zenity

SOLUTION BRIEF

Zenity AISPM for Microsoft Fabric

Securing business users as they build Reports, Semantic Models, Apps, AI Skills, and Dashboards

Microsoft Fabric is an end-to-end, human-centered analytics platform that brings together all an organization's data and analytics in one place and allows anyone to collaborate to foster a well-functioning data culture. Power BI is a tool within Fabric that helps users analyze and visualize data to make informed decisions.

Using PowerBI, anyone can also easily create and tailor reports and dashboards, generate and edit DAX calculations, create narrative summaries, and ask questions about their data all using drag-and-drop interfaces and natural language. Further, with Copilot in Power BI, anyone can leverage AI to analyze and pull the right data from reports and dashboards.

Fabric users can also build AI Skills to create their own conversational Q&A functions for Fabric resources. When building an AI Skill, business users can provide and configure it with instructions and examples to guide the AI to the correct answer for any given question in your organization. This allows the maker to ensure that the AI understands their organization and data context before sharing this capability more broadly with others in the organization or team.

Zenity's AI Security Posture Management (AISPM) solution helps customers gain full visibility, identifying any AI Skills, reports, semantic models, or other resources in the environment, assessing them all for risks, and incorporating automated prevention and detection & response capabilities.

Key Risks

In previous iterations, even though PowerBI contained pathways to sensitive data, it was largely used as a way of ingesting data, rather than exporting it. However, in today's world, PowerBI is a full-fledged development platform, meaning business users of all technical backgrounds can create powerful business systems and access data outside of the traditional software development lifecycle (SDLC). This means that there are few guardrails in the way of ensuring that business users are building secure and properly shared resources.

These resources are then frequently shared throughout the enterprise. Particularly when granted with the power of AI, it can be challenging to identify where data leakage is happening. This includes gaps in knowledge for who is building what, who is accessing those resources, and where data is flowing.

While Microsoft offers native security controls inside of the Fabric Admin Portal and Defender, these tools are focused on the platform itself and lack the granular visibility and impact analysis needed to secure the individual resources built.

The Solution

Zenity has built an agent-less AISPM solution to secure anything built within Microsoft Fabric, including how end users are interacting with those resources using Copilot and other queries. Zenity's solution is built on three pillars:

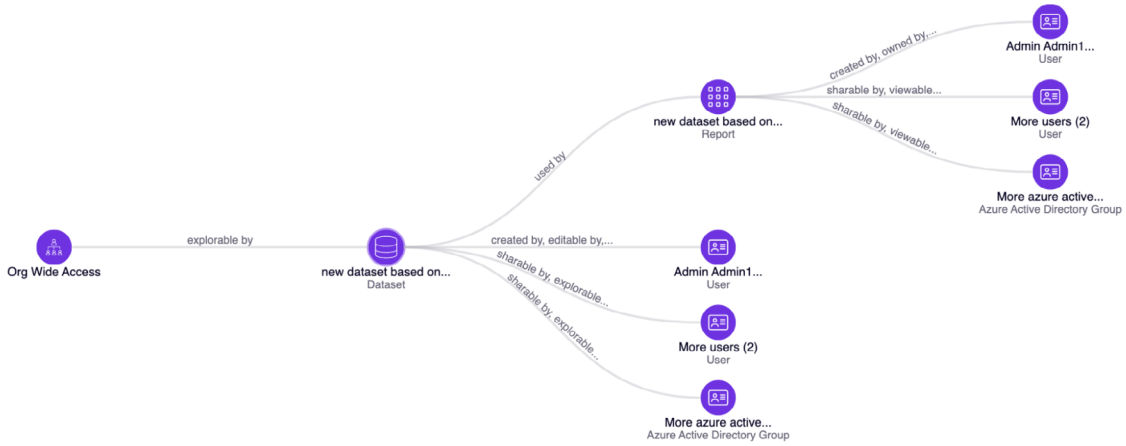
Key Stats

Zenity researchers have identified some statistical ranges for the most common risks stemming from citizen led development in Power BI[1]

