The AI Paradox

Enhancing Security or Empowering Hackers

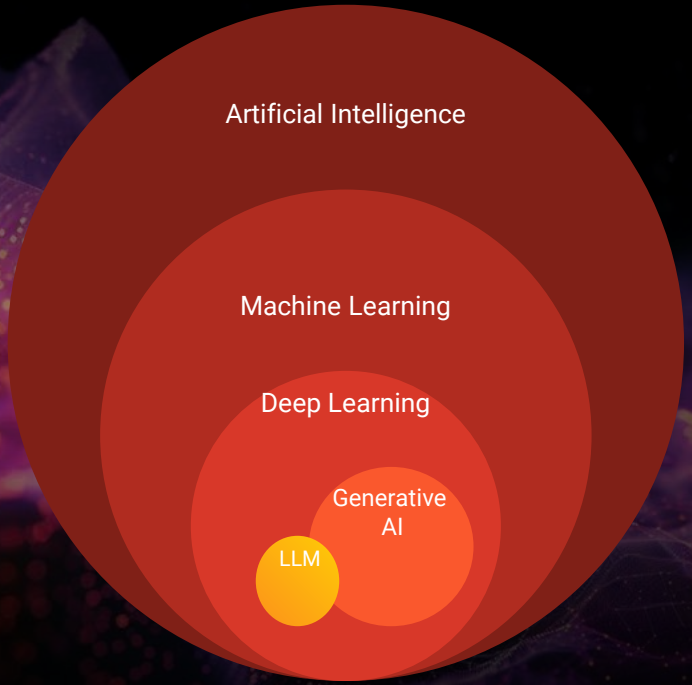
Gilbert Joseph
Systems Engineer - Palo Alto Networks

What is a Deepfake?

The Rise of Adversarial AI

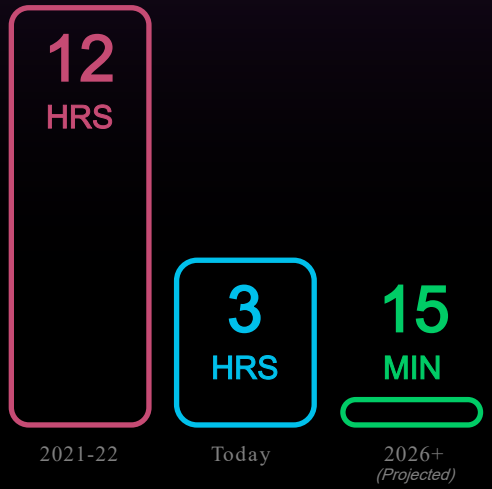
paloalto NETWORKS

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

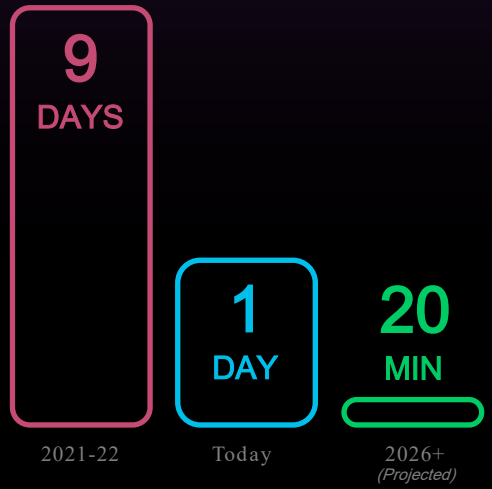
AI Is Turbocharging the Speed and Scale of Attacks

Build Ransomware



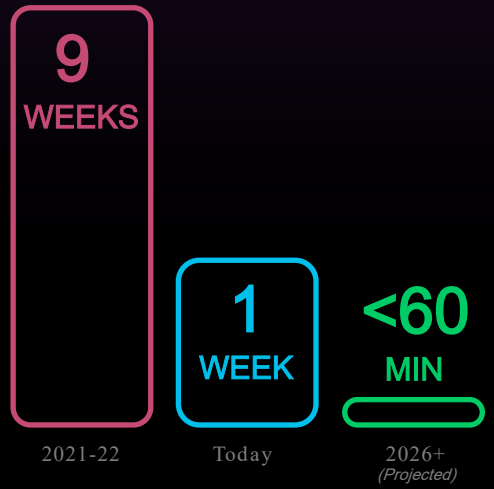
$2B impact from attack on a US health insurer in 2024

