



#AITK

Uhka vai mahdollisuus?

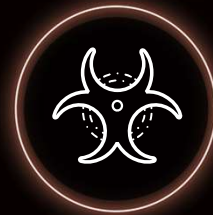
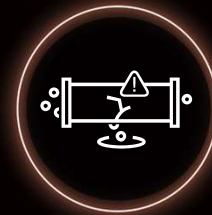
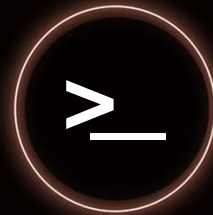
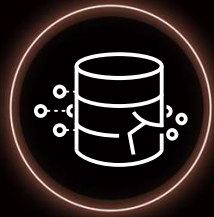
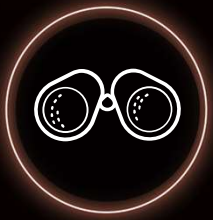




**WE ARE THE BEST
FRIEND OF MANY
CFO'S, CIO'S
AND CISO'S**

**(EVEN MOST NERDS LOVE US)
YOU WILL LIKE US TOO!**

AI is Both the **Attack Surface** and the **Attack Vector**



Reconnaissance

Data
Exfiltration

Modification of
System Prompts

Leakage of RAG
and Agent Data

Malicious
Outputs

2 Hours

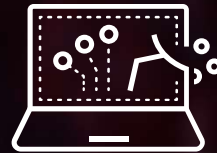
AI is Introducing New Security Risks



AI model
vulnerabilities



