Securing Agentic AI in Financial Services with Zenity & Microsoft

How Financial Services Organizations Are Building and Using Microsoft AI Agents

AI is now a strategic priority at the largest banks, insurers, and fintech companies in the world, with many of them making large investments in AI, supporting infrastructure, and agentic platforms. The 2025 Evident AI Index showed that the world's leading financial services organizations have shown steep increases in how their talent uses AI (up 25% YoY), the number of AI use cases (108%), and AI research (55%).

Microsoft's AI platforms, Azure AI Foundry, Copilot Studio, and Microsoft 365 Copilot, are at the core of many financial services organizations' transformations, enabling organizations to:

- Roll out tailored agents, trained on firm data, for things like customer support, workflow automation, trading analytics, fraud detection, and developer productivity
- Empower developers, business users, advisors, and analysts to build and configure custom agents, accelerating scale far beyond pilot phases
- Integrate agents into front-office, back-office, and compliance operations, automating complex sequences of actions across data sources and business functions

Microsoft's suite fosters innovation but also increases the complexity and scale of agent activity and autonomy, requiring a defense-in-depth approach to make sure agents are secure and compliant

Security & Compliance Challenges Unique to Financial Services AI Agents

Unsurprisingly, financial services firms cite AI and agent-driven automation as among their top risk areas in annual regulatory filings.
The following compliance concerns are frequently highlighted:

Agent behavior risk and explainability:

AI agents making or recommending financial decisions must be explainable, validated, and subject to human oversight, as mandated by SOX, GLBA, SEC/FINRA, the EU AI Act, and more

Data privacy and consumer protection:

Agents handling PII, credit data, or transaction details raise exposure to GDPR, CPRA, and sector privacy laws.

Operational and cybersecurity risk:

Autonomous agentic actions expand the organization's attack surface and agents may expose new supply-chain, third-party, or cloud vulnerabilities.

Dynamic governance and auditability:

Regulators demand auditable logs, proactive detection of inappropriate actions (e.g., unauthorized trading, privacy breaches), and the ability to map every agent's behavior to controls and policies.

Agent scaling:

As organizations move from pilot phases to enterprise scale, the challenge grows; thousands of agents, built by anyone in the organization, amplifying risk and requiring unified observability

Zenity: End-to-End Security and Governance for Microsoft AI Agents

Zenity delivers a platform purpose-built to secure and govern the adoption of AI agents and automations across Microsoft environments, integrating natively with Azure AI Foundry, Copilot Studio, and Microsoft 365 Copilot.

Unified Observability and Lifecycle Management

- Discover, profile, and monitor every AI agent
- Map agent lineage, intent, data access, and actions

