nagomi

Evaluation Framework: Capabilities Matrix

Introduction

The *Evaluation Framework: Capabilities Matrix* is designed to clarify how **Nagomi** aligns to and differentiates within the evolving **Exposure Management** landscape. As security programs mature beyond traditional vulnerability management, this framework maps Nagomi's capabilities against the leading **categories** and **methodologies** shaping the market.

By consolidating industry research and customer use cases, the framework provides a structured way to evaluate how Nagomi "fits" across these adjacent technologies. Each section explains the problem these markets aim to solve, the common capabilities they encompass, and where Nagomi extends or enhances those functions through its unified exposure management approach.

In short, this document serves as a **capability alignment guide**, helping security and risk leaders understand Nagomi's role as the **execution layer for CTEM**, bridging the gap between visibility, validation, and measurable reduction of exposure.

CATEGORY ACRONYM KEY

Acronym	Full Term	Description
CTEM	Continuous Threat Exposure Management	A repeatable process for discovering, prioritizing, validating, and mobilizing exposure reduction across digital assets.
ASCA	Automated Security Control Assessment	Automates validation of technical security control configuration and effectiveness.
EAP	Exposure Assessment Platform	Aggregates and prioritizes vulnerabilities, misconfigurations, and context into a unified exposure view.
AEV/BAS	Adversarial Exposure Validation / Breach & Attack Simulation	Validates exposures through simulated attack scenarios and adversarial testing.
CAASM	Cyber Asset Attack Surface Management	Consolidates asset and coverage data to identify visibility and protection gaps.
CCM	Continuous Controls Monitoring	Continuously evaluates and reports on the effectiveness of implemented security controls.
RBVM	Risk-Based Vulnerability Management	Prioritizes remediation efforts based on exploitability, impact, and business context.

Asset & Coverage Management

WHY IT MATTERS

You can't protect what you can't see. Attackers exploit blind spots like unmonitored cloud resources, unmanaged endpoints, and shadow IT. Complete asset visibility, combined with context around protection status, is essential for reducing risk. It's not enough to know what exists. Security teams also need to understand whether those assets are properly covered and how their security posture is evolving.

WHY NAGOMI IS DIFFERENT

Nagomi consolidates asset data across tools such as EDRs, CSPMs, and vulnerability scanners into a single, deduplicated view. It enriches that data with business context like ownership and criticality, then validates security control coverage dynamically. Instead of a static inventory, teams gain a real-time view of what matters, what's exposed, and what actions to take next.

Capability	Explanation	CTEM	ASCA	EAP	AEV/ BAS	CAASM	CCM	RBVM	Nagomi
Asset Discovery	Identify and inventory all assets (endpoints, servers, cloud, OT, IoT, SaaS).	✓		✓		✓		✓	Correlates asset data from multiple tools into a unified inventory (focusing on endpoints, servers and accounts).
Asset Metadata Enrichment	Add business context such as ownership, location, and criticality.	✓		✓		✓		✓	Enriches assets with ownership, tool coverage, and business impact to prioritize meaningfully.
Coverage Gap Identification	Detect when assets lack required security tool coverage.	✓		✓		✓		✓	Flags unmanaged or under-protected a ssets by correlating expected vs. actual tool coverage.
Coverage Rules Customization	Define coverage expectations (e.g., all Windows devices must have Intune) and track compliance.	✓				✓			Lets admins define custom coverage rules (e.g., Intune on Windows only) and validates compliance dynamically.

Vulnerability & Exposure Management

WHY IT MATTERS

Traditional vulnerability management surfaces thousands of alerts with little clarity on what truly matters. Risk often results from ***combinations*** of weaknesses like a critical CVE on an internet-facing asset that lacks endpoint protection. Teams need a way to connect the dots, highlight material risk, and deprioritize noise.

WHY NAGOMI IS DIFFERENT

Nagomi doesn't just list vulnerabilities. It correlates them with misconfigurations, control gaps, and threat intelligence to identify ***exposure findings***: prioritized issues that represent actual risk. These findings account for exploitability, business context, and control status, allowing teams to act on high-impact issues instead of chasing down low-value CVEs.

Capability	Explanation	CTEM	ASCA	EAP	AEV/ BAS	CAASM	CCM	RBVM	Nagomi
Vulnerability Correlation & Normalization	Deduplicate and enrich vulnerabilities across scanners and tools.	✓		✓				✓	Aggregates vuln data from multiple sources into a single correlated view.
Exploitable Vulnerability Prioritization	Focus on vulnerabilities actively exploited in the wild.	✓		✓				✓	Highlights exploitable CVEs tied to live adversary campaigns for faster focus.
Threat-Informed Exposure Mapping	Combine vulnerabilities, coverage gaps, and misconfigs with live threat intel.	✓		✓					Maps exposures against adversary techniques (e.g., Lazarus, ransomware) with correlated config and coverage data.
Exposure Toxic Combinations	Identify multi-factor exposures (e.g., vuln + misconfig + missing control).	✓		✓				✓	Detects and highlights "toxic combinations" that compound risk across vulnerabilities, configs, and tool coverage.
MITRE ATT&CK Mapping	Map defenses and exposures against adversary techniques.	✓	✓		✓				Links policies and exposures to MITRE ATT&CK, showing strengths and gaps vs. adversary TTPs.

