IT RESILIENCE: BUILDING FAULT-TOLERANT ARCHITECTURES
# Table of Contents

**Introduction** 3  
- What Is IT Resilience? 3  
- IT Resilience Is More than Just Disaster Recovery or Business Continuity 3  

**Challenges of Today’s IT Leaders** 4  
- Do More with Less 4  
- Unpredictability 4  
- Constant Threats 4  

**The Anatomy of an Effective Resilience Strategy** 5  
- The Five Points of Enterprise Resilience 5  

**Resilience Architectures** 10  
- Two Approaches to Architecting Resilience 10  

**The Rise of Cloud-Based IT Resilience** 13  
- Business Continuity and Disaster Recovery 14  
- Data Protection 15  
- Archiving and Compliance 15  
- Testing and Development 15  
- Cybersecurity 15  

**Evaluation Criteria for Cloud-Based IT Resilience** 16  

**The Race to Resilience** 17  

**Introducing Axcient Fusion** 18  

**Sources** 19
Introduction

WHAT IS IT RESILIENCE?

IT Resilience

Noun | I·T·Re·sil·i·en·ce | ĭ·tēˌrēzəlˈi-nəns
Sustained availability and agile delivery of IT services, as well as integrity and confidentiality assurance for business information assets (Gartner®).

IT leaders are constantly being asked to deliver higher levels of service and availability with shrinking budgets and staff. Demands can be unpredictable, data is constantly growing, and retention requirements are increasing. It’s hard to pinpoint how quickly things will move, and when, so capacity planning and budgeting exercises are more complex than ever.

For years, teams have been reacting to sudden shifts in demand, constant threats, and IT outages. Until now, it’s been a game of catch up. These challenges have driven a new era where IT leaders are being proactive and building resilient IT architectures that enable teams to get out in front of issues and deliver continuous service availability, improve operational agility, and reduce costs.

IT RESILIENCE IS MORE THAN JUST DISASTER RECOVERY OR BUSINESS CONTINUITY

IT resilience is sustained availability and agile delivery of IT services, as well as integrity, privacy, and confidentiality assurance for business information assets.

The hierarchy above shows the evolution of IT architectures based on the increasing needs of businesses.
Challenges of Today’s IT Leaders

From finding new ways to transform IT into a competitive advantage for the business to delivering nonstop operations for internal and external customers, today’s IT leaders are faced with many challenges.

**DO MORE WITH LESS**

IT leaders are constantly asked to deliver higher levels of service and availability with shrinking budgets and limited staff.

**UNPREDICTABILITY**

Planning, forecasting, and budgeting exercises are becoming increasingly more difficult as IT departments are asked to deploy and support new applications, data continues to grow, and regulations continue to increase.

**CONSTANT THREATS**

With the rise of cyberattacks, like Cryptolocker, and unforeseen disasters, IT leaders need to find ways to make their IT more resilient, their processes more efficient, and their responses swifter.

“IT leaders should focus on two objectives: ① advancing the enterprise’s strategic agenda by supporting goals that drive improvement in enterprise performance and growth, and ② creating an infrastructure, which includes opportunistic adoption of cloud services, that delivers the IT services required while consuming the fewest technical and financial resources possible.”

Source: Gartner
The Anatomy of an Effective Resilience Strategy

THE FIVE POINTS OF ENTERPRISE RESILIENCE

There are five critical points to consider when building out an effective strategy to achieve complete IT resilience and operational agility. These include:

1. Business Continuity and Disaster Recovery

Preparing for site-wide outages, natural disaster, or any other large-scale IT incident requires having a plan and embracing that it’s not a matter of if, but when. Infrastructure requirements include performant storage targets for replicated machines and access to on-demand CPU, memory, and network resources for machine or site-wide failover.

Companies will also want orchestration tools in place to recreate mirrors of production networks and a preconfigured way to sequence failover of machines in order of importance. Recovery needs to happen fast and is ideally tiered by impact of application downtime, such that critical machines are accessible in less than one hour.

Lastly, teams will need to be able to test and validate IT resilience so they can be better prepared to deal with an unexpected service disruption. As a best practice, teams should test business continuity and disaster recovery strategy and operations quarterly.