Shadow AI in
the
Enterprise



Sensitive
data
exposure



AI apps
exploitation

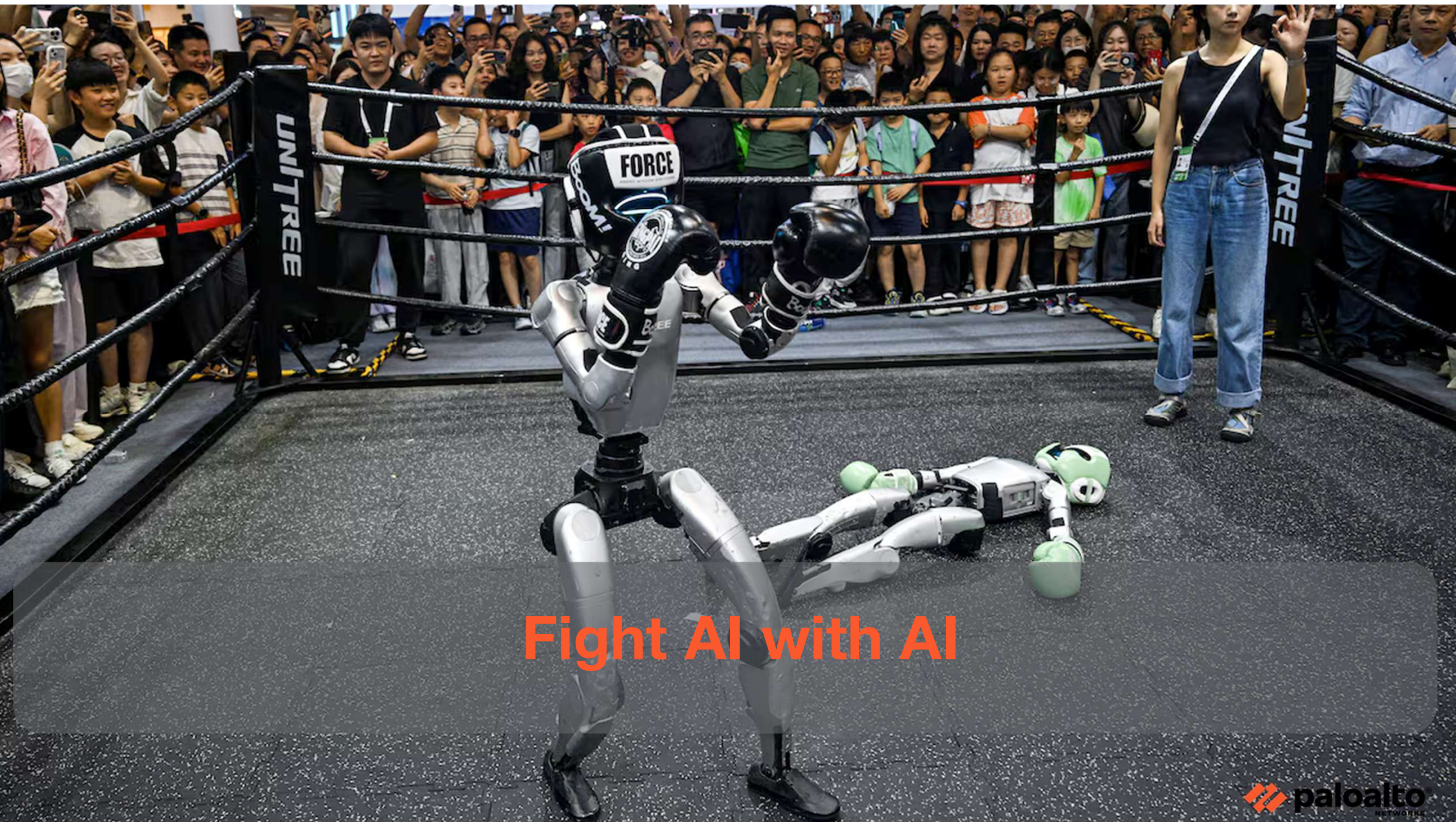


Rogue
AI Agents

only 6% of organizations have a robust AI security strategy

Source: [The 2025 AI Index Report](#), Stanford University, 2025.

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.



Fight AI with AI

AI Is Expanding Across Every Digital Surface

AI
Applications



Enterprise
Agents



Agentic
Endpoints



Agentic
Browsers



The Browser Is the New Workspace

85%

Of Work Happens in
the Browser

95%

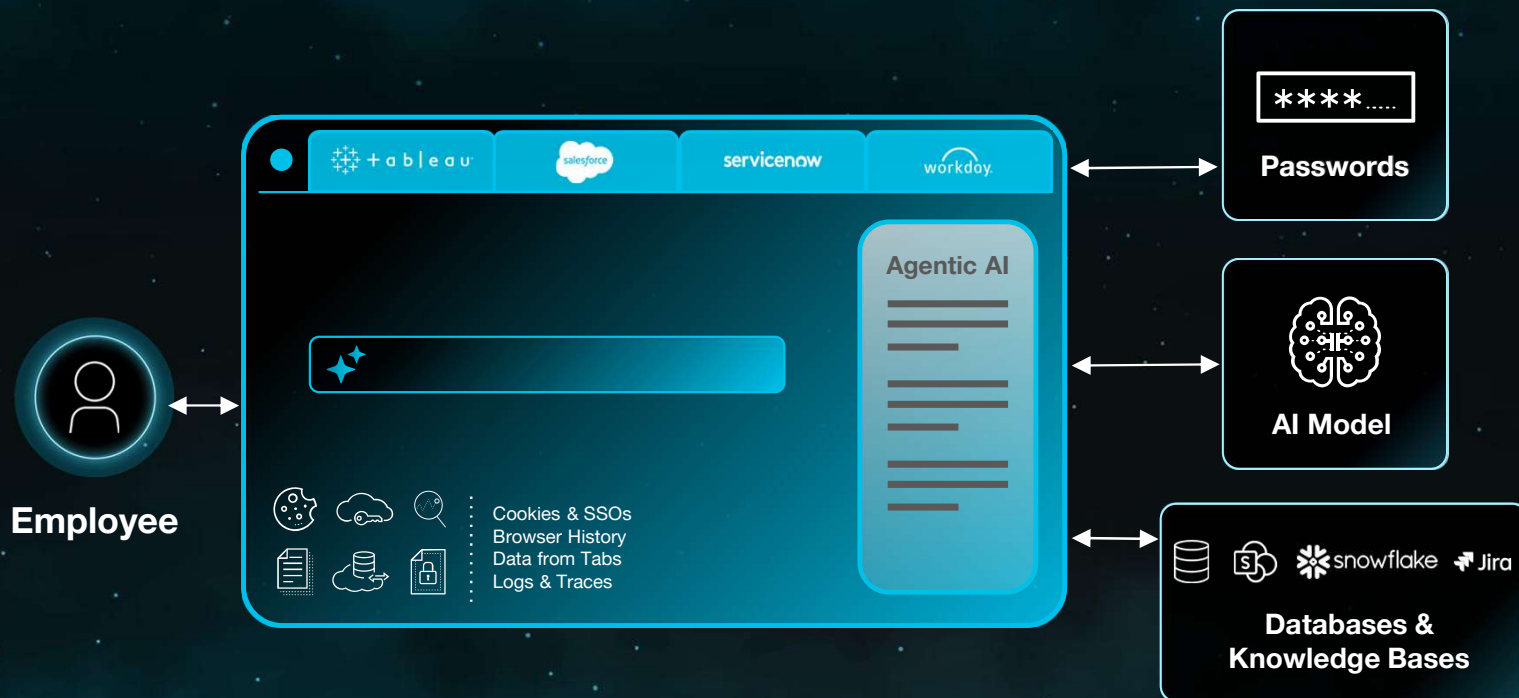
Of Organizations Report
a Browser-Based Attack



