



Driving Digital Transformation through Business Continuity

WHY CONTINUITY AND DISASTER RECOVERY ARE ESSENTIAL COMPONENTS OF ANY TRANSFORMATION STRATEGY



Introduction

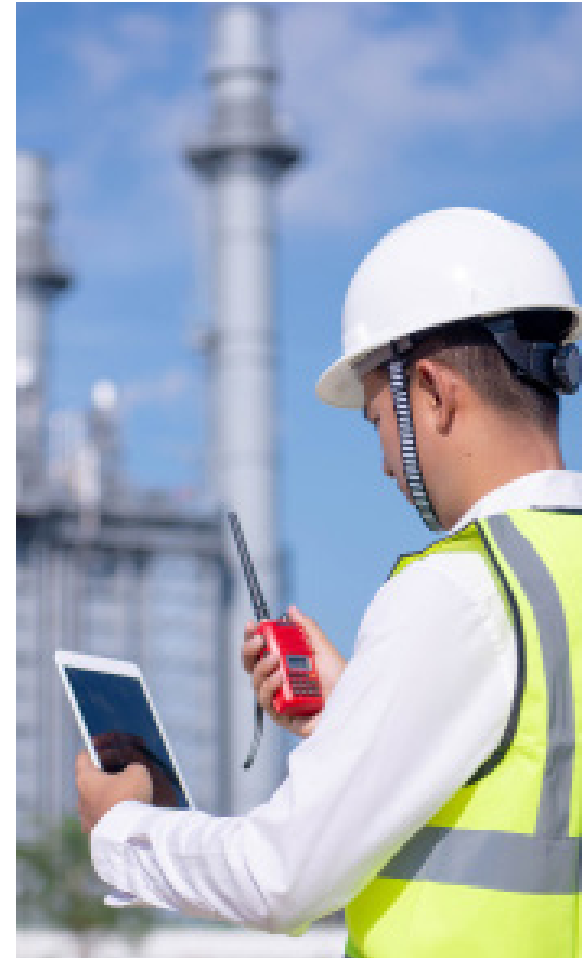
The resiliency of your IT system is paramount; after all, one hour of downtime is estimated to cost over \$300,000.

For many organizations, this comes in the form of productivity loss. For others, downtime can lead to legal complications or even higher-risk stakes. In finance and healthcare, for example, the lives and livelihoods depending on technology can reach far beyond a single organization.

But while the case for uptime is fairly clear, backup, disaster recovery (DR), and business continuity aren't always viewed as strategic priorities. Instead, efforts often focus on simply checking off a box.

Given what's at stake, take a closer look at your continuity strategy, processes, and technology and you'll discover that **business continuity is not only vital to protect your organization against downtime and security threats, but it also enhances and even speeds up your overall digital transformation efforts.**

In this guide we'll dig into the business case for continuity and explain why it should be a cornerstone for any organization pursuing ongoing digital transformation.



Bringing Continuity Into the 21st Century

Business continuity is a wide field encompassing the people, workplaces, and tools required for your organization to run smoothly. Digital transformation is changing the balance of this equation on a constant basis. For example, in the face of the COVID-19 pandemic, many industries have had to implement ways to deliver services remotely. Even operations that typically require a physical presence, like healthcare, have turned towards video consultations to meet with and service their clients.

Although a physical presence may continue to be necessary for continuity of some services (the most relevant in the case of disaster being emergency services, law enforcement, logistics, and construction), many organizations are

finding that they can assist their customers within a new remote paradigm.

So how does this all affect business continuity? **Organizations further along in their digital transformation journey have proven to be more prepared for the new world** that has emerged in the wake of unprecedented global crisis, reacting faster to enable increased collaboration, business efficiencies, and resiliency.

Investing in digital transformation enables the decoupling that workforce from traditional service delivery methods. [By architecting strong cloud computing architecture and services you reduce the need for physical alternative sites and make your business more agile and responsive.](#)



One Citrix survey found that 48% of IT leaders did not have a continuity plan that considered the majority of their employees working from home. 61% found it difficult to make this change.

How Digital Transformation Improves Continuity

Many digital transformation efforts lend themselves nicely to business continuity, simply due to the **distributed, resilient nature of digital operations.**

Transformation is about digitizing previously manual processes, embracing cloud services where possible, and exploring new technology solutions alongside processes to deliver efficient and innovative business operations.

Some of the more practical applications of these efforts are:

- Remote access to company networks, applications, and data, so your workforce is not tied to a specific office site and can instead access centralized services from anywhere, any time

- Process digitization in which you convert manual processes to digital ones wherever possible
- Cloud-based collaboration and productivity solutions, including video calls, web chat, email, Office applications, and file sharing
- Automation of digital workflows including IT administration and configuration

You can see how this paradigm inherently improved continuity by allowing users to access and control how they interact with corporate information systems, fostering collaboration and efficiency through modernization and automation. In addition, cloud-based systems are designed to be

resilient and avoid single points of failure such as document storage on a local workstation or single storage array.