Key Takeaways

1. Ensure applications can failover in under an hour to minimize productivity loss in the event of an outage.
2. Choose solutions with orchestration and automation tools to recreate complex networks and recover applications in the order of importance.
3. Test the end-to-end disaster recovery process quarterly.
The Anatomy of an Effective Resilience Strategy

THE FIVE POINTS OF ENTERPRISE RESILIENCE

There are five critical points to consider when building out an effective strategy to achieve complete IT resilience and operational agility. These include:

1. BUSINESS CONTINUITY AND DISASTER RECOVERY
2. DATA PROTECTION
3. TESTING AND DEVELOPMENT
4. ARCHIVING
5. CYBERSECURITY

2. Data Protection

Modern resilience infrastructures have transitioned from simple backup to machine-level replication and snapshotting. This gives IT organizations the ability to, not just restore critical information, but also roll back machines to a point in time before data corruption at the system or database level or cyber intrusions like Cryptolocker occur. Rather than replicating data hourly or daily, truly resilient infrastructure will provide near-continuous data replication. This helps teams minimize loss risk when it comes to protecting enterprise data.

It’s not simply a matter of frequency when it comes to backing up and protecting data; it’s about how quickly a business can recover. This is where software user experience and data transfer optimization are important. Finally, ensure that deduplication is embedded in your data protection solution to avoid generating large amounts of copy data.

Key Takeaways

1. Choose application or machine-level protection technologies to ensure application consistency and minimize possible corruption.
2. Replicate data continuously or near continuously as opposed to on a fixed schedule to minimize data loss.
3. Ensure technologies have efficiencies in place, like WAN optimization and data deduplication, to reduce bandwidth consumption and data footprint.
The Anatomy of an Effective Resilience Strategy

THE FIVE POINTS OF ENTERPRISE RESILIENCE

There are five critical points to consider when building out an effective strategy to achieve complete IT resilience and operational agility. These include:

- Business Continuity and Disaster Recovery
- Data Protection
- Testing and Development
- Archiving
- Cybersecurity

3. Testing and Development

Problems are always best addressed early in the cycle, and there’s no better time to address a software or load issue than before it’s been deployed in production. The proactive and preventative nature of resilient infrastructure enables teams to rapidly transform real-time data into sandbox test environments. Robust testing and development strategies can ensure that patching and software upgrades roll out smoothly across the organization and that new software applications or existing application migrations don’t have any adverse effects. Ideally, teams are able to test and develop on comparable infrastructure to their production environments and create run books to automate the process of spinning up or spinning down networks and test servers.

Key Takeaways

1. Leverage on-demand testing environments to reduce costs and eliminate the need for replicated infrastructure.
2. Transform backup data into testing and development datasets to increase efficiency and accuracy of testing processes.
3. Automate processes with run books to simplify and streamline testing operations.
The Anatomy of an Effective Resilience Strategy

THE FIVE POINTS OF ENTERPRISE RESILIENCE

There are five critical points to consider when building out an effective strategy to achieve complete IT resilience and operational agility. These include:

BUSINESS CONTINUITY AND DISASTER RECOVERY | DATA PROTECTION | TESTING AND DEVELOPMENT | ARCHIVING | CYBERSECURITY

4. Archiving

Resilient infrastructure enables customizable retention policies to accommodate company policies and industry regulations to protect and retain critical information. Archived data should be accessible with minimal recovery times and should be stored in a secure and compliant state. Companies with off-site requirements should adopt streamlined processes for moving and transporting data and leverage efficient replication and deduplication technologies to minimize the amount of copy data that is created by archiving. Best practices are to restore random archival data from different periods of time to ensure data integrity and auditability.

Key Takeaways

1. Optimize and deduplicate data prior to archiving it to minimize the amount of copy data that is created.
2. Archive data in cost-effective, long-term storage.
3. Periodically restore archived data to ensure data integrity and auditability.
The Anatomy of an Effective Resilience Strategy

**THE FIVE POINTS OF ENTERPRISE RESILIENCE**

There are five critical points to consider when building out an effective strategy to achieve complete IT resilience and operational agility. These include:

The new mantra of cyber resilience is “You’ve already been hacked (you just don’t know it yet).” IT resilience demands having a system of protect, detect, and recover. Resilient organizations have cyber security and threat detection systems at the edge of their networks to protect them from being hacked. Once intruded, they are able to rapidly detect malware and other viruses. Finally, resilient IT organizations have a way to rapidly remove the cyber threat or roll back data or systems to before it infected the network.

