MANIFEST

Summer 2025 Overview

Know the risk in the software and AI you build and buy

Manifest empowers private and public sector organizations to operate critical systems and applications with confidence. We detect and manage hidden software supply chain and AI risks at scale.

Manifest's platform is used across defense, healthcare, automotive and other regulated industries to enhance product & AI security, third-party risk & compliance.

SUPPLY CHAIN CHALLENGES

It’s hard to see what’s inside the software you build and buy, especially with the growing dependency on AI models, and third-party vendors. Existing solutions miss critical details, are not automated, and don’t scale across programs or suppliers. Without a complete picture it's difficult to spot vulnerabilities, ensure compliance, or respond quickly when something goes wrong.

MANIFEST BENEFITS

- Uncover hidden supply chain risks
- Respond to vulnerabilities efficiently
- Manage AI security risks
- Automate software risk-assessments, at scale
- Centralize software risk management in one place
- Drive third-party compliance
- Onboard your team in seconds
- Deploy securely in cloud or on-prem

USE CASES

Build Secure Software

Empower Product Security, DevSecOps, and AppSec teams to identify and resolve software supply chain risks early, before they impact customers or compliance.

Mitigate Third-Party Risk

Acquisition, and supply chain teams can simplify third-party risk assessments by using SBOMs to understand vulnerabilities and compliance. Automation reduces manual effort, flags issues early, and streamlines procurement with real-time risk insights.

Remediate Faster

CISOs, IR teams, and SOCs save time and costs by quickly identifying vulnerable software and AI components. Prioritized inventories and automated reports make it easy to stay ahead of incidents and keep stakeholders informed.

Manage AI Risk

Protect your organization with better AI security by knowing exactly which GenAI models and data are being used in your software. With clear records of what’s being used and where, it’s easier to follow policies, answer customer questions, and reduce risk.

Simplify Compliance

Software makers can stay ahead of global regulations by proving what’s in their code and how it’s secured. In regulated industries, SBOMs are now a compliance standard; manageable at scale with speed and simplicity.

HOW IT WORKS

1 From Zero to SBOM

Generate and merge SBOMs from in-house applications within seconds. Solicit SBOMs from your vendors, and store them all in a secure repository for sharing with approved parties.

2 Context Enrichment

Turn raw, hard-to-use SBOMs into actionable files with automatic enrichment from leading vulnerability and exploitability databases.

3 Vulnerability Identification

Make risk-informed decisions using a complete supply chain view, with vulnerability matching based on data from major sources (e.g., CVE.org, NVD) and vulnerability criticality.

4 Risk Visualization

Interact with supply chain risk analysis data in a platform purpose built for practitioners and decision makers.

5 Actionable Insights

Turn SBOM and prioritized vulnerability data into outcomes via automatic ticketing, proactive outreach messaging, and risk reporting tailored for less technical audiences.

Specs

SUPPORTED IMPORT METHODS

Import SBOM:
- CycloneDX
- SPDX
- CSAF or OpenVEX

Import OSS:
- GitHub

Import AI Model:
- HuggingFace

SUPPORTED ECOSYSTEMS

- Alpine
- C
- C++
- Dart
- Debian
- Elixir
- Erlang
- Go
- Haskell
- Java
- JavaScript
- Jenkins plugins
- .NET
- Nix
- PHP
- Python
- Red Hat
- Ruby
- Rust
- Swift
- Others

SUPPORTED REGULATIONS AND STANDARDS

- EU NIS 2
- NIST 800-218
- UNECE R155
- OWASP SAMM
- ISO/SAE 21434
- Executive Order 14028
- Executive Order 14144
- OMB M-22-18
- FDA Cybersecurity Guidance
- EU Cyber Resilience Act

API AND INTEGRATIONS

API Uses:
- SIEMs
- Ticketing Systems
- Vulnerability Scanners
- Assest Management
- Messaging Systems

Intergrations:
- GitHub
- JIRA
- ServiceNow
- Linear

WHO WE SERVE

Manifest is trusted by some of the world's largest and most critical institutions. Our flagship supply chain security platform can be deployed anywhere your team needs, from virtual private clouds (VPCs) to more sensitive environments, is SOC2 certified, meets GDPR controls, and is FedRAMP High Authorized.

Government | Defense Industrial Base | Medical Device Manufacturers | Financial Services | Manufacturing

> "Manifest's capabilities are some of the most forward-thinking I have ever seen. They are moving well left of our current state, getting ahead of cyber incidents before they precipitate."
>
> - Fleet Cyber Command, United States Navy

OUR ACCREDITATIONS

FedRAMP High | GDPR | SOC 2 TYPE 2 | DOD Impact Level 5 | NIST 800-171 Compliant

Start securing your software supply chain with Manifest. Contact us at info@manifestcyber.com