- Average enterprise has upwards of 16,500 resources created in PowerBI
- Reports accessible by the entire tenant: 10-33%
- Datasets accessible by the entire tenant: 10-33%
- Data sources suspicious of poisoning: 8-19%
- Workspaces with excessive privileged access: 16-41%

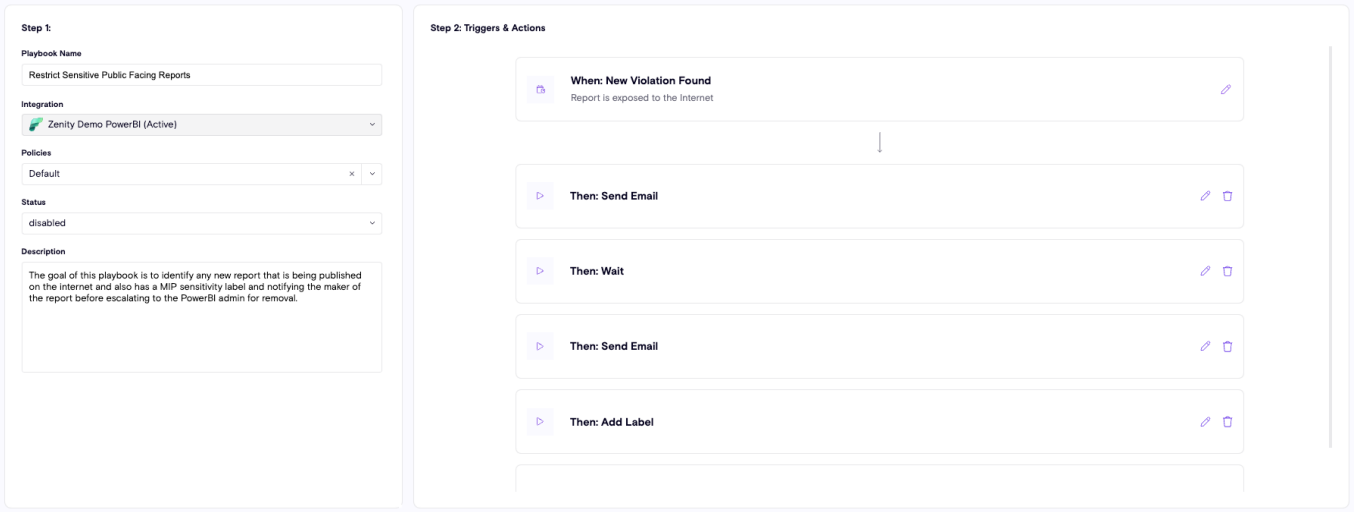
[1] https://www.zenity.io/resources/white-papers/the-state-of-enterprise-copilots-and-low-code-development/

- **Visibility:** Zenity provides a real-time inventory, covering both Personal and Shared workspaces and everything in between that is built in Fabric, including Reports, Semantic Models, AI Skills, Apps, Dashboards, Datasources, and more. This inventory includes detailed metadata of the resource lifecycle, access to sensitive data, SBOM files, maker information, and adoption trends.



- **Risk Assessment**: All resources are ran through the Zenity risk engine, which contains over 100 security, hygiene, and compliance policies to identify risks. Zenity contextualizes those risks by mapping them to popular security frameworks like the OWASP Top 10 for LLMs and Low-Code/No-Code. Common risks include sensitive data leakage, least privilege violations, guest access mismanagement, data poisoning, and more. Using the Zenity Attack Graph, security teams can map relationships, uses, users, and components that might be exposing the organization to risk.

- **Governance**: Zenity's Automated playbooks and policy engine allows security teams to quickly enforce guardrails to ensure continuous secure adoption of Fabric, as well as execute burndown campaigns of existing risks within the enterprise.



zenity

About Zenity

Zenity, the world's first application security platform for Agentic AI, protects organizations from security threats, helps meet compliance, and enables business continuity. Established in 2021, many of the world's leading organizations trust Zenity to help configure security guardrails, generate prioritized lists of vulnerabilities, and accurately pinpoint and remediate vulnerabilities by continuously scanning business-led development platforms and providing centralized visibility, risk assessment, and governance. Visit us at https://www.zenity.io for more.