N NSAUDITOR AI

ENTERPRISE EDITION · NETWORK SECURITY AUDITING SINCE 2004

# One scan. Six compliance evidence packs. Zero data exfiltration.

NSAuditor AI Enterprise is an AI-assisted network and cloud security auditor that turns your AWS, Azure, and GCP accounts into signed, timestamped, framework-mapped compliance evidence — entirely on your own infrastructure.

SOC 2 | HIPAA §164.312 | NIST CSF 2.0 | PCI DSS v4.0.1 | ISO/IEC 27001:2022 | CIS Controls v8

**28**
scanner plugins
network + multi-cloud

**6**
compliance frameworks
from a single scan

**3**
clouds audited
AWS · Azure · GCP

**0**
bytes of scan data
leave your infrastructure

WHY NSAUDITOR AI ENTERPRISE

# Your auditors will ask for proof. Your scanner shouldn't leak it.

SOC 2 auditors, HIPAA assessors, PCI DSS QSAs, ISO/IEC 17021-1 certification bodies, CIS self-attestation tooling, and cyber-insurance underwriters all ask the same question: *can you prove your cloud enforces the controls you claim?* Most teams answer with screenshots and spreadsheets — or with SaaS scanners that upload their security posture to someone else's cloud.

NSAuditor AI Enterprise answers differently. One scan generates **six signed, timestamped, framework-mapped evidence packs in parallel** — and no ePHI, no cardholder data, no cloud credentials, and no scan data ever leaves your infrastructure. **Zero BAA required.**

### ■ Security-first by architecture, not by policy

Local-first execution · cloud auditing with **read-only, least-privilege credentials** (AWS ReadOnlyAccess/SecurityAudit, Azure Reader, GCP Viewer) · Zero Data Exfiltration policy engine with data classification, external-call guard, and full audit logging · air-gapped deployment for federal-contractor / DFARS / CMMC environments and payment-processing CDE isolation.

## HOW IT WORKS

STEP 01 — INSTALL

### Deploy in minutes

npm package, Docker images (amd64 + arm64), or offline tarballs with bundled NVD feeds for air-gapped networks.

STEP 02 — SCAN

### Audit network + clouds

28 plugins fan out across hosts, services, TLS, DNS/email, and your AWS, Azure & GCP accounts — every account-enabled region, verified findings, MITRE ATT&CK mapped.

STEP 03 — EVIDENCE

### Hand packs to auditors

Six framework-mapped evidence packs with per-control coverage, explicit gaps, RFC 3161 trusted timestamps, and Ed25519-signed suppressions.

```
$ nsauditor scan --cloud aws --aws-region all --compliance soc2,hipaa,nist,pci,iso27001,cis
```

## WHAT MAKES IT DIFFERENT

### ■ Verified, not guessed

Findings are confirmed with safe, non-destructive probes instead of raw version matches — reports your engineers won't dismiss as false-positive noise.

### ■ No silent false-cleans

When evidence can't be collected — truncation, AccessDenied, missing SDKs — the affected controls fail closed and the gap is disclosed. A clean report means it was actually checked.

### ■ AI that stays home

AI-assisted analysis and prioritization run with your own API keys under the ZDE policy engine, with policy-based redaction of sensitive values before any model call.

### ■ Open-core foundation

Built on the MIT-licensed NSAuditor AI Community Edition — inspect the scanner core, extend it, and avoid black-box lock-in.

ENTERPRISE CAPABILITIES

# Everything compliance-grade auditing needs, in one platform

### Multi-Cloud Scanners

AWS security groups, IAM Deep Auditor, S3/KMS/CloudTrail/Lambda/RDS and more · GCP firewall rules, IAM bindings & Cloud Storage · Azure NSGs, RBAC & Storage. Multi-region fan-out across every account-enabled region — using your own read-only credentials.

