

Governance and Security Operations for the AI Workforce

Refoundry AgentShield provides governance and security operations designed specifically for the AI workforce, helping organizations discover, govern, monitor, and protect AI agents before they become business risk.

The AI workforce is already here. **Who's governing it?**

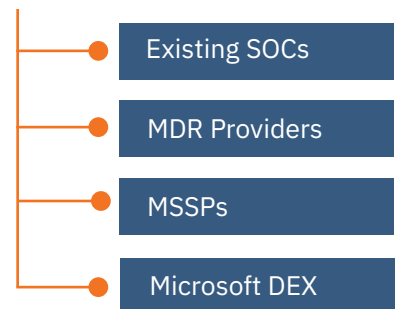
Organizations are rapidly deploying Microsoft 365 Copilot, Copilot Studio agents, Agent 365, Power Platform automations, and custom AI solutions to accelerate productivity, streamline operations, and transform the way work gets done.

These digital workers can access data, invoke tools, execute workflows, and take actions on behalf of users. Yet most organizations lack the visibility, ownership, governance, and operational controls needed to manage them responsibly at scale.

5 Questions Every Organization Must Answer

- ① What AI agents do we have?
- ② Who owns them?
- ③ What can they access?
- ④ What are they doing?
- ⑤ What happens when something goes wrong?

Compatible with:



AgentShield Delivers

Observe

- Identify AI agents, digital workers, and agentic workflows operating across your Microsoft ecosystem.
- Gain visibility into inventory, purpose, ownership, activity, and associated risk.

Govern

- Establish ownership, accountability, risk classifications, lifecycle controls, and governance processes for your AI workforce.
- Ensure agents remain aligned with policies, security requirements, and business objectives.

Protect

- Understand what agents can access and reduce unnecessary risk.
- Evaluate permissions, connected systems, data access, and potential exposure across the Microsoft platform.

Monitor & Respond

- Monitor agent activity, investigate unusual behavior, and coordinate response actions when risk is identified.
- Extend operational confidence beyond human identities to include the growing AI workforce.

Why AgentShield?

- **Governance First:** AgentShield goes beyond monitoring by providing ownership validation, lifecycle management, governance reviews, reporting, and operational oversight for AI agents.
- **Built for Microsoft AI:** Designed for Microsoft 365 Copilot, Copilot Studio, Agent 365, Power Platform, and custom AI solutions operating across the Microsoft ecosystem.
- **Works Alongside Existing Security Investments:** Complements your SOC, MDR, MXDR, MSSP, Microsoft Unified, or internal security operations team without requiring replacement of existing providers.
- **Microsoft Security & AI Expertise:** Delivered by specialists with deep experience across Microsoft identity, security, governance, compliance, and AI technologies.

Service Options

AgentShield Security Operations

Extend governance with monitoring, investigation, and response capabilities.

- Agent activity monitoring
- Security event investigation
- Alert triage and analysis
- Incident response coordination
- Operational reporting
- Ongoing risk management

AgentShield Governance

Build the operational foundation required to govern your AI workforce.

- Agent inventory and discovery
- Ownership assignment and validation
- Risk classification
- Lifecycle management
- Governance reporting
- Executive visibility and oversight

Govern the Future Workforce

The industry spent the last decade securing human identities.

The next decade will require organizations to govern and secure digital workers, AI agents, automations, and agentic workflows with the same rigor applied to the human workforce.

Refoundry AgentShield helps organizations confidently adopt AI by providing the visibility, governance, and operational controls needed to manage the AI workforce at scale.

