

The Webinar Will Begin Momentarily...

What our clients are asking us:

- ☑ “Which AI tools should we let people use?”
- ☑ “How do we control spend and measure ROI?”
- ☑ “How do we keep up when it changes every month?”
- ☑ “What data should we share with each tool?”
- ☑ “How do we stop people from using personal accounts or unauthorized tools?”

AI Without Blind Spots: Securing AI in Regulated Industries

OCTOBER 21, 2026

FEATURING



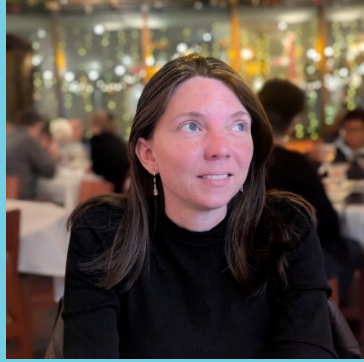
Meet the Panel



**DIRECTOR OF
CYBERSECURITY**

Travis DeForge

Abacus



**SR. DIRECTOR OF DATA
AND APPLICATION
ENGINEERING**

Amy Bruce

Abacus



**HEAD OF PARTNER
SUCCESS**

Michael Maier

Cavelo



**AI STRATEGY,
MODERATOR**

Jean McCabe

Abacus

Agenda



01 **Mature AI Adoption**

02 **Shadow AI**

03 **Secure vs. Vibe Coding**

04 **AI-Assisted Vulnerability Management**

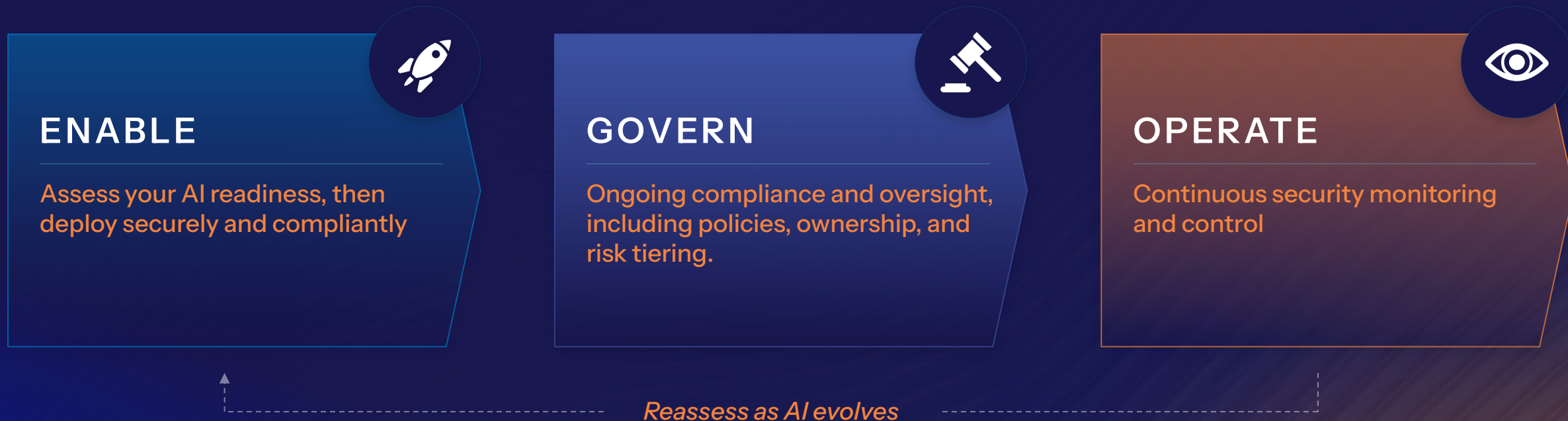
05 **Building a Secure AI Roadmap**

Webinar Duration: 30-45 minutes

Recording: Webinar will be recorded and emailed

Q&A: Please use Q&A function in GoToWebinar to ask questions

What Mature AI Adoption Looks Like: It Starts with Your Data



WHY THE STEPS WORK BETTER TOGETHER

An assessment finds the gaps. Deployment closes them and implements your tools. Ongoing governance and security programs keep them closed.

