mPHATEK
Achieving Greater Heights

ARGUS — SEE EVERYTHING

SBOM

Software Bill of Materials

Complete software composition analysis with dual-engine vulnerability scanning

2,700+	7	2	5
COMPONENTS/SCAN	COMPLIANCE FRAMEWORKS	SCAN ENGINES	OUTPUT FORMATS

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

Dual-Engine Vulnerability Scanning

Grype Engine (Anchore)

Matches SBOM components against NVD, GitHub Advisory, OSV, and RHSA databases. CVSSv3.1 scoring with fix-version tracking. Cross-references PURL identifiers for precise matching.

Trivy Engine (Aqua Security)

Independent vulnerability detection with container layer analysis. Comprehensive coverage of OS packages, language-specific libraries, and configuration issues. Results cross-correlated and deduplicated.

EPSS Enrichment (FIRST.org)

Real-time Exploit Prediction Scoring from FIRST.org. Prioritize remediation by actual exploit likelihood, not just CVSS severity. Cached for performance.

KEV Flagging (CISA)

Flags Known Exploited Vulnerabilities from CISA's catalog. Identifies CVEs actively being exploited in the wild for immediate action and escalation.

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.

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 ≥ 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).

Compliance Framework Coverage

ARGUS SBOM validates your software inventory against 7 major regulatory frameworks.

FRAMEWORK	REGION	KEY REQUIREMENTS	STATUS
CISA 2025	US Federal	Minimum elements for software bills of materials	**FULL**
NTIA 2021	US Federal	Supplier, component, dependency relationships	**FULL**
EO 14028	US Federal	Improving the Nation's Cybersecurity — SBOM mandate	**FULL**
EU CRA	European Union	Digital product security obligations	**FULL**
PCI DSS 4.0	Global Finance	Requirement 6.3.2 — software component inventory	**FULL**
CERT-In v2.0	India	SBOM minimum data elements mandate	**FULL**
RBI IT Gov	India Banking	Complete software component visibility (Apr 2024)	**FULL**

CISA 2025 Minimum Elements — All 10 Verified

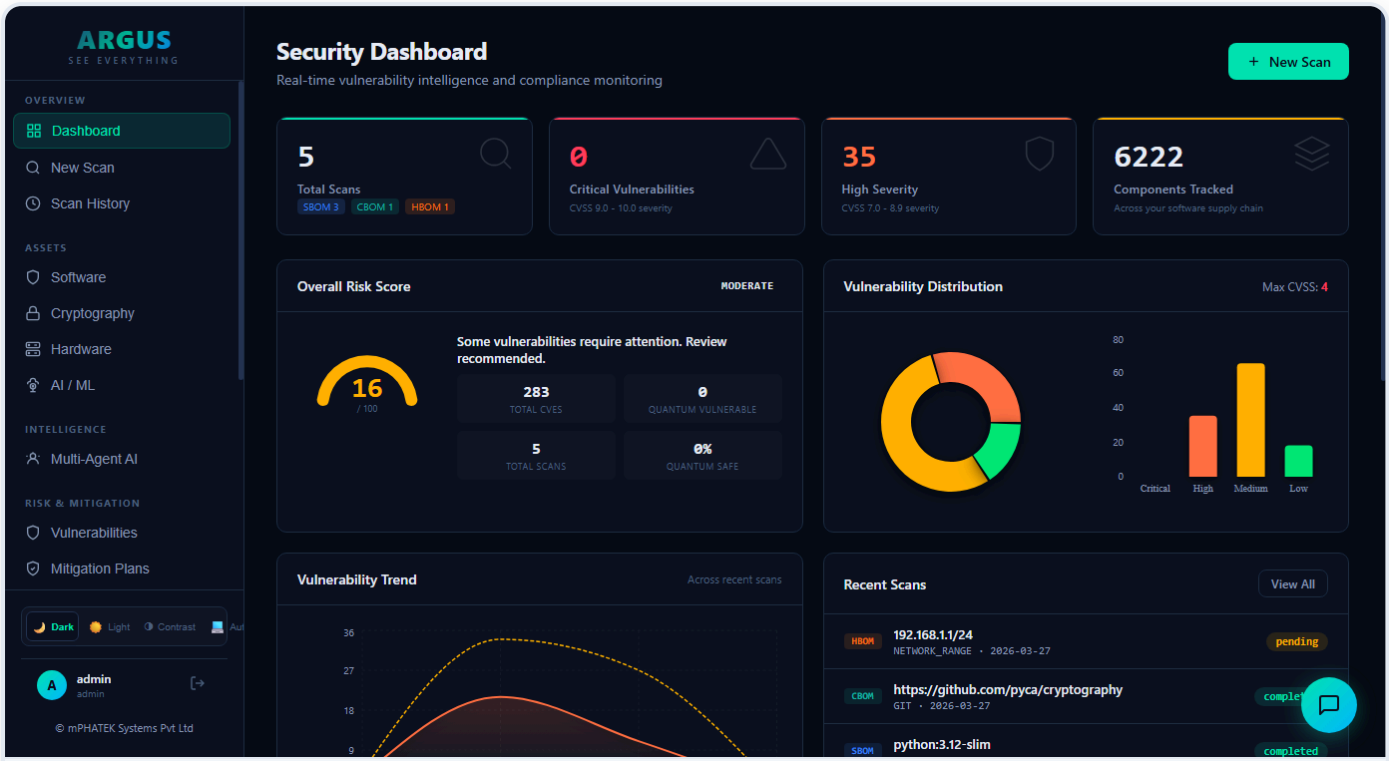
- ✓ Component Name — extracted from package metadata
- ✓ Component Version — semantic versioning captured
- ✓ Component Hash (SHA-256) — integrity verification
- ✓ PURL Identifier — universal package identification
- ✓ License Information — SPDX license IDs
- ✓ Tool Name — "ARGUS" in SBOM metadata
- ✓ Generation Context — target, type, timestamp
- ✓ SBOM Author — mPHATEK ARGUS v3
- ✓ Timestamp — ISO 8601 UTC
- ✓ Dependency Relationships — full graph in CycloneDX

