capabilities**
- Cloud and Infrastructure
- Cloud Strategy and Operating Model
- Cloud Governance and culture
- Cloud Cyber Security and Risk

**Depth of Technical Experience**
- Certified Solution Architects
- Deep Cloud & Security Expertise

### Proven Capabilities

**Mature Capabilities and tools**
The proprietary assets have been built through the successful design and build-out of cloud models in ‘like’ global complex institutions

**Top Industry Recognition**
- Forrester
- Gartner
- Kennedy
- ALM

### Industry Insight

**Deep Industry presence and competences**
- Financial Services
- Life Sciences & Healthcare
- Energy Resources
- Retail & Manufacturing
- Technology, Media & Telecommunications
- Public Sector

### Trusted Relationships

**Broad Network of Alliances and Strategic Partners**
- Global Deloitte Team (Delivery Center across regions)
- Enterprise Ready Solutions
Why Deloitte

Deloitte will guide you

Security: Security is a very important aspect which we address when considering the cloud. Deloitte offers dedicated team of security experts that will evaluate every choice taken along the way.

Costs Optimizations: Costs are continuously changing in the cloud. We provide continuous monitoring of your cost usage and provide advice on how to decrease them when possible.

Data Privacy: We make sure that technical and administrative controls are implemented to control and protect your data in cloud. We can provide also reviews, risk assessments or audits to confirm the data privacy standards.

Compliance: We will make sure that when in cloud your workload and infrastructure is compliant with all the needed regulations. Continuous checks will be performed so that your business is compliant at any time.

Automation (Infrastructure as Code): Operational overhead can be overcome automating the processes. We try to automate every procedure where applicable, through code and massive use of API, to minimize any human errors and make everything more easily controllable in a centralized way.
The combination of Deloitte's expertise and experience with technology of the most advanced Cloud platforms allows us to provide added value to customers, supporting them in the transformation process towards a digital company.

Deloitte partnership with AWS...since 2017

Achieved Competencies & Designations

Certified Capabilities

Customer Value

630 Qualified Professionals on AWS Technologies

240 AWS Certified Professionals

SIGNIFICANT Number of DR followed

Cost Reduction

IT Staff Productivity

Move Quickly

Innovate

Risk Mitigation

Rapid Scaling
DELOITTE CLOUD ENGINEERING CAPABILITIES

How We Provide Business Continuity...

We provide continuity thanks to a structured approach and a comprehensive implementation.

Cloud Director

Manager

Cloud Solution Architect

Cloud Integration Engineer

Cloud Migration Engineer

Cloud Developer Engineer

---

Sprint 1

- Failure Modes Analysis
- Environment
- Integration

Sprint 2

- Identification of Critical Resources
- Integration

Sprint 3

- Business Impact Analysis
- Integration

DR Plan & Implementation

Architecture Implementation

A simple, clear and detailed Plan

Primary Site Secondary Site

Copyright © 2020 Deloitte Development LLC. All rights reserved. | 22
Deloitte’s division of DR solutions

Our practice is guided by a consolidated experience in the sector which led us to classify the main needs of our customers

### TYPES

**Cloud Services utilized**

Each Cloud Service that is going to be utilized has a fixed cost for its runtime. This cost can be easily estimated under a pay as you go model. Some examples of services:

- Virtual machines
- PaaS databases
- LoadBalancers

**Storage**

The storage on every cloud has a fixed price per GB and can be estimated based on the amount of GB that are going to be stored in cloud. This value is dependent of the storage solution that is implemented on premise.

**Network Traffic**

The network traffic is not that easy to estimate because it depends on multiple factors. To have an idea the following components are taken into consideration:

- Traffic from the on premise towards the cloud region
- Possible traffic between Availability Zones
- Possible traffic between Cloud Regions
- Possible Internet traffic

**Defining Parameters**

These parameters are tightly coupled with the costs because smaller RPO&RTO brings a solution that is composed from higher network traffic, higher number and size of the cloud services and bigger storage. The graph shows the dependency between these parameters and the costs. RSL refers to the recovery Service Level

### COST FACTORS

#### BACKUP & RESTORE

- **RTO**
- **RPO**
- **Cost**
- **Switch Effort**

#### WARM STANDBY

- **RTO**
- **RPO**
- **Cost**
- **Switch Effort**

#### MULTISITE

- **RTO**
- **RPO**
- **Cost**
- **Switch Effort**
Deloitte customizes your own DR

Design the best DR solution
There are many options and variations that could be applied for the implementation of a disaster recovery.