Build the Rails Once, Then Swap the Tools

TOOLS AND MODELS Change every quarter
Chat assistants, copilots, agents, whatever ships next

RAILS Build once
Approved access · Data boundaries · An identity for every agent ·
Logging · Monitoring

YOUR DATA AND WORKFLOWS The asset
Client data, positions, and the processes you run every day

You can't evaluate every new tool.

You can decide once what any tool is allowed to touch.

Shadow AI Discovery & Monitoring: Eliminate Your Blind Spots

How Shadow AI Turns into Data Exposure

A shortcut

Someone pastes patient notes, client data or code into a free AI tool to save time.

Data leaves

The provider may retain prompts, train on them or store them outside your agreements.

No record

No BAA, no vendor review, no log of what was shared, so no way to scope it.

A reportable event

Possible HIPAA or Reg S-P notification, exam findings and lost client trust.

WHERE SHADOW AI HIDES

Consumer chatbots

Browser extensions

AI features switched on in SaaS you already own

Meeting note-takers

AI agents with access to email and files

Personal devices

Blocking alone just pushed AI further underground. Offer a safe, approved path.

Discover

A continuous inventory of AI tools, features and agents across network, identity and endpoints.

Classify

Rate each by the data it touches and the risk it carries. PHI and client data raise the bar.

Decide

Approve, approve with controls, or block, with a sanctioned alternative for anything blocked.

Monitor

DLP on prompts and uploads, alerts on new AI apps, and metrics for leadership.

Secure Coding vs. Vibe Coding: Same Tools, Different Outcomes

	Vibe coding	Secure AI-assisted development
Who builds	Anyone with a prompt	Trained, approved builders
Code review	If it runs, ship it	Human review of every change
Testing	Manual spot checks	SAST, SCA and secret scanning
Packages	Whatever the model suggests	Allowlisted, verified packages
Data	Real PHI and client data in prompts	Masked or synthetic data only
Ownership	Unclear once it's live	Named owner in the AI register

RISKS OF AI-ASSISTED DEVELOPMENT

- Insecure patterns
- Hallucinated packages
- Leaked sensitive information
- Over-privileged agents
- Shadow apps

Questions you should be asking

WHAT WAS BUILT

What have your people built with Claude, Copilot or ChatGPT that IT did not know about?

WHERE THE LINE IS

Where is the line between citizen developer and developer and who enforces it?

WHAT GETS A “YES”

What would a safe sandbox need to look like for you to say yes more often?

AI-Assisted Vulnerability Management: Find and Remediate, Faster

Where AI speeds up each stage:

Find

Continuous asset discovery; scanner, cloud and endpoint data merged into one view.

Prioritize

Ranks findings by exploitability, exposure and business context, beyond CVSS alone.

Remediate

Drafts fixes, patch plans and tickets; groups work so one change closes many findings.

AI accelerates. People stay accountable.

Let AI handle:

- Correlating and deduplicating findings
- Drafting remediation steps and tickets
- Summarizing risk for leadership
- Watching for new exposures around the clock

Keep people on:

- Approving changes to production systems
- Accepting or granting exceptions for risk
- Anything touching patient care or trading
- Communicating with regulators and clients

Building a Roadmap for Secure AI: Start With Data Readiness

Classify sensitive data

See exactly what sensitive and business-critical data exists in the environment today.

Map over-permissions

Understand who can access that information – including Copilot, Claude, Gemini, etc.

Set guardrails

Establish clear policies around what information employees can interact with.

Monitor continuously

Continuously monitor the environment and help maintain visibility – including what LLMs are interacting with.

HAVE THESE READY:

AI policy

AI inventory

Use-case register

Risk assessments

AI vendor due diligence

AI incident response playbook

AI risk reports

Key Takeaways

- 1 Know your maturity stage, then close the gap between policy and practice.
- 2 You can't govern AI you can't see. Inventory it, shadow AI included.
- 3 Treat AI-generated code like any other code: reviewed, scanned and owned.
- 4 Prioritize vulnerabilities by the data at stake.
- 5 Build the roadmap in phases, and document as you go.