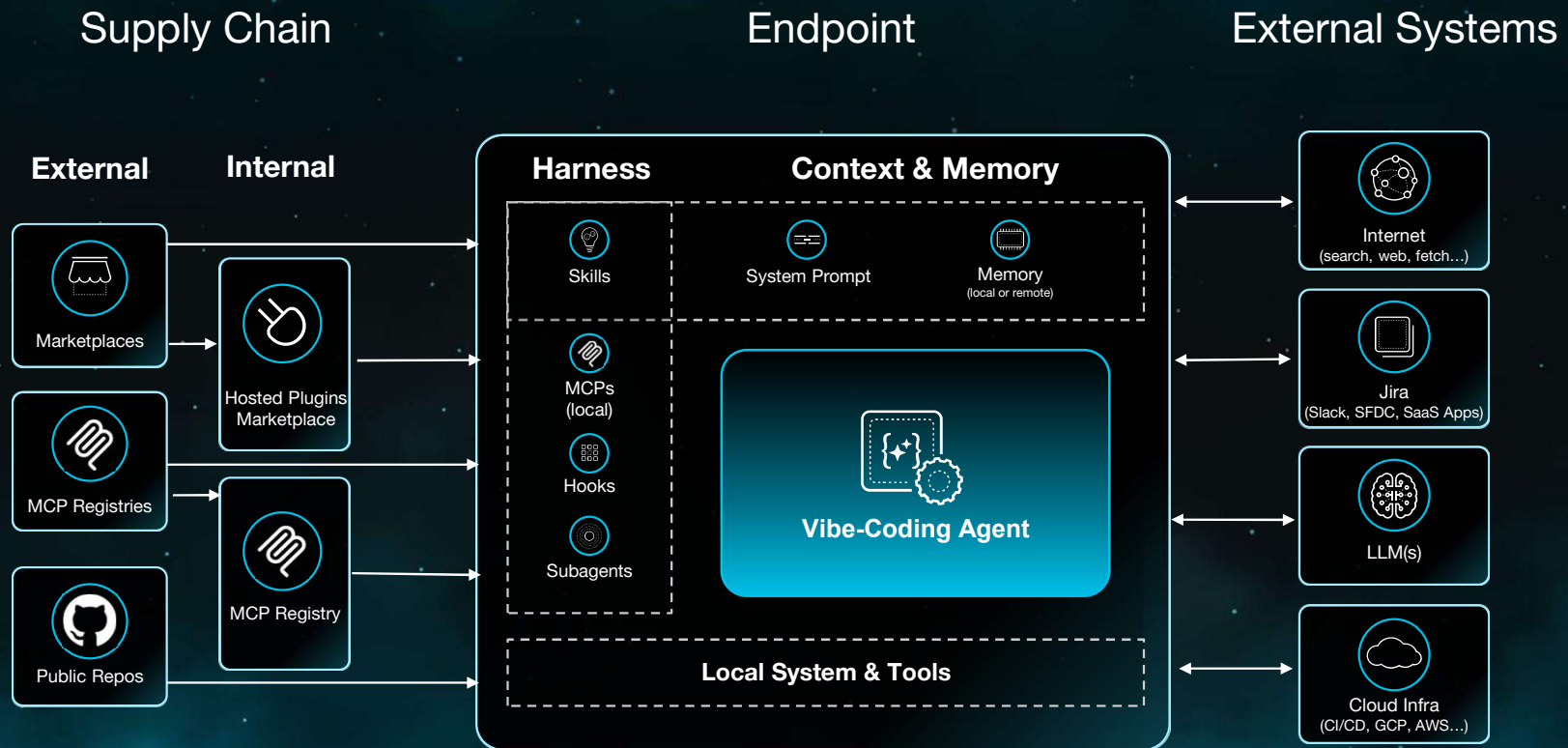
Source: The State of Workforce Security, Omdia Research, January 2025.

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Agentic Browsers Bring Autonomous Actions to Every Tab



AI Agents Have Moved to the Endpoint...

