Redjack

Redjack for Financial Services
The insight you need to achieve cyber resilience

For financial services firms, resilience is not optional—it's expected. Regulators across the globe are demanding clear, auditable evidence that firms can withstand and recover from cyber and operational disruptions. From a cyber resilience perspective, this includes maintaining accurate asset inventories, conducting rigorous disaster recovery testing, and demonstrating a clear understanding of how your IT infrastructure supports your critical business functions.

At the same time, the threat environment continues to evolve. New technologies introduce new vulnerabilities, and threat actors are becoming more sophisticated. Achieving true resilience means preparing not just for today's risks, but for tomorrow's unknowns. It's also the foundation for strategic growth—your ability to innovate, adopt new technologies, and respond to market changes depends on the confidence that your operations can adapt without compromise. The Redjack platform provides the data to help financial institutions meet these demands with clarity, speed, and confidence.

Highlights

- An accurate asset inventory is the foundation of an effective resilience program

- Passive sensors quickly compile and dynamically maintain a complete list of internal and external connected assets across environments

- Automated mapping of IT complexity to business activity enables more effective resilience planning and compliance

- Analytics engine automates dependency mapping and delivers business-centric risk scores and IT recovery plans

Redjack has revealed more in two months than all of my consultants have in ten years combined."

— Fortune 50 VP of Risk

How does it work?

The Redjack platform uses passive, strategically placed sensors to discover all your connected assets, both internal and external. It then uses an AI-powered analysis engine to identify your asset dependencies, map your infrastructure to your critical business functions, provide asset criticality and resilience scores, and generate phased recovery plans for each business function.

This data is updated continuously, giving you ongoing and complete visibility even as your environment changes.

Superior Asset Visibility

The asset data is dynamically updated in real-time for both internal and external assets whether in the cloud or on-premises.

Build Effective Cyber Resilience

AI-enabled critical business function and asset dependency, based on observed behavior, helps you prioritize and allocate resources.

Spot Risks

Identify dependencies, unsecured assets, shadow IT, and other risks and prioritize them based on business impact.

Lightweight & Massively Scalable

Built for the enterprise it is massively scalable, quick to deploy, has a minimal footprint, and supports complex and evolving hybrid environments.

Product Features

Asset discovery with automated dependency mapping

An asset is anything communicating in your network, whether on-premises or in cloud or hybrid environments. This also includes any third-party assets that are communicating with assets in your environment. Redjack uses passively captured communications and asset metadata to give you a complete, behavior-based view of your connected infrastructure.

Map infrastructure to critical business functions

Business functions are the activities that keep an organization running smoothly and generate revenue. Identifying and prior-itizing critical business functions is crucial for building cyber resilience, allocating security and IT resources, and developing effective business continuity and disaster recovery plans.

AI engine applied to high-quality data

The analytics engine within the Redjack platform produces asset criticality and resilience scores, and generates phased recovery plans for each business function. These AI-powered features use the objective evidence captured by the Redjack sensors, ensuring you can trust the output.

Cornerstone of Compliance and Best Practice Frameworks

There is a good reason why many industry regulations and compliance standards require organizations to maintain an accurate inventory of their IT assets and map them to business functions; it is the cornerstone of an effective resilience program. Examples include:

Digital Operational Resilience Act (DORA)

Article 8 of the Act addresses the requirement for financial entities to identify, classify, and document business functions, assets, and dependencies.

Federal Financial Institutions Examination Council (FFIEC)

Requires, as a baseline, that organizations have an asset inventory. Ideally, an organization with advanced cybersecurity capabilities would also have an automated tool to track, update, prioritize, and report on the asset inventory.

New York State Department of Financial Services (NYDFS) Cybersecurity Regulations (23 NYCRR 500)

The update released on November 1, 2023, added the requirement that organizations create and maintain a comprehensive asset inventory.

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 →

Redjack