Our practice aims to identify the best solution according to the customer’s needs and budget.
Build a Resilient System for a continuous business

Can your systems survive a disaster?

Cost Optimization
Build a resilient model regarding IT costs in case of DR. Rethink your IT costs and pay to avoid incurring in too much damage to develop a solid DR plan.

New Offerings
With this approach new solutions can be developed and adopted faster, thus enabling continuous innovation.

Security
Cyber attack attempts are rising in volume, finding clever ways to hack in your company’s system.

Future of Work
In the future, more lock down periods or social distancing measures are expected. The future of work includes working from home more than ever in the past.

Strategic
Re-invent the way your business operates, enhance flexibility and respond to future scenarios.

Infrastructure Flexibility
Cloud adapts to your needs, without having to obtain and install hardware on premise, to cope up with disasters or spikes in demand. DR will allow you to be highly fault tolerant and readily available: a robust yet cost efficient system.

A Resilient system will allow you to ensure Business Continuity to your clients and/or employees everywhere in the world when disasters occur.
ISSUE
The customer acquired a company that managed all their Spanish infrastructural assets. For a particular critical application, an on-site disaster recovery solution was already in place on another datacenter, but from an internal assessment was clear that this DR was not able to support the entire workload during a real disaster scenario.

CONTEXT
The client asked Deloitte Italy’s to drive the design and implementation of a new disaster recovery solution on cloud and roll out this solution in few months to correctly protect the critical application. Among the difficulties, a deep one network evolution was needed to ensure the connectivity of all branch offices during a possible disaster.

IMPACT
The client asked Deloitte Italy’s to drive all the governance of the new DR solution; thanks to the knowledge of cloud tools, the Deloitte’s team was able to obtain excellent values of Recovery Point Objective and Recovery Time Objective.

Solution & Benefits
RESULTS AND MAIN BENEFITS
To respond to this need, the DR solution with network evolution was implemented by Deloitte Italy. The solution focused on the following components:

• Protection of a part of VMs involved with automatic disaster recovery tool;
• Re-building of a set of VM that always being on and assure more rapidly start of the DR environment;
• Extension of the SQL Always on Cluster;
• Governance of the whole project which involved more than 8 third party suppliers;
• Architectural management of the citrix environment that hosts the critical application;
• Successful design and execution of a disaster simulation test;
Disaster Recovery scenarios on AWS
Diego Colombatto
Solution Architect

Diego has more than 15 years of experience in IT Service Delivery and IT Service Operations, with comprehensive experience in Digital and IT Transformation.

Experienced on designing Hybrid and Cloud solutions, including Business Continuity, DR and back-up solutions and architectures.
Cloud disaster recovery benefits

Traditional disaster recovery

Relevant upfront investment in hardware & ongoing costs
Data growth increases hardware and operational costs
Hard to actually test without business disruption
Management and infrastructure overhead for globally distributed businesses
Vulnerable to cyber threats/hacking

DR in the cloud

No upfront hardware investment needed
Only pay for rightsized compute/storage when actually needed
Lower IT management overhead
(Much) More automation
Easy and repeatable testing
Systems up in minutes (not hours/days)
AWS offers four levels of backup and DR support across a spectrum of complexity and time:

1. **Backup & Restore**
   - **RPO/RTO:** Hours
   - **Features:**
     - Lower priority use cases
     - Solutions: Amazon S3, AWS Storage Gateway
     - Cost: $

2. **Pilot light**
   - **RPO/RTO:** 10s of Minutes
   - **Features:**
     - Meeting lower RTO & RPO requirements
     - Core services
     - Scale AWS resources in response to a DR event
     - Cost: $$

3. **Warm standby**
   - **RPO/RTO:** Minutes
   - **Features:**
     - Solutions that require RTO & RPO in minutes
     - Business critical services
     - Cost: $$$

4. **Hot standby (with multi-site)**
   - **RPO/RTO:** Real-time
   - **Features:**
     - Auto-failover of your environment in AWS
     - Cost: $$$$$
AWS Global Infrastructure

24 geographical regions, 1 local region, 77 availability zones, 200+ POPs

**Region & Number of Availability Zones (AZs)**

- **GovCloud (US)**
  - US-East (3), US-West (3)

- **US West**
  - Oregon (4)
  - Northern California (3)

