EVOLVING SOLUTIONS | 30 YEARS

Cyber Resilience

Recover Critical Business Services Faster

- Plan recovery around critical business services and business impact
- Understand the dependencies required to bring those services back online
- Sequence recovery around what the business needs first
- Validate clean, usable recovery points before disruption occurs
- Improve recovery speed with visibility, prioritization, and tested recovery paths

Modern cyber resilience gives organizations a clearer path to keeping critical business services running when disruption hits.

As environments become more distributed and cyber threats become more deliberate and pervasive, recovery has to be planned around the services the business depends on most. That means understanding which capabilities need to come back first, what they depend on, and how they can be restored quickly and cleanly.

For IT leaders, the opportunity is to shift recovery planning from a system-by-system exercise to a service-level strategy focused on keeping people working, customers served, and the business operating. When that service-level strategy is in place, resilience becomes a practical way to protect business continuity.

Restore the Service, Not Just the Data

A service-level view changes the role of backup. It still matters, but resilience depends on whether protected data can be turned back into a working business service.

That gap is where many recovery plans break down. A critical service may depend on identity, network access, cloud or SaaS connections, application components, automation code, and other systems required to make the data usable. If those pieces aren't understood and recoverable, the data may be restored while the business process remains unavailable.

Modern resilience starts with visibility into the dependencies behind each critical service.

Recover the Services That Matter First

Once dependencies are visible, recovery can be prioritized around business impact. Not every application, workflow, or data set needs to come back at the same time. The first priority is the smallest set of services the organization needs to keep operating, serve customers, protect revenue, and meet its obligations.

That requires IT and business leaders to define recovery in business terms. Prioritization is ultimately about time. IT teams need to know which services must come back first, what can wait until the business is stable, and in what sequence the dependencies that support those services must be recovered.

Together, those decisions determine where fast recovery is required.

Validate That Recovery Will Work

A resilience strategy must also be proven. It's one thing to document which services should come back first. It's another to know the organization can recover them in the right order, within the right window, and with clean data.

That validation matters even more in a cyber event. Threat actors may try to compromise backup environments, corrupt recovery copies, or leave behind dormant issues that surface later. A usable recovery point must be protected, trusted, and ready when the business needs it.

The goal is confidence. Leaders need to know the organization has more than a backup plan. It has a path to restore the services that keep the business running.

Build Resilience Into Business Operations

Evolving Solutions helps organizations take a more complete view of cyber resilience across data protection, backup and recovery, and the infrastructure that supports critical business services. That work starts with understanding business impact, identifying dependencies, and building a recovery strategy that can be validated before it's needed.

The goal isn't simply to restore data. It's to help the business recover faster, operate with confidence, and get back to work after a disruption.

EVOLVING SOLUTIONS

We're here to help your organization prepare for disruption and recover with confidence.

Let's Get to Work!