### Hexa-Framework Compliance Engine

Findings map to SOC 2, HIPAA Security Rule, NIST CSF 2.0, PCI DSS v4.0.1, ISO/IEC 27001:2022 and CIS Controls v8 — gap reports with evidence references, per-control coverage discipline, and explicit out-of-scope declarations.

### Docker Scan Isolation

Each scan runs in an ephemeral container — isolated, parallel, destroyed after completion, on a read-only filesystem with resource limits.

### Zero Trust Assessment

Segmentation boundaries, encryption-in-transit, identity posture, and lateral-movement risk — rolled into a composite readiness score.

### Air-Gapped Deployment

Docker images (amd64 + arm64), offline NVD vulnerability-feed bundles, and installation tarballs. Runs in fully isolated networks — built for DFARS / CMMC and CDE-isolated payment environments.

### ZDE Policy Engine

Data classification (public / internal / sensitive / secret), external-call guard, policy-based redaction, and full audit logging — Zero Data Exfiltration, enforced in code.

### Enterprise CTEM

Continuous threat-exposure management on a PostgreSQL backend: unlimited scan-history retention, a query API for historical analysis, and compliance dashboards that show drift between audits.

### MCP Server for AI Agents

First-class Model Context Protocol integration: drive scans, query vulnerabilities, and produce compliance evidence from Claude and other AI agents — with the same ZDE guarantees.

### Built for evidence integrity

RFC 3161 trusted timestamps on evidence packs · Ed25519-signed finding suppressions with reviewer trails · conservative classification — anything unverifiable is labeled an evidence gap, never silently passed · native push to GRC platforms (e.g. Vanta) when *you* choose to share.

COMPLIANCE COVERAGE

# Six frameworks. Honest coverage. No theater.

Every framework matrix declares exactly which controls the scanner covers, which it partially evidences (with documented manual procedures), and which are architecturally out of scope for any infrastructure scanner. Auditors notice the difference.

| Framework | Covered | Partial | Scope & notes |
|---|---|---|---|
| **SOC 2 (AICPA TSC)** | 10 | 4 | Auditor-ready pre-audit evidence; PARTIAL controls carry AT-C 320 manual procedures; WORM storage validation |
| **HIPAA Security Rule §164.312** | 7 | 3 | Technical Safeguards with R/A discipline + HHS-OCR priority view · **Zero BAA required** |
| **NIST CSF 2.0 (CSWP 29)** | 13 | 10 | Subcategory-level coverage across 106 of 107 Subcategories; Govern function OOS-by-design |
| **PCI DSS v4.0.1** | 20 | 8 | Sub-requirement level (MVP-67), QSA-oriented views, CDE scoping badges, TPSP matrix |
| **ISO/IEC 27001:2022** | 17 | 14 | All 93 Annex A controls classified; Statement-of-Applicability discipline; 2013→2022 transition mapping |
| **CIS Controls v8** | 17 | 22 | Per-Safeguard over 153 Safeguards / 18 Controls; cumulative IG1–IG3; CSAT / CIS-CAT compatible attestation |

Counts current as of EE 0.19.3 (June 2026). Remaining controls per framework are explicitly declared out-of-scope (e.g. physical security, workforce training, governance paperwork) — domains no infrastructure scanner can honestly evidence. Full matrices: nsauditor.com/ai/docs/

### For compliance teams

One scan replaces six evidence-collection sprints. Per-control citations, gap lists your engineers can action, and an audit trail of what was checked, when, and how.

### For your underwriter

The CIS IG1 attestation cyber-insurance underwriters increasingly require — generated from live infrastructure evidence, not questionnaire answers.

### For regulated industries

Healthcare (no-BAA HIPAA evidence) · payments (CDE-isolated PCI auditing) · federal supply chain (air-gapped DFARS/CMMC deployment) · certification-bound ISMS programs (ISO 27001 SoA).

### For engineering teams

SARIF / JSON / HTML / CSV outputs, CI-friendly CLI, MCP tools for AI agents, and findings ranked by verified exploitability — not raw CVSS noise.

