MajorKey

Leveraging AI in Identity Security

Navigating AI Opportunities and Risks Through the Lens of Identity Security

25+
Years of Service

In Identity Security, a Threat Can Be Defined As:

> A potential event or circumstance that could exploit vulnerabilities within identity security systems, resulting in unauthorized access, privilege escalation, identity compromise, or disruption of legitimate access.

> Any potential event, action, or entity that could exploit vulnerabilities in an identity security system to compromise identities, abuse access privileges, or undermine security policies—leading to unauthorized access, data breaches, or system disruptions.

> Any circumstance, event, or action with the potential to exploit a vulnerability in the system or infrastructure, which can lead to unauthorized access, disclosure or modification of sensitive information, or disruption of services. Threats may originate from various sources, including malicious actors, internal threats, or unintentional errors.

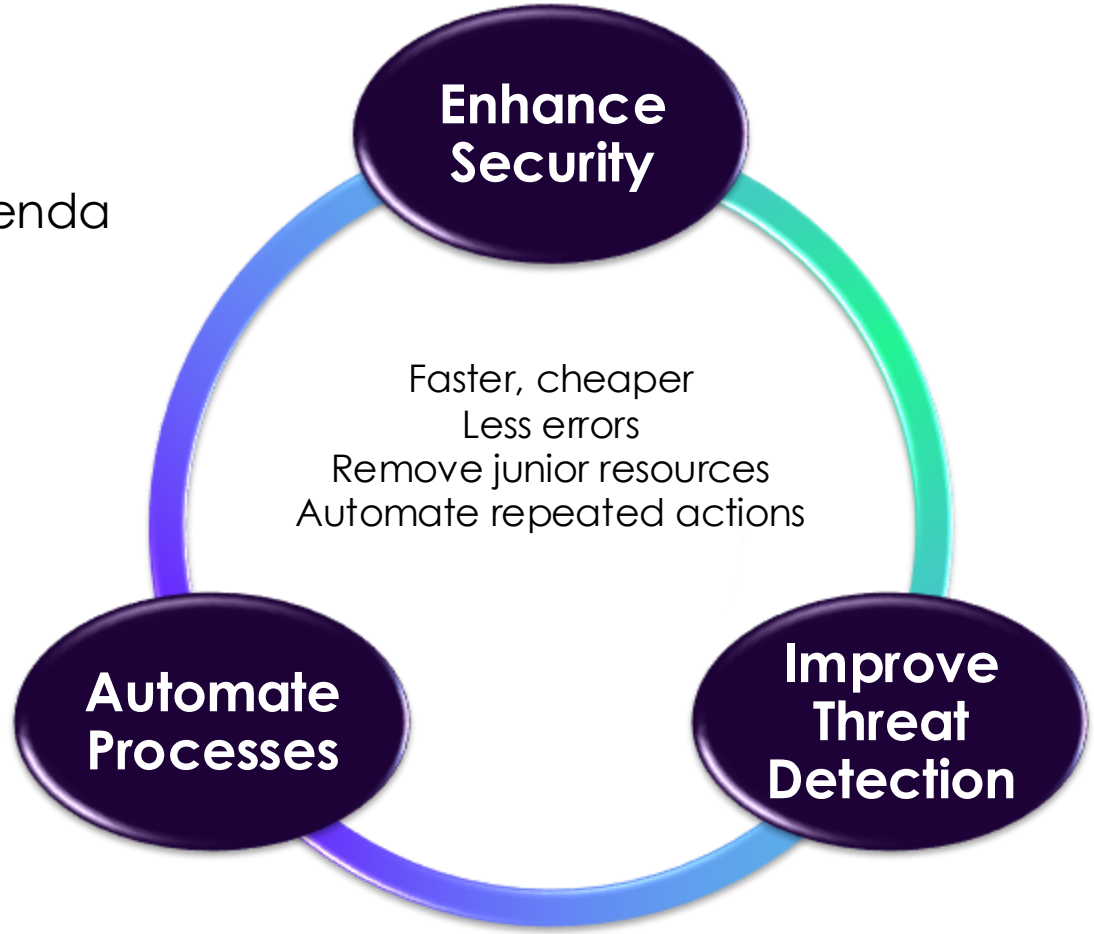
In simpler terms, a threat in Identity Security is anything that could negatively impact the security or integrity of digital identities or access controls, leading to risks such as data breaches, unauthorized access, or interruption of services.

AI-Powered Identity Security:

Opportunities and New Risks

The is NO "Single AI Solution" for Identity Security

- Vendors pushing their agenda
- Peer pressure
- Upper management
- General anxiety of FOMO
- Lack of clarity



Agentic AI: New Risks and Opportunities

- Ignoring agentic identity can lead to stalled projects, security breaches, and failed adoption.
- Early adopters who solve these challenges will gain a significant competitive edge.

