Kavryl

Public product output preview

Built for the AI agent era

Kavryl Azure and AWS AI Agent Risk Report

Synthetic cloud report based on Kavryl Azure and AWS scanner findings, including fake subscription, account, and resource IDs.

Cloud scope

Sample customer	Northstar Health Cloud
Azure subscription	4b812c7f-301d-45fb-8a4d-8a7750c4c19f / Northstar AI Prod
AWS account	391742608155 / nstar-prod-ai
Regions	Azure eastus, westus2; AWS us-east-1, us-west-2
Resource groups	rg-ai-agents-prod, rg-rag-data-prod, rg-api-prod
Data note	Synthetic cloud resource IDs modeled on Kavryl Azure and AWS scanner output.

Cloud exposure summary

Kavryl found that the cloud environment contains agent-like services with public endpoints, broad identity permissions, static-key authentication, and sensitive data stores used by RAG and support workflows. The most urgent fixes are identity scoping and public network restrictions.

Representative resource IDs

Azure AI	/subscriptions/4b812c7f-301d-45fb-8a4d-8a7750c4c19f/resourceGroups/rg-ai-agents-prod/providers/Microsoft.CognitiveServices/accounts/nstar-openai-prod
Azure Key Vault	/subscriptions/4b812c7f-301d-45fb-8a4d-8a7750c4c19f/resourceGroups/rg-ai-agents-prod/providers/Microsoft.KeyVault/vaults/kv-nstar-agent-prod
Azure Storage	/subscriptions/4b812c7f-301d-45fb-8a4d-8a7750c4c19f/resourceGroups/rg-rag-data-prod/providers/Microsoft.Storage/storageAccounts/nstarragdocsprod
AWS IAM Role	arn:aws:iam::391742608155:role/agent-bedrock-admin-role
AWS API Gateway	arn:aws:apigateway:us-east-1::/apis/a1b2c3d4ef/stages/prod
AWS S3	arn:aws:s3:::nstar-agent-rag-docs-prod

Top cloud findings

CLD-001	Critical	Azure IAM	agent-orchestrator-sp has Owner role at subscription scope	Replace Owner with scoped custom role and managed identity
CLD-002	High	Azure AI	nstar-openai-prod allows broad public network access	Restrict to private endpoint and approved networks
CLD-003	High	Azure Storage	RAG docs storage allows blob public access flag	Disable public blob access and review container ACLs
CLD-004	High	AWS IAM	agent-bedrock-admin-role includes wildcard action signal	Replace wildcard permissions and restrict trust policy
CLD-005	Medium	AWS API	Public agent API endpoint lacks documented owner and throttling evidence	Assign owner, confirm auth, enable rate limits and schema checks
CLD-006	Medium	Azure Search	AI Search local key authentication remains enabled	Disable local auth and use managed identity where supported

How to interpret this

Cloud findings should not be read as isolated hygiene issues. In an AI agent environment, a public endpoint plus a broad role plus a static secret can become an agent blast-radius path. Kavryl prioritizes combinations that let an agent retrieve sensitive data, call APIs, mutate cloud resources, or persist access.

Cloud remediation sequence

0-7 days	Remove subscription Owner from agent-orchestrator-sp and pause new tool grants.	Stop the highest cloud privilege expansion path.
7-21 days	Move Azure AI, Key Vault, Storage, Search, and API endpoints behind private networking where feasible.	Reduce public attack and misuse surface.
21-45 days	Replace static keys with managed identity / workload identity federation.	Reduce credential reuse by agents, tools, and CI/CD.
45-60 days	Run monthly Kavryl cloud and SaaS correlation scan.	Detect new agent access paths before production rollout.