

Software Bill of Materials

Complete software composition
analysis with dual-engine vulnerability scanning



2,700+
COMPONENTS/SCAN

7
COMPLIANCE
FRAMEWORKS

2
SCAN
ENGINES

5
OUTPUT
FORMATS

Output Formats

FORMAT	STANDARD	USE CASE
CycloneDX 1.5 JSON	OWASP CycloneDX	Primary SBOM format — components, hashes, licenses, PURLs
SPDX 2.3 JSON	Linux Foundation SPDX	Compliance-focused — license mapping, supplier relationships
VEX Document	CycloneDX VEX 1.5	Vulnerability status per CVE — machine-readable exploitability
PDF Executive Report	ARGUS Proprietary	Per-scan report with charts, risk score, remediation plan
Portfolio PDF Report	ARGUS Proprietary	Cross-portfolio 27-page board-ready report (13 sections)

Policy Governance Gate

8 Built-in Security Policies — CI/CD Integration

- **Critical CVE Gate** — Fail if any critical vulnerability found
- **High CVSS Threshold** — Fail if max CVSS $\geq$ configurable threshold
- **Copyleft License Gate** — Warn/fail on GPL, LGPL, AGPL components
- **CISA 2025 Compliance** — Verify all minimum SBOM elements present
- Returns HTTP 200 (PASS) / 403 (FAIL) for Jenkins, GitHub Actions, GitLab CI, Azure DevOps
- API key authentication (kvc_ prefixed, 32-byte entropy) for secure CI/CD integration

SBOM Diff & Comparison

Compare any two scan versions to track supply chain drift: added/removed components, version upgrades, new vulnerabilities, license changes, and risk direction indicator (improving/degrading).



What is SBOM?

A Software Bill of Materials is a comprehensive inventory of every component in your software — libraries, frameworks, packages, and their dependencies.

Why SBOM Matters

- Software supply chain attacks increased 742% from 2019–2024 (Sonatype)
- U.S. Executive Order 14028 mandates SBOM for federal software suppliers
- EU Cyber Resilience Act requires component transparency for digital products
- RBI Master Directions (April 2024) require complete software component visibility for Indian banks



Supported Scan Targets

TARGET TYPE	SUPPORTED SOURCES	AUTHENTICATION
Container Images	Docker Hub, AWS ECR, Google GCR, Azure ACR, Harbor, GHCR, Quay.io, all OCI registries	Username/Password, IAM roles
Git Repositories	GitHub, GitLab, Bitbucket, Azure DevOps, any Git URL	Username/Token, SSH keys
File Systems	Local paths, mounted volumes, network shares, remote servers (SSH)	OS-level or SSH credentials
Package Manifests	package.json, requirements.txt, pom.xml, go.mod, Gemfile, Cargo.toml, etc.	None required

Scan Results & Analysis

Five detailed analysis tabs provide complete visibility into your software supply chain.

Vulnerability Analysis

CVE ID, severity badge, CVSS score & vector, affected package, installed vs. fix version, EPSS percentile, KEV status, source engine. Summary: average CVSS, max CVSS, fixable count.

Component Inventory

Complete package list: name, version, type, PURL identifier, SHA-256 hash, license SPDX ID. Supports npm, pip, Maven, Go, Rust, NuGet, Ruby, PHP, and 30+ ecosystems.

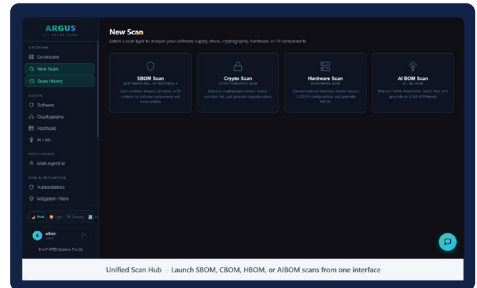
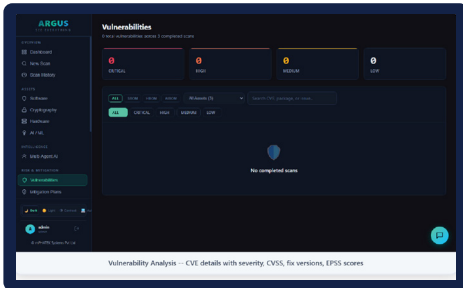
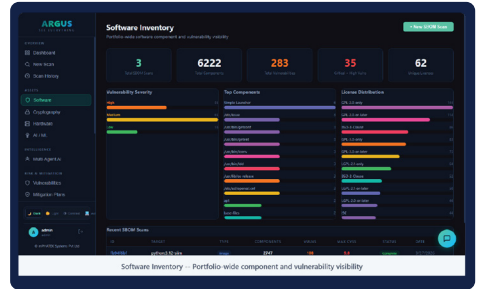
VEX Documents

Auto-generated CycloneDX VEX with exploitability assessment per CVE: status (exploitable/not_affected/under_investigation), response code, affected PURL. Machine-readable for automation.

License Compliance

SPDX license IDs extracted per component. Classification: Permissive (MIT, Apache), Copyleft (GPL, LGPL), Commercial, Unknown. Copyleft risk assessment for legal review.

Platform Walkthrough



Ready to Secure Your Communications?
Contact us for a demo or proof-of-concept deployment

contact@mphatek.com | Visit: www.mphatek.com

Head Office - India
5th Floor, B Wing,
Pride Silicon Plaza,
S.No.106, Near
Chaturshringi Temple,
Senapati Bapat Road
Pune - 411 016

UAE
mPHATEK COMPUTER
SYSTEM LLC.
Office No. 21, 30th
Floor, Al Moosa
Tower 2, Sheikh Zayed
Road, Dubai

South Africa
1st Floor, Aptus
House, Riverpark,53,
Autumn Street,
Rivonia,
Johannesburg 2128

Canada
mPHATEK Systems Inc.
534 Lawrence Avenue
West, Suite 220
Toronto ON M6A 1A2

USA
mPHATEK Systems Inc.
8 The Green,
Dover, Delaware
19901