Redjack

Asset Inventory Solution

Comprehensive visibility into your connected infrastructure

Highlights

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

An asset inventory is a deceptively simple idea. At the most basic level, a comprehensive list catalogs all the technology assets within an organization's IT environment. However, an asset inventory is more than that.

To secure your environment, you need to know what to protect. An accurate asset inventory provides visibility into your organization's technology landscape. With an inventory, your organization may recognize critical components, making it easier for attackers to exploit weak points.

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.

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 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.

> Redjack has found that companies they work with find 20% more assets than competing solutions.”
>
> — Fortune 50 CISO

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.

Required for Compliance and Best Practice Frameworks

Creating an asset inventory is the foundation of an effective cybersecurity program, a fact recognized by cybersecurity regulators as well as major cybersecurity frameworks. Here is a brief sample of regulations and frameworks that incorporate asset inventory management in their requirements.

ISO 27001
Outlines what qualifies as an asset as well as how you can create an asset inventory.

NIST Cybersecurity Framework (NIST CSF)
In Version 1.1 the Identify Function includes the requirement to identify assets and maintain a hardware and software inventory. In the current draft of Version 2.0, which is expected to be published in early 2024, the Identify Function requires that inventories of hardware, software, services, and systems are created and maintained. Additionally, assets should be prioritized based on classification, criticality, resources, and their impact on the organization.

New York State Department of Financial Services (NYDFS) Cybersecurity Regulations (23 NYCRR 500)
The update released on November 1, 2023, added the requirement to 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.

Center for Internet Security (CIS)
The first CIS Control is called Inventory and Control of Enterprise Assets, which includes the requirement to create an inventory of an organization’s assets.

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