Redjack

Redjack for Financial Services

The insight you need to protect your organization and customers

A lot of ink has been spilled about cybersecurity threats to the financial services industry. Articles cover a veritable laundry list of threats including advanced persistent threats (APTs), ransomware, phishing attacks, and insider threats, just to name a few. Financial services leaders have to wrestle with cloud adoption, mobile banking, the cybersecurity talent shortage, and managing third-party risks and legacy IT systems all while while preventing data breaches and ensuring regulatory compliance.

In order to secure your environment you need to know what to protect. An accurate asset inventory provides visibility into your organization's technology landscape. Without an inventory, your organization may overlook critical components, making it easier for attackers to exploit weak points.

Redjack gives you visibility into your environment on an ongoing basis that lets you understand the connections between assets, identify areas of risk, and prioritize which measures to take.

Highlights

- An asset inventory is the foundation of an effective cybersecurity program
- Software sensors quickly compile a comprehensive list of assets
- Visibility into hybrid environments, including cloud, on-premises, or containers
- Identify risks and prioritize them based on business impact
- Asset inventories are the foundation of cybersecurity regulations and frameworks

Redjack has found that companies we work with find 20% more assets than competing solutions.

How does it work?

The Redjack platform uses non-intrusive software-based network sensors to collect communications data and compile a comprehensive asset inventory, giving you a comprehensive view of your connected infrastructure. It then uses an AI-driven analysis engine to identify your critical business functions, asset dependencies, and key vulnerabilities.

The Redjack platform automatically identifies which assets are connected to critical business functions and the interdependencies between assets. Furthermore, the Redjack platform updates continuously, giving you ongoing and complete visibility even as your environment changes.

Superior Asset Visibility

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

Build Effective Cyber Resilience

AI-enabled critical business function and asset mapping, based on observed behavior, helps you prioritize your security efforts and allocate resources accordingly.

Spot Vulnerabilities

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

Identify assets

An asset is anything communicating in your network, whether on-premises or in cloud or hybrid environments. Some examples include computers, servers, networking equipment, and mobile devices as well as many other types of assets. This also includes any third-party assets that are communicating with assets in your environment.

Identify critical business functions

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

Prioritize critical business functions

- **High Priority:** Indicates critical functions that demand immediate attention and resources.
- **Medium Priority:** Important functions that contribute significantly to your organization.
- **Low Priority:** Functions that, while still essential, may not have an immediate impact on operations.

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 assets; it is the cornerstone of an effective cybersecurity program. Including, but not limited to, the following:

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.

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.

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