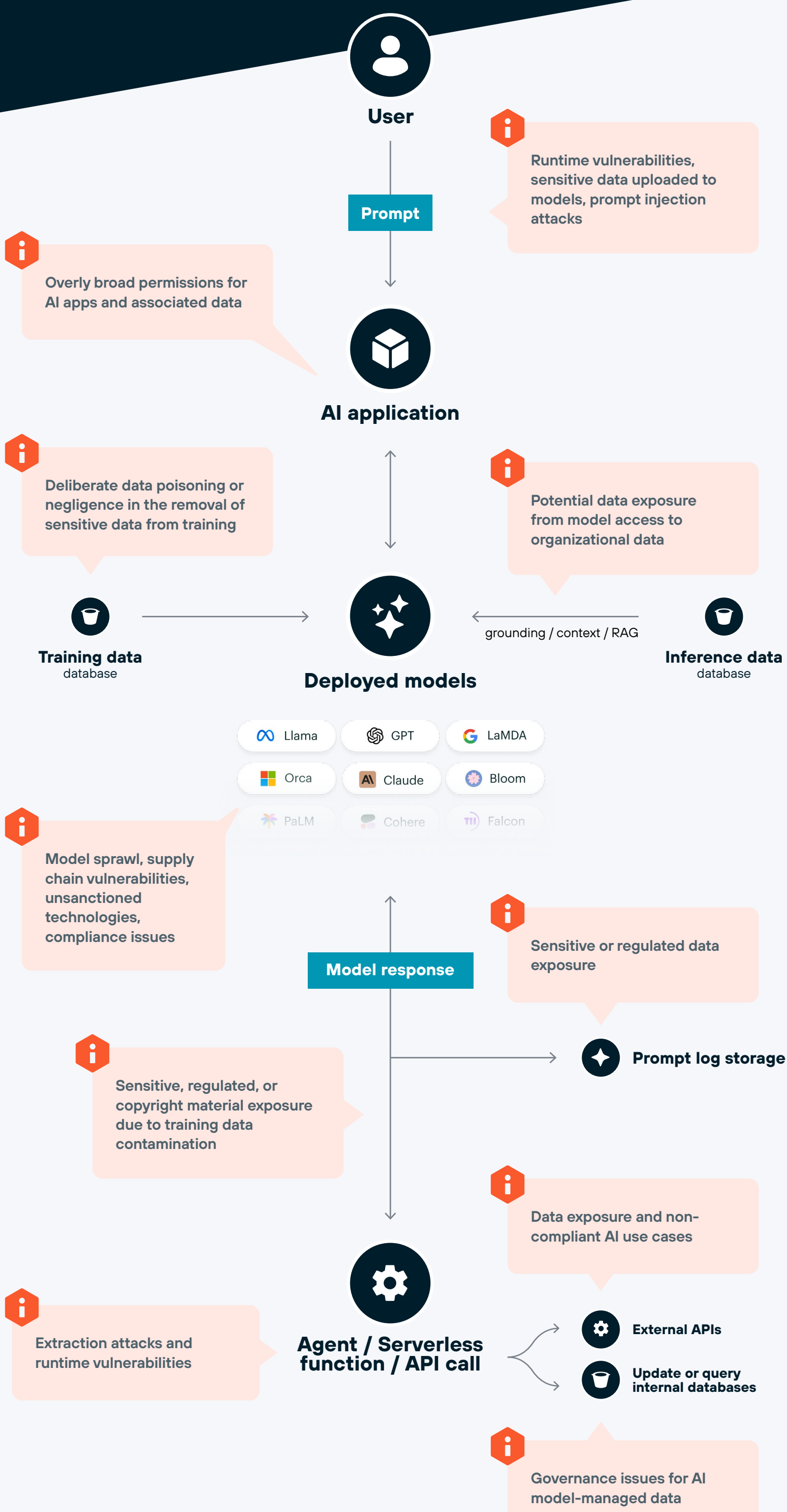
Understanding the Attack Surface for LLMs in Production

Training and deploying AI models lead to new vulnerabilities – from sensitive data exposure in the AI supply chain to prompt injection attacks. **Here are some of the potential risks in a generative AI workflow.**



Improve your AI security posture with Prisma Cloud AI-SPM

AI Model Discovery and Inventory

Discover deployed models across the different cloud environments. Project associated resources, and gain end-to-end visibility into your entire AI pipeline.

Posture and Risk Analysis

Identify vulnerabilities in the AI supply chain faster. Find misconfigured models and related cloud resources that can lead to data exfiltration or organizational resource misuse.

Data Exposure Prevention

Apply data discovery and classification capabilities specifically designed for AI inference and training data. Receive alerts of potential data leaks or unauthorized access.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com