Compromise & Exfiltrate



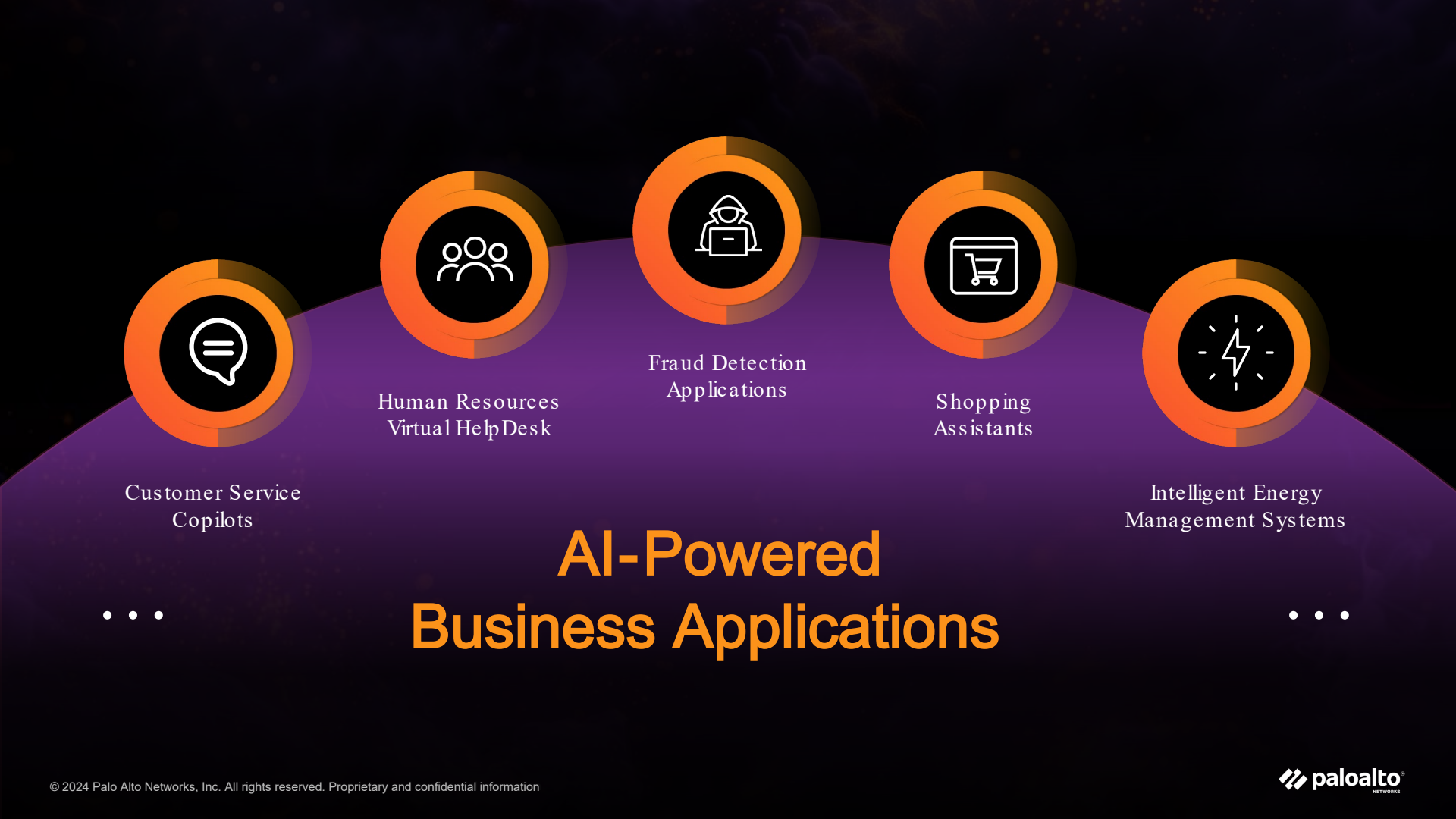
15 million users' PII and confidential data exfiltrated in Jan 2024

