SAMURAI Networks

Discipline in every packet.

Company & Product Briefing

2026

Too many devices, too little visibility.

Every added firewall, switch, and controller is another panel to check. Teams end up with fragments of visibility, no continuous monitoring, no way to correlate or trace an anomaly across the estate, and no clean record to prove compliance.

WHY NOW

Security tooling hasn’t kept up with multi-vendor infrastructure.

$30B+

Global network security & monitoring market, 2026

12%

Projected CAGR through 2030 as hybrid estates grow

70%

Of enterprises now run 3+ network security vendors side by side

Figures are illustrative market estimates for planning purposes.

THE SOLUTION

Single control plane across the entire network.

SAMURAI unifies firewalls, fabric controllers, identity services, hypervisors, routers, and switches into a single dashboard.

Discover every point. **Trace** every path. **Detect** every change.

10+ vendor families, native integrations, not screen-scraped, not agent-based.

CAPABILITIES

Six primitives, one platform.

01 · Discovery

Find every endpoint

Correlates MAC, IP, ARP, DHCP, CDP/LLDP, and 802.1X across every switch, router, and fabric controller.

02 · Analysis

Hop-by-hop trace

5-tuple path simulation across routers, switches, and firewalls, evaluating ACLs from live config.

03 · Monitoring

Smart change detection

Compares real device state, not audit logs. Noise filtered automatically; only meaningful diffs stored.

04 · Performance

Sub-second queries

Cache-first architecture with background sync. Updates as fast as the network changes.

05 · Reliability

Clustering & failover

Cluster controllers with automatic primary election and configurable thresholds.

06 · Compatibility

Auto-detect every platform

IOS, NX-OS, IOS-XR, PAN-OS, FMC, ASA: automatically identified, profiled, and queried.

DISCOVERY

Find every endpoint, automatically.

One correlated table, built live from MAC tables, ARP, DHCP, and fabric data across every vendor.

MAC	IP	Vendor	Switch
00:1a:2b:3c:4d:5e	10.10.3.42	Cisco	n9k-leaf-04
48:f8:b3:11:22:33	10.10.3.87	Dell	cat-9300-15
a4:bf:01:aa:bb:cc	10.20.1.12	HP	n9k-spine-01
00:50:56:9c:14:b2	10.20.5.42	VMware	n9k-leaf-02
fc:ec:da:88:99:aa	10.10.4.21	Ubiquiti	cat-9300-15

MONITORING

Change detection that filters the noise.

SAMURAI compares real device state, not audit logs. Volatile noise is filtered automatically, and only meaningful diffs are stored.

AI ANALYSIS

An AI agent that learns your network.

- Auto-curated network memory, learned as durable facts.
- Every change classified by severity, so real anomalies surface.
- Self-auditing, human-in-the-loop: edit or lock any fact.
- Runs on your model, on-prem or cloud, your choice.

core-leaf-03 · mac_table +7 −6 ROUTINE · SUPPRESSED

VM mobility matches a learned SAFE memory. No alert raised.

edge-fw-1 · security_policy +1 −2 REVIEW · MEDIUM

New permit rule to 0.0.0.0/0 with no matching memory. Surfaced for review.

DEPLOYMENT

Five minutes to full visibility.

- Your data never leaves your perimeter. Ever.
- One self-contained container. Runs on a single VM.
- Free test license, no email required.

```
$ docker run -d \
--name samurai \
-p 443:443 \
beyrak44/samurai

Dashboard ready · 00:04:52
```

THE HONEST COMPARISON

Your incumbent covers part of the job.

We concede where AlgoSec is stronger, and show where a six-dashboard stack quietly loses the audit trail.

Capability	SAMURAI	AlgoSec	Tufin	ManageEngine
Multi-vendor topology in one pane	✓	✗	✗	✗
Endpoint & identity discovery	✓	✗	✗	✗
Config diff without an agent	✓	✗	✗	n/a
Air-gapped deployment	✓	✗	✗	n/a
Firewall policy analysis	✓	✓	✓	✓
Policy change automation & push	✗	✓	✓	✗
Docker single-container install	✓	✗	✗	✗

INTEGRATIONS

Route every event where your team already works.

CHAT & ALERTING

- Slack
- Microsoft Teams
- Telegram
- Discord
- Email (SMTP)

OPS & TICKETING

- Syslog (SIEM)
- Webhook
- Jira
- TheHive

AI MODELS

- Claude (Anthropic)
- OpenAI / compatible
- Amazon Bedrock
- Ollama (local)

PROOF IN THE NUMBERS

Built to hold up under real load.

10+

vendor families, native integrations

<400ms

p50 query latency, cache-first architecture

5 min

to first dashboard, one docker run

BUSINESS MODEL

Self-hosted, no lock-in.

TRIAL

Free evaluation

- Self-hosted, single node
- Core discovery & tracing
- Time-limited license, no email required

TEAM

Annual license

- Clustering & failover
- Alerting integrations, SSO/LDAP
- Priority support

ENTERPRISE

License + support

- AI analysis, on-prem or cloud model
- Air-gapped deployment
- Dedicated support & onboarding

TEAM

The people behind it.

Small team. Big ambitions. Real-world network experience.

BA — **Beyrak A.**
Founder & Security/System Engineer

DK — **Dashgin Kh.**
Co-Founder, Software Engineer

TA — **Turkan A.**
Security Engineer

MA — **Mahammadali A.**
Security Engineer

+7 — **Plus 7 more**
Engineers & Operators

TAKE THE DEMO

Your network deserves discipline.

See SAMURAI run against your real environment. Most demos are scheduled within 24 hours.

nometa.az/en/contact

info@nometa.az

SAMURAI

SAMURAI Networks