zenity

SOLUTION BRIEF

Zenity for Microsoft Power Platform

Securing business users as they build Apps, Automations, Websites, Copilots, and Reports without needing coding expertise

Microsoft Power Platform is a suite of low-code tools that are built to help anyone build custom business applications, automate workflows, analyze data, create websites, and build their own copilots, AI agents and apps. The five products within Power Platform are:

- Power Apps to build custom apps
- Power Automate to automate repetitive tasks and workflows
- Copilot Studio to create and customize AI agents, bots and extensions
- Power BI to analyze data and gain insights via dashboards and reports
- Power Pages to create and manage modern and responsive websites

All of these products have been infused with AI to allow business users to more easily navigate and leverage them. Power Platform products can be used individually or together to create comprehensive solutions that integrate throughout the Microsoft ecosystem, including Azure, Dynamics 365, Microsoft 365, and more. With over 1,000 Power Platform connectors, Microsoft enables anyone to connect data across the application stack using simple drag-and-drop interfaces and natural language prompts.

As business users are able to build powerful business systems that leverage internal data, the upside is easy to spot. However, when using Power Platform, there is an implicitly shared responsibility model between Microsoft and its customers that security teams need to be aware of so they can properly foster secure adoption.

Key Risks

As part of the shared responsibility model, Microsoft instills native security controls built to protect the underlying infrastructure of the tools themselves including uptime, data security, and availability.

Further, the Microsoft Center of Excellence (CoE) Starter Kit contains a collection of Power Automate flows that can do things like generate an inventory of active and inactive resources, contact owners of new environments, and generate welcome emails. With this open source toolkit, security teams can configure high-level visibility and governance into the Power Platform tenant.

However, the various business applications that are being created by business users across the Power Platform environment, as well as the adoption of Microsoft Copilots (365 Copilot, Sharepoint Copilot, Copilot for Sales, et al) require a deep understanding of business logic and context in order to properly secure them; and this falls on the enterprise to manage and secure.

The Solution

Zenity has built an agent-less, cross-platform solution to secure resources built across Microsoft Power Platform, including agents, copilots, and other AI apps, working in tandem with the CoE to provide comprehensive security and governance throughout the Microsoft low-code ecosystem. Zenity's solution is built on three pillars.

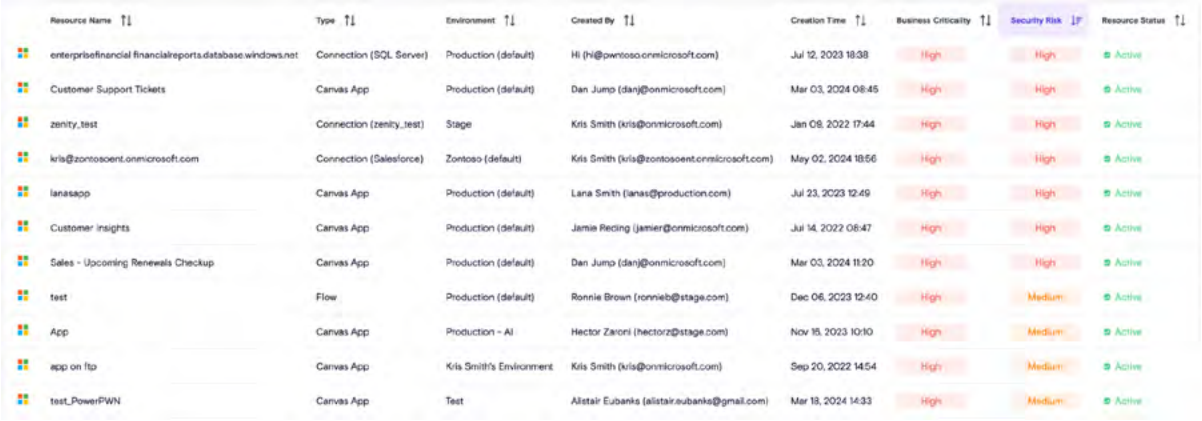
Key Stats

Zenity research has identified that the average large enterprise has[1]:

- Upwards of 79,600 individual apps, automations, and copilots built across the low-code estate
- More than 11,000 of those contain access to sensitive data
- 63% of copilots that are built on Power Platform are overshared
- 8,641 instances of untrusted guest users containing access to Power Platform apps
- Nearly 8,400 apps that do not require authentication, with 3,910 exposing credentials in plain text or via insecure steps