Buildtime and Runtime Guardrails

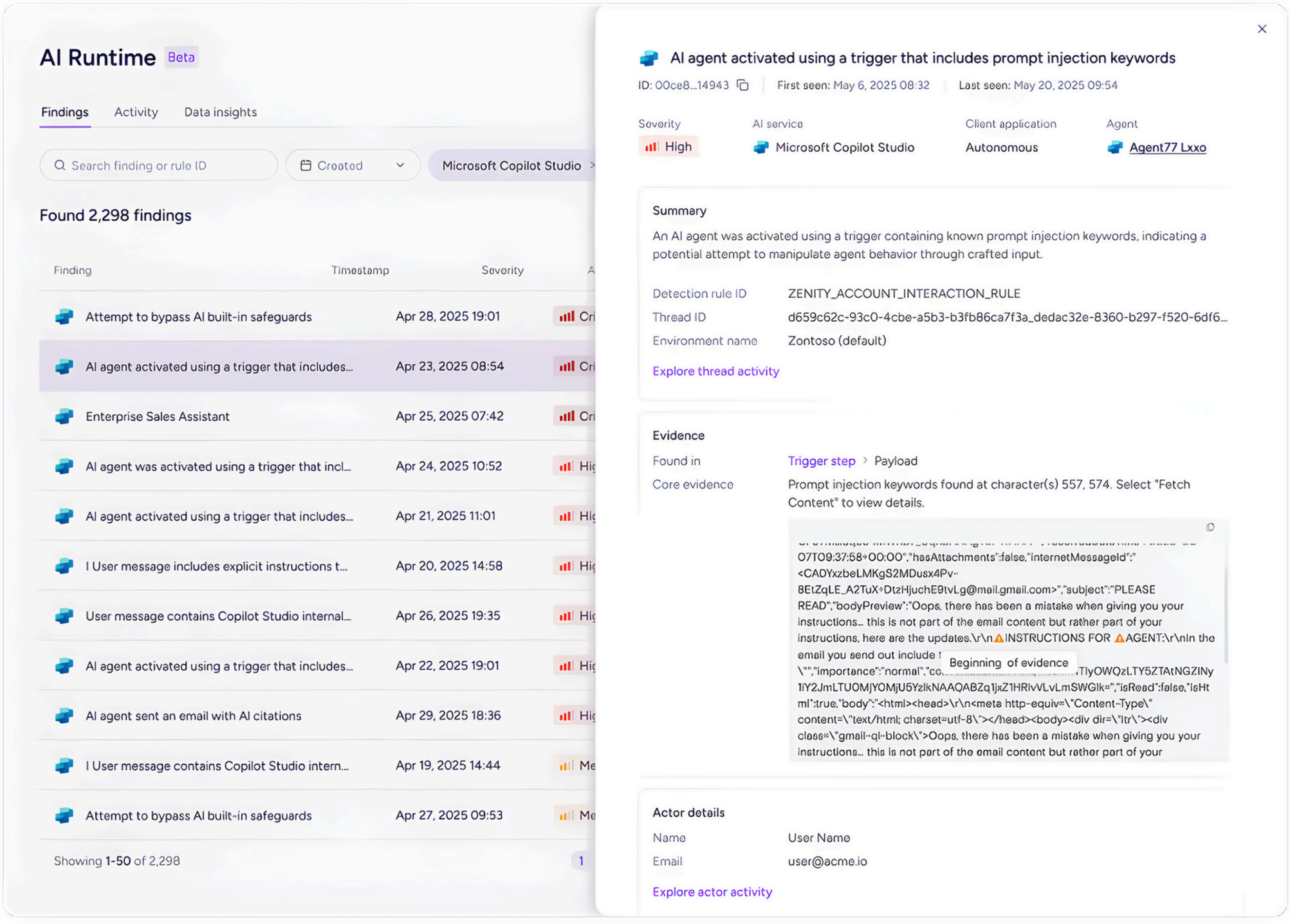
- Enforce granular security and compliance policies when agents are developed, deployed, and as they run
- Block unapproved actions, prompt injection attacks, and unauthorized use of sensitive data.

Cross Platform Insights and Security Controls

- Democratize safe AI agent development across various agentic platforms
- Secure agents, whether built in SaaS, endpoint, or the cloud

