nagomi

NAGOMI EXPOSURE OPS PLATFORM

Turn the tools you already own into a coordinated defense

Nagomi unifies asset, control, vulnerability, and threat data into one view of real exposure. Autonomous agents investigate, remediate, and verify around the clock, so exposure closes and stays closed.

Tools aren't the problem. Coordination is. Exposure lives in the gaps.

Signals scattered
Asset, control, vulnerability, and threat data sit in separate consoles. No single view of real exposure. Risk hides in the gaps.

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

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

One coordinated loop. Exposure closes. Nothing carries over.

Nagomi runs the work the manual process can't keep up with.
Agents investigate, direct precise remediation, and verify that exposure stays eliminated.

Find live exposure

Asset, control, vulnerability, and threat data correlated into one view. Teams work what actually matters, not another CVSS list.

Act with less effort

Agents open the case and run the same investigation a senior analyst would. Analysts spend their time on judgment, not lookup.

Know it stays closed

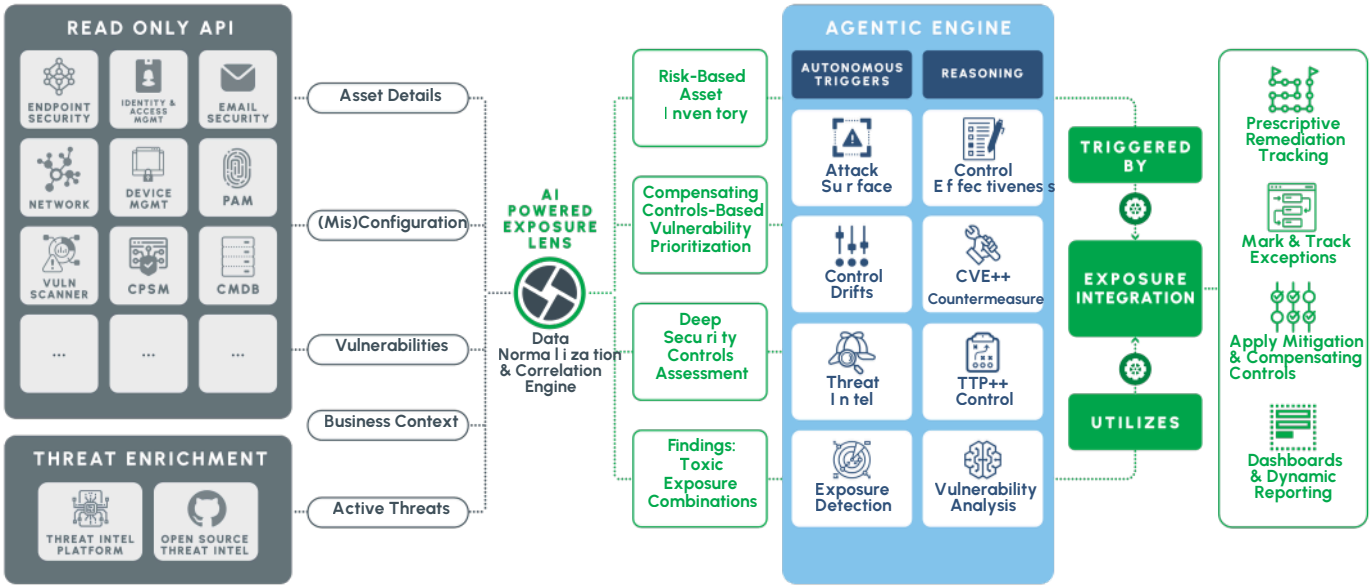
Remediation tracks through to verified closure. Nagomi confirms the patch landed, the control deployed, the drift stopped. If it didn't, it flags again.

Trusted by:

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

The loop runs. Exposure closes. Defenders stay ahead.

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

"The biggest shift for us was speed and alignment. Exposure is no longer a separate workflow from security operations. This isn't another visibility tool. It's helping us operationalize exposure in a way that actually scales."
Iain Paterson, CISO, WELL Health Technologies

Learn more at nagomisecurity.com

Gartner COOL VENDOR 2024