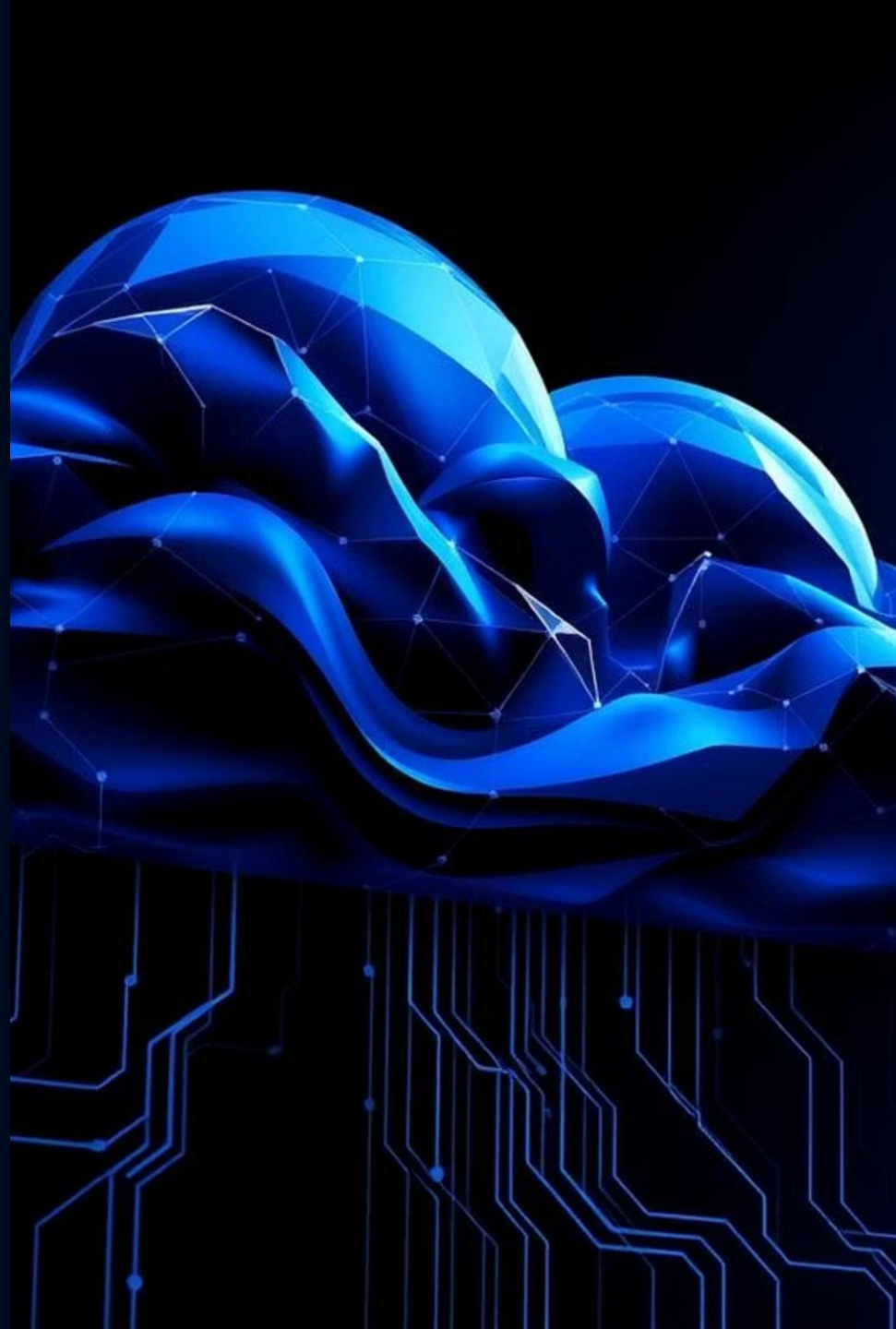
Hype Vs Reality: The Role of AI in Enhancing Cloud Security

Cutting through the noise to uncover practical value and risks

Presented by:

Gautam Kashyap



The Hype – Myths About AI in Cloud Security

AI can stop all cyberattacks

Overpromised tools often under-deliver, leaving critical gaps.

AI enables fully autonomous cloud defense

AI is a tool, not a replacement for human oversight and strategic decision-making.

The more AI, the more secure your cloud

Blind trust in AI without proper validation increases overall risk.

The Reality – What AI Actually Does Well

Anomaly Detection

Flags unusual access patterns and deviations from baselines.

Threat Correlation

Connects dispersed logs and alerts to identify complex threats.

Automated Response

Speeds up reaction time for known threats, reducing breach impact.

Predictive Analytics

Forecasts potential breach risks based on historical data and trends.

AI shines in data-heavy environments. It filters the noise and finds threats faster.

Case in Point – AI in Action

AI-driven tools are already enhancing cloud security operations in several key areas, providing tangible benefits and faster response times.

- **Cloud Workload Protection:** AI monitors and secures applications and data across cloud environments.
- **IAM Behavior Modeling:** AI analyzes identity behavior to detect compromised accounts or insider threats.
- **SOC Agents:** AI autonomous agents apply the logic for their actions within their instructions scope.
- **DevSecOps Automation:** AI based security testing and response leads to enhanced build quality, thus improving secure-by-design principle
  .

Red Flags – Risks of Over-Relying on AI

False Positives/Negatives

Can lead to alert fatigue or missed critical threats.

Opaque Decisions

Lack of explainability makes auditing and trust difficult.

Regulatory & Ethical Dilemmas

Bias in data can lead to unfair or discriminatory outcomes.

Attack Surface Risks

Improper setup & data poisoning can create new vulnerabilities.

AI needs context and human oversight. It’s not immune to blind spots or bias.

The Way Forward – Balanced Adoption Strategy

- **Combine Automation with Human Judgment:** Use AI to augment, not replace, human expertise.
- **Use Explainable AI (XAI):** Prioritize tools that provide clear reasoning for their decisions.
- **Maintain Governance & Risk Management:** Ensure transparency and accountability in AI operations.
- **Train Teams to Validate AI Decisions:** Equip staff with the skills to oversee and correct AI outputs.