Kavryl

Built for the AI agent era

Kavryl SaaS, Identity, and Agent Permission Risk Report

Synthetic SaaS and identity report based on Kavryl GitHub, Microsoft 365 / Entra, Google Workspace, and MCP scanner outputs.

SaaS and identity scope

Sample customer	Northstar Health Cloud
Microsoft tenant	7a62d5b4-91d0-4cf5-ae83-4dd9e3d8a210
Google Workspace customer	C03nstar742
GitHub organization	northstar-health-cloud
Agent systems	support-triage-agent, clinical-docs-rag, devops-pr-agent, billing-copilot
Data note	Synthetic SaaS and identity data modeled on Kavryl M365, Google Workspace, GitHub, and MCP scanner output.

SaaS exposure summary

Kavryl found that agent-like OAuth apps and service accounts can reach sensitive user data, repositories, and knowledge bases. The highest risk path combines delegated Microsoft Graph access, Google Drive folder access, and GitHub repository automation tokens.

Agent inventory

AGT-001	High	Support	support-triage-agent reads tickets, Drive docs, and posts Slack updates	Add approval before outbound messages and restrict source folders
AGT-002	High	RAG	clinical-docs-rag retrieves from broad Drive folder shared with All Clinical Ops	Apply retrieval-time authorization and folder-level least privilege
AGT-003	Medium	GitHub	devops-pr-agent can comment on PRs and read multiple private repos	Restrict repo scope and rotate token
AGT-004	Medium	Finance	billing-copilot has Salesforce and Google Sheets connector access	Split read-only analysis from write actions
AGT-005	Info	Inventory	MCP tool owner missing for internal filesystem connector	Assign owner and approval policy

OAuth and SaaS findings

SAA-001	High	M365	Support Agent OAuth App has Mail.Read, Files.Read.All, offline_access	Remove unused scopes, require admin consent, split high-risk app
SAA-002	High	Google	Service account nstar-rag-reader can read shared clinical-docs folder	Limit folder access and require data classification labels
SAA-003	High	GitHub	Agent token can read 14 private repos but only 3 are used in workflow	Move to fine-grained token scoped to required repos
SAA-004	Medium	Slack	Agent can post into #support-escalations without approval check	Add human approval for external/customer-impacting messages
SAA-005	Medium	MCP	Filesystem and shell tools are available in same MCP server profile	Separate profiles and require allowlisted commands

Action interpretation

The action priority is based on blast radius, not only severity labels. Kavryl recommends fixing paths where an agent has both sensitive read access and outbound/write capability first, because those combinations create the highest business impact during prompt injection, compromised token, or unsafe automation events.

SaaS remediation sequence

0-7 days	Disable offline_access for agent OAuth apps where persistent access is not required.	Reduce persistence if an agent token is compromised.
0-14 days	Create separate service identities for support, RAG, GitHub, and billing agents.	Avoid shared blast radius between unrelated workflows.
15-30 days	Restrict Drive, GitHub, and Salesforce connectors to exact datasets needed.	Reduce data exposure from broad SaaS permissions.
30-60 days	Adopt recurring agent owner review and permission attestation.	Keep agent inventory and approvals current.