zenity

PRODUCT BRIEF

Security Governance for AI and Business-Led Development

Major SaaS vendors like Microsoft, Salesforce, and ServiceNow all embed and promote business-led development in their offerings, providing anyone with the ability to build powerful business applications, conversational bots, automations, and more. AI is only making it easier and faster to promote this type of professional and citizen development, with Gartner estimating that by 2026 more than 80% of enterprises will have used Generative AI APIs and models, and/or deployed Gen AI enabled applications in production environments.

However, as more and more apps are built by business users throughout the enterprise the risks for data leakage grow astronmically.

Development Challenges

As business users are developing their own apps, automations, and copilots, there are a new set of challenges that security teams must be mindful of:

- Business users of all technical backgrounds are building their own apps and automations on a variety of SaaS platforms whether you know it or not, resulting in a new wave of shadow application development
- These new development platforms reduce and obfuscate the amount of code, rendering code-based security scanning tools obsolete
- Business users largely lack the technical and security know-how that is more commonly practiced by professional developers and members of IT
- Due to the speed and volume at which applications are developed, there are no official standards for the Software Development Lifecycle (SDLC) that apply to modern business app development
- Business applications often are required to access, transfer, and process sensitive data

Data Leakage

As applications are being built, there are a variety of ways that each individual resource can leak data, increasing the risks of security vulnerabilities, non-compliance, and business operations disruptions.

- **Over-Shared Resources:** Often-times, builders will grant too much access to the applications they are creating, violating the principle of least privilege and giving access to data to people that don't need it
- **Hard-Coded Secrets and Embedded Identities:** When building applications, it is easy for professional and citizen developers to embed their own identities and credentials into the application, which is then shared any time the app is used
- **Guest Access:** Third-party users will typically be granted access to low-code tools like Microsoft Power Platform, Salesforce, and ServiceNow, and are hard to monitor, meaning data can spill beyond the corporate boundaries
- **Risky Components:** Modern development platforms allow people to build apps using a series of drag-and-drop commands or AI-chat commands. However, some of these components are unverified and potentially insecure, and can be the root cause of data being exfiltrated.

There is a clear need for a new solution to bring application security controls to AI and business-led development.

Numbers to Know

80%
Will have used GenAI APIs and models and/or deployed Gen AI apps by 2026 [1]

90%
The amount that low-code/no-code development platforms can reduce dev time by [2]

750,000+
Average number of apps developed within low-code platforms

[1] Gartner Press Release, "Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026," October 11, 2023

[2] 451 Research Pathfinder Report | February 2018 | Commissioned by Red Hat

The Solution

The Zenity platform is built from the ground up with a security-first approach centered on three pillars: **Discovery, Risk Assessment, and Governance.** With SOC 2 Type 2 and GDPR compliance, Zenity's agent-less platform is uniquely positioned to help enterprises unleash modern application development, and are comprised of the following products:

Citizen Development Application Protection Platform (CDAPP)

Continuously scan all AI, low-code, and no-code environments, assessing each individual application for risk, and providing graph-based visibility and response

Application Security Posture Management (ASPM)

Centralize visibility of all applications created across different platforms, identifying each application that interacts with sensitive data and implementing corresponding guardrails for secure development

AI Security Posture Management (AISPM)

Scan the entire environment to identify bots and copilots that are leveraging and/or built with Generative AI. ensuring that each has appropriate authorization in place especially for those that are interacting with sensitive data, and similarly implementing guardrails for secure development

Vulnerability Management

Scan each individual app, automation, and copilot for risk and mapping those risks to popular security frameworks like OWASP and MITRE.

Secrets Scanning

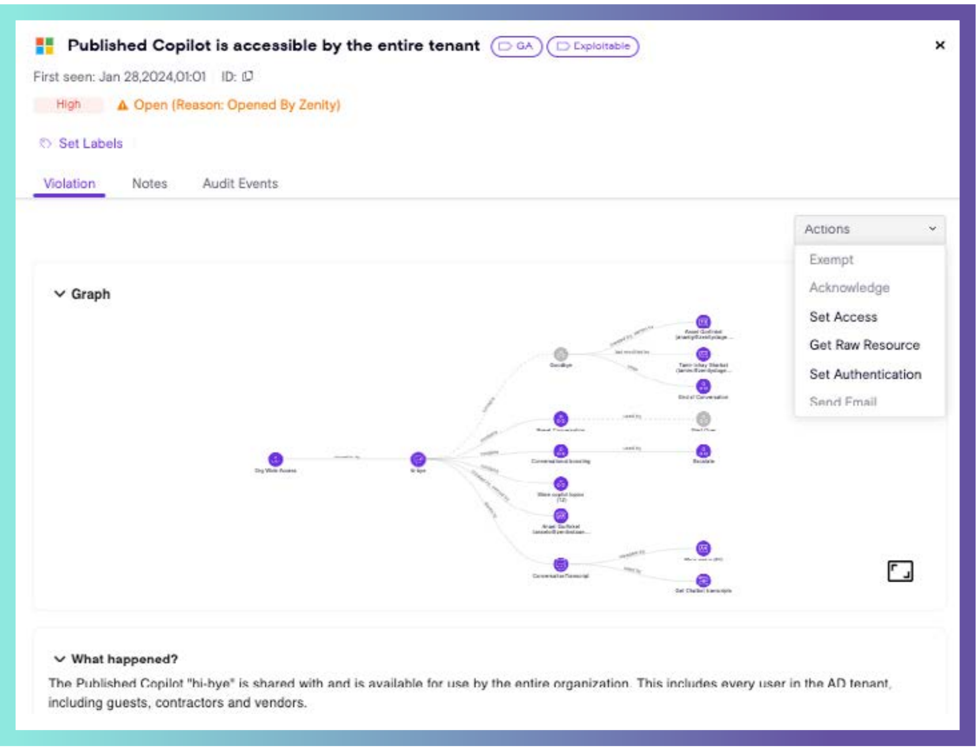
Identify hard-coded credentials that are baked into applications as they are built and automate security response to prevent malicious or unauthorized use

Software Composition Analysis

Craft robust third-party dependency analysis and SBOMs for all applications and AI copilots to identify individual components that are used in each individual application to pinpoint vulnerabilities

Data Security Posture Management (DSPM)

Identify and classify data that business-developed applications are interacting with and analyze all dataflows to establish what data is being taken outside of the corporate environment into personal accounts and external users.



Published Copilot is accessible by the entire tenant

First seen: Jan 28,2024,01:01 ID:

High ⚠ Open (Reason: Opened By Zenity)

The Published Copilot "hi-hye" is shared with and is available for use by the entire organization. This includes every user in the AD tenant, including guests, contractors and vendors.

About Zenity

Zenity, the world's first company focused on securing and governing low-code/no-code and Generative AI based development, 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 all connected low-code/no-code and GenAI development platforms with centralized visibility, risk assessment, and governance. For more information, visit us at https://www.zenity.io