

Redjack AI: Recover Business Operations with Confidence

Understand Your Risks. Recover Faster. Stay Operational.

Downtime—whether from cyberattacks, misconfigurations, or infrastructure failure—is costly. Business continuity depends on knowing how to bounce back when something breaks. Redjack gives you a clear, phased recovery plan to bring operations back online after an outage—without guesswork.

Key Benefits

- ✓ **Reduce Recovery Time**
AI-generated, dependency-aware plans bring critical services back faster—minimizing lost revenue and downtime impact.
- ✓ **Eliminate Manual Effort**
No more hand-built dependency maps or stale documentation. Redjack keeps everything current automatically.
- ✓ **Focus on What Matters**
Our platform highlights what's most important to recover—so your team can act strategically.
- ✓ **Clear, Actionable Plans**
Step-by-step instructions in plain text or markdown—ready for IT to execute.

Why Redjack?

Our AI-powered platform maps your dynamic, complex infrastructure to real-world business activity—automatically and continuously.

Here's how it works:

- We analyze real-time communications data across your IT, OT, and IoT environments
- We identify and catalog all your assets and their dependencies—including third parties
- We map each of these to specific business functions

This gives you a living model of your operational environment—based on objective evidence, not stale CMDB data or stitched-together tools. No manual updates required.

High-Quality Data Enables Smarter AI

Redjack's AI leverages this deep, accurate, and real-time asset map to power IT disaster recovery. We automatically generate step-by-step recovery plans based on the last known working state of your environment:

- Plans are tailored to each business function
- Each phase restores key dependencies in the right order—so you bring the most critical assets online first
- Every recovery plan is exportable in markdown or text, with supporting CSV appendices for practical execution

Example Recovery Plan Snippet:

```
##### Phase 2:
Linux Servers and Critical Asset
fulltunnelsrvr.widgetcorp.com
- **Asset Types**:
  36 assets, including Application
  Servers and Backups, all running
  on Linux.
- **Instructions**:
  - Restore all 36 assets in this
    phase.
  - Pay special attention
    to the critical asset
    fulltunnelsrvr.widgetcorp.com,
    which serves 46 assets in
    later phases using tcp-22.
  - Verify that the critical
    asset is operational and can
    establish tcp-22 connections.
  - Test the connectivity of
    the critical asset to ensure
    it can serve its dependent
    assets.
- **Dependencies**:
  This phase does not depend on
  any outside phases.
```

**Redjack Recovery Plans:
Clarity When It Matters Most**

Our recovery plans aren't just conceptual—they're execution-ready. Generated directly from the infrastructure data, they tell you what to do, when, and why.

Export Options:

- CSV appendices for asset, dependency, and service details
- Markdown or plaintext for immediate consumption by IT teams

Bring Resilience into Focus

With Redjack, you get clear, automated guidance rooted in real infrastructure and business context—so you can respond faster, more confidently, and with less disruption.

About Redjack

Redjack delivers total asset and dependency visibility and AI-powered business insights for cyber resilience. Our platform empowers enterprises to safeguard vital business functions, meet cyber regulatory standards, and digitally transform to align with business objectives.

Visit redjack.com 

