Kavach SBOM

Enterprise Software Supply Chain Security Platform

Complete SBOM lifecycle management, vulnerability intelligence, and regulatory compliance purpose-built for the Banking & Financial Services sector

Banking Edition v3.1.0

Prepared by: **mPhatek Systems Pvt. Ltd.**

Date: February 2026

Classification: Confidential

Table of Contents

Document structure and navigation

1

Executive Summary

Why your bank needs SBOM management now

The Regulatory Imperative

The RBI Master Directions on IT Governance (effective April 2024), CERT-In SBOM Guidelines (October 2024, expanded July 2025), PCI DSS 4.0 Requirement 6.3.2 (effective March 2025), and SEBI CSCRF all now mandate that financial institutions maintain complete visibility into software components across their entire technology stack. Non-compliance exposes the bank to regulatory penalties, audit findings, and unmanaged cyber risk.

Kavach SBOM is an enterprise-grade Software Bill of Materials platform that provides complete software supply chain visibility, continuous vulnerability monitoring, and automated regulatory compliance — purpose-built for the banking sector. It generates, manages, and monitors SBOMs across your entire application portfolio, producing bank-grade PDF reports, compliance artifacts, and real-time security intelligence.

6,954	434	285	6
Components Tracked	CVEs Identified	Suppliers Mapped	Compliance Frameworks

Value Proposition

Kavach replaces manual SBOM processes with automated, continuous monitoring. A single scan identifies every software component, maps every vulnerability, scores every supplier risk, checks every license, and produces audit-ready PDF reports — in under 3 minutes. It deploys 100% on-premise with no data leaving your network.

2

The Problem

Software supply chain risk is the #1 unaddressed threat in banking

⚠️ Invisible Dependencies

A typical banking application contains 500–3,000+ open-source components. Most banks cannot enumerate what software is running inside their production systems, leaving blind spots for attackers.

🔒 Known Vulnerabilities

New CVEs are published daily. Without continuous SBOM monitoring, banks run software with known, exploitable vulnerabilities — often for months before detection.

📜 Regulatory Mandates

RBI, CERT-In, PCI DSS 4.0, and SEBI now require SBOM generation, software component inventories, and supplier risk assessment. Manual processes cannot scale.

💰 Tool Complexity & Integration Gaps

Commercial SBOM tools require extensive integration effort, lack native Indian regulatory mapping (RBI, CERT-In), and offer limited on-premise deployment options for air-gapped banking environments.

Real-World Impact: Key Incidents

Log4Shell (Dec 2021) — Banks without SBOMs took 2–4 weeks to determine if they were affected. Banks with SBOM tools knew within hours.

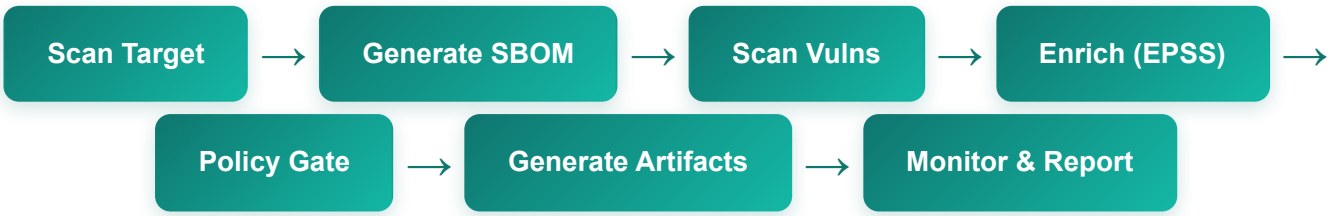
SolarWinds (2020) — Supply chain attack compromised 18,000+ organizations. SBOM + VEX would have enabled rapid triage.

XZ Utils (2024) — Backdoor in a core compression library used across Linux systems. SBOM-equipped organizations identified exposure immediately.

3

How Kavach Works

End-to-end SBOM lifecycle in 7 steps — told as a story



1

Define the Target

The security analyst logs into Kavach and initiates a new scan. Kavach accepts **Docker images** (e.g., your core banking app image), **Git repositories** (your internal codebase), or **filesystem directories** (vendor-delivered packages). The analyst selects the target and chooses the scanner combination.

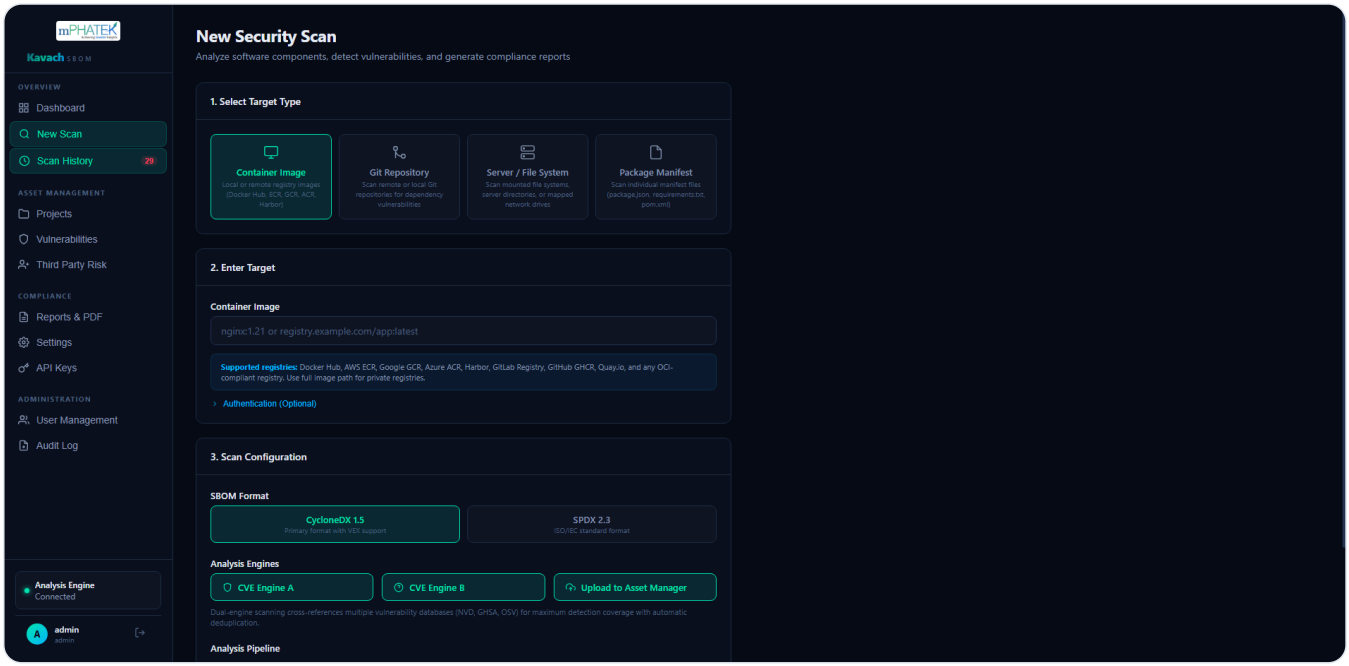


Figure 3.1 — New Scan interface: select target type, enter target, choose scanner

2

SBOM Generation

Kavach uses **Syft** (by Anchore) to perform deep component analysis. It extracts every package, library, and dependency — producing both **CycloneDX 1.5** and **SPDX 2.3** formatted SBOMs simultaneously. A typical scan identifies 500–3,000+ components, including transitive dependencies invisible to manual audits.

3 Multi-Scanner Vulnerability Analysis

The SBOM is then fed through **two independent vulnerability scanners** — Grype and Trivy. Results are merged, deduplicated, and enriched with CVSS scores. This dual-scanner approach catches vulnerabilities that any single scanner might miss, providing defense-in-depth.