Control Effectiveness & Assurance

WHY IT MATTERS

Having security tools deployed isn't enough. If configurations drift, policies aren't enforced, or agents silently fail, protections break down. Without assurance that controls are working as expected, security programs are vulnerable to silent failure.

WHY NAGOMI IS DIFFERENT

Nagomi continuously evaluates controls across the environment like EDR, IAM, and vulnerability management, surfacing issues such as partial deployment, missing MFA enforcement, or misaligned policies. These findings are paired with remediation guidance and ownership context, giving teams a clear, current picture of control health.

Capability	Explanation	CTEM	ASCA	EAP	AEV/ BAS	CAASM	CCM	RBVM	Nagomi
Control Configuration Assessment	Validate security controls for misconfigs, insecure defaults, or gaps.	✓	✓	✓			✓	✓	Continuously checks control configs across devices, identities and domains including security tools such as EDR, IAM, and email security.
Policy Drift Detection	Identify when controls deviate from intended baseline.	✓	✓	✓					Surfaces policy drift (e.g. devices added without EDR or MFA) and suggests remediation steps.
Misconfiguration Detection	Surface insecure defaults or weak settings.	✓	✓	✓					Identifies and flags risky misconfigurations.
Continuous Assurance	Continuously monitor controls for ongoing effectiveness.	✓	✓	✓			✓		Provides continuous validation that deployed controls remain configured and effective.

Mobilization & Remediation

WHY IT MATTERS

Identifying exposures is only valuable if teams can respond. Without effective handoff, prioritization, and remediation, risk persists. But in many organizations, fixes stall due to unclear ownership, fragmented workflows, or lack of guidance.

WHY NAGOMI IS DIFFERENT

Nagomi accelerates remediation by integrating with ticketing systems like Jira and ServiceNow to automatically generate enriched, actionable tickets. It includes step-by-step guidance tailored to the finding, and enables safe automation for common fixes like hardening policies or improving tool coverage. This ensures teams can act quickly without introducing unnecessary risk.

Capability	Explanation	CTEM	ASCA	EAP	AEV/ BAS	CAASM	CCM	RBVM	Nagomi
Remediation Guidance	Provide step-by-step fix instructions.	✓	✓	✓	✓	✓		✓	Generates actionable guidance with tool-specific fix steps for IT and security teams.
Ticketing & Workflow Integration	Route remediation to the right teams via ITSM tools.	✓	✓	✓	✓	✓		✓	Creates enriched ServiceNow/JIRA tickets with asset lists and remediation steps prefilled.

Reporting, Dashboards & Program Oversight

WHY IT MATTERS

Executives, boards, and auditors need more than technical metrics. They expect evidence that risk is decreasing and that security tools are delivering return on investment. Clear, business-aligned reporting helps teams demonstrate impact, secure budget, and support oversight.

WHY NAGOMI IS DIFFERENT

Nagomi provides customizable dashboards that track exposure reduction and control health over time. Executive-ready views translate technical detail into business impact. Teams can export reports for audits, cyber insurance, and board meetings, helping turn security insights into measurable outcomes.

Capability	Explanation	CTEM	ASCA	EAP	AEV/ BAS	CAASM	CCM	RBVM	Nagomi
Tool ROI & Utilization Metrics	Measure adoption and effectiveness of security tools.	✓	✓				✓		Tracks whether all security tools are fully deployed and used as intended.
Program Effectiveness & ROI Tracking	Link exposure reduction to tool/program investments.	✓	✓				✓		Shows how tool utilization and program improvements reduce risk and exposure over time.
Custom Metrics & Dashboards	Build and track any metric over time.	✓		✓			✓		Lets users create dashboards to highlight changes in exposures, coverage, and more.
Business-Aligned Dashboards	Tailor dashboards for execs, operators, and board audiences.	✓		✓			✓		Provides executive-level trend views and tactical dashboards for ops teams from the same dataset.
SLA Compliance Dashboards	Track remediation timelines against SLAs.	✓					✓	✓	Monitors remediation performance for accountability.
Exposure-Aware Reporting	Report exposures across vulns, configs, and coverage.	✓		✓			✓	✓	Delivers reporting that includes coverage gaps and misconfigs, not just vulnerabilities, as well as toxic combinations of all three.
Continuous Maturity Baselining	Track posture vs. frameworks and improvements over time.	✓					✓		Provides baseline scoring against frameworks (MITRE, NIST, CIS) with improvement trends.
Executive / Board Reporting	Summarize risk reduction and trends for leadership.	✓					✓		Exports metrics and dashboards tailored for board and executive communication.
Regulatory / Cyber Insurance Support	Provide defensible evidence for compliance or insurance.	✓					✓		Generates defensible evidence packages for audits and cyber insurance reviews.