

Redjack provides a cyber resilience platform that delivers total asset and dependency visibility with AI-powered business insights.

Our platform gives IT, security, compliance, and risk management leaders evidence-based, unbiased visibility into their organization's IT assets, connections, and unique risks.

Our Mission

To make digital enterprises safe and confident against threats, and build a more resilient infrastructure for the future.

About Us







The Redjack platform puts a business lens on asset inventory. Unlike traditional asset inventory solutions, Redjack uses observed communication data and data science to allow customers to truly understand what assets keep their business running — across on-premises, cloud, hybrid, and container environments. The platform gives our customers a clear picture of the assets that matter, their relationships, their internal and external interdependencies, and their resilience levels. This complete, business-focused view helps organizations prioritize resource allocation and achieve resilience through data-driven decisions.

Who We Serve

Enterprises with complex network environments who need to keep their businesses running no matter what. Our customers use Redjack to help safeguard vital business functions, meet cyber regulatory standards, and digitally transform their organizations to align with business objectives. Redjack is particularly relevant in industries like Financial Services and Healthcare, which are highly regulated and heavily targeted by cyber attackers.

Key Use Cases

A complete inventory of assets and dependencies mapped to critical business functions addresses a variety of use cases, including:

-  Business continuity and disaster recovery planning (BCDR)
-  Cloud migration planning
-  Risk assessment for security modernization and budgeting
-  M&A-related cyber risk assessment & integration planning
-  Cyber insurance planning & negotiation
-  Compliance with DORA, NIST, and other regulations & standards