Brazil also shows a clear unmanaged API problem. More than a third (37%) of organizations say they experienced incidents involving unmanaged APIs such as shadow or zombie APIs, and AI- and LLM-linked APIs. Our Brazilian respondents also pointed to authorization vulnerabilities and the limits of legacy tools like traditional WAFs as recurring causes of their API security incidents.

Q: Which of the following types of API security tools or platforms does your organization currently use? (Top six responses)

Tool	Global average/total	Mexico	Brazil
WAF (web application firewall)	80%	83%	73%
API gateway	70%	69%	69%
SAST (static application security testing)	65%	73%	59%
SIEM/SOAR	59%	72%	59%
DAST (dynamic application security testing)	50%	39%	53%
API security (dedicated)	35%	41%	33%

At a time when organizations worldwide are expected to spend US$37 billion on generative AI in 2025 — including $19 billion at the application layer — stronger visibility into AI-linked APIs is becoming a basic requirement for protecting that investment.

Among Brazilian respondents, security teams are being asked to protect expanding API estates without the visibility needed to act early or the testing needed to keep up.