A Phased Path to Secure AI Adoption

**As your AI use matures,
here's what we recommend
at each stage.**

Initial Evaluation

Risk & Readiness Assessment

A scored baseline and a prioritized roadmap in 3-4 weeks.

Implementation

Secure AI Deployment

The right AI platform for your environment, secured under one framework.

Continuous Monitoring & Governance

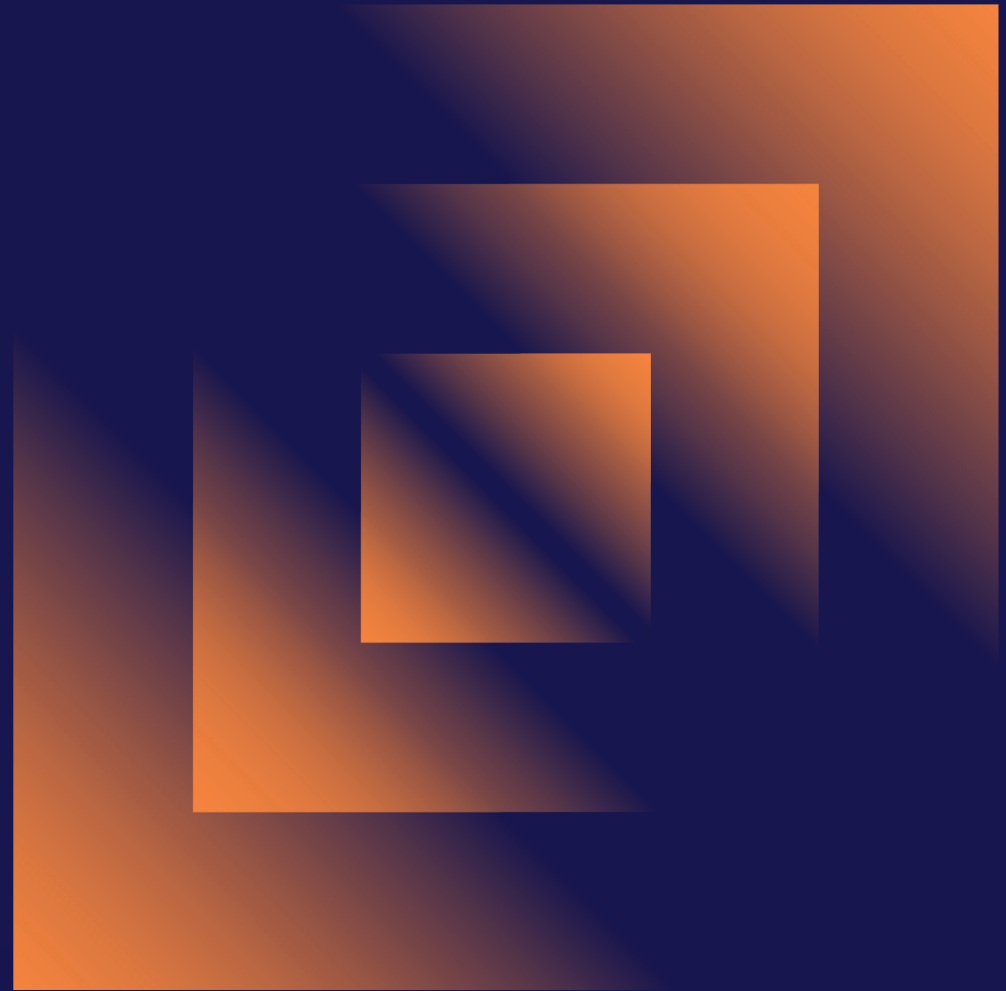
AI Governance Advisory

Policy, oversight, and the evidence to prove compliance.

Managed AI Security & Controls

Continuous visibility and control over how your people use AI.

Q&A





ABACUS

 **cavelo**

thank *you.*