

GET CONTROL OF SHADOW AI

PILOT TO **GOVERNED**
IN 30 DAYS



GenAI adoption is outpacing governance. Employees are using ChatGPT, Claude, and MCP-connected AI agents that can directly access enterprise tools, databases, and APIs from a single prompt. Shadow AI is no longer unapproved chat. It is unapproved automation, and for regulated industries, the path forward starts with visibility and control, not restriction.

“
80%
OF EMPLOYEES
USE UNAPPROVED
AI TOOLS AT
WORK
”

“
43%
SHARE SENSITIVE
DATA WITH AI
WITHOUT EMPLOYER
APPROVAL
”

“
\$670K
ADDED BREACH
COST FOR
ORGANIZATIONS
WITH HIGH SHADOW
AI
”

Sources: UpGuard State of Shadow AI 2025 | CybSafe / National Cybersecurity Alliance 2025 | IBM Cost of a Data Breach 2025

RSM Collective's GenAI Governance and Guardrails professional services engagement is powered by SurePath AI. In less than 10 days, we provide full visibility into what GenAI tools are being used, by whom, and for what purpose, surfacing your organization's real use cases.

Understanding who is using what and why allows us to quickly begin implementing a governance strategy tailored to your environment. Given the pace of AI models and technology advancements, your compliance strategy has to be continuous, not a one-time exercise. After the 10-day pilot, we deliver the insights, document the ROI, and provide the cost of a production governance framework, all within 30 days.

Phase 1: Discovery

days 1-10

- Identify all GenAI tools and data flows in use (including Shadow AI). Quantify ROI and usage trends across departments.
- Assess exposure risks and compliance gaps. Integrate with existing,
- AWS, Palo Alto, Netskope, & Zscaler environments.

Phase 2: Governance

days 11-30

- Define and enforce policies for compliant GenAI use
- Implement role-based access controls and data classification
- Configure content redaction to block PII/PHI from public models
- Establish secure connections

WHY GOVERNANCE CAN'T WAIT

THE GOVERNANCE GAP BY THE NUMBERS









- **98%** of organizations have employees using unsanctioned AI apps
- **75%** of organizations admit governance has not kept pace with AI adoption
- **86%** aware of upcoming AI regulations, but only 25% have a governance program
- **20%** of organizations have already suffered a security breach tied to shadow AI
- **3 in 5** employees have received no formal training on safe AI use at work

Sources: Varonis 2025 | Informatica CDO Insights 2026 | AuditBoard 2025 | IBM 2025 | CybSafe 2025

Governance & Guardrails

WHAT YOU GET?

- ✓ Complete GenAI application inventory across your organization
- ✓ Risk and compliance gap analysis with prioritized remediation plan
- ✓ ROI and usage analytics by department and tool
- ✓ Governance framework with role-based access controls and data classification policies
- ✓ Content redaction and PII/PHI protection configuration
- ✓ SurePath AI Governance Platform deployed for continuous monitoring
- ✓ Automated compliance reporting aligned to HIPAA, SOC 2, and ISO 27001
- ✓ Exportable audit trails for regulators, auditors, and board reporting

USER ACTIVITY		
USER	MODEL	VIOLATION
Maria Dyer Sept 5 · 10:40:55	 ChatGPT	 PII
Alan Davies Sept 5 · 10:39:20	 Gemini	 Intent
Tim Walsh Sept 3 · 16:34:51	 Claude	 Access
Claire Arnold Sept 3 · 15:47:12	 SurePath AI	 None



Purchase: \$10k Pilot to Production

Web: rsmc.ai

eMail: surepath@rsmc.ai

AWS Marketplace: Search RSM Collective