Akamai Security

INTRODUCTION

Rupesh Chokshi

Senior Vice President and General Manager, Application Security

At customer meetings and industry events, and nearly every day when I read the news, one thing has become clear to me — as we fulfill the promise of the new era of AI, we need to be aware of the security challenges it's creating.

Already, we've seen some high-profile examples of what happens when AI isn't properly locked down. In perhaps the most famous incident of malicious AI manipulation, a man convinced a Watsonville, Calif. Chevrolet dealership's chatbot to agree to sell him a new Chevy Tahoe for $1. Months later, in February of 2024, a Canadian court found Air Canada liable for misinformation that its AI-powered chatbot had given to a consumer.

Those are just a couple of early examples, of course. Right now, companies around the world may be unwittingly introducing new AI vulnerabilities into their environments. The costs can be significant — to your reputation, to your bottom line, in compliance penalties, and to the very large investments so many have made into implementing AI in the first place.

Recently, at a checkup, my doctor asked if he could use an AI agent to take notes. That conversation extended beyond just my health — to weekend plans, my daughter's college choices and more. I wondered where that information was going. Did the doctor even know? Was there a potential HIPAA violation taking place?

These are the sorts of questions being asked in conference rooms and board meetings around the world — are we using AI safely? Are we building it securely? And if they aren't being asked, they need to be. AI has created a wave of optimism and innovation. But it brings with it a whole new realm of cybersecurity vulnerabilities, which existing security solutions are ill-equipped to handle. Already, we've seen a natural tension emerge between two parties:

- Chief AI officers and their development teams rushing to deploy new AI applications and business models
- CISOs who are left wondering how to protect against threats they may not even know about