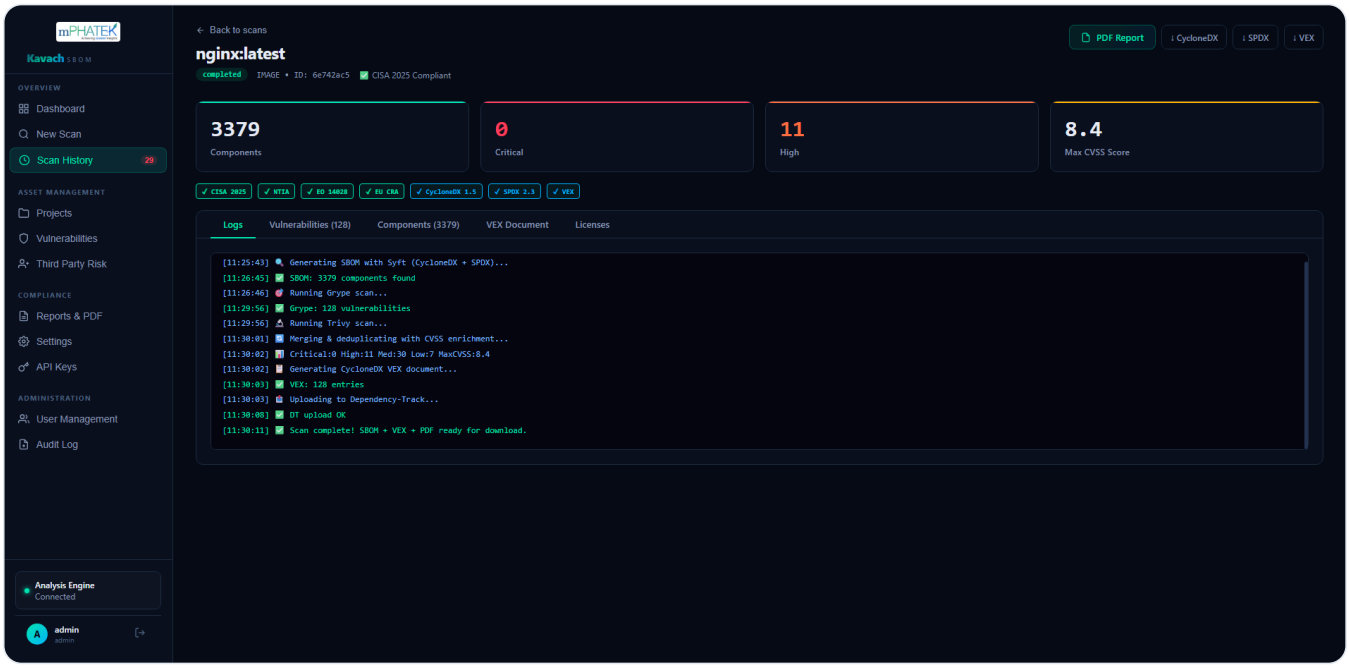


Figure 3.2 — Completed scan showing 3,379 components, 128 vulnerabilities, CISA/NTIA/EO14028 compliance badges

4 EPSS Exploit Probability Enrichment

Every CVE is enriched with real-time **EPSS scores** from FIRST.org — the industry standard for predicting which vulnerabilities will actually be exploited in the wild. This transforms a flat list of CVEs into a **prioritized, actionable risk view** that focuses remediation on the threats most likely to be weaponized.

5 Policy Governance Gate

Kavach evaluates every scan against **8 built-in governance policies**: no critical vulnerabilities, maximum high-severity threshold, copyleft license detection, minimum compliance score, EPSS threshold, total vulnerability cap, required SBOM fields, and fix-available SLA. The result is a clear **PASS / WARN / FAIL** verdict that integrates into CI/CD pipelines for automated release gating.

6 Artifact Generation

For every completed scan, Kavach automatically produces **6 downloadable artifacts**: CycloneDX SBOM (JSON), SPDX SBOM (JSON), VEX document (CycloneDX VEX), executive PDF report with charts, vulnerability listing, and license analysis. These artifacts satisfy CERT-In, CISA, NTIA, and PCI DSS requirements.

7

Continuous Monitoring & Executive Reporting

The security dashboard provides a real-time view across all scanned assets: vulnerability trends, risk score evolution, component counts, and supplier risk. Executive stakeholders receive **portfolio-level PDF reports** covering all applications, suitable for Board presentations, RBI audits, and IS audit submissions.

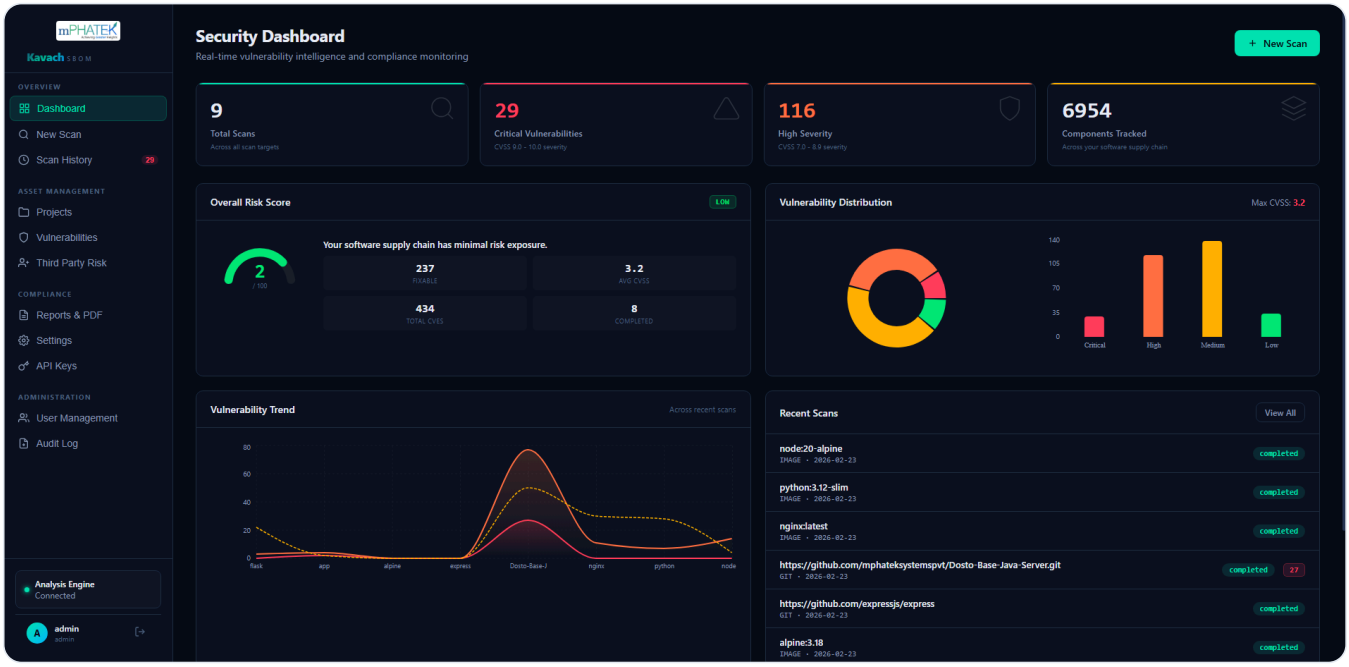


Figure 3.3 — Security Dashboard: real-time portfolio-wide risk overview

4

Platform Walkthrough

Every screen of Kavach SBOM with live screenshots

4.1 — Secure Login

Role-based authentication with brute force protection, progressive lockout, and session management.

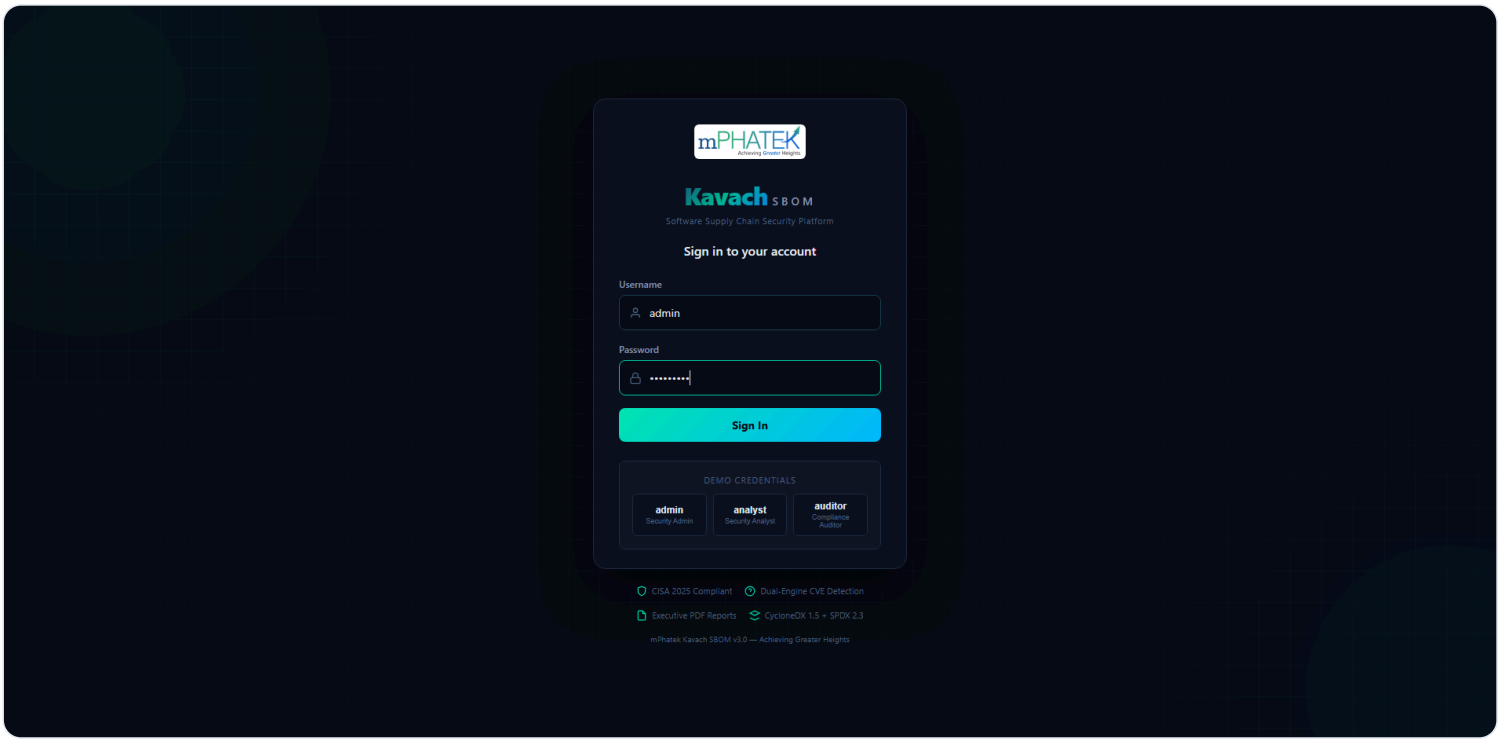


Figure 4.1 — Secure login with RBAC (Admin, Analyst, Auditor roles)

