DTM Consulting, LLC

Agentforce Security & Governance Enablement

Making Agentforce auditable, governed, and defensible

The problem CISOs are facing

Agentforce accelerates automation, but it also introduces a new risk surface that most security programs aren't designed for.

Security leaders are asking:

- Will AI agents **bypass existing security controls**?
- Who actually **owns agents once they're live**?
- Can we **audit and defend agent behavior** to regulators, auditors, and the board?

Without clear answers, Agentforce adoption stalls... or worse, moves forward without governance.

DTM exists to close that gap.

What DTM does

DTM helps organizations deploy **Agentforce in a way that is auditable, policy-aligned, and clearly owned**.

This is not about selling tools.
This is about making Agentforce **defensible inside real security programs**.

Who this is for

- CISOs and security leadership teams
- Organizations evaluating, piloting, or scaling Agentforce
- Security teams expected to "sign off" on AI-driven automation

The DTM Agentforce Offering

Tier 1 — Agentforce Readiness Assessment

Best for: Security teams evaluating or early in Agentforce adoption

Core question it answers

> *Are we actually safe to deploy agents — and do we know who owns them?*

What's included

- Review of Agentforce use cases and planned capabilities
- Mapping of agent behavior to existing security controls
- Identification of:
    - Control bypass risk
    - Ownership gaps
    - Audit and logging blind spots

Deliverables

- Agentforce Risk & Ownership Findings Summary
- Clear Go / Fix / Don't Deploy Yet guidance
- Executive-ready language security can use internally

Outcome

> Confidence before scaling Agentforce.

Typical investment: *Range provided upon request*

Tier 2 — Secure Agentforce Deployment

(Primary engagement)

Best for: Teams actively deploying Agentforce

Core problem it solves

> Agentforce is moving faster than governance.

What's included

- Definition of a clear Agentforce ownership model
- Alignment of agent actions with:
  - Security policy
  - Identity and access expectations
  - Audit requirements
- Guardrails for:
  - Agent permissions
  - Escalation paths
  - Traceability and accountability

Deliverables

- Agentforce Security & Ownership Model
- Deployment guardrails security can stand behind
- Artifacts suitable for leadership, audit, and compliance review

Outcome

> Agentforce is live — without creating unmanaged risk.

Typical investment: *Range provided upon request*

Tier 3 — Agentforce Operationalization

Best for: Organizations scaling Agentforce beyond pilots

Core problem it solves

> Governance doesn’t end at launch.

What’s included

- Long-term ownership and operating model for agents
- Framework for:
  - New agent onboarding
  - Changes and approvals
  - Incident response involving agents
- Security-to-executive translation support

Deliverables

- Agentforce Operating & Governance Model
- Ongoing security oversight framework
- Board- and audit-ready narratives

Outcome

> Agentforce delivers value without long-term security debt.

Typical investment: *Range provided upon request*

Why DTM

DTM sits at the intersection of:

- SaaS security
- Agentforce capabilities
- Real-world security governance

Led by Sarah Swenson, DTM specializes in translating emerging Salesforce and Agentforce capabilities into *enforceable, auditable security models* that security leaders can actually defend.

This work is designed to complement — not replace — your existing Salesforce and security teams.

Engagement model

- **Time-boxed:** 14-30 days
- **Salesforce-adjacent:** Designed to work alongside Agentforce programs
- **Vendor-neutral:** Focused on governance, ownership, and outcomes

The result

Security teams walk away able to say:

> *"Our Agentforce deployment is auditable, policy-aligned, and clearly owned."*

Next steps

If Agentforce is on your roadmap and security is being asked to approve it, DTM can help.

Contact:
Sarah Swenson
DTM Consulting