

AI RISK POSTURE · EXECUTIVE BRIEFING

Your AI attack surface, measured and prioritized.

Discovery, exposure scoring and board-ready proof across the fleet.

Prepared for

Northwind Trading Co.

REPORTING PERIOD Q3 2026 · as of 12 Aug 2026	SCOPE 320 endpoints · fleet-wide	CLASSIFICATION Sample
REPORT ID SAD-EXEC-2026-0142	PREPARED BY Sargha · Araghatta LLC	AUDIENCE Board & senior management

AI risk posture — Northwind Trading Co.

1,284

AI artifacts discovered

320

Endpoints monitored

39

Open risks (4 critical · 13 high)

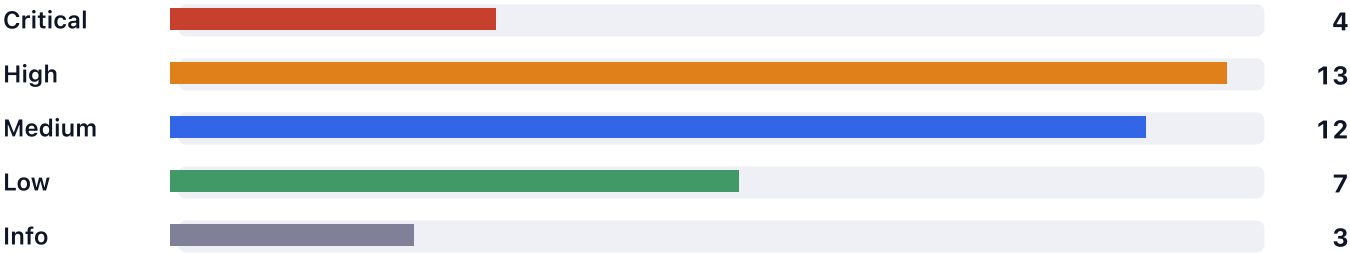
92%

Findings AI-validated

Posture at a glance

Across 320 monitored endpoints, Sargha discovered 1,284 AI artifacts — unsanctioned LLM tools, coding agents, MCP servers and exposed API keys — and scored 39 open risks (4 critical, 13 high). The dominant exposures are provider keys left in files and unregistered MCP servers on vulnerable versions. Posture improved 6 points this quarter as high-severity items were remediated, but critical secret-exposure remains above target.

Risk severity mix



Key exposures

SEVERITY	FINDING	AFFECTED
CRITICAL	API keys in files and environment Provider keys in shell profiles and .env files	14 endpoints
CRITICAL	Unregistered MCP server (vulnerable) server-filesystem on a vulnerable version	3 endpoints
HIGH	Unapproved coding agents Code + credential access, unattended	31 endpoints
HIGH	Offboarded-user AI access Identities still active after departure	9 identities
MEDIUM	Shadow browser AI extensions Data-egress risk via AI-enabled extensions	48 endpoints