

# OPKALLA

## Securing AI Adoption: Understanding Key Risks

June 30, 2026



# We make IT easy.

**We're data driven, vendor-neutral Technology Advisors. We work directly with you to assess your technology needs and select the best IT solutions for your organization.**

# Core Values.



**TRUST**



**TRANSPARENCY**



**SPEED**

Your best interest is always our focus.

We operate by these core values to serve clients around the world as their trusted partner.

# WE'RE YOUR TECHNOLOGY ADVISOR. NOT ANOTHER VENDOR.

**Sitting on the same side of the table as you, we work to:**

- Understand your current state
- Create a strategic plan for reaching your target state
- Compare solutions that answer your challenges
- Provide unbiased advice
- Advocate for your interests
- Negotiate for the best price
- Treat every step with urgency
- Act with transparency, always

*And we do all of this at no charge.*



# WHERE WE ENGAGE



Unified  
Communications



Mobility



SASE /  
SD-WAN



Microsoft 365  
for Business



Public Cloud  
Solutions



Colocation



Cloud Contact  
Center



Connectivity



Cybersecurity



AI & Data



Infrastructure



Disaster Recovery  
& Backup

# COMMON CHALLENGES

## Data Quality & Silos

This remains the most fundamental and persistent challenge. AI models are useless with poor-quality data. Many companies find their data is fragmented across legacy systems and different departments, making it difficult to access and consolidate for training AI.

## Skill Gaps & Talent Shortages

A lack of specialized AI talent (data scientists, AI engineers) is a major obstacle. Furthermore, a new challenge is the gap in "AI fluency" across the rest of the workforce. Companies need to train their employees not only on how to use AI tools but also on how to think and work with AI.

## Organizational & Cultural Resistance

AI implementation can spark internal friction and power struggles. Employees may resist new technologies out of fear of job displacement, and departments may be reluctant to share data. A people-first approach and clear communication from leadership are crucial to overcome this.

## Scaling From Pilot to Production

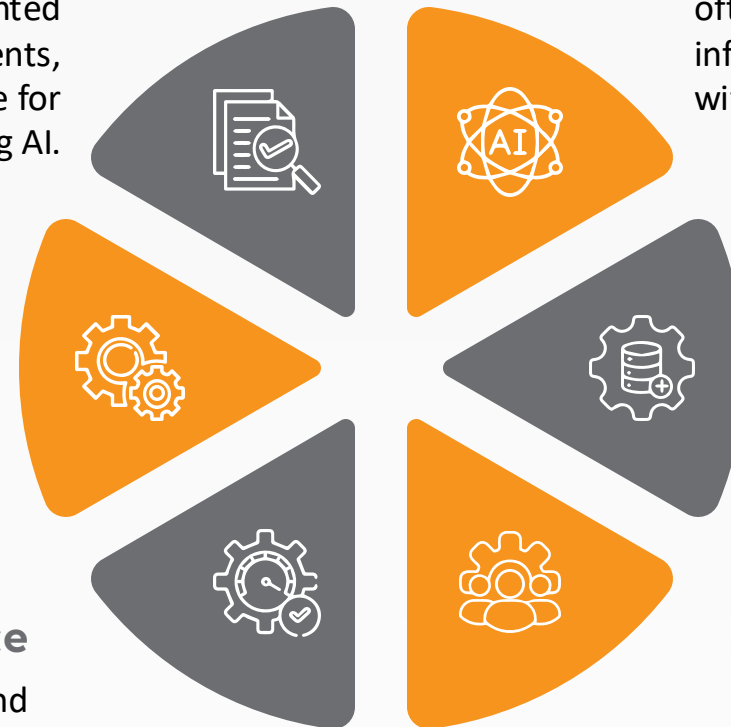
Many organizations successfully run a small AI pilot but struggle to scale it across the entire enterprise. This is often due to a lack of a clear strategy, insufficient infrastructure, or an inability to integrate the AI system with core business operations.

## Uncertain ROI & High Costs

While AI has the potential for significant returns, the upfront costs for infrastructure, talent, and implementation can be substantial. Many decision-makers struggle to justify these costs without a clear and quantifiable ROI, making it difficult to secure the necessary budget.

## Security & Trust

Organizations face significant hurdles in securing the unique risks of modern AI workloads. Key challenges include preventing Shadow AI and data leakage via unauthorized external tools, managing fragmented access policies across siloed data environments, and securing the sprawl of non-human identities that operate with elevated permissions.



# DATA AND AI STRATEGY: THE OPKALLA APPROACH

0



## AI Readiness & Security Pre-Flight

Are we *allowed* to do this securely?

**CORE OBJECTIVE:** Mitigate legal, ethical, and reputational risk.

1



## AI Foundations

Is our *data* ready and centralized?

**CORE OBJECTIVE:** Eliminate data silos and create a clean, scalable data environment.

2



## AI Operationalization

Can we use off-the-shelf AI to get *quick value*?

**CORE OBJECTIVE:** Achieve immediate gains in employee productivity and customer experience.

3



## AI Strategic Impact

Can we use our *unique data* to build a competitive edge?

