RELIZA

ReARM

Digital Asset Management System

ReARM is a Supply Chain Security and Digital Asset Management System for Releases, SBOMs, xBOMs, and other Security and Compliance Artifacts

https://rearmhq.com

About ReARM

ReARM is an abbreviation for "Reliza's Artifact and Release Management". It is a DevSecOps Digital Asset Management tool to organize product releases with their metadata, including various Bills of Materials (SBOMs / xBOMs).

xBOM Compliance

ReARM allows organizations to maintain up-to-date inventory of digital assets, including SBOMs/xBOMs, in compliance with various regulatory frameworks, including:

- EU CRA, BSI TR-03183, NIS2, DORA
- US EOs 14028, 14144
- US OMB Memorandum M-22-18
- Section 524B of the US FD&C Act
- US Army Memorandum on SBOMs
- India RBI and SEBI

Native SDLC Integration

ReARM is designed to work with your Software Development Life Cycle.

ReARM provides unique internal data model describing relationships between Products, Feature Sets, Product Releases, Components, Branches, Component Releases, and their metadata.

ReARM integrates with any CI/CD workflow.

Per Release Metadata

Unlike legacy cybersecurity tools, ReARM stores and processes all metadata per release.

With this, you can view security posture of each specific release and trace vulnerabilities according to lifecycle states of your products.

Aggregation Engine

ReARM includes built-in aggregation engine that can automatically merge and profile Bills of Materials with certain commonality.

For example, it is possible to produce an aggregated BOM for a Product Release from all its Component Releases in a few clicks.

Capabilities

Inventory

ReARM maintains up-to-date inventory of organization's digital assets, driven by CI/CD tooling

Storage / Retrieval

ReARM allows for storage and retrieval of SBOMs / xBOMs for software and hardware, per release, including signatures and signing details

Aggregation

ReARM allows for seamless creation of aggregated BOMs on Product and Component Release levels

Processing

ReARM supports tight integration with OWASP Dependency-Track, continuously analyzing each SBOM for vulnerabilities and policy violations, with aggregated results available at the release level

Multi-Domain

ReARM enables complex workflows, including combinations of software and hardware components within the same product, making it an invaluable tool in the fields like IoT and medical devices

Why ReARM

- Built for secure and compliant software and hardware supply chains
- Automates end-to-end xBOM workflows, including versioning, changelogs, storage, processing and retrieval
- Includes SBOM augmentation, aggregation and filtering capabilities
- Provides release-level insights and traceability
- Integrates natively into CI/CD workflows
- Comes in enterprise and community editions

The Facts

Core Platform

>5 YEARS

IN PRODUCTION

Storing

>50,000

RELEASES

With

>10

INTEGRATIONS

Comparison with Legacy Tools

ReARM represents the next generation of xBOM-centric cybersecurity tools. The key differences with previous generation are highlighted in the chart below.

REARM BY RELIZA

	Supports variety of xBOM, Compliance and Security documents
	xBOMs organized by Releases and integrated into Digital Asset Management
	Configurable automated versioning and changelogs
	Extensive integration options via CLI and event triggers
	Fixed predictable pricing only based on organization size, FOSS CE version available.

LEGACY SBOM TOOLS

SBOM-only focused	
Single SBOM for the whole Project	
Requires other tooling for versioning and release management	
Limited pre-defined integrations	
Pricing depends on usage	