4.2 — Security Dashboard

Portfolio-wide risk score, vulnerability distribution donut chart, trend analysis, and recent scan activity.

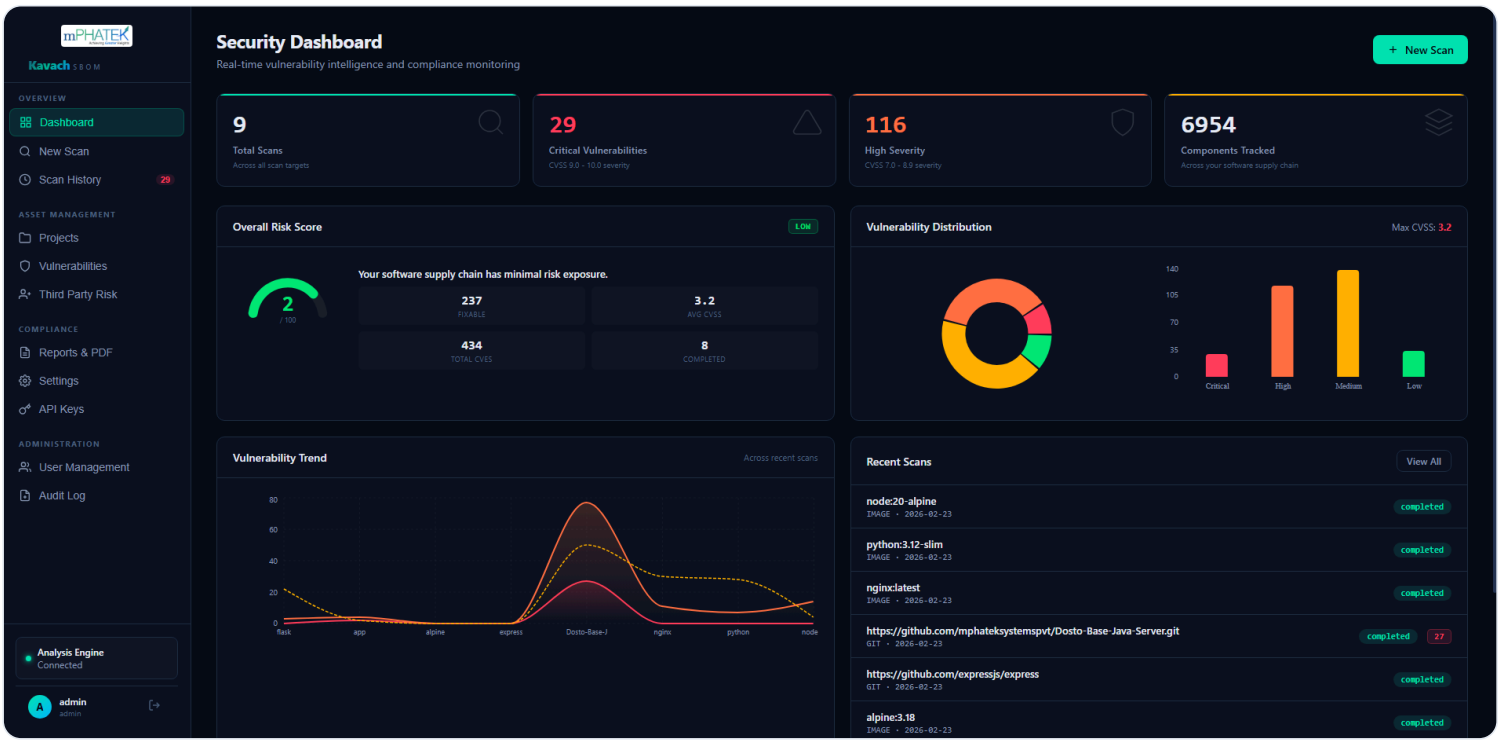


Figure 4.2 — Executive dashboard with risk gauge, vulnerability distribution, trend chart

Figure 4.3 — Vulnerability trend across scans and recent scan activity feed

4.3 — Scan History

Complete history of all SBOM scans with status, component counts, and quick access to details.

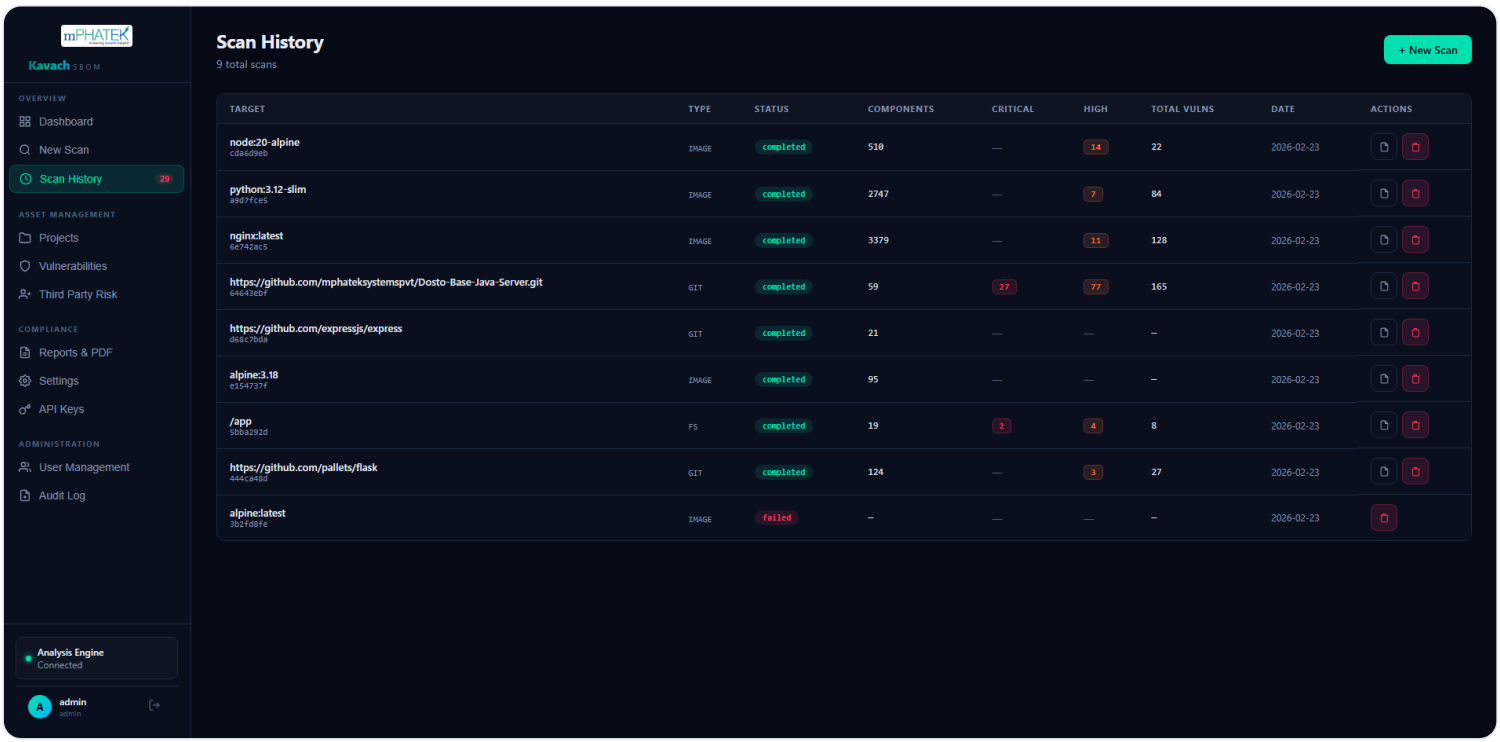


Figure 4.4 — Scan history with status indicators and filtering

4.4 — Scan Detail View

Deep dive into any scan: component inventory, vulnerability table, VEX document, license analysis, and compliance badges.