**CORE OBJECTIVE:** Build custom, proprietary solutions that solve complex, specific business problems.

# AI SECURITY: THE OPKALLA WAY

1



## USAGE GOVERNANCE

Control What AI can be used and how.

Ensures only approved AI applications and models are used under defined policies and guardrails.

2



## DATA PROTECTION

Protect data from exposure and misuse.

Discover, classify, and protect sensitive and proprietary data across all sources and flows used by AI.

3



## IDENTITY & AGENT SECURITY

Secure identities, agents, and their access.

Protect human, machine, and agent identities. Control how they authenticate, access, and interact across systems.

# AI SECURITY: THE OPKALLA WAY

4



## AI RUNTIME PROTECTION

Secure every AI interaction in real time.

Inspect prompts and outputs, block harmful content, and prevent threats like prompt injection and data leakage.

5

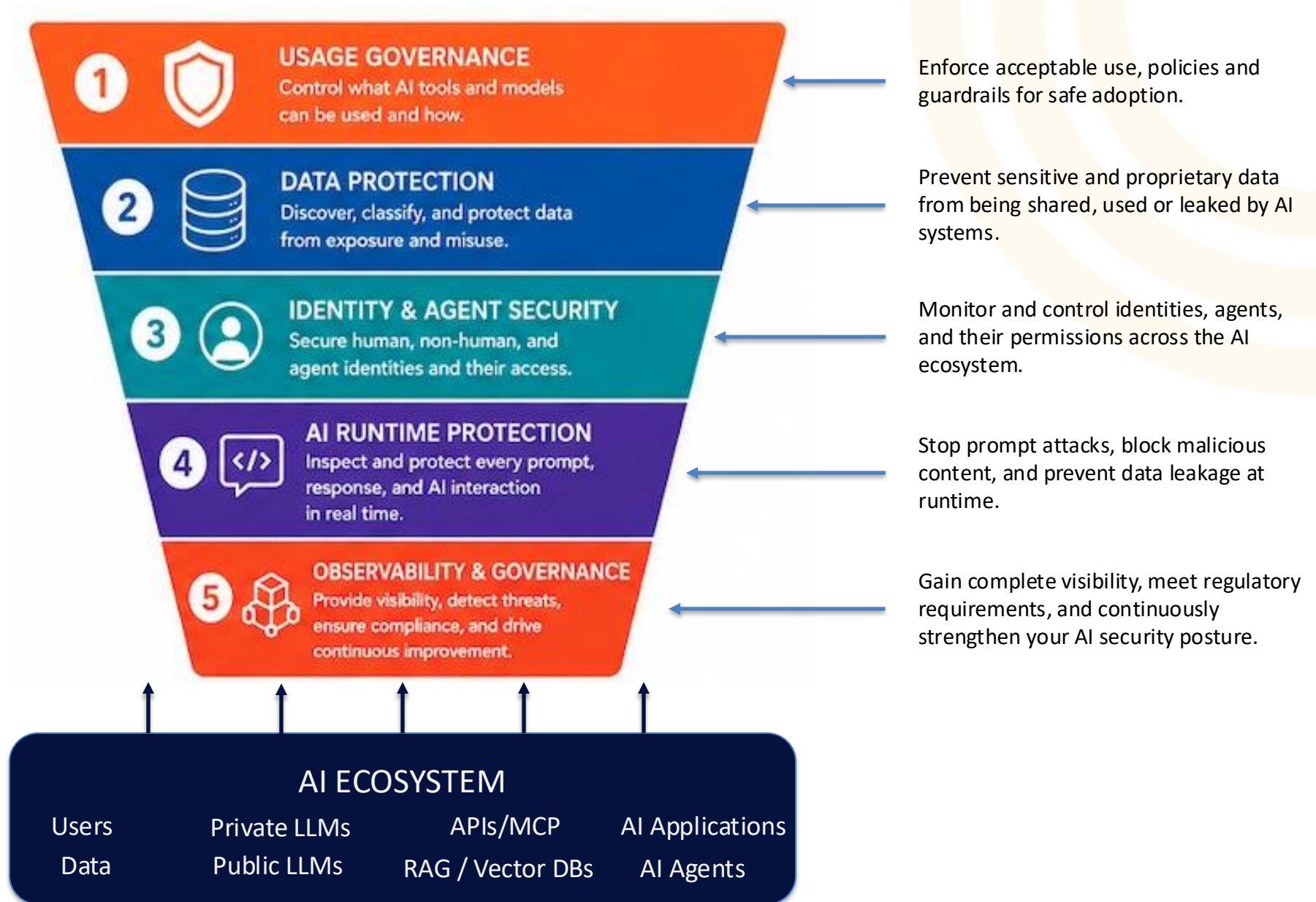


## OBSERVABILITY & GOVERNANCE

See everything. Govern everything. Improve continuously.

Unify visibility, detect threats, ensure compliance, and drive continuous improvement across the AI ecosystem.

## HOW AI SECURITY WORKS TOGETHER



# WHAT SUCCESS LOOKS LIKE



Safe AI Adoption at Scale



Threats Detected and Stopped



Protected Data and IP



Regulatory Confidence



Secure Agents and Identities



Business Value Realized

# NEXT STEPS