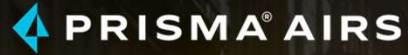


Secure AI by Design

 **PRISMA BROWSER™**
BY PALO ALTO NETWORKS



 **PRISMA AIRS™**
BY PALO ALTO NETWORKS

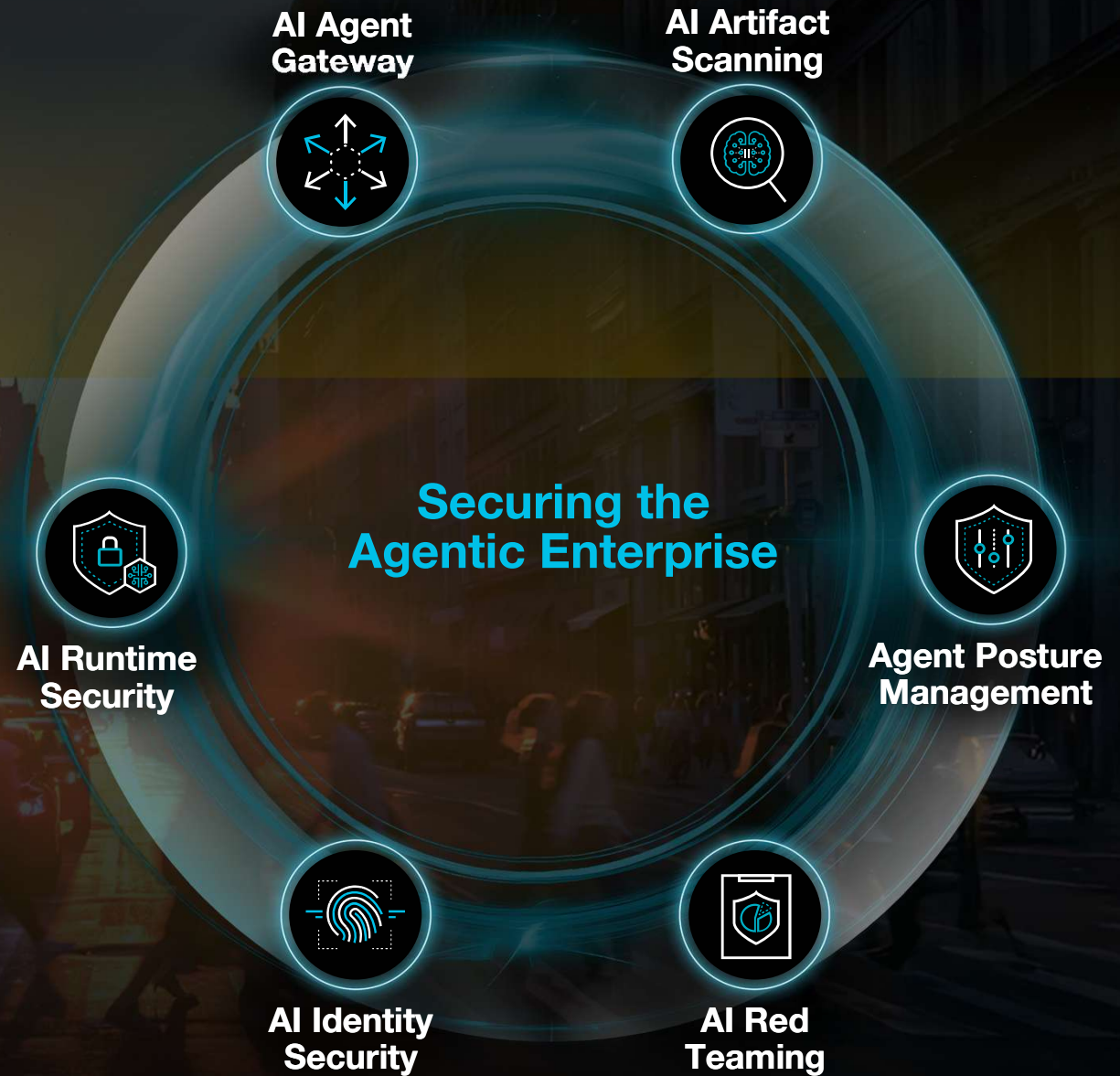


Introducing Prisma AIRS 3.0

Discover agents wherever they live

Assess agent risk continuously

Protect agent interactions in real-time





Now the Industry's Most Secure Browser for **Agentic**

AI

Any LLM

AI



Embedded AI Runtime Security



Safeguards on AI & Agentic Workflows



Identity-Aware Visibility & Governance



The Industry's Most Secure Browser



Malware Prevention



Web Security



Data Loss Prevention



Secure GenAI Access



Extension Security

Secure AI By Design Framework

SECURE USE OF
EXTERNAL AI TOOLS

MONITOR AND
CONTROL AI AGENTS

SAFELY BUILD AND
DEPLOY AI APPS

Discover

all AI tools in use

Govern

access to risky AI tools

Protect

data from exposure

Discover

your entire AI ecosystem

Assess

your AI risks

Protect

AI deployments against threats

Platformization Allows Our Customers to Focus on What's Next: AI Security



AI Security PRISMA AIRS

World's most comprehensive AI security platform



Network Security

STRATA

Best-in-class security across hardware, software, and SASE



SecOps + Cloud

CORTEX

#1 AI-driven SecOps platform, from code to cloud to SOC



Identity Security

CYBERARK

Leader in identity security for human, agentic, and machine identities