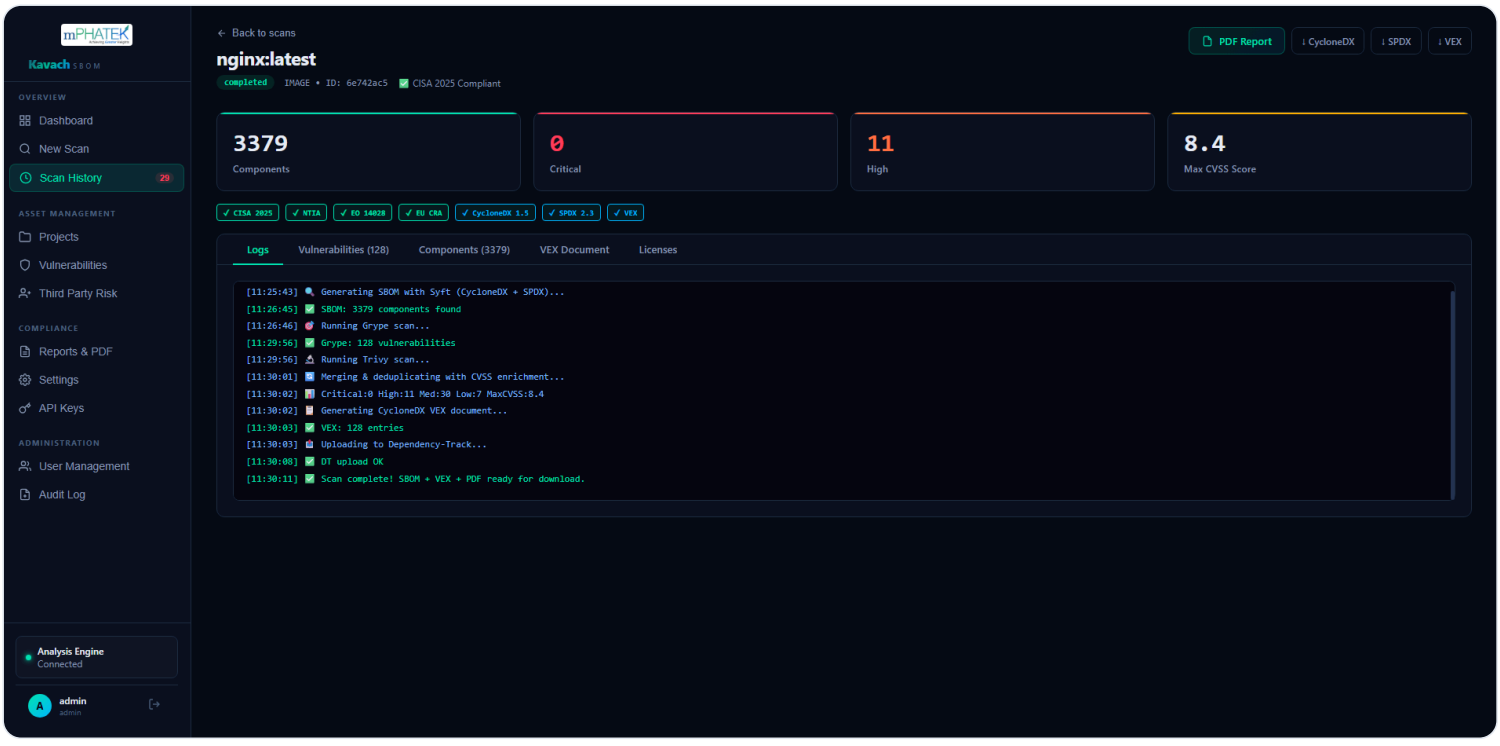


Figure 4.5 — Scan detail with logs, compliance badges, and download buttons

4.5 — Dependency-Track Projects

All scanned targets are automatically uploaded to Dependency-Track for continuous monitoring.

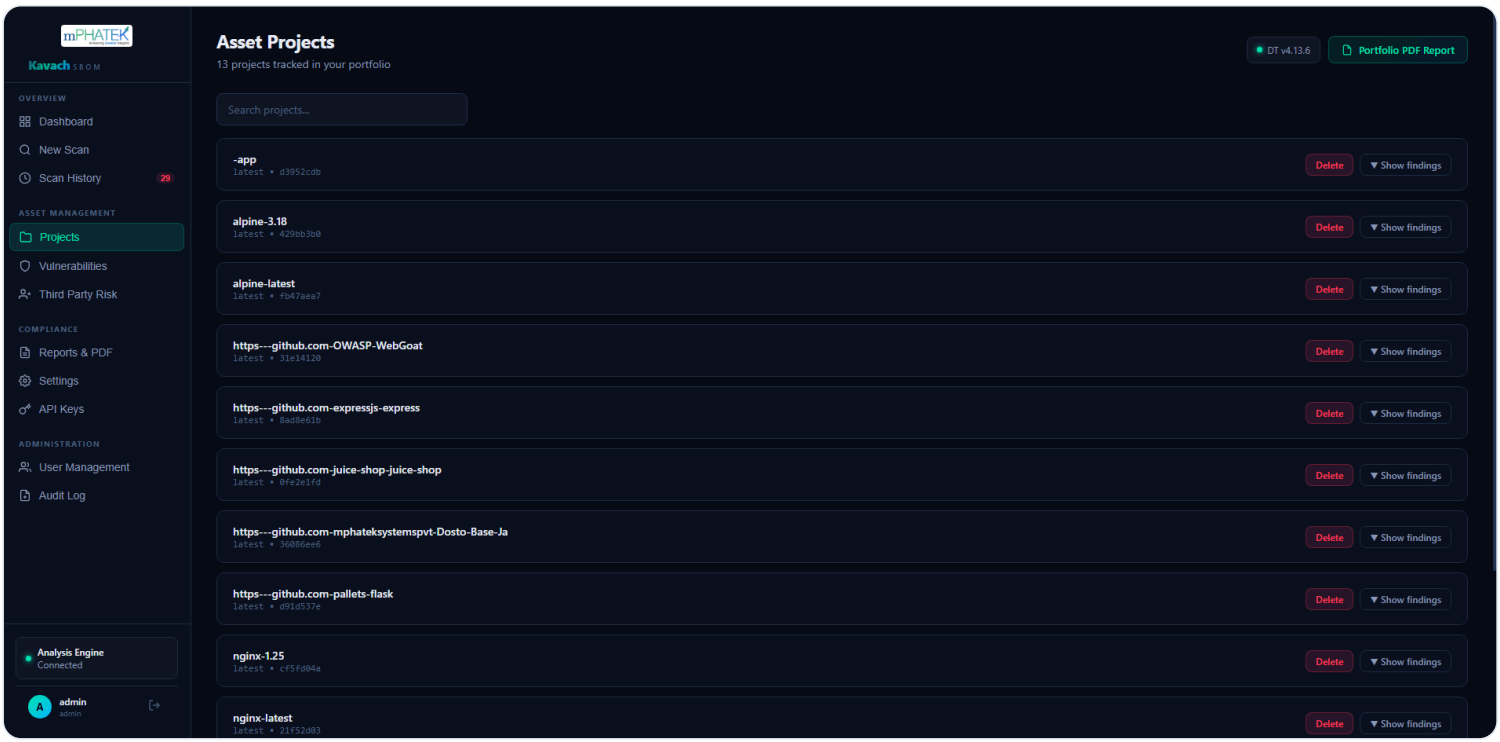


Figure 4.6 — Project portfolio synchronized with Dependency-Track

4.6 — Vulnerability Explorer

Cross-scan vulnerability view with severity filtering, CVSS scores, and affected component mapping.

