The Logical Advantage

TeamLogicIT®
Your Technology Advisor

MAY 2026

Drive Transformation via Cloud Services

Analysts predict the market for cloud computing will reach $1 trillion in the next three years.

What is cloud computing? Here are three core elements:

- **Cloud services** – an array of applications hosted by third parties outside of an enterprise and operated via the internet
- **Cloud infrastructure** – the backbone of hardware and software that delivers cloud services
- **Cloud storage** – a method of storing a broad range of data for enterprises on remote servers maintained by third-party providers

Why so much investment in these technologies? Because in concert these modules have become an essential engine for **digital business transformation (DBX)**, an inescapable competitive requirement for today's organizations.

How can leaders of small- to medium-sized businesses (SMBs) maximize the momentum of this spending trend?

In other words, get the most of their cloud investments? As a premier IT managed services provider (MSP), TeamLogic IT advocates applying cloud computing as leverage to reap these benefits:

- Ensuring reliable **remote access** from anywhere at anytime
- Boosting the **flexibility and scalability** of tech infrastructure
- Converting capital expenses to operational expenses – i.e., **pay as you go**
- **Reducing costs** of purchasing, managing and replacing hardware
- Delivering **cross-platform support**

And we help you do so through **co-managed IT services**, which enable your team to focus on the rigors of your business while our team maintains your full technology infrastructure.

The Logical Advantage

Viewpoint

Make Cyber Resilience Your Priority

Recent studies reveal that **cyber resilience** now outweighs prevention as a priority for organizations small and large. Why? Because statistics show the costs of recovering from data breaches persist in the $1 million to $5 million. What is the driver of this expense? Operational downtime caused by cyber attacks such as ransomware, the leading cause of digital business disruptions.

What is cyber resilience? IBM defines the concept as a company's ability to withstand adverse cyber events repeatedly by adapting and recovering quickly to minimize damages to the enterprise, tangible like downtime and intangible like reputation.

How can leaders of small- to medium-sized businesses (SMBs) embrace this shift in cybersecurity thinking? By adopting **"Zero Trust"** practices:

- Monitor every type of network traffic for the full spectrum of cyber threats continuously.
- Identify and continuously validate users of all kinds and devices of every sort.
- Adjust and refine cybersecurity policies, protocols and procedures continually in response to data gleaned from practicing the first two methods.

And by combining these measures with a robust **backup and disaster recovery (BUDR)** routine:

- Maintain regular local image backups of core technology.
- Generate and store offsite and/or cloud backups of these images daily.
- Sustain this hybrid configuration for rapid restoration in the wake of cyber disasters.

IT Strategy

How MSPs Enable Robust BUDR for SMBs

Analysts predict the phenomenon known as **"Shadow AI"** will rise to extraordinary levels this year as the unprecedented expansion of **artificial intelligence (AI)** continues. What is Shadow AI? The term is a reference to the established concept, **Shadow IT**, when team members procure and use devices and/or software without their IT department's knowledge and permission. And surveys validate that workers are using unsanctioned AI tools at an increasing rate.

Shadow AI is a vexing trend for leaders at small- to medium-sized businesses (SMBs) striving to mitigate cyber risks like ransomware that increasingly are being powered by AI apps. Studies show the annual cost of managing what's called "Insider Threats" is escalating into millions of dollars, leaving SMBs at a relative disadvantage among larger competitors with deeper cybersecurity budgets.

That's why as a premier managed services provider (MSP), we recommend robust **backup and disaster recovery (BUDR)** systems. A comprehensive BUDR routine ensures company data is safe, intact and recoverable despite the rise of phenomena like Shadow AI by:

- Maintaining regular local image backups of operating systems, applications and databases
- Generating and storing offsite backups daily as protection against disruptions and breaches
- Sustaining this hybrid configuration for rapid restoration in the wake of cyber disasters like a ransomware incursion

We have proven BUDR practices and protections to share. Visit teamlogicit.com to learn more.