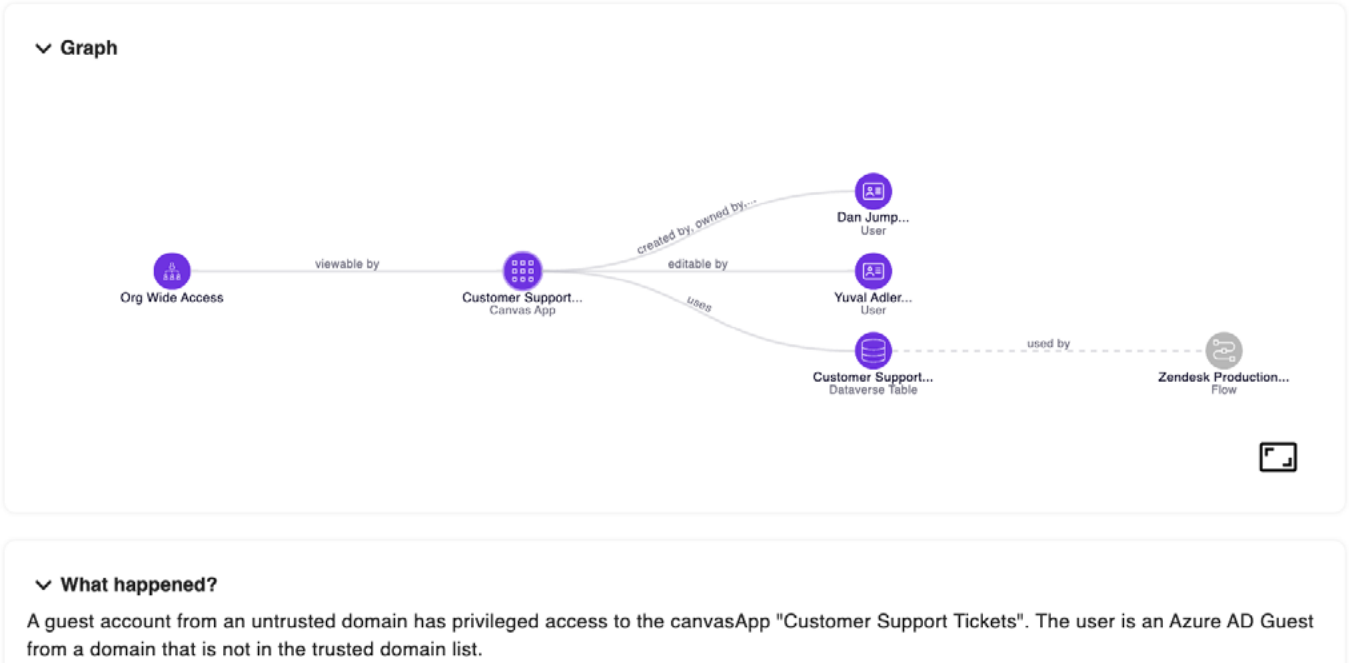
[1] https://www.zenity.io/resources/white-papers/the-state-of-enterprise-copilots-and-low-code-development/

- **Visibility:** Zenity provides a real-time inventory, covering Canvas Apps, PowerBI reports and dashboards, AI agents, and anything in between that can be built. This inventory includes detailed metadata of the resource lifecycle, which resources contain access to sensitive data, SBOM files, business criticality labels, and more.



Resource Name	Type	Environment	Created By	Creation Time	Business Criticality	Security Risk	Resource Status
enterprisefinancial.financialreports.database.windows.net	Connection (SQL Server)	Production (default)	Hi (hi@pwntoso.onmicrosoft.com)	Jul 12, 2023 18:38	High	High	Active
Customer Support Tickets	Canvas App	Production (default)	Dan Jump (danj@onmicrosoft.com)	Mar 03, 2024 08:45	High	High	Active
zenity_test	Connection (zenity_test)	Stage	Kris Smith (kris@onmicrosoft.com)	Jan 09, 2022 17:44	High	High	Active
kris@zontosoent.onmicrosoft.com	Connection (Salesforce)	Zontoso (default)	Kris Smith (kris@zontosoent.onmicrosoft.com)	May 02, 2024 18:56	High	High	Active
lanasapp	Canvas App	Production (default)	Lana Smith (lanas@production.com)	Jul 23, 2023 12:49	High	High	Active
Customer Insights	Canvas App	Production (default)	Jamie Reding (jamier@onmicrosoft.com)	Jul 14, 2022 06:47	High	High	Active
Sales - Upcoming Renewals Checkup	Canvas App	Production (default)	Dan Jump (danj@onmicrosoft.com)	Mar 03, 2024 11:20	High	High	Active
test	Flow	Production (default)	Ronnie Brown (ronnieb@stage.com)	Dec 06, 2023 12:40	High	Medium	Active
App	Canvas App	Production - AI	Hector Zaroni (hectorz@stage.com)	Nov 15, 2023 10:10	High	Medium	Active
app on ftp	Canvas App	Kris Smith's Environment	Kris Smith (kris@onmicrosoft.com)	Sep 20, 2022 14:54	High	Medium	Active
test_PowerPWN	Canvas App	Test	Alistair Eubanks (alistair.eubanks@gmail.com)	Mar 18, 2024 14:33	High	Medium	Active

- **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, hard-coded secrets, guest access mismanagement, least privilege violations, 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 Power Platform, as well as execute burndown campaigns of existing risks within the enterprise. Ex. An existing customer noticed 80,000 security violations upon deploying Zenity, and within 3 months had mitigated upwards of 70,000 of them

zenity

About Zenity

Zenity is the first platform designed to help enterprises secure and govern copilots and low-code/no-code development. The Zenity platform is built from the ground up with a security-first approach centered on three pillars: Visibility, Risk Assessment, and Governance. As the founding member of the OWASP Top 10 project specifically focused on low-code/no-code development as well as authoring the GenAI Attacks Matrix, inspired by MITRE ATLAS, Zenity takes a community-oriented approach to this rapidly evolving security vector.

With SOC 2 Type 2 and GDPR compliance, Zenity's agent-less platform is uniquely positioned to help enterprises truly know their business apps.

For more information, visit us at https://www.zenity.io.