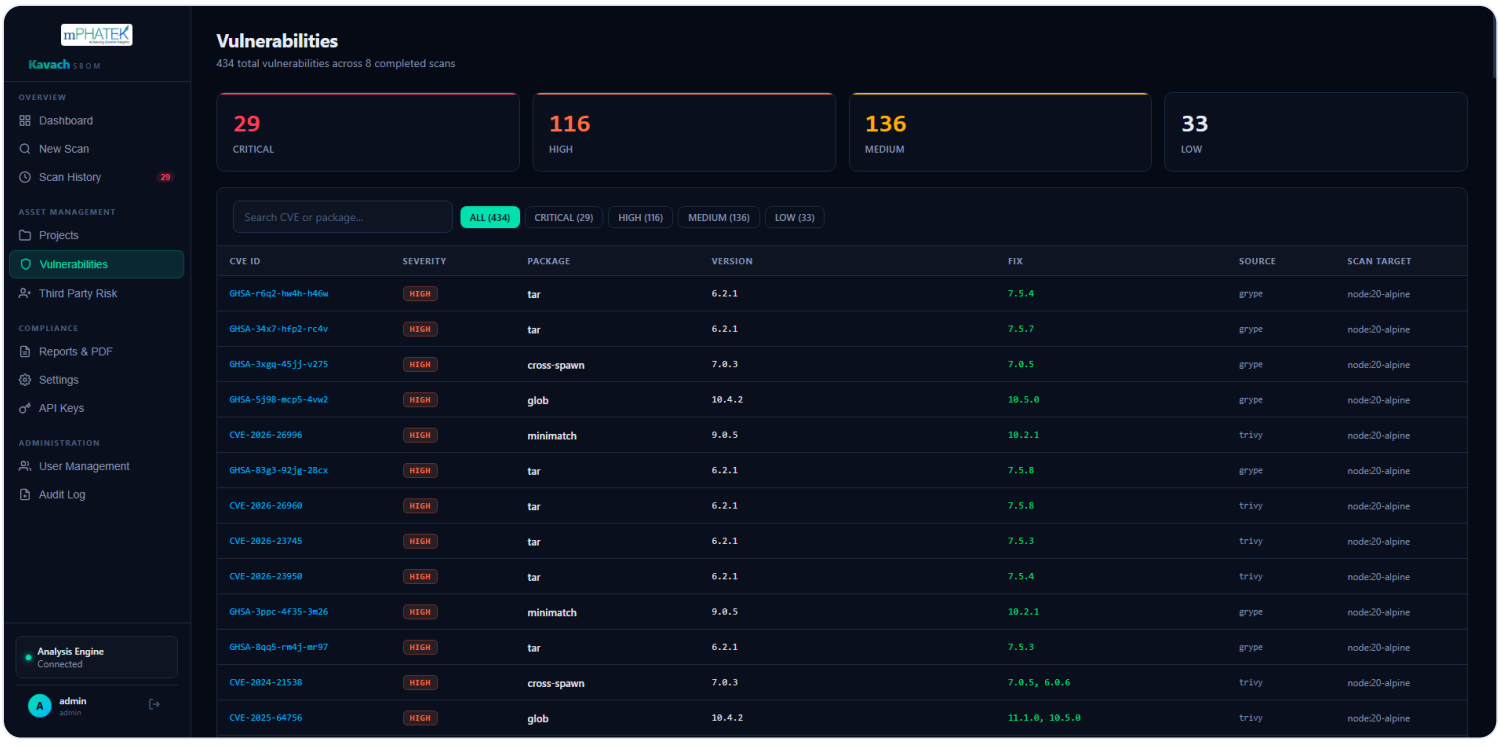


Figure 4.7 — Vulnerability explorer with CVE details and severity breakdown

4.7 — Third-Party Risk Management (TPRM)

Supplier risk scoring, component risk distribution, license composition analysis, and risk register.

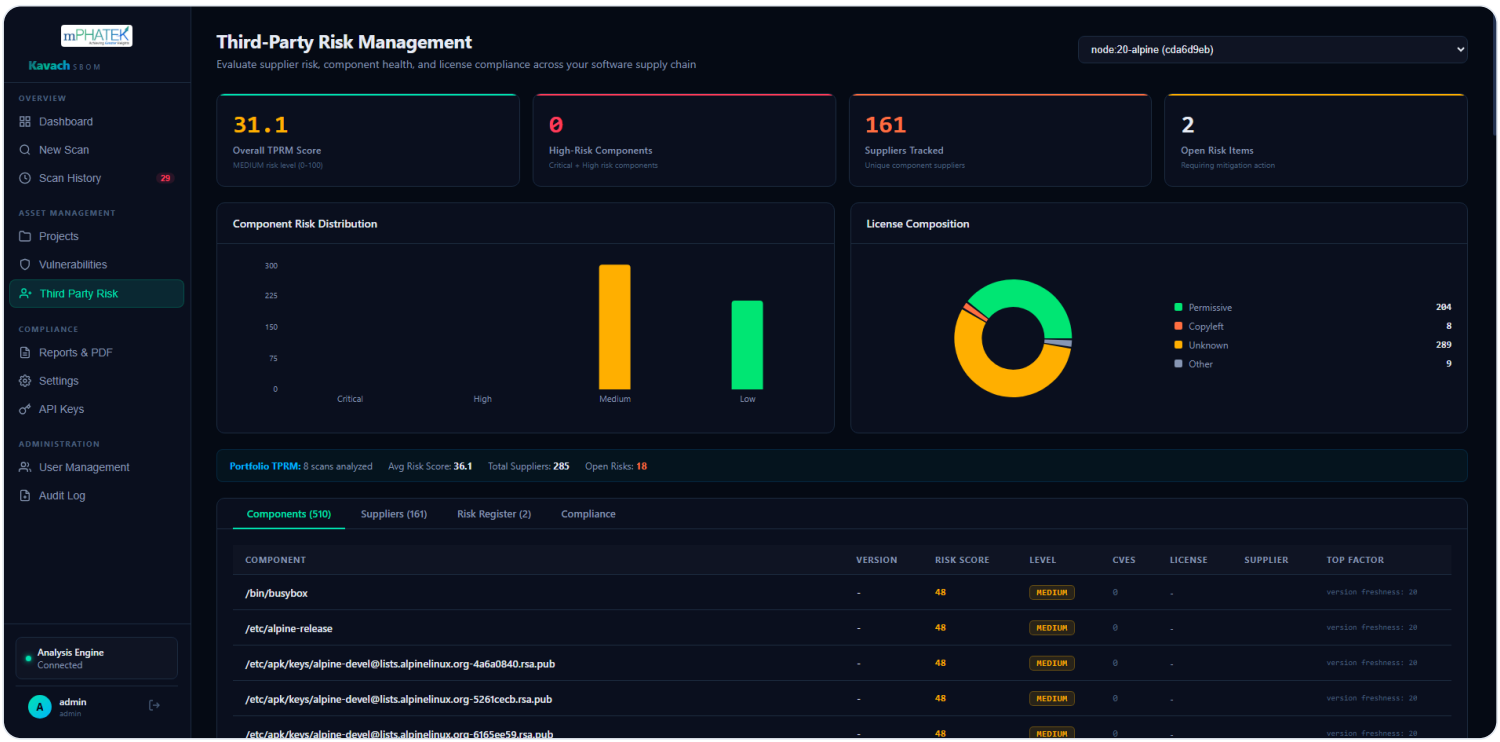


Figure 4.8 — TPRM: supplier tracking, risk scores, license distribution donut chart

4.8 — Reports & Compliance

Compliance framework coverage (CISA, NTIA, EO 14028, EU CRA, PCI DSS) with one-click PDF generation.