That means if your primary office location is unavailable for any reason, your workforce can disperse without losing access to critical data or services.



Leverage Your Continuity Toolset for Hybrid Migrations

For many digital transformation initiatives, your continuity tools - in particular, disaster recovery software - can also be used for cloud migrations and workload mobility, [providing an on-ramp to the cloud that is cost-effective and fast.](#)

Migrating via DR ensures that you avoid extended downtime when recovery cuts over to cloud servers, as your target environment is already tested and functional. Datasets and application servers are synchronized without using snapshots and with minimal performance impact to your current production servers, then kept continuously updated as defined by your Recovery Point Objective and SLAs. Testing your migration is as simple as a single click.

Research surveying UK IT decision makers found that 72% identified cloud migration as the top transformational priority³.



After your data is copied, your planned migration mostly involves changing DNS settings and reconfiguring networking or storage. **Leading disaster recovery products are compatible with many cloud platforms and hybrid configurations will leverage on-premise resources as well, enabling true multi-cloud mobility.** Traditional manual migration methods are slower, can introduce risk, and are proven to be more sluggish in data transfer rates.

Using cloud-based DR solutions allows seamless migration of large VM sets, even in the hundreds. And you can pull them back quickly by implementing policies to validate configurations and functionality before committing to the migration.

Transform Security for the New Perimeter

As organizations continue on their path of digital transformation and adopt distributed remote work scenarios, security becomes more complex.

Modern information security includes a diversity of devices from corporate-owned to personal desktops, laptops, and mobile devices, meaning you can no longer count on controlling VPN access. After all, employees and customers alike expect to access resources from anywhere, on virtually any device.

This necessitates **a shift from perimeter security hardening to zero trust models and a focus on access and identity management**. Security strategy must include the cloud services and apps used for business-critical operations, as one cannot

assume that IaaS, SaaS, and end-user devices are threat-free environments. This is the essence of Zero Trust: all activity is explicitly verified and security controls are automatically enforced.

Although the network perimeter is still an important vector to protect, it is not necessarily the front line of attack. Access rights, such as those dictated by Active Directory, are now paramount to effective front-line security by providing and controlling granular privileges that ultimately protect various services and data storage.

When security is applied to continuity, those access controls must be maintained even when your central workplaces are inaccessible. Cloud-based ID management and multi-factor authentication are essential

components that help you deliver on continuity goals. Downtime and data breaches go hand-in-hand, with one often causing the other. Security and compliance are inherent components of a strong continuity strategy to protect data in the recovery environment as well.

#1
In a Frost & Sullivan Survey from 2020, security was listed as the number one critical decision-making factor behind ongoing digital transformations⁴.

Taking the Transformative Next Step

Once you have recovery and continuity tools in place - whether you use them for migration or solely as your ongoing continuity strategy - you'll be in better position to support innovation and take the next step in your continuous transformation journey.

A baseline recovery strategy and a tested plan for continuity also gives peace of mind as you pursue other digital transformation and modernization projects like serverless computing and automated processes. [This confidence makes it easier to experiment with automated provisioning and configuration or infrastructure as code as you pursue optimized and efficient digital operations.](#)

With experience delivering hardware-based data center solutions alongside modern cloud architectures,



Lunavi's service delivery teams and in-house application developers can help you identify the strongest candidates for investment and discover how your technology can further your business goals by:

- **Modernizing** business applications and the underlying IT stack
- **Migrating** solutions to the cloud
- Applying **Agile and DevOps** practices to build new, innovative solutions
- **Automating** IT processes
- **Managing** routine administration tasks

Discover how Lunavi can accelerate your transformation efforts.

[Contact us to learn more.](#)

References

1. ITIC: Hourly Downtime Costs Rise: 86% of Firms Say One Hour of Downtime Costs \$300,000+; 34% of Companies Say One Hour of Downtime Tops \$1Million

<https://itic-corp.com/blog/2019/05/hourly-downtime-costs-rise-86-of-firms-say-one-hour-of-downtime-costs-300000-34-of-companies-say-one-hour-of-downtime-tops-1million/>

2. Continuity Central: COVID-19 is acting as a catalyst for digital transformation finds survey

<https://continuitycentral.com/index.php/news/technology/5197-covid-19-is-acting-as-a-catalyst-for-digital-transformation-finds-survey>

3. Capita: Embracing the power of cloud on the journey to digital innovation

<https://go.capita-it.com/cloud-research-report>

4. Frost & Sullivan: Top End User Priorities in Digital Transformation

https://go.frost.com/LA_PR_ICT_FValente_K40C_PrioritiesInDT_Jan20

Navigating what's next



866.995.3282

lunavi.com