EDITIONS & PRICING

# Start free. Scale to enterprise.

Open-core licensing: the Community Edition is MIT-licensed and free forever. Pro adds verification and intelligence. Enterprise adds the cloud scanners, the compliance engine, and deployment controls.

| | **Community** open source | **Pro** for practitioners | **Enterprise** for organizations |
|---|---|---|---|
| Price | **Free** · MIT license | **$49** /mo | **from $2,000** /yr |
| Scanner plugins | Full Community set | Everything in Community | All 28 incl. cloud auditors |
| Vulnerabilities | AI analysis (your keys) | Offline CVE matching (NVD) + verified findings via safe probes | Everything in Pro + cloud misconfiguration auditing |
| Compliance | — | — | Six-framework evidence engine |
| Deployment | npm · MCP server | + risk scoring & prioritization | + Docker isolation · air-gapped · CTEM/ PostgreSQL · ZDE policy engine |

ENTERPRISE TIERS — ANNUAL INVOICING · NET-30 · VOLUME DISCOUNTS

| **Base — $2,000/yr** | **Growth — $5,000/yr** | **Scale — $10,000+/yr** |
|---|---|---|
| ✓ Up to 5 seats / scanning nodes<br>✓ Full Enterprise feature set<br>✓ Email support<br>✓ Onboarding call included | ✓ Up to 25 seats / scanning nodes<br>✓ Everything in Base<br>✓ Dedicated Slack / email channel<br>✓ Priority response · custom compliance-mapping help | ✓ Unlimited seats · custom SLA<br>✓ 4-hour critical / 24-hour standard<br>✓ Dedicated support engineer<br>✓ Custom plugin development |

All Enterprise tiers include everything in Pro. Pricing current as of June 2026 — see nsauditor.com/ai/pricing/ for the live page. Custom requirements: enterprise@nsasoft.us

### ■ Procurement-friendly

Annual invoicing with net-30 terms · perpetual-style license keys delivered instantly on purchase · read-only credential requirement written into the EULA — your security team will approve of our least-privilege defaults.

RESELLER PARTNER PROGRAM

# Turn cybersecurity into recurring revenue

MSSPs, cloud-security consultants, GRC advisors, and DevSecOps teams resell NSAuditor AI Enterprise to offer clients multi-cloud AI security auditing and six-framework compliance evidence — under your engagement, on the client's infrastructure, with zero data ever reaching us *or* you.

### ■ Why partners choose NSAuditor

A differentiated, privacy-first story your clients' security teams approve quickly · evidence packs that plug straight into the audits you already run · margin on every seat plus services revenue on remediation.

### ■ What you get

Partner pricing, co-branded collateral, direct engineering support channel, and the same dedicated onboarding we give enterprise customers. Program details: nsasoft.us/partners/

TWO DECADES OF NETWORK SECURITY AUDITING

Nsasoft shipped the first **Nsauditor Network Security Auditor** for Windows in **2004** — years before "network security audit" became standard industry vocabulary. Twenty-two years later, that experience powers an open-core, AI-assisted platform trusted to audit production clouds without ever seeing them. We've held page-one search positions for network security auditing for most of two decades — because the product keeps earning it.

### ■ See it run in 30 seconds

Sample scan output (no signup): **nsauditor.com/ai/docs/sample-scan/** · Getting started guide: **nsauditor.com/ai/docs/getting-started/** · Free Community Edition: `npm install -g nsauditor-ai`

### ■ Contact

Enterprise & partner inquiries: **enterprise@nsasoft.us**
Support: **support@nsauditor.com**
Web: **nsauditor.com/ai/enterprise/**
Nsasoft US LLC · Las Vegas, NV, USA

### ■ Follow the engineering

X: **@Nsasoft** · LinkedIn: **NSAuditor.ai**
GitHub: **github.com/nsasoft/nsauditor-ai**
Release notes, coverage-matrix changes, and audit-engineering deep dives ship with every version.