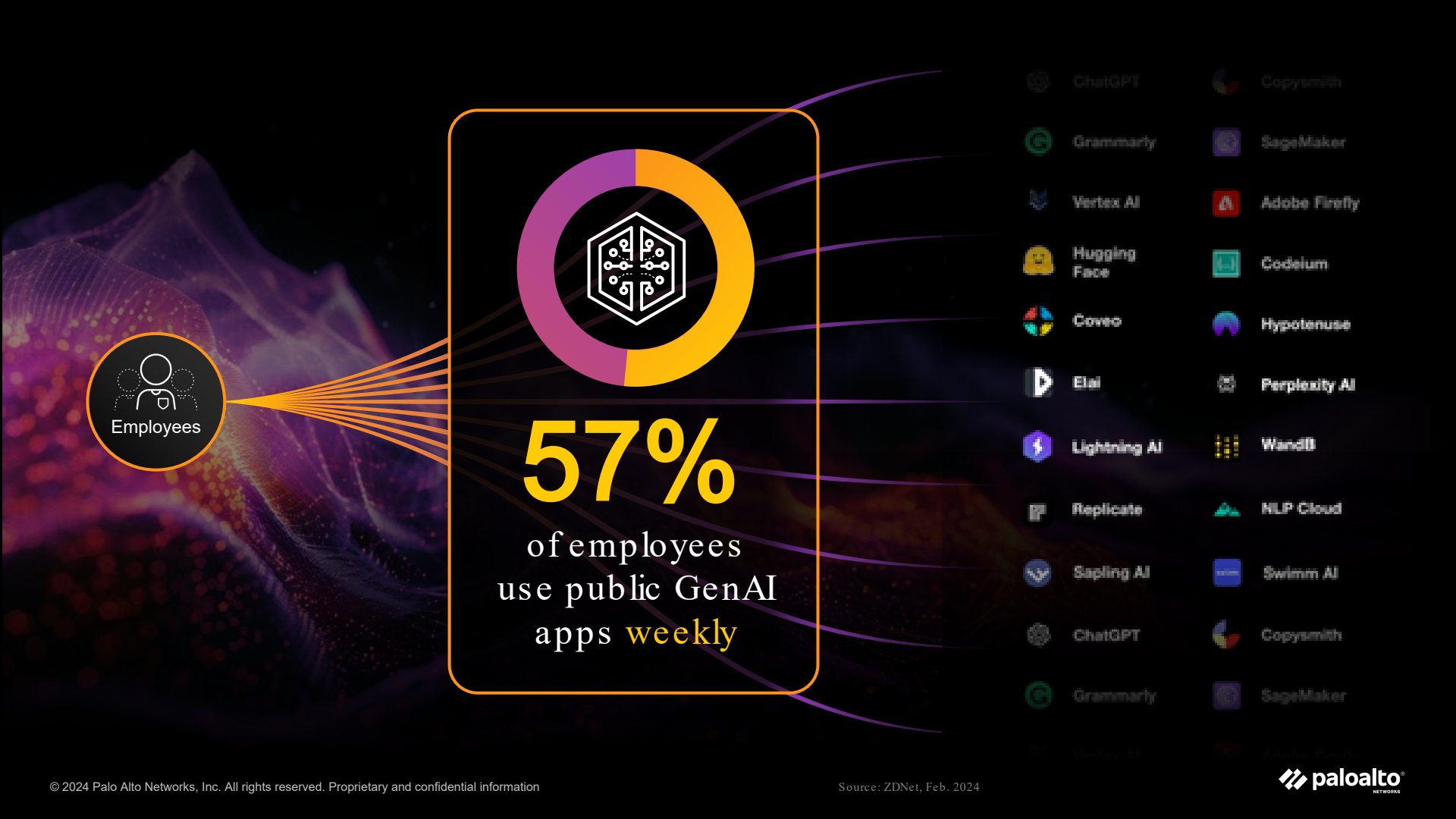
Exploit Vulnerability



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

paloalto NETWORKS





Source: ZDNet, Feb. 2024

paloalto NETWORKS

AI-powered applications introduce new security risks

Supply Chain

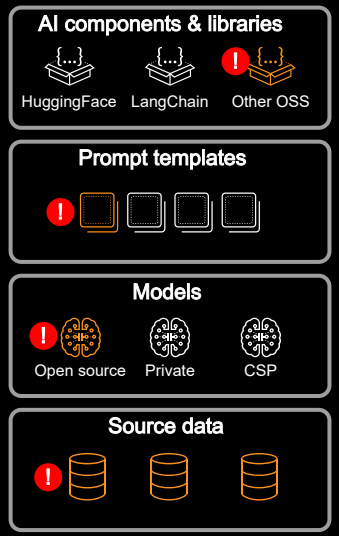
Build with AI components & code

Corrupt AI/ML packages & libraries

Insecure prompt templates

Model vulnerabilities

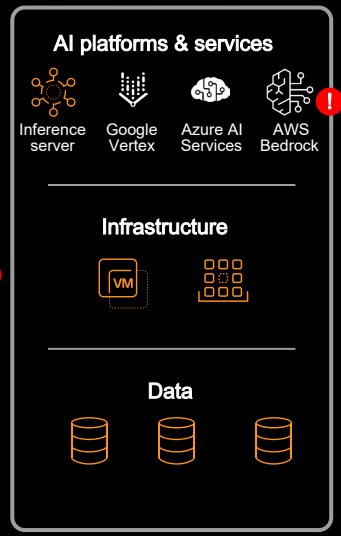
Obscure data lineage; hard to trace issues



App Stack

Leverage AI services, infrastructure & data

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

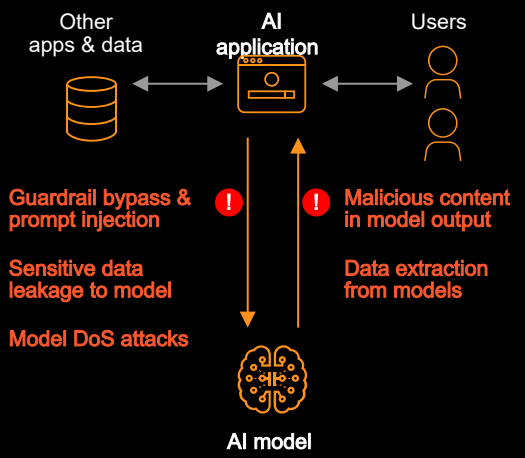


Limited visibility & context into AI usage

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

Runtime

Real-time app-to-model interactions



paloalto NETWORKS

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

paloalto NETWORKS

paloalto NETWORKS