**Key Takeaways**

1. Create multiple recovery points when protecting data to ensure data and applications can be rolled back to a point in time prior to infection.
2. Secure protected data and applications with enterprise-grade, key-based encryption to minimize the amount of data that can be compromised by a cyber attack.
3. Test and document restore processes to ensure recoverability of data and applications and reduce the business impact of ransomware attacks.
Resilience Architectures

TWO APPROACHES TO ARCHITECTING RESILIENCE

The resilient enterprise ensures that business keeps moving no matter what. When it comes to building an architecture that supports this promise, CIOs have two options: build out traditional replicated infrastructures or leverage the cloud.

1. Traditional Hardware

Traditionally, organizations built out secondary and even tertiary data centers to achieve IT resilience. This involves maintaining multiple facilities, purchasing two or three copies of every piece of hardware, and having the replication software and networks to ensure data is available. In addition, this involves managing multiple solutions and vendors and building out complex integration strategies to ensure all the pieces work together.

On average, over 80% of annual IT budgets go to data center operations and maintenance costs, which include facilities, personnel, power, and cooling.

(Source: IDC®)

ALLOCATION OF AVERAGE ANNUAL OPERATING BUDGET BY DATA CENTER FUNCTION

<table>
<thead>
<tr>
<th>IT Infrastructure</th>
<th>Personnel</th>
<th>Facilities Infrastructure</th>
<th>Power</th>
<th>Coding</th>
<th>IT Consulting Services</th>
<th>Building Rental</th>
<th>DCM Tools</th>
<th>Facilities Consulting and Services</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>15</td>
<td>10</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>4</td>
</tr>
</tbody>
</table>

% OF RESPONDENTS

Source: IDC’s Enterprise Datacenter Survey, 2015
Legacy architectures have resulted in multiple silos of infrastructure to achieve various workloads. A company might have five times the compute, network, and storage infrastructure, each with their own copies of data, to handle business continuity, data protection, testing and development, and analytics use cases. In addition to the exorbitant capital and operating expenses of redundant infrastructure, legacy architectures require more data center footprint, increasing operational overhead.

According to a recent IDC survey, over 80% of annual IT operating budgets are spent supporting the soft costs of IT infrastructure, which include personnel, power, cooling, consulting, and building leases.

CIOs are looking to the cloud to augment traditional infrastructure and accommodate the ebb and flow of business needs — without the bloat of added infrastructure.

The hub-and-spoke model of legacy infrastructure creates redundant silos for each workload. This not only increases complexity and cost but drastically limits IT’s ability to quickly respond to incidents, outages, and security breaches.

78% of businesses report having more than five copies of their production data that is used for additional use cases such as disaster recovery and data protection. (Source: ESG®)
2. Consolidated Hybrid Cloud

The second approach to IT resilience leverages the cloud and consists of one copy of on-premise infrastructure for production workloads and offloading non-production workloads to the cloud.

To effectively achieve IT resilience with this architecture, data is optimized, encrypted, and replicated offsite to the cloud, with variable lengths of snapshot and data retention. The data can then be used for failover in the event of a disaster, to create on-demand testing and development environments, to recover information or roll back systems to a specific point in time, or to search archives. Unlike the traditional, on-premise approach, this architecture leverages the power, scale, and cost advantages of the cloud to deliver a centralized and consolidated approach to achieving IT resilience. Ideally, there is a single silo of data to reduce copy data footprint. Because networking and compute are both elastic and on-demand, cost reductions are significant over traditional infrastructure architectures.

By leveraging the power and elasticity of the cloud, IT organizations can reduce infrastructure overhead and cost, regain valuable IT staff time, and deliver more reliable and high-performing IT to internal and external customers.

“Unlike the traditional, on-premise approach, this architecture leverages the power, scale, and cost advantages of the cloud...”

CONVERGE IN THE CLOUD

With one on-demand platform, teams are able to manage vulnerabilities more effectively while maintaining dedicated strategies for critical aspects of IT resilience.

PRIMARY IT

On-premise production workloads

CLOUD

Cloud non-production workloads

ONE COPY OF DATA WITH ELASTIC COMPUTE TO POWER...