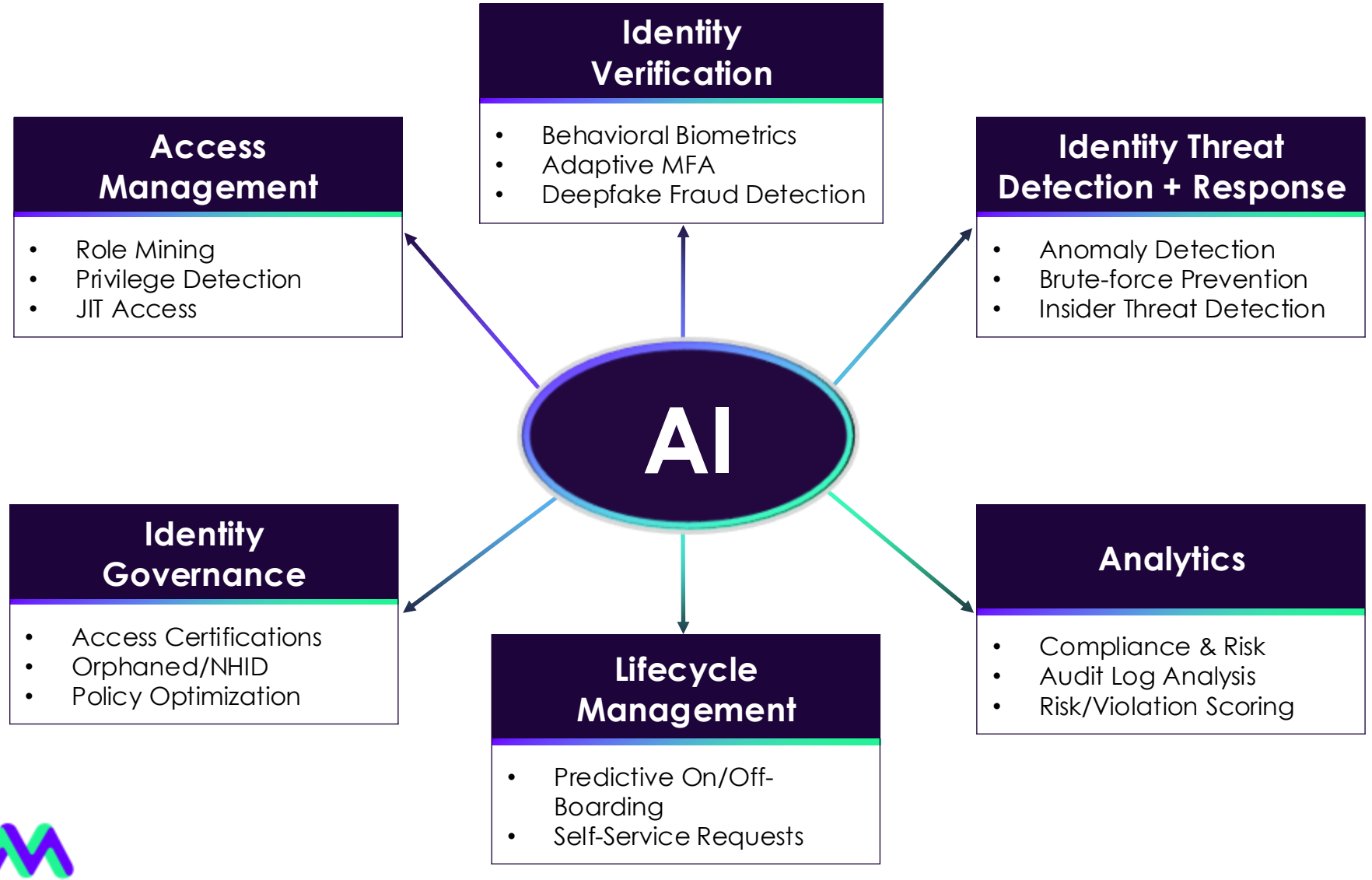
Gartner Perspective:

"Agentic AI combines machine-like scale, speed, and geographic reach with human-like autonomy and unpredictability. Ignoring the agentic identity blind spot risks stalled implementation, security breaches, and failed agentic AI adoption."

(Gartner, Tech FutureSight: Enterprise AI Scaling Requires Solving Agentic Identity Challenges, 2025)

Beyond Traditional Identity Security:

Governing Agentic AI



Agentic Identity: The Key to Scaling AI

- AI agents with autonomy require their own identity governance—beyond traditional users and machines.
- Failure to define, secure, and manage agentic identities will prevent AI deployments from reaching enterprise scale.
- Addressing agentic identity is foundational for success.

Gartner Perspective:

"Unresolved issues with agentic identity observability, governance, authentication, authorization, delegation, and monitoring threaten to completely prevent agentic AI deployments from scaling."

(Gartner, 2025)

The Readiness Gap:

Are You Prepared for Agentic AI?

#1 Threat – CONFUSION

- **Ambiguity about AI Capabilities**
- **Terminology and Buzzwords**
- **Scope and Applicability**
- **Data Quality and Volume**
- **Explainability and Transparency**
- **Bias and Fairness**

$$

- **Integration Complexity**
- **Privacy and Compliance Concerns**
- **Security Risks**
- **Resource and Skills Gap**
- **Who are we trying to convince**
- **What are the justifications**

Emerging Risk: Agentic Identity Blind Spots

- Most organizations are unaware of the complexities agentic AI introduces to identity security.
- Over 50% of AI initiatives will halt by 2028 due to unresolved agentic identity challenges.