Intelligence Sources

SOURCE	DATA PROVIDED	PURPOSE
NVD (NIST)	CVSSv3.1, CWE, CPE matching	Severity classification and impact scoring
EPSS (FIRST.org)	Exploit probability percentile	Prioritize by real-world exploit likelihood
KEV (CISA)	Known Exploited Vulnerabilities	Flag actively exploited CVEs for immediate action
Fix Versions	Available patches per package	Clear remediation path with upgrade targets
SBOM Diff	Component delta between versions	Track supply chain drift across releases

Platform Walkthrough

Live screenshots from the ARGUS SBOM scanning platform.

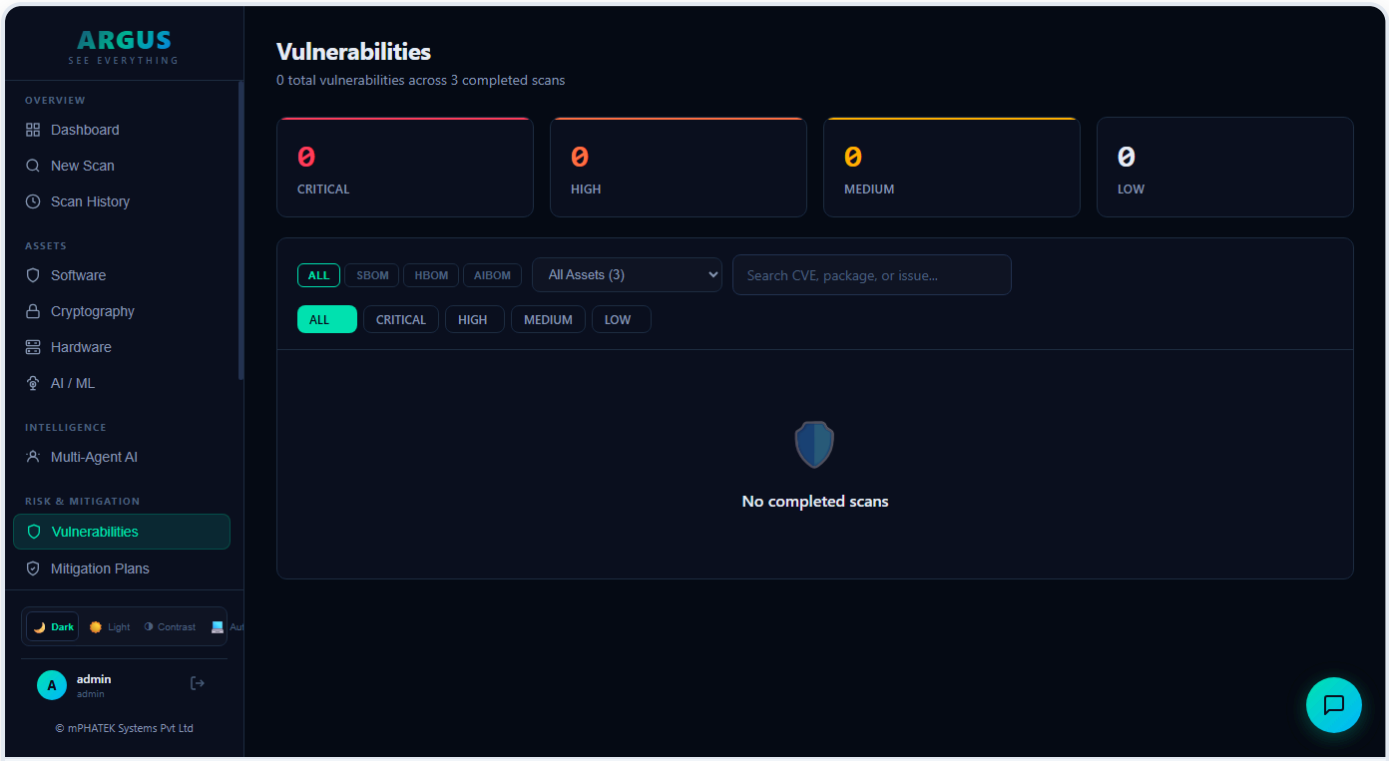


Security Dashboard -- Real-time risk score, vulnerability distribution, compliance status

Software Inventory -- Portfolio-wide component and vulnerability visibility

Platform Walkthrough

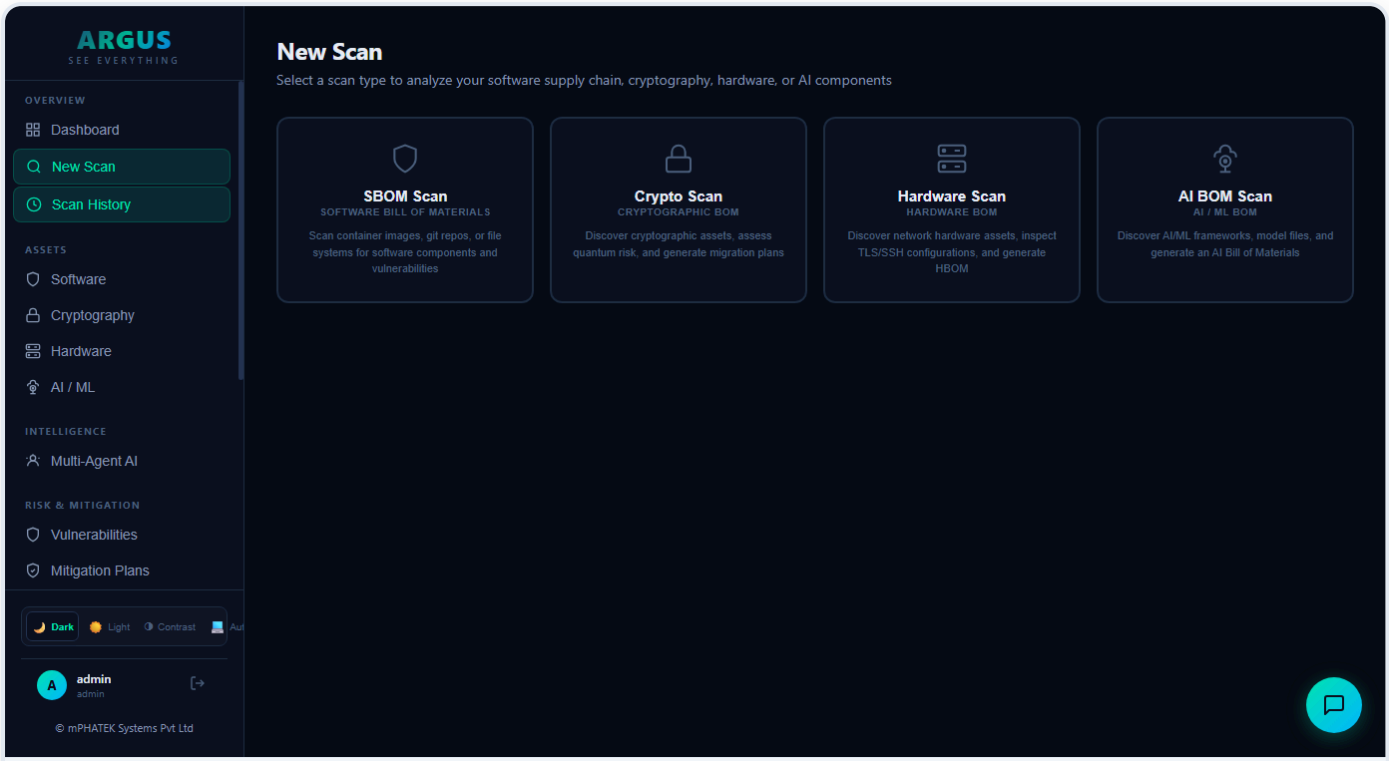
Vulnerability analysis and component inventory.



