

The AI Paradox

Enhancing Security or Empowering Hackers

Gilbert Joseph
Systems Engineer - Palo Alto Networks



What is a Deepfake?



A futuristic, orange-toned scene featuring a robotic hand hovering over a glowing 'AI' button on a control panel. The background is filled with various mechanical components, buttons, and a glowing screen, creating a high-tech, industrial atmosphere.

The Rise of Adversarial AI

Given the pace of innovation in cybersecurity, **threat actors** are adopting AI unlike anything we have seen before.





Artificial Intelligence

Machine Learning

Deep Learning

Generative
AI

LLM



AI Is Turbocharging the Speed and Scale of Attacks

Build Ransomware



\$2B impact from attack on a US health insurer in 2024

Compromise & Exfiltrate



15 million users' PII and confidential data exfiltrated in Jan 2024

Exploit Vulnerability



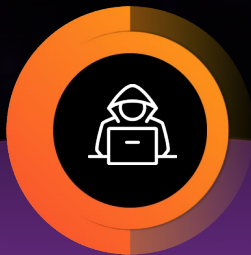
500+ organizations and 35+ million people affected by MoveIT vulnerability



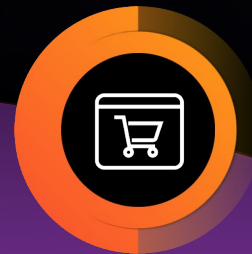
Customer Service
Copilots



Human Resources
Virtual HelpDesk



Fraud Detection
Applications



Shopping
Assistants



Intelligent Energy
Management Systems

...

AI-Powered Business Applications

...



Employees



57%

of employees
use public GenAI
apps **weekly**

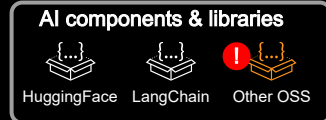
- ChatGPT
- Grammarly
- Vertex AI
- Hugging Face
- Coveo
- Elai
- Lightning AI
- Replicate
- Sapling AI
- ChatGPT
- Grammarly
- Copysmith
- SageMaker
- Adobe Firefly
- Codellum
- Hypotenuse
- Perplexity AI
- WandB
- NLP Cloud
- Swimm AI

AI-powered applications introduce new security risks

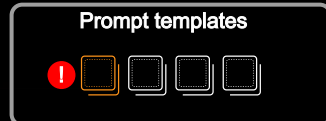
Supply Chain

Build with AI components & code

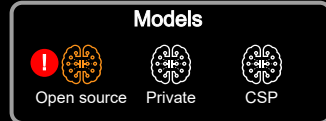
Corrupt AI/ML packages & libraries



Insecure prompt templates



Model vulnerabilities



Obscure data lineage; hard to trace issues

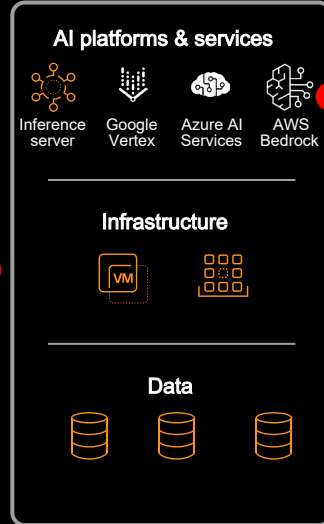


Inability to correlate & prioritize risks across AI services, models, & data

Risk from misconfigured data stores & infra (e.g., data poisoning)

App Stack

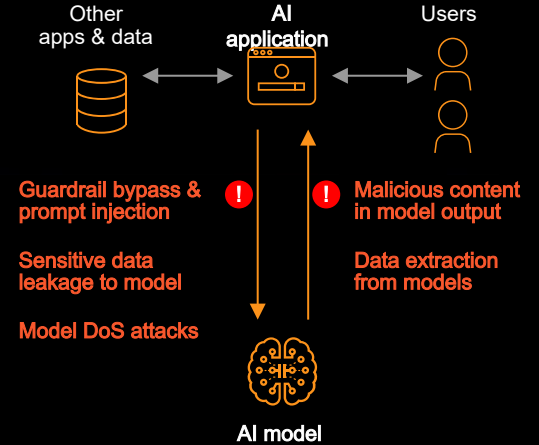
Leverage AI services, infrastructure & data



Limited visibility & context into AI usage

Runtime

Real-time app-to-model interactions



Steps to Secure AI by Design

Track and monitor AI usage for every employee

Secure every step of AI app development lifecycle and supply chain

Protect AI data from unauthorized access and leakage at all times

Delivered as an extension of existing cybersecurity solutions



**PREPARING
YOU FOR A
BRAND-NEW
FIGHT**