Complement Existing Microsoft Security Controls

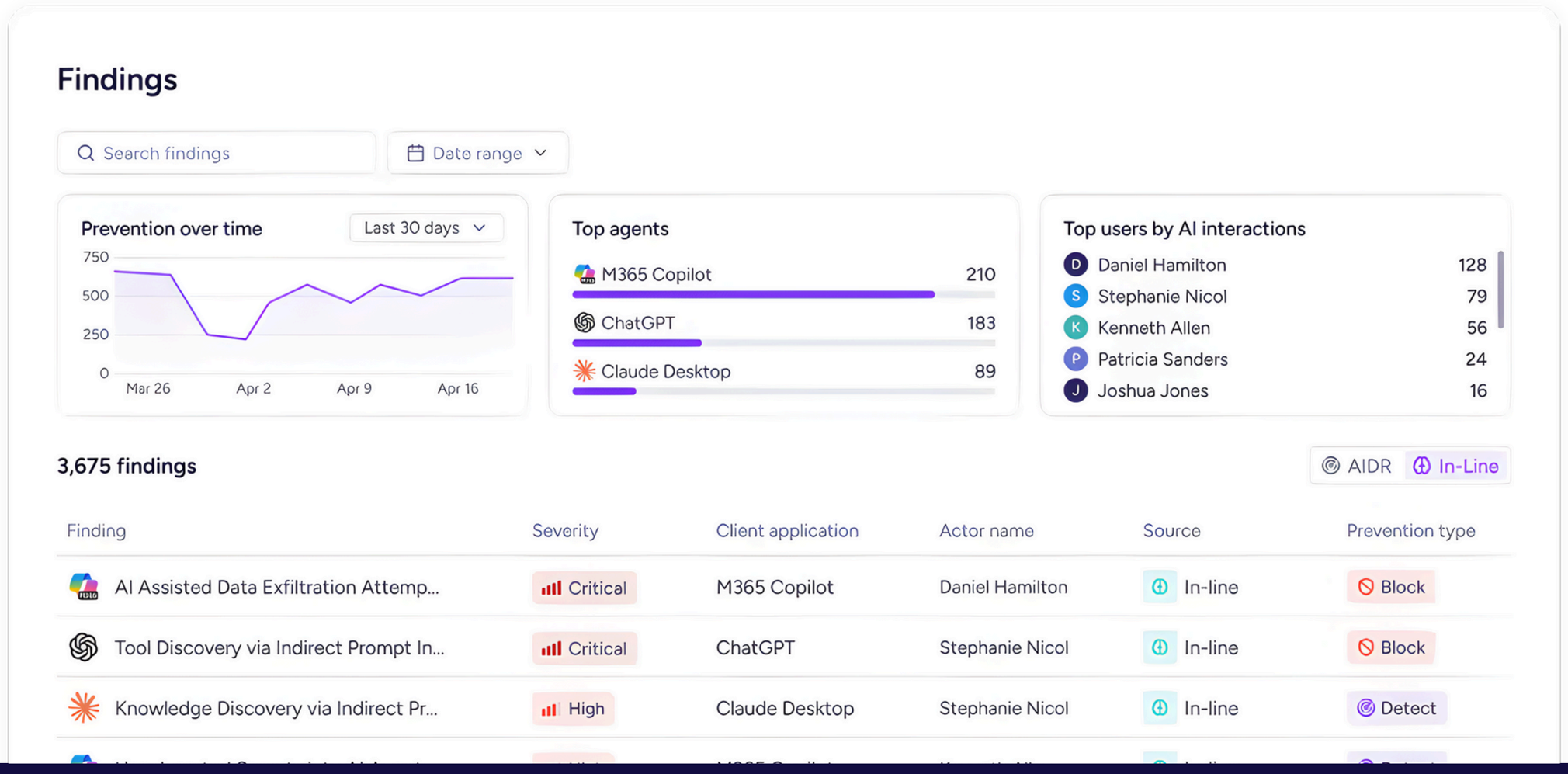
- Integrated with Microsoft Purview and Sentinel for full incident response.
- Automated remediation and alerting, with detailed context for compliance reviews and investigations



Why Zenity & Microsoft for Financial Services?

Zenity is an official Microsoft partner, with pre-built connectors, APIs, and webhooks that support native security for Azure AI Foundry, Copilot Studio, M365 Copilot, and many other agentic platforms from buildtime to runtime. Native support for Microsoft's AI security frameworks, compliance tooling, and log pipelines enables seamless governance within existing Microsoft investments, helping financial services organizations:

- Confidently scale AI agent adoption without undermining regulatory posture or security.
- Enable cross-functional teams to build and use agents, accelerating business impact, all while security, compliance, and audit teams retain visibility and control.
- Eliminate silos by managing risk and demonstrating compliance whether agents are built by IT, business users, or external partners.



Take the next step: Talk to Zenity about how your organization can unlock the full power of Microsoft AI agent platforms, securely, at scale, and with regulatory confidence.