nagomi

PLATFORM DATA SHEET

Agentic Exposure Operations

Prevent the preventable breach.

4 min
mean AI investigation time
vs. hours of manual triage

49%
reduction in open exposure cases
via autonomous re-verification

Balance restored.
When adversaries move,
you have already made yours.

What Nagomi Is

Nagomi is the Agentic Exposure Operations platform that gives organizations a unified view of every exposure, powered by a team of AI Exposure Eliminators. Nagomi continuously reconstructs the environment from an attacker's perspective — identifying what scanners miss, what CMDBs overlook, and what remains undocumented.

01
Discover
Connect to 100+ tools via read-only APIs. Unified picture in days.

02
Detect
CVE + missing control + critical asset = exposure. 80K findings → 996 real exposures.

03
Investigate
Agent mirrors a senior analyst: threat intel, campaign, control check.

04
Neutralize
Optimal fix chosen — patch, config, or control. One click to authorize.

05
Verify
Rescan confirms closure. If exposure resurfaces, a new case triggers.

06
Report
Board-ready evidence. Program ROI. Security earns a seat at the table.

The Problem

- **Tool Fragmentation** — silos between EDR, scanners, identity, and cloud
- **Manual Correlation** — weeks of analyst work to answer one exposure question
- **Alert Overload** — 80K findings, no context, every CVE looks equal
- **No Verified Closure** — tickets marked done, exposures still open

Who It's For

- Enterprise CISOs managing fragmented stacks and exposure overload
- Security Operations teams drowning in isolated findings and reactive triage
- Vulnerability Management programs that need to close risk, not just rank it
- Security Engineering and IT teams that need one authoritative source of truth

Mission: prevent the preventable breach
Aligned with CTEM, Unified Exposure Management, and ASCA frameworks

CAPABILITIES · DIFFERENTIATORS · INTEGRATIONS · OUTCOMES

nagomi

Five Pillars

Always-On Discovery
Every asset enriched with every tool that touches it. Normalized, correlated, deduplicated. Nothing new goes unnoticed.

Exposure, Not Vulnerabilities
CVE + missing control + critical asset = exposure. 80,000 findings become 996 real exposures. Toxic combinations surface in real time.

Agentic Investigation
Agent mirrors a senior analyst: threat intel, campaign attribution, vuln validation, control check. Mean time: 4 minutes.

Respond and Verify
Routing follows your rules. Validation runs on every rescan. If exposure resurfaces, a new case triggers automatically.

Enable the Business
Board-ready evidence. Coverage gaps surfaced. Program ROI quantified. Security earns a seat at the table.

What Makes Nagomi Different

AI Exposure Eliminators
Agents that mirror a senior analyst at scale — autonomous where it counts, with the team keeping the final call on every action.

Exposure, not CVEs
Tracks misconfigs, identity gaps, control failures, and toxic combinations alongside CVEs — the full exposure surface.

No agents, no rip-and-replace
Connects through read-only APIs to tools already deployed. Unified exposure picture builds in days, not quarters.

Validated closure, not ticket closure
Nagomi verifies from the sensor itself that a fix holds. Configuration drift and silent failures caught before attackers find them.

Integrations (100+)

EDR / Endpoint
CrowdStrike, Microsoft Defender, PANW Cortex XDR, SentinelOne

Vulnerability Mgmt
Tenable (Nessus, io, sc), Qualys, Rapid7

Identity & Access
Entra ID, Active Directory, Intune, CyberArk EPM, BeyondTrust

Cloud Security
Wiz, Microsoft Defender for Cloud, Cyera

Network
Guardicore, Zscaler, Netskope CASB, Cloudflare, Cisco ISE

ITSM
ServiceNow, Jira — enriched tickets, custom field mapping

Patch / IT Ops
Automox, NinjaOne, LanSweeper

SaaS · Secure Gateway (on-prem) White-label MSSP · Multi-tenant

Proven Outcomes

4 min
Mean agentic investigation time

2.5 mo → daily
Threat-mapping cycle (major tech provider)

49% fewer
Open exposure cases (large manufacturer)

89% coverage
Unified exposure view (global hospitality)

Hours
Time to first POC value (leading insurer)

879 hrs
Analyst hours saved per year