• Disaster Recovery
• Data Protection
• Archiving and Compliance
• Testing and Development
The Rise of Cloud-Based IT Resilience

At its core, IT resilience is a fundamental shift away from reactive systems and workflows toward a more proactive approach to IT. For the enterprise, this shift has become a critical competitive advantage.

For large companies, service outages can cost hundreds of thousands of dollars per hour. And when interruption strikes, whether by ransomware, hardware failures, extreme weather conditions, or anything else, the financial damage — as well as the damage to reputation and customer loyalty — can be substantial.

70% of recovery and continuity inquiries in 2016 were specific to IT resilience and cloud-based continuity.

(Source: Gartner)
BUSINESS CONTINUITY AND DISASTER RECOVERY

More and more enterprises are turning to service providers to deliver business continuity with cloud-based offerings. Solutions such as disaster recovery as a service (DRaaS) can be used to boost IT resilience and eliminate the need for redundant on-premise infrastructure.

There are two types of DRaaS providers. Some providers have integrated software for managing VM replication, VM activation, network recreation, machine boot sequencing, exercise management, and servicing customer disaster declarations. Others will just provide VM activation and shutdown, and the customer is responsible for managing replication, exercise management, network recreation, and other recovery operations following a disaster declaration.

A resilient business has defined aggressive service levels for their applications and ensured that their disaster recovery provider can achieve the required recovery time objectives (RTOs) and recovery point objectives (RPOs). Resilient companies have streamlined failover operations by leveraging technologies with native orchestration and automation capabilities and will be able to bring their business from catastrophic failure to full IT productivity in less than 60 minutes.
DATA PROTECTION

Data protection can be costly and complex for businesses, with many companies using three or more solutions to ensure data is backed up and can be recovered. In addition to software solutions, businesses must also consider the type of media on which protected data is stored to ensure recovery times meet their business needs.

Resilient enterprises are leveraging near-continuous replication technologies to provide RPOs of minutes for their applications and data. These enterprises are optimizing replication times and bandwidth utilization by deduplicating, compressing, and replicating only the changed data to the cloud — often referred to as “incremental-forever” backups.

ARCHIVING AND COMPLIANCE

With data explosion comes an increase in the costs associated with it. Resilient companies have rethought infrastructure to curb archival spending. Companies archiving data in the cloud can reduce or eliminate the need for long-term storage media such as tape and can benefit from data deduplication to reduce storage footprint. In addition, resilient companies can create customizable retention policies and secure data with encryption for data both in flight and at rest.

TESTING AND DEVELOPMENT

In order to ensure performance and reliability for applications, enterprises need a dependable method for testing and development. To prevent issues and identify vulnerabilities with new application rollouts or software upgrades, businesses need to test against datasets that are as close to real production data as possible. Resilient enterprises are using a clone of their real-time replicated data to perform testing and development. The cloud’s ability to rapidly spin up on-demand sandbox environments using replicated data provides resilient enterprises with a way to test and develop against real-time datasets at a fraction of the cost of adding on-premise infrastructure.

CYBERSECURITY

With new threats around every corner, enterprises are forced to build out proactive strategies to ensure sustained service availability and data recoverability in the event of a cyber attack. Resilient enterprises are choosing IT architectures that enable rapid failover of applications and deliver near-instant recovery of data in an effort to keep the business operational and employees productive. In addition, resilient enterprises are taking a preventative approach to dealing with the increase in cyber threats by testing their failover and recovery capabilities annually or semi-annually.
Evaluation Criteria for Cloud-Based IT Resilience

**WHAT TO CONSIDER WHEN CHOOSING A CLOUD-BASED IT RESILIENCE SOLUTION**

Here are some sample questions to help choose the right cloud-based IT resilience provider for your business:

