Lowenstein Sandler

RSAC CONFERENCE 2026
AI Governance Evidence

Exhibitor Cheat Sheet

Where available, vendors are marked with their exhibiting location on the RSAC Expo Floor plans (see Exhibitors | RSAC Conference). For the Moscone Center, “N” denotes the North Expo and “S” denotes the South Expo.

> *Vendors that are marked with an asterisk do not appear to be exhibiting onsite. We recommend reaching out directly to schedule a demonstration outside the conference, as several offer compelling technologies worth evaluating.

Given the size of the Moscone Center footprint, grouping vendors by location can significantly reduce walking time. The groupings below are intended to minimize unnecessary back-and-forth across the Expo halls. Where applicable, we have also included links to vendors’ published RSAC event pages.

North Expo vendors in this chart include IBM, Wiz AI-SPM; Microsoft offerings such as Semantic Kernel, AutoGen, Copilot Studio, Purview, and Azure AD; and Google Workspace DLP, Robust Intelligence, and Hiddenlayer.

South Expo vendors include Orca Security, Noma Security, Amazon Bedrock, Netskope, Cyberhaven, Okta, and Protectt.ai.

Lowenstein Sandler

Domain 1 – Governance and Risk Orchestration			
*Credo AI	IBM N-5770	*Collibra	*Monitaur
Q: How are the governance decisions recorded in these platforms connected to the systems running AI?			

Domain 2 – AI Discovery and Security Posture Management				
*Pillar Security	*Cranium	Wiz AI-SPM N-4435	Orca Security S-1035	Noma Security S-1261
Q: Can your organization identify every AI system touching your data right now?				

Domain 3 – Agent Orchestration and Workflow Control							
*Lang Graph	Microsoft Semantic Kernel N-5744	Microsoft AutoGen N-5744	Microsoft Copilot Studio N-5744	*Perfect	*Dagster	Amazon Bedrock S-0466	*Apache Airflow
Q: What actions are your AI agents authorized to take, and how are those actions recorded?							

Domain 4 – Data Security Posture Management					
Netskope S-1127	*Nightfall AI	Cyberhaven S-1355	*Bedrock Data	Microsoft Purview (Partial Tool) N-5744	Google Workspace DLP N-6062
Q: *What sensitive data has already reached your models, and did you know before today?*					

Domain 5 – Data Lineage and Pipeline Visibility			
*Collibra	*Monte Carlo	*Apache Atlas (Open Source)	*OpenLineage (Open Source)
Q: Can you trace, step-by-step, how a specific model output was produced?			

Domain 6 – Identity and Access Governance for AI Systems		
*ConductorOne	Okta (trad. IAM) S-1427	Azure AD (trad. IAM) N-5744
Q: *What systems can your AI agents access, and who last reviewed those authorizations?*		

Domain 7 – Runtime Protection and Behavioral Monitoring							
*Lakera Guard	*Lasso Security	Protectt.ai S-2060	*Arthur AI	Robust Intel (now Cisco) N-6044	*Garak (Open Source)	*MLflow (Open Source)	*Giskard (Open Source)
Q: *If a deployed AI system began behaving unexpectedly tomorrow, how quickly would you know, and what, if anything, would automatically stop it?*							

Domain 8 – AI Supply Chain and Model Integrity		
Hiddenlayer N-6377	Protectt.ai S-2060	*ModelScan
Q: If your AI vendor pushed a model update tonight, how would you know whether system behavior changed?		