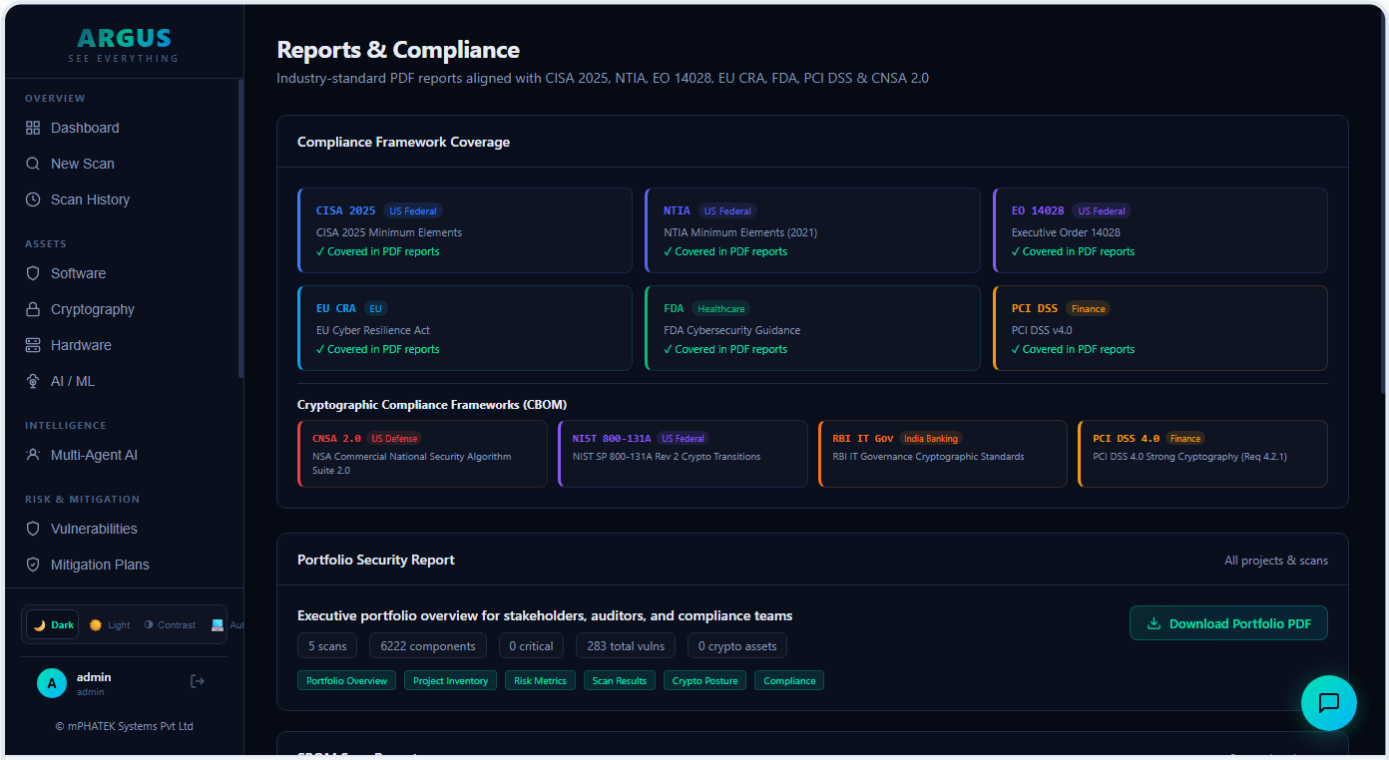
Vulnerability Analysis -- CVE details with severity, CVSS, fix versions, EPSS scores

Platform Walkthrough

Scan management and compliance reporting.



Unified Scan Hub -- Launch SBOM, CBOM, HBOM, or AIBOM scans from one interface



Reports & Compliance -- PDF reports, CycloneDX, SPDX, and VEX exports

Ready to Secure Your Supply Chain?

Schedule a live demo or request a proof-of-concept deployment for your organization.

contact@mphatek.com

mPHATEK Systems Pvt Ltd • v3.1.0 Enterprise Edition
On-premise • Air-gapped • Docker/Kubernetes