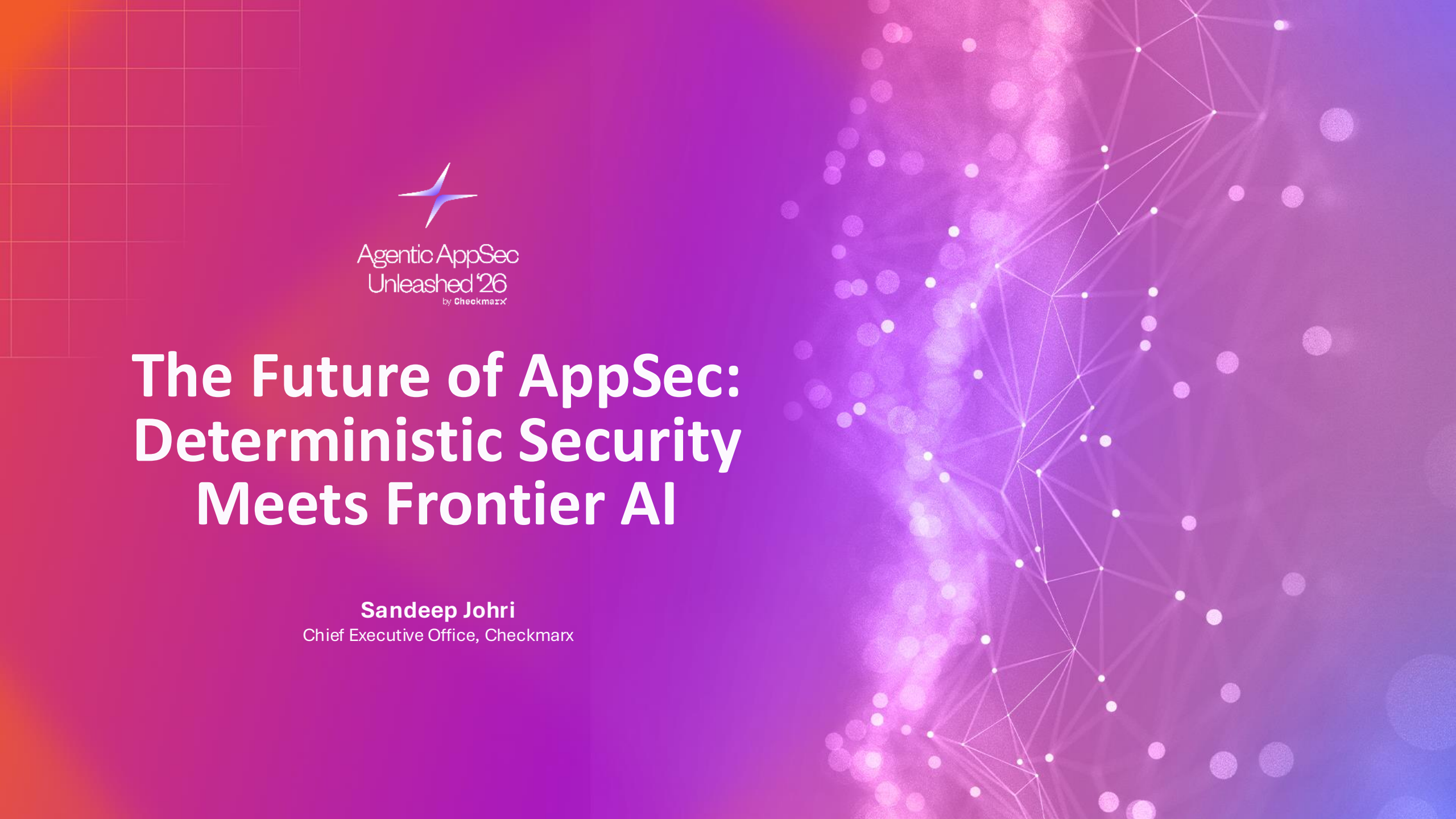
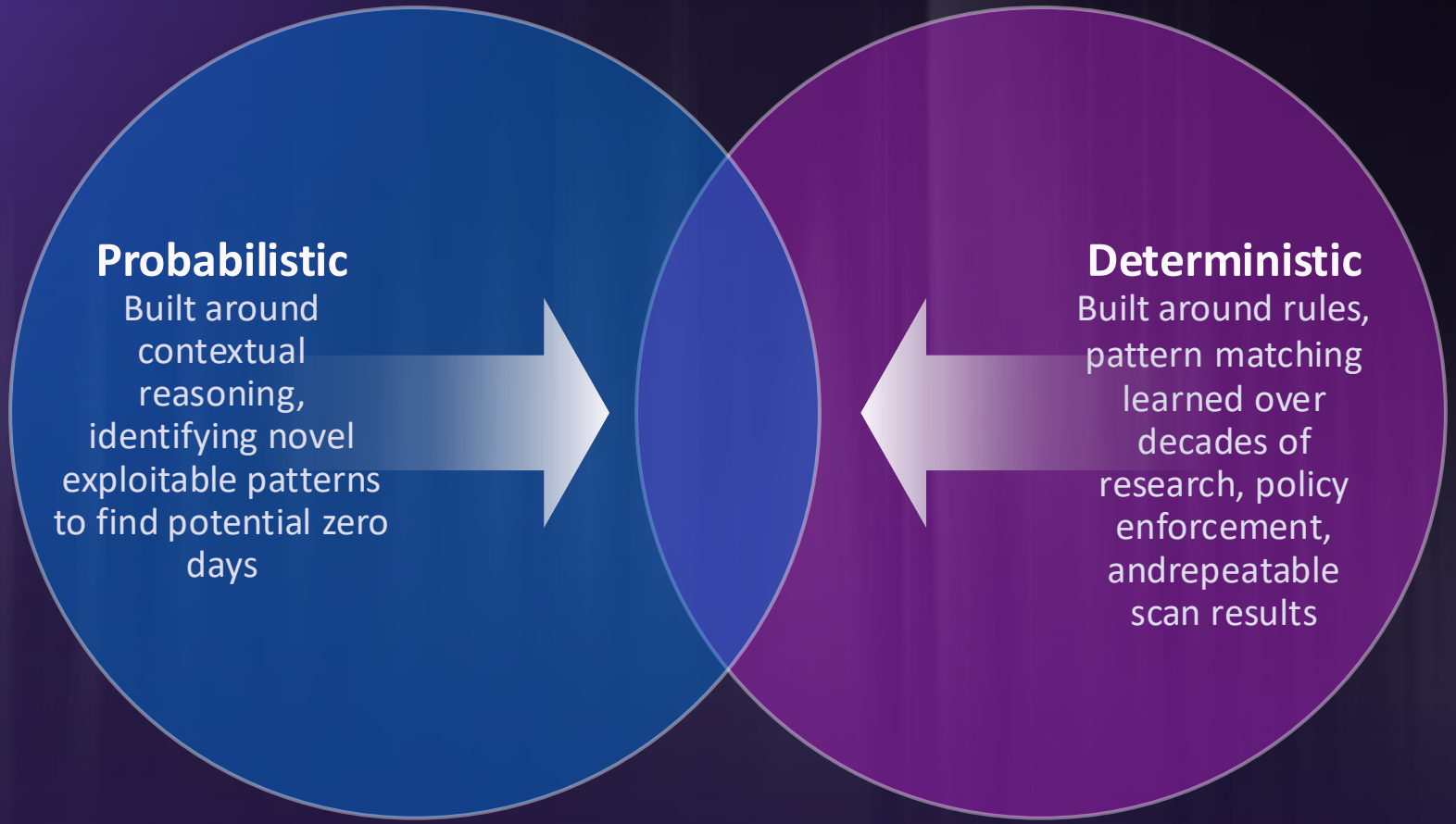


