nagomi

## NAGOMI EXPOSURE OPS PLATFORM

# Eliminate the exposure your tools leave open.

Nagomi runs the work from investigation to verified resolution before it becomes backlog or gets exploited. Every issue is completed and re-validated so it actually holds.

### Adversaries see what your tools miss. They move in minutes. Manual triage takes weeks. That gap is where breaches happen.

**Signals missed**
Exposures hide between tools. No single view across vulnerabilities, controls, and threat intel. Gaps stay invisible until something breaks.

**Cases backlogged**
Analysts manually cross-reference scanners, CMDBs, and threat feeds. The same 30-minute investigation, every time.

**Fixes stalled**
Tickets without context. No ownership mapping. Engineers spend hours reconstructing relevance before anyone acts.

## The loop runs. Exposure closes. Nothing gets added to the backlog.

Nagomi replaces the manual investigation, triage, and coordination that keep exposure open. Agents analyze, direct, and carry work forward.

### Identify what's exposed

Signals are correlated across assets, controls, threats, and exposures, so teams work what actually needs action, not another CVSS-based list.

### Move faster with less effort

The agent runs the full workflow: resolves the CVE, pulls exploit status, checks compensating controls, identifies affected assets, and prepares owner-assigned tickets.

### Know it's truly resolved

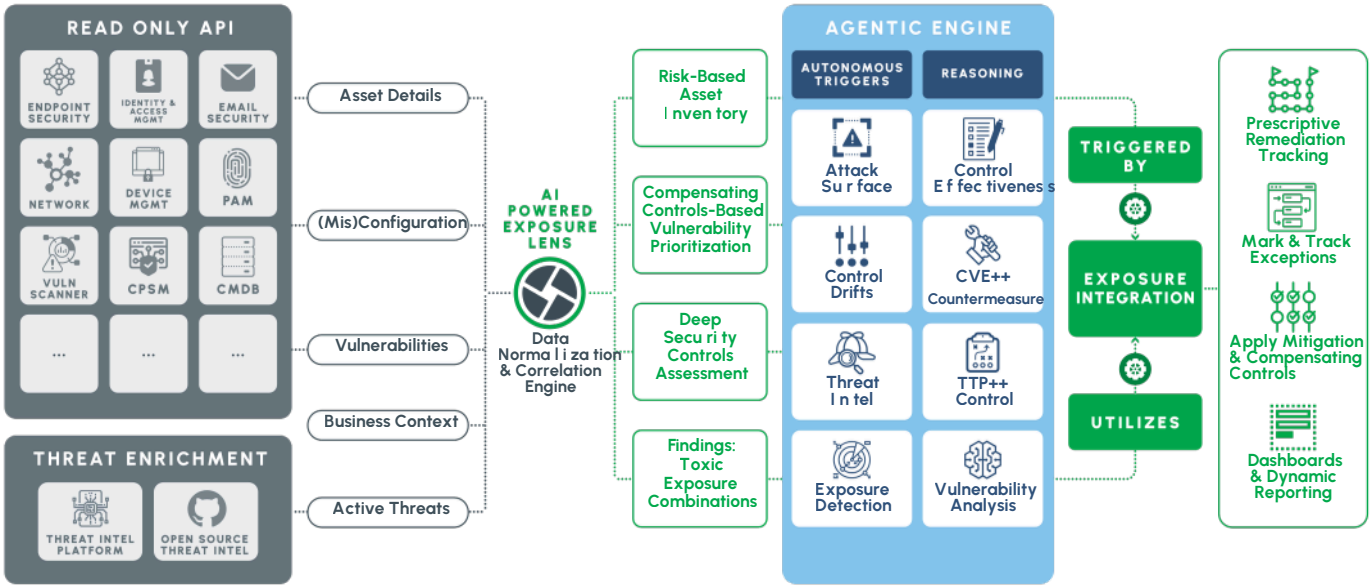
Remediation tracks through to verified closure. Tickets are grouped by fix. Nagomi confirms if the patch landed, the control deployed, the drift stopped. If it didn't, it flags again.

TRUSTED BY

PriceSmart · Coca-Cola HBC · MERCURY INSURANCE · JACKSON HEALTHCARE · APPLIED · Booking.com · ALERAGROUP

# Agents are the multiplier. Context is the foundation.

Your tools generate the signals. Nagomi connects them, reasons across them, and acts on them. Read-only API connections feed into a unified correlation engine. Autonomous agents run investigations, surface dangerous combinations, and push prescriptive fixes to the right owner. No manual stitching. No spreadsheet triage.




## HOW TEAMS APPLY NAGOMI

### VALIDATE DEFENSIVE POSTURE
Continuously confirm controls are actually preventing live threats.

### HUNT AND MITIGATE THREATS
Map active threats to your environment, expose coverage gaps, and close them before exploitation.

### MODERNIZE VULNERABILITY MGMT
Replace scan-and-spreadsheet workflows with prioritized, orchestrated remediation, grouped by fix, not CVE.

### ORCHESTRATE REMEDIATION
Reduce MTTR by routing fixes to the right team with root cause, business impact, and required action.

### ALIGN TEAMS ON EXPOSURE
Give VM, SecOps, GRC, and IT one shared view of exposure, with aligned priorities and a single definition of "closed."

### GOVERN ENTERPRISE
Track mean-time-to-verified closure across programs and business units. Report on risk reduced, not tickets opened.

**80%**
OF EXPOSURE TRIAGE ELIMINATED BEFORE ANALYST REVIEW

**4-Minute**
AUTOMATED INVESTIGATIONS VS 30–60 MINUTE MANUAL ANALYSIS

**1-Click**
REMEDIATION TICKET CREATION WITH FULL CONTEXT

**2+FTE**
OF ANALYST CAPACITY RETURNED ANNUALLY

nagomi

**Learn more at: nagomisecurity.com**

Gartner COOL VENDOR 2024