SYNAPSE

NetscanXi

Version 13

Self-hosted network discovery, vulnerability & compliance intelligence

Turn one network scan into a board-ready compliance posture.

Synapse-NetscanXi maps every device, service, container and vulnerability on your network — then cross-references each finding against **eight regulatory frameworks**. Self-hosted, multi-tenant, and deployed with a single `docker compose up`. Your data never leaves your infrastructure.

New in Version 13: 🔧 **Patch and Remedy** — apply **operating-system updates & upgrades** (apt / dnf / yum / zypper / apk, auto-detected) over SSH to a single asset, an asset group, or every asset — or update Docker images. Synapse-NetscanXi now **acts** on what it finds, **auto-creates and updates a remediation record** for every run, and uses **per-run credentials that are never stored**. Don't just find the risk — fix it.

NCSC CAF | NIST CSF | PCI DSS | GDPR | ISO 27001 | SOC 2 | HIPAA | Cyber Essentials

Why Synapse-NetscanXi

Compliance, not just a scan

Every finding maps to named controls across 8 frameworks — the only affordable self-hosted tool with native **NCSC CAF** mapping.

Built for MSPs & multi-team

True multi-tenancy: one install, many isolated client tenants with scoped data. White-label-friendly recurring revenue.

Your data stays yours

100% self-hosted on Debian. No cloud, no per-asset metering, no data egress — ideal for public sector & CNI.

Evidence on demand

Branded executive & per-host PDF reports for audits, ticketing and system owners — generated from a single scan.

Capabilities

- **Asset discovery** — live hosts, OS, services & software inventory
- **Vulnerability scanning** with CVE enrichment & CISA KEV tagging
- **Risk scoring** + tailored, official mitigation guidance
- 🔧 **Patch and Remedy (v13)** — OS updates/upgrades over SSH (+ Docker images) per asset / group / all, auto-tracked, with credentials never stored
- 🐳 **Deep Docker scanning (v10r1)** — container & image inventory, image CVE scanning (Trivy/Grype), CIS Docker audit
- **AD / DC & TLS certificate** auditing and expiry tracking
- **Change detection** & alerting between scans
- 📡 **Passive (zero-probe) discovery** for sensitive / OT segments **(v9)**
- 🆔 **Unique asset IDs bound to MAC** — de-duplicated vuln tracking **(v9)**
- 🗓️ **Day & time scheduling** + editable asset type **(v9)**
- **Accounts · Roles · TOTP MFA · Activity audit log**

Who it's for

Buyer	The win
MSPs / MSSPs	One install, many tenants. Resell continuous scanning & compliance as a managed service.
UK public sector & OES	NCSC CAF posture from a scan. Fully self-hosted — data never leaves the network.
Enterprise security	NIST CSF + PCI / ISO / SOC 2 / HIPAA mapping without a per-asset cloud bill.
SMB & IT teams	Enterprise-grade visibility from `docker compose up` — no heavy tooling.

How it compares

	Synapse-NetscanXi	Typical scanner
Self-hosted	✓ Yes	Often cloud
Multi-tenant	✓ Built-in	Add-on / no
8-framework mapping	✓ Incl. CAF	Rare
Passive (zero-probe) mode	✓ Built-in	Rare
Deep container scanning	✓ Built-in	Add-on / no
Per-asset fees	✗ None	Common
Deploy time	Minutes	Hours+

Deploy in minutes

One command: `docker compose up` on Debian. Then point it at your network and export your first branded compliance report the same day.

Flask + nmap | Single-container | No cloud dependency | Free community tier | Pro & MSP licensing

🔧 New in Version 13 — Patching & Remediation

🖥️ OS updates & upgrades over SSH
The **Patch and Remedy** tab auto-detects the package manager (apt / dnf / yum / zypper / apk) and applies updates — with optional full distribution upgrade and a simulate (no-change) mode.

🐳 Docker image updates
Or update Docker images: pulls the latest image for every running container over the same authenticated Engine API used for scanning, with an optional experimental recreate.

🔒 Credentials never stored
SSH/sudo and registry credentials are entered per run, used once, then discarded — never written to the database, never logged, never returned.

📝 Auto-tracked remediation
Every patch run creates a remediation item per asset and updates it to **resolved** or **blocked** — one source of truth for what was fixed, by whom.

👁️ Dry-run preview
Preview the targeted assets and detected OS (or images) with zero side effects — OS preview doesn't even contact SSH — before you commit.

🛡️ Role-gated & tenant-safe
Patching requires the operator role; scoped users can only ever target their own tenant's assets.

🐳 New in Version 10r1 — Deep Docker Container Scanning

📦 Authenticated container & image inventory
Agentless Docker Engine API inventory — containers, images, ports, privileged flags, docker.sock mounts and engine posture.

🔎 Image vulnerability scanning
Per-image CVE scanning via **Trivy**/**Grype**, enriched with **CISA KEV** so exploited container CVEs rank first.

🛡️ CIS Docker benchmark audit
Exposed API, no-TLS daemon, privileged containers, socket mounts, host net/PID, insecure registries — pass/warn/fail.

📊 Docker dashboard & host views
A dedicated Docker dashboard panel plus deep per-host container detail — with every existing view kept.

🔄 Container drift detection
Flags new/removed containers, new-privileged or socket-mount changes, and new known-exploited image CVEs between scans.

📝 SBOM, registry & orchestration
SBOM-capable scanning, insecure-registry flags and Swarm / Kubernetes awareness.

✨ New in Version 9.1

📊 Customisable interactive charts
OS distribution, vulnerability severity, network risk & compliance and regulatory compliance now sit in equal-sized tiles — switch any chart between **pie**, **horizontal** or **vertical bars**, resize and rearrange the tiles, then click a slice to filter the asset table.

✅ Vulnerability lifecycle management
Mark CVE findings **Remediated**, **Accepted Risk** or **False Positive** — cut the noise, track remediation and prove progress to auditors.

☑️ Multi-select asset table
Act on many assets at once: bulk export and bulk re-scan in a couple of clicks instead of one host at a time.

👥 Tenant Admin role
Delegate full administration inside a tenant for true multi-tenant operations — MSP/MSSP-friendly, with hard tenant isolation.

🔍 Global search

🗄️ Configurable data retention
Set retention policies right in the Admin UI — control database growth and meet data-governance requirements.

🩹 Patch-aware scanning
Assess against installed patch levels, not just the distro version — dramatically more accurate results with far fewer false positives.

📈 Historical trend graphs
Track network risk score and compliance posture as a historical trend line — or switch the same tile to a pie or bar view — to show measurable improvement over time.

🎟️ Native ITSM integrations
Jira, ServiceNow and Zendesk — open remediation tickets for findings without ever leaving Synapse-NetscanXi.

🧩 Customisable dashboard
Drag, drop, pin or hide components — and resize, reorder and re-style each chart tile — so every team sees exactly what matters to them. Layout persists per user.

Find any asset, CVE or software across the whole estate instantly from the top bar.

Synapse-NetscanXi — see your network *and* your containers the way an auditor would.

Free community tier · Pro (per-install) · MSP licensing (per managed network). Self-hosted — your data, your infrastructure.

Book a demo