The Future of AppSec: Deterministic Security Meets Frontier AI

Sandeep Johri
Chief Executive Office, Checkmarx

The Future of AppSec Lies in a New Hybrid Approach

It’s No Longer a Choice Between AI and AppSec; It’s Both



The AI Paradox

While AI Creates Many Benefits, It Also Creates Downstream AppSec Challenges

AI Can Build

AI Can Scan

AI Can’t Fix Itself

Project Glasswing identified 20K vulns of which only 97 were patched

AI Can’t Defend Itself

Each new prompt or token used, can become an attack surface extension

The Economic Rupture

AI Necessitates Significantly Higher Velocity and Scale

Exploits can now be generated in minutes

Public exploits are weaponized faster than ever

Cost of attack is approaching zero

AI is removing the cost and skill barriers for attackers

Exploitation moving towards real-time

Time to weaponization is collapsing rapidly

The Governance Imperative

You Can’t Control What You Can’t See

AI BOM and Policy Enforcement

The New AI Attack Surface

Foundational Models

- **LLMs** — Training Data Poisoning
- **System Prompts** — Prompt Injection

Integration and Tooling Layer

- **AI SDKs & Client Libraries** — Malicious Packages
- **MCP Servers** — Tool Poisoning, Hijack

Developer Attack Surface

- **IDE Extensions** — Code Suggestion Hijack
- **AI Coding Assistants** — Insecure Completions

Runtime Agentic Surface

- **Autonomous Agents** — Data Exfiltration/Agent Hijacking
- **External Data / RAG Pipelines** — Context Poisoning

Security can no longer stand at the gates of software.

It must live inside the forge where software is created.

Agentic AppSec Unleashed '26

by Checkmarx