<table>
<thead>
<tr>
<th>Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>• How are RTOs and RPOs guaranteed with the service?</td>
</tr>
<tr>
<td>• Will these RTOs and RPOs meet my business requirements?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Onboarding Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>• How long will it take to stand up this solution?</td>
</tr>
<tr>
<td>• Are services required?</td>
</tr>
<tr>
<td>• To what extent does the provider offer recovery assurance and the creation of an automated disaster recovery playbook?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Past Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>• How are RTOs and RPOs guaranteed with the service?</td>
</tr>
<tr>
<td>• Will these RTOs and RPOs meet my business requirements?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• How do I know my data is not accessible by other cloud tenants?</td>
</tr>
<tr>
<td>• Are the data centers and infrastructure audited?</td>
</tr>
<tr>
<td>• What compliance certifications does the provider have?</td>
</tr>
<tr>
<td>• Is encryption available for data in flight and at rest?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What efficiency features does the provider offer to reduce storage requirements (e.g., data deduplication)?</td>
</tr>
<tr>
<td>• How does the provider reduce bandwidth requirements (e.g., WAN optimization, compression)?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>• How is the solution priced?</td>
</tr>
<tr>
<td>• Are there fees associated with declaring a disaster?</td>
</tr>
<tr>
<td>• How often can I perform tests — and are there charges associated with these tests?</td>
</tr>
</tbody>
</table>
# The Race to Resilience

As enterprises move to a more resilient approach to IT, they’ll compete to stay nimble in the face of unpredictable events. Use the checklist to determine your company’s place on the resilience spectrum.

<table>
<thead>
<tr>
<th></th>
<th>Proactive &lt;&lt;&lt;</th>
<th>&gt;&gt;&gt;&gt; Reactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many data protection solutions does your company use?</td>
<td>1</td>
<td>2-3</td>
</tr>
<tr>
<td>How many copies of production data are you currently using to support secondary workloads?</td>
<td>1</td>
<td>2-3</td>
</tr>
<tr>
<td>How old is your data protection solution?</td>
<td>Less than 1 year old</td>
<td>Between 1 and 2 years old</td>
</tr>
<tr>
<td>How much of your IT budget are you spending on non-production IT?</td>
<td>Less than half</td>
<td>Half</td>
</tr>
<tr>
<td>How streamlined is the management of the data flow between third-party solutions?</td>
<td>Very streamlined</td>
<td>Somewhat streamlined</td>
</tr>
<tr>
<td>How easily can you scale your target storage and your backup software?</td>
<td>Very easily</td>
<td>Somewhat easily</td>
</tr>
<tr>
<td>Do you lose money when you miscalculate your anticipated data growth?</td>
<td>No</td>
<td>Only a small amount</td>
</tr>
<tr>
<td>How often are you able to perform backups?</td>
<td>Continually</td>
<td>Once a day</td>
</tr>
<tr>
<td>What’s the average amount of time it takes you to recover data?</td>
<td>Under an hour</td>
<td>Between 1 and 2 hours</td>
</tr>
<tr>
<td>What’s the failover process like when you experience an outage?</td>
<td>No significant costs incurred</td>
<td>Somewhat costly</td>
</tr>
<tr>
<td>How quickly can you bring up a replica network?</td>
<td>Under an hour</td>
<td>Between 1 and 2 hours</td>
</tr>
<tr>
<td>Are these recovery times meeting your SLAs?</td>
<td>Yes</td>
<td>Somewhat</td>
</tr>
<tr>
<td>How often do you perform DR tests?</td>
<td>Twice a year</td>
<td>Once a year</td>
</tr>
<tr>
<td>Do tests require you to bring down any parts of your production infrastructure?</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

If the majority of your answers were on the left end of the spectrum, your approach to IT is at the proactive end of the resilience spectrum. If not, you’ll need to adopt a more proactive, lean-forward approach to defend against any cyber attack or disaster that may come.
Introducing Axcient Fusion

Axcient Fusion is the world’s first cloud-converged platform for IT resilience. Fusion enables businesses to converge and consolidate their workloads into a unified cloud platform. With Fusion, IT departments can eliminate redundant on-premise IT infrastructure, simplify and streamline operations, and achieve the resilience and agility of the world’s largest enterprises.

For more information about IT resilience, visit axcient.com/fusion or call 800.715.2339.
Sources

IHS
The Cost of Server, Application & Network Downtime Survey & Calculator
Matthias Machowinski
January 2016

IDC
End-User Survey Results: Enterprise Datacenter Budgets and Spending
Kelly Quinn
March 2016

Gartner
Hype Cycle for Small and Midsize Businesses 2016
Mike Cisek et al.
June 2016

ESG
2015 Trends in Data Protection Modernization
Jason Buffington et al.
September 2015

Gartner Presentation
IT Resilience: Can We Get There from Here
John P. Morency
May 2016