- **US East**
  - N. Virginia (6), Ohio (3)

- **Canada**
  - Central (3)

- **South America**
  - São Paulo (3)

- **Africa**
  - Cape Town (3)

- **Europe**
  - Frankfurt (3), Paris (3), Ireland (3), Stockholm (3), London (3), Milan (3)

- **Middle East**
  - Bahrain (3)

- **Asia Pacific**
  - Singapore (3), Sydney (3), Tokyo (4), Osaka-Local (1)*
  - Seoul (3), Mumbai (3), Hong Kong (3)

- **China**
  - Beijing (2), Ningxia (3)

**Announced Regions**

Three Regions and 9 AZs in Indonesia, Japan, and Spain
AWS Region design

AWS Regions are comprised of multiple AZs for high availability, high scalability, and high fault tolerance. Applications and data are replicated in real time and consistent in the different AZs.

A Region is a physical location in the world where we have multiple Availability Zones.

Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.
Storage for Back-up and DR: more choice for more applications

**Block storage**
- General Purpose SSD
- Provisioned IOPS SSD
- Throughput-Optimized HDD
- Cold HDD

**File storage**
- EFS Standard
- EFS Infrequent Access
- FSx for Windows
- FSx for Lustre

**Object storage**
- S3 Standard
- S3 Standard-IA
- S3 One Zone-IA
- S3 Intelligent-Tiering
- S3 Glacier
- S3 Glacier Deep Archive

**Backup**
- AWS Backup
Amazon S3 (Simple Storage Service)

- Web accessible object store (through API or HTTPS)
- Highly durable (99.999999999% design)
- Limitlessly scalable
- Multiple Tiers to match your workload
- Data Lifecycle Rules
- Static Website Hosting
- Security, Compliance, and Audit capabilities
- Standard Storage Pricing (us-east-1) - $0.023 per GB
AWS storage hierarchy and lifecycle management

- **S3 Standard**: Active data
  - Synchronous access
  - $0.023/GB/mo.

- **S3 Standard Infrequent Access**: Infrequently accessed data
  - Synchronous access
  - $0.0125/GB/mo.

- **S3 Glacier**: Archive data
  - Async access
  - $0.004/GB/mo.

- **S3 Glacier Deep Archive**: Long term archive
  - Async access
  - $0.00099/GB/mo.

Pricing is for us-east-1
Backup from on-premises to AWS

- Backup data flows from on-premises into AWS object storage services
- One of the most common use cases
**Hot site**

www.example.com

- **Corporate data center**
  - Reverse proxy/caching server
  - Application server
  - Database server
  - Master

- **Active**

- **Elastic load balancing**
  - Reverse proxy/caching server
  - Application server
  - Subordinate database server
  - Data volume

- **AWS Region**

- **Route 53**

- **Hot site**
Hot site recovery

www.example.com

Corporate data center

Reverse proxy/caching server

Application server

Master

Database server

AWS Region

Elastic load balancing

Reverse proxy/caching server

Application server

Subordinate database server

Data volume

Hot Site
CloudEndure: Better, faster, more affordable disaster recovery

**Flexible**
- Replicate from any source
- Wide range of OS, application, and database support
- Failback to cloud/on-prem

**Reliable**
- Robust, predictable, non-disruptive continuous replication
- RPO: subsecond
- RTO: minutes
- Protection against ransomware, corruptions, and human errors

**Highly automated**
- Minimal skill set required to operate
- Easy, non-disruptive DR tests
- Automated lightweight staging area reduces TCO

- Improve recovery objectives & reduce TCO
- Simple setup lets you start in minutes
- Same highly automated process for all workloads
- Minimizes complexity and reduces risk
- Easy failover and failback
CloudEndure lightweight staging and DR test

- Reduce DR site compute costs by 95%+
- Reduce DR site storage costs by 70%+
- Zero DR site duplicate OS license fees!
- Zero DR site software/DB license fees!
- Zero DR site networking equipment fees!
- Continuous replication with subsecond RPO
- Rapid machine recovery (RTO of minutes)
- Self-service DR dashboard
- Unlimited free non-disruptive DR tests
Q&A
Thank you

This publication contains general information only, and none of the member firms of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collective, the “Deloitte Network”) is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte USA LLP, Deloitte LLP and their respective subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2020 Deloitte Development LLC.
All rights reserved. Member of Deloitte Touche Tohmatsu Limited