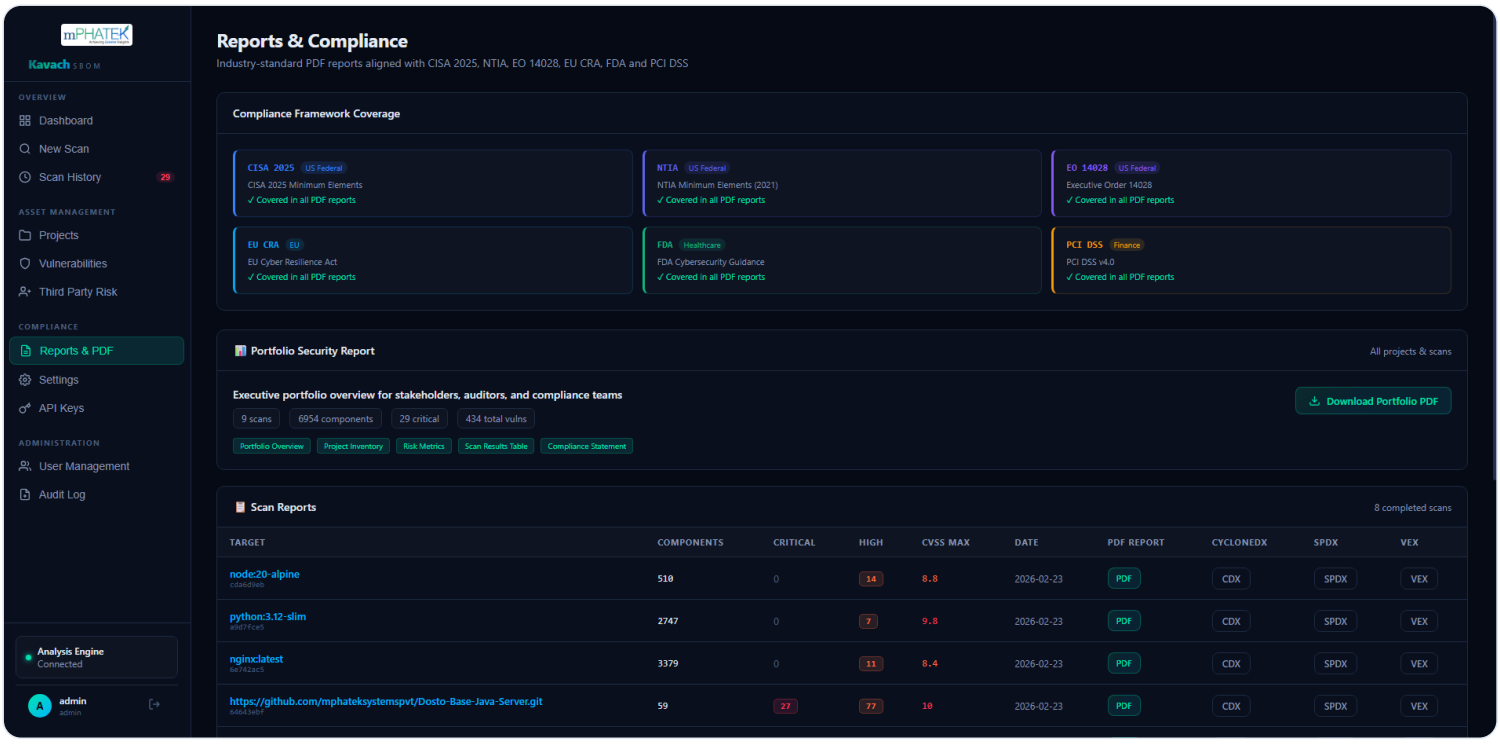


Figure 4.9 — Reports page: compliance badges, portfolio PDF, per-scan downloads (PDF, CycloneDX, SPDX, VEX)

4.9 — User Management

RBAC with Admin, Analyst, and Auditor roles. Password complexity enforcement per RBI/PCI DSS standards.

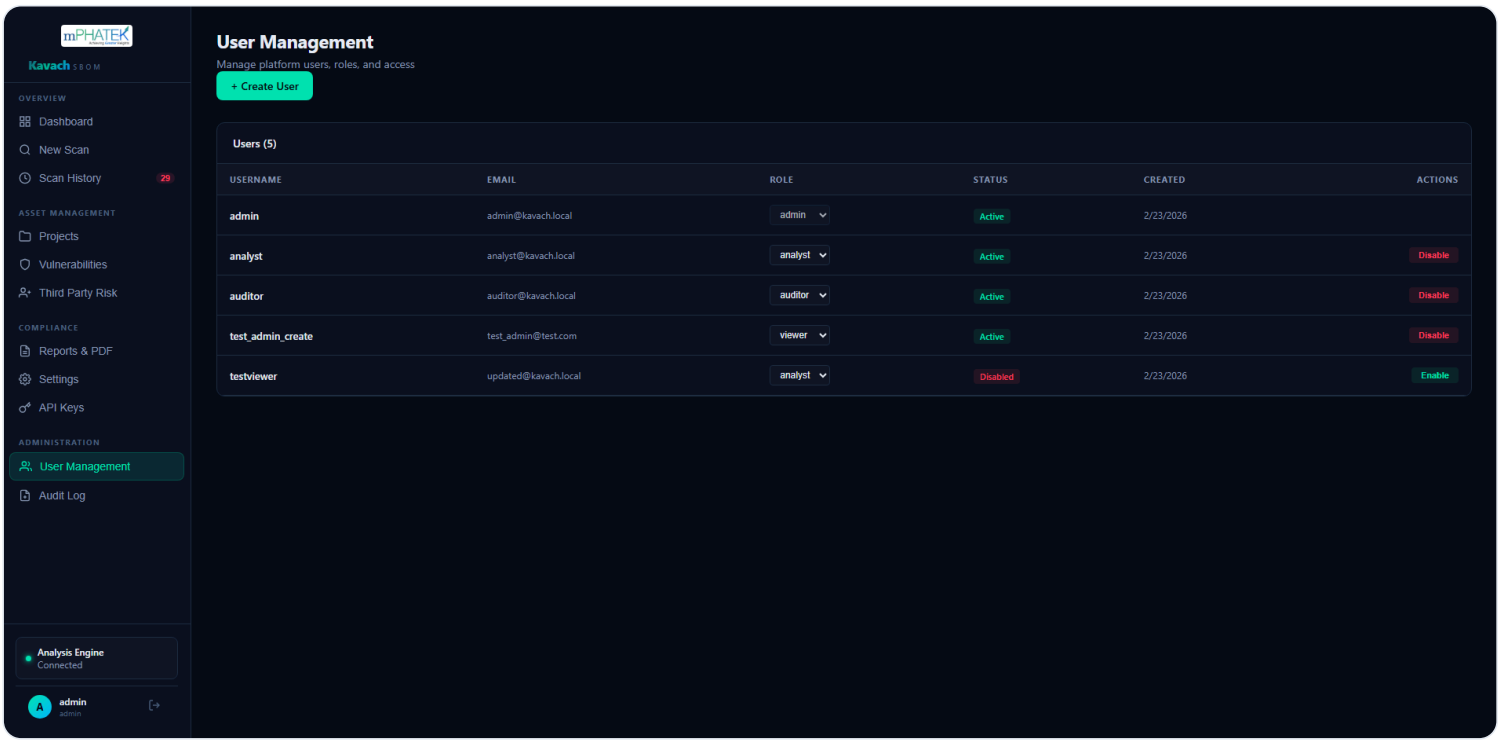


Figure 4.10 — User management with role-based access control

4.10 — Audit Trail

Immutable audit log of every API action: login, scan creation, report downloads, user changes. Required for IS audit.

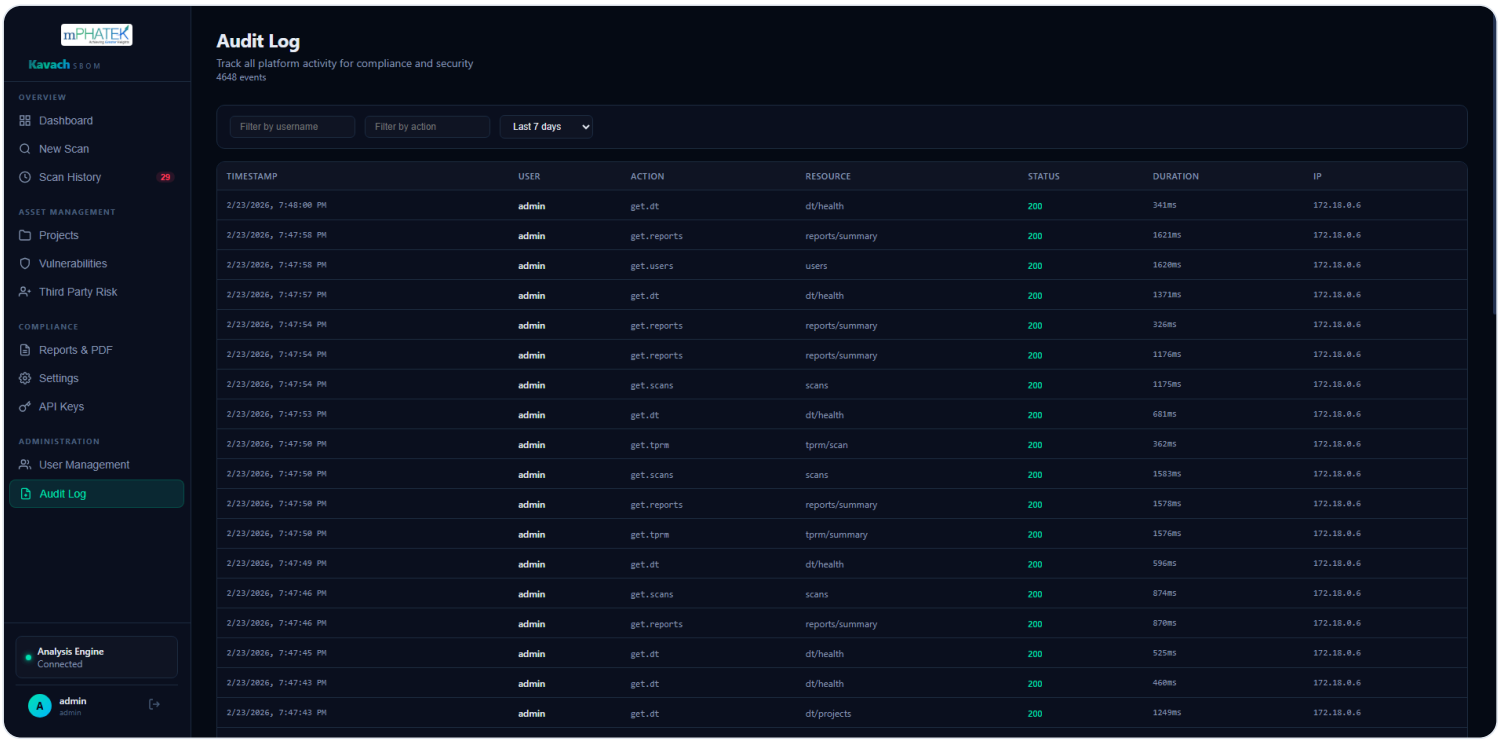


Figure 4.11 — Complete audit trail with user, action, IP address, timestamp

4.11 — API Key Management

Generate API keys for CI/CD pipeline integration and programmatic access.

