QUISITIVE

The Invisible Threat — Agent Sprawl

You Can't Govern What You Can't See

Overview

The **Agentic AI Security Foundation & Readiness** offering is a focused, execution-led engagement designed to help enterprises establish early control and visibility across agentic AI systems. As organizations move from AI pilots to autonomous and semi-autonomous agents, traditional human-centric security models no longer provide sufficient governance, attribution, or risk containment. This solution creates a defensible security baseline that enables innovation while limiting unmanaged exposure.

Why This Matters

Agentic AI introduces new security dynamics:

- Non-human identities now outnumber human users
- Access paths are dynamic, API-driven, and continuously changing
- AI agents can access and move data without human checkpoints

Without early visibility and baseline controls, risk accumulates silently—leading to ownership gaps, audit exposure, and costly remediation after agents are already in production.

Benefits & Value

- **Reduced Unmanaged AI Risk** – Make AI agents and non-human identities visible, attributable, and reviewable
- **Baseline Access Control** – Limit over-privileged agents and uncontrolled access paths
- **Early Security Signals** – Surface hidden exposure across identity, data, and AI workloads
- **Executive Confidence** – Evidence-based insight into current AI security posture
- **Defensible Starting Point** – Foundation for governance, threat modeling, and secure scale

What to Expect

1. **Agent Identity & Control**
   Identify AI agents and non-human identities, establish ownership, and baseline access patterns across identity and infrastructure.
2. **AI & Data Security Visibility**
   Baseline data access and exposure paths and enable security signals across identity, data, and AI workloads using Microsoft security telemetry.
3. **Validation & Executive Readout**
   Validate controls, synthesize findings, and deliver an executive-ready posture summary with a prioritized roadmap.

Quisitive's Approach

Quisitive delivers this engagement as a pragmatic accelerator—**designed to establish control before governance and scale.**

- **Execution-first, low-impact delivery**
- **Audit and discovery-mode leverage of Microsoft security tooling**
- **Foundation-before-governance mindset, purpose-built for agentic AI realities**

Why Choose Quisitive

- Proven enterprise security delivery experience across complex Microsoft environments
- Microsoft-first depth across Entra ID, Defender, Purview, and Sentinel
- Risk-aware execution that improves posture without disrupting production systems
- End-to-end capability spanning advisory, implementation, and managed security services

Outcomes / Value Delivered

- Clear visibility into deployed AI agents and associated non-human identities
- Baseline access controls aligned to Zero Trust principles
- Security signals enabled and correlated across identity, data, and AI workloads
- Reduced uncertainty and unmanaged risk exposure
- Executive-ready findings and a prioritized roadmap for next-phase governance and scale

Getting Started / Entry Points

Agentic AI Security Foundation & Readiness Accelerator

A 3-week, execution-focused engagement to establish control, visibility, and security posture

Secure Agentic AI & Zero Trust Workshop

A focused session aligning stakeholders on agentic AI risk and modern security principles

AI & Data Security Readiness Assessment

A targeted evaluation of data access, exposure, and security signals supporting AI workloads

Take the first step toward securing agentic AI with confidence.

Contact Quisitive to establish your AI security foundation and enable safe scale.