Full-cycle application security testing to protect patient data, clinical software, and regulated development pipelines

Healthcare organizations run some of the most complex software environments in any industry – patient-facing systems, clinical pipelines, billing integrations, connected devices – many of them built years apart, on different stacks, by different teams. Keeping all of it secure is not a one-time project.

$7.42M

avg. healthcare breach cost in 2025

279 days

avg. time to identify & contain a healthcare breach

76%

of healthcare breaches involve web app attacks or application-layer errors

DerScanner is a full-cycle application security testing platform (SAST, DAST, SCA, Supply Chain Security) that enables healthcare organizations to analyze proprietary code in 43 programming languages, including rare ones, audit open-source dependencies with automatic SBOM generation, and inspect third-party binary components without source code access – all from a fully on-premise, air-gapped deployment

Core challenges facing healthcare software security

Challenge 1

Legacy and modern stack side by side

A dental network runs patient portals in PHP, billing in Delphi, DICOM viewers in C++. A biopharma company runs COBOL in manufacturing, ABAP in SAP, Java, Python microservices in LIMS – often in the same environment.

Scanning only the modern stack leaves the most sensitive modules unreviewed. CTMS, eLab notebooks, SAP pipelines, cardiac monitoring platforms with hard-coded credentials, IoT firmware compiled without source code – each requires its own analysis approach.

Challenge 2

Regulatory obligations that require evidence

HIPAA, PCI DSS 4.0.1, GDPR, 21 CFR Part 11, EMA Annex 11, EU MDR – each framework asks a version of the same question: can you show what was scanned, who reviewed it, and what was done about it?

A pentest report from six months ago and a flat findings list don't answer that question. Regulators want a repeatable process, timestamped evidence, and clear ownership of every vulnerability.

Challenge 3

Blind spots in supply chain and third-party code

Open-source libraries in clinical pipelines, compiled firmware from suppliers, COTS components from acquisitions – all carry risk that isn't visible until something breaks.

A compromised dependency in a validated system can leak data or trigger a regulatory notification. Supplier binaries with decade-old vulnerabilities still reach production in pharmacy manufacturing systems.

How DerScanner Addresses Each Challenge

Secure the full stack

DerScanner covers 43 languages in a single scan – Delphi, COBOL, ABAP, Perl, Pascal, alongside the modern stack. Binary analysis of .dll, .exe, .apk, and .ipa files covers components delivered without the source code.

Analyze every layer of your healthcare software without switching tools or leaving gaps:

- **SAST for Delphi, COBOL, ABAP, PL/SQL** in legacy clinical and manufacturing systems
- **SAST for Java, Python, Go, PHP** in modern backends and APIs
- **MAST for iOS and Android** patient-facing mobile apps
- **DAST for runtime testing** of web applications and APIs
- **Incremental scans in CI/CD on every commit** – shift security left without slowing delivery

Verify Components

Every finding maps to HIPAA, PCI DSS 4.0.1, OWASP, and CWE directly in the interface. The event log records who reviewed what and when.

Assess supplier deliverables and COTS medical software even without the source code:

- **Binary analysis of .dll, .exe, .apk, and .ipa files** from Tier-1/Tier-2 suppliers
- **Unified vulnerability reports** across own code and supplier deliverables
- **Findings mapped to CWE and OWASP** for standardized supplier benchmarking
- **Coverage of codebases and components** obtained through M&A without the source

Control Open Source Risk

SCA continuously tracks dependencies against CVEs, and scores supplier health across 8 risk metrics. Hybrid SAST+SCA call-graph analysis shows which vulnerable functions your code actually calls – separating real risk from background noise.

Track what's in your dependencies before it reaches production:

- **SCA with SBOM generation** (CycloneDX) for Python, Java, Go, Rust, JS/TS, C/C++ and more
- **Hybrid SAST+SCA call-graph analysis** – shows which vulnerable functions are actually reachable
- **Supply Chain scoring** across 8 risk metrics: MavenGate, Starjacking, Typosquatting
- **License risk analysis** for procurement policy compliance

Regulatory & standards coverage

HIPAA §164.312

SAST, DAST, and on-premise scanning support ePHI technical safeguard compliance

PCI DSS 4.0.1

CI/CD scanning satisfies Req. 6.4.2; SCA generates SBOM for Req. 6.3.2

EMA Annex 11

Vendor qualification dossier available for regulated pipeline validation

GDPR Art. 32 + NIS2

On-premise deployment satisfies Art. 44; healthcare is essential entity under NIS2

21 CFR Part 11 (FDA)

Timestamped per-vulnerability event log supports electronic records audit trail

EU MDR IEC 62304

Per-commit scan records support continuous cybersecurity risk management evidence

Why DerScanner

Wide language coverage

Delphi in dental PMS, COBOL in manufacturing, ABAP in SAP pipelines, modern Python and Java alongside them. DerScanner covers the full stack in a single platform – so nothing goes unreviewed by default.

On-premise & air-gapped deployment

Runs inside your own infrastructure. Source code, scan results, and AI modules never leave the network.

Supports air-gapped environments.

AI triage & automated remediation

DerTriage cuts false positives by up to 90% using real-world exploitability data to let developers focus on what actually matters. DerCodeFix shows how to fix it, inline. Both run offline.

Audit trail, RBAC & finding lifecycle

Every finding tracked from discovery to close – owner, status, timestamps. System-level events forward via syslog CEF. Role-based access scoped per project, including read-only auditor views.

Supply Chain & SCA

Open-source dependencies tracked against CVEs continuously. Supply Chain health scored across 8 risk metrics. Call-graph analysis shows which vulnerable functions your code actually reaches.

Audit-ready compliance reports

Findings mapped to HIPAA, PCI DSS 4.0.1, OWASP, and CWE.
Export to PDF or CSV, and hand it over – for OCR, QSA, or IQ/OQ/PQ packages.

Vendor risk & source code trust

Your source code stays in your environment.

Vendor security assessment materials available upon request at company@derscanner.com

Binary analysis without source code

Executable .dll, .exe, .apk, and .ipa files from suppliers or acquisitions can be scanned directly.

No source code needed.

DerScanner is a MITRE certified and NIST recommended solution.

With over a decade of expertise in application security, DerScanner provides powerful analysis capabilities in an easy-to-start setup.

NIST MITRE

Contact us at company@derscanner.com