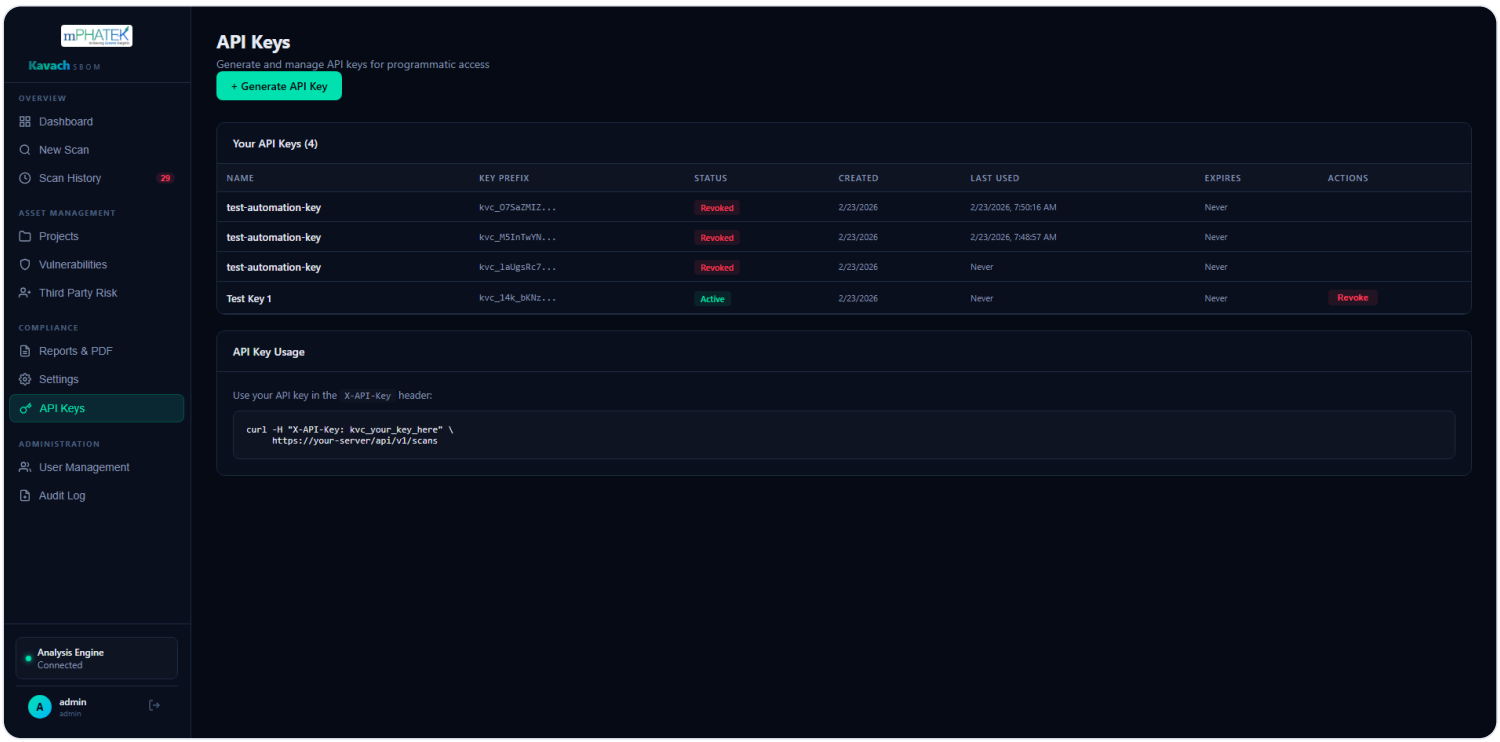


Figure 4.12 — API key management for CI/CD integration

5

Complete Feature Matrix

Every capability available in Kavach SBOM Banking Edition

CATEGORY	FEATURE	STATUS
SBOM Generation	CycloneDX 1.5 SBOM output (JSON)	AVAILABLE
	SPDX 2.3 SBOM output (JSON)	AVAILABLE
	Docker image scanning	AVAILABLE
	Git repository scanning	AVAILABLE
	Filesystem / directory scanning	AVAILABLE
Vulnerability Analysis	Multi-scanner: Grype + Trivy (dual engine)	AVAILABLE
	CVSS v3.1 scoring with severity classification	AVAILABLE
	EPSS exploit probability scoring (FIRST.org)	AVAILABLE
	VEX (Vulnerability Exploitability eXchange) document	AVAILABLE
	Fix-available tracking per vulnerability	AVAILABLE
Third-Party Risk	Supplier identification and enumeration	AVAILABLE
	Component-level risk scoring (0–100)	AVAILABLE
	License composition analysis (Permissive/Copyleft/Unknown)	AVAILABLE
	Supplier risk register with mitigation tracking	AVAILABLE
Policy & Governance	8 built-in governance policies	AVAILABLE
	CI/CD gate endpoint (PASS/FAIL for pipelines)	AVAILABLE
	SBOM diff / version comparison	AVAILABLE

CATEGORY	FEATURE	STATUS
Reporting	Executive PDF report per scan (charts, vulns, licenses)	AVAILABLE
	Portfolio PDF report (all scans, board-ready)	AVAILABLE
	Compliance framework mapping (CISA, NTIA, EO14028, EU CRA, PCI DSS)	AVAILABLE
	Prometheus metrics endpoint for monitoring	AVAILABLE
Security Controls	HSTS, CSP, X-Frame-Options security headers	AVAILABLE
	Rate limiting (per-IP, per-user, per-endpoint)	AVAILABLE
	Brute force protection with progressive lockout	AVAILABLE
	Password complexity (RBI/PCI DSS compliant)	AVAILABLE
	Session management (max concurrent, idle timeout)	AVAILABLE
	IP whitelisting with CIDR support	AVAILABLE
	Webhook notifications (8 event types, HMAC signed)	AVAILABLE
Administration	Role-based access control (Admin/Analyst/Auditor)	AVAILABLE
	Immutable audit trail with full action logging	AVAILABLE
	API key management for CI/CD integration	AVAILABLE
	Data retention auto-purge (configurable per entity)	AVAILABLE
Deployment	100% on-premise (Docker Compose)	AVAILABLE
	Air-gapped deployment support	AVAILABLE
	TLS/HTTPS with certificate management	AVAILABLE

6

Regulatory Compliance

How Kavach addresses every applicable regulation for Indian banks

REGULATION / STANDARD	REQUIREMENT	KAVACH CAPABILITY
RBI Master Directions on IT Governance (Apr 2024)	Software component visibility, vendor risk management, incident response preparedness	Full SBOM generation, TPRM supplier risk scoring, VEX for incident triage, audit trail
CERT-In SBOM Guidelines (Oct 2024, v2.0 Jul 2025)	SBOM with minimum data elements: component name, version, supplier, PURL, dependencies, vulns, licenses, hashes	CycloneDX 1.5 + SPDX 2.3 with all CERT-In mandatory fields populated automatically
PCI DSS 4.0 (Req 6.3.2, Mar 2025)	Maintain inventory of bespoke and custom software, including third-party components	Automated component inventory per scan. Portfolio-wide tracking across all applications
NIST CSF 2.0 (GV.SC category)	Supply chain risk management with software transparency	SBOM + VEX + TPRM + EPSS scoring for risk-based prioritization
EO 14028 (US Executive Order)	SBOM for all software sold to government; NTIA minimum elements	NTIA-compliant SBOMs with all minimum elements. CISA 2025 compliance badges
EU CRA (Cyber Resilience Act)	Vulnerability handling, SBOM for products with digital elements	EU CRA compliance tracking and VEX document generation
SEBI CSCRF	SBOMs for all software in core/critical business operations	Portfolio-wide SBOM management with compliance reporting
ISO 27001:2022 (A.8.28)	Secure coding, asset inventory, vulnerability management	Component inventory, vulnerability tracking, license compliance, audit log
IT Act 2000 / CERT-In Directions	6-hour incident reporting, 180-day log retention	SBOM enables rapid incident root cause analysis. Configurable data retention (365 days for audit logs)

RBI-Specific Compliance Advantage

Kavach is the **only SBOM platform** that maps its capabilities directly to RBI Master Directions and CERT-In guidelines. Commercial alternatives (Black Duck, Snyk, Sonatype) have no dedicated RBI compliance module — Kavach provides this out of the box for the Indian banking sector.

7

Artifacts & Deliverables

Files produced by every scan

ARTIFACT	FORMAT	STANDARD	PURPOSE
CycloneDX SBOM	JSON (.json)	CycloneDX v1.5	Machine-readable software inventory with components, versions, PURLs, hashes, suppliers, and dependencies
SPDX SBOM	JSON (.json)	SPDX v2.3	ISO/IEC 5962:2021 standard SBOM for international compliance and interoperability
VEX Document	JSON (.json)	CycloneDX VEX	Vulnerability Exploitability eXchange — communicates which CVEs are actually exploitable in your context
Scan PDF Report	PDF (.pdf)	Proprietary	Executive-grade report with donut charts, vulnerability histograms, risk gauges, component tables, license analysis, compliance statement
Portfolio PDF Report	PDF (.pdf)	Proprietary	Board-ready portfolio overview: all scans, aggregate risk metrics, cross-project vulnerability analysis
Audit Log Export	JSON / API	Internal	Complete API action trail: who did what, when, from which IP

CERT-In SBOM Minimum Data Elements Coverage

CERT-IN REQUIRED FIELD	KAVACH FIELD	STATUS
Component Name	name (CycloneDX/SPDX)	✓
Component Version	version	✓
Component Supplier	supplier.name / publisher	✓
Unique Identifier (PURL/CPE)	purl + cpe	✓
Author of SBOM Data	metadata.authors	✓
Timestamp	metadata.timestamp	✓
Component Dependencies	dependencies[] (full tree)	✓

CERT-IN REQUIRED FIELD	KAVACH FIELD	STATUS
Vulnerabilities with Severity	vulnerabilities[] with CVSS	✓
Patch Status	fix_available, fixed_in_version	✓
Component License	licenses[]	✓
Checksums / Hashes	hashes[] (SHA-256, SHA-1, MD5)	✓

8

Competitive Analysis

Kavach SBOM vs. industry-leading commercial platforms

FEATURE	KAVACH SBOM	BLACK DUCK (SYNOPSYS)	SNYK	FOSSA	MEND	SONATYPE LIFECYCLE	ANCHORE ENTERPRISE
CycloneDX SBOM	✓ v1.5	✓	✓	✓	✓	✓	✓
SPDX SBOM	✓ v2.3	✓	✓	✓	✓	✓	✓
VEX Document	✓ CycloneDX VEX	~ Limited	✗	✓	✓	✓	✓
EPSS Scoring	✓ Real-time	✓	✓	✓	✓	✓	✓
Dual-Scanner Engine	✓ Grype + Trivy	Single	Single	Single	Single	Single	Single (Grype)
Policy Engine / CI-CD Gate	✓ 8 policies	✓	✓	✓	✓	✓	✓
TPRM / Supplier Risk	✓ Built-in	~ Partial	✗	✓	~ Partial	~ Partial	~ Partial
Executive PDF Reports	✓ Charts + Gauges	✓	~ Limited	~ Limited	~ Limited	✓	✗
SBOM Diff / Comparison	✓	✓	~	~	~	✓	~
On-Premise Deployment	✓ Full	✓	✗ SaaS only	✓	~ Partial	✓	✓
Air-Gapped Support	✓	✓	✗	~	✗	✓	✓
RBI / CERT-In Compliance Mapping	✓ Native	✗	✗	✗	✗	✗	✗
Webhook Notifications	✓ 8 events	✓	✓	✓	✓	✓	✓

FEATURE	KAVACH SBOM	BLACK DUCK (SYNOPSYS)	SNYK	FOSSA	MEND	SONATYPE LIFECYCLE	ANCHORE ENTERPRISE
Immutable Audit Trail	✓	✓	✓	~	✓	✓	✓
License Compliance	✓	✓	✓	✓ **Best-in-class**	✓	✓	✓

Key Differentiators vs. Commercial Alternatives

1. **Dual-Scanner Engine** — Only platform running two independent scanners (Grype + Trivy) for maximum coverage.
2. **Native RBI/CERT-In Mapping** — No other platform offers built-in Indian regulatory compliance.
3. **Built-in TPRM** — Supplier risk scoring integrated directly — no separate TPRM tool needed.
4. **Full On-Premise / Air-Gapped** — Zero data leaves your network. Critical for banking data sovereignty.
5. **Executive PDF Reports** — Board-ready reports with charts, unlike most competitors which offer only dashboards.

9

Banking Security Controls

Security hardening built into every layer

🔒 Security Headers

HSTS with preload, Content-Security-Policy, X-Frame-Options DENY, X-Content-Type-Options nosniff, Referrer-Policy, Permissions-Policy, Cache-Control no-store for API responses.

⏱ Rate Limiting

Sliding window rate limiting: 100 req/min global, 10/min for auth, 10/5min for scans, 200/min per user. Configurable via environment variables.

🛡 Brute Force Protection

5 failed attempts trigger account lockout. Progressive escalation: 5 min → 15 min → 1 hour. Admin unlock capability. IP + username dual tracking.

🔐 Password Complexity

RBI/PCI DSS compliant: min 12 characters, uppercase + lowercase + digit + special char, no username inclusion, no common patterns, no sequential characters.

👤 Session Management

Max 3 concurrent sessions per user. 15-minute idle timeout. 8-hour absolute timeout. Oldest session eviction. Admin force-terminate capability.

🌐 IP Whitelisting

CIDR-based IP allowlisting. Restrict platform access to specific network ranges. Essential for bank internal network deployment.

🔔 Webhook Alerts

8 event types with HMAC-SHA256 signed payloads: scan completion, policy violations, critical vulns, account lockouts, login events. 3 retries with exponential backoff.

🗃 Data Retention

Automated data purge: audit logs 365 days, scan data 180 days, failed scans 90 days, expired tokens 30 days. Configurable. Scheduled background task.

Default Credential Detection

Kavach detects when users log in with factory-default passwords and forces a password change. This prevents production deployments from running with known credentials — a common audit finding.

10

Deployment Architecture

100% on-premise, containerized, bank-network isolated

Data Sovereignty Guarantee

Kavach runs entirely within your network. No telemetry, no cloud calls, no SaaS dependency. All source code, container images, and vulnerability databases can be pre-loaded for air-gapped deployments. Your SBOM data never leaves your infrastructure.

Component Architecture

COMPONENT	TECHNOLOGY	PORT	PURPOSE
Frontend	React + Nginx (HTTPS/TLS 1.2+)	3443	Web interface with security headers
Backend API	Python FastAPI	8000	REST API with all security middleware
Database	PostgreSQL 16	5432	Scan data, users, audit log, sessions
Analysis Engine	Dependency-Track	8080	Continuous vulnerability monitoring
SBOM Generator	Syft (by Anchore)	—	CycloneDX + SPDX generation
Scanner 1	Grype	—	Vulnerability scanning engine
Scanner 2	Trivy (Aqua Security)	—	Secondary vulnerability scanner

Minimum Hardware Requirements

RESOURCE	MINIMUM	RECOMMENDED (PRODUCTION)
CPU	4 cores	8 cores
RAM	8 GB	16 GB
Storage	50 GB SSD	200 GB SSD
OS	Any Docker-compatible (Linux/Windows)	RHEL 8+ / Ubuntu 22.04 LTS

RESOURCE	MINIMUM	RECOMMENDED (PRODUCTION)
Network	Intranet access only	Dedicated VLAN

11

Why Kavach for Your Bank

Summary recommendation

35+	100%	9
Enterprise Features	On-Premise	Regulations Mapped
Bank-grade security built-in	Zero data leaves your network	RBI, CERT-In, PCI DSS, NIST, EO14028...

🎯 Purpose-Built for Indian Banking

Kavach is the only SBOM platform with native RBI Master Directions and CERT-In SBOM guidelines mapping. No other tool — commercial or open-source — provides this out of the box. Your compliance team can immediately demonstrate audit readiness.

💰 Flexible Deployment with Full Customization

Kavach offers flexible deployment models with the ability to customize for your specific requirements. No vendor lock-in — your team retains full control over the platform, its roadmap, and its deployment model.

🔒 Bank-Grade Security from Day One

Every security control required for bank deployment is built-in: HSTS, CSP, brute force protection, progressive lockout, password complexity, session management, rate limiting, IP whitelisting, audit trail, data retention, and HMAC-signed webhooks. No additional hardening needed.

📈 Complete Supply Chain Visibility

Dual-scanner engine (Grype + Trivy), EPSS exploit probability scoring, built-in TPRM with supplier risk registers, policy governance gates for CI/CD, and SBOM diff tracking provide end-to-end supply chain risk management in a single platform.

Ready to Secure Your Software Supply Chain?

Kavach SBOM can be deployed in your bank's infrastructure within one business day.
Contact us for a live demonstration with your actual applications.

Enterprise Software Supply Chain Security

contact@mphatek.com

Kavach SBOM — Banking Edition v3.1.0

Prepared by mPhatek Systems Pvt. Ltd. | February 2026

This document contains proprietary information and is intended solely for the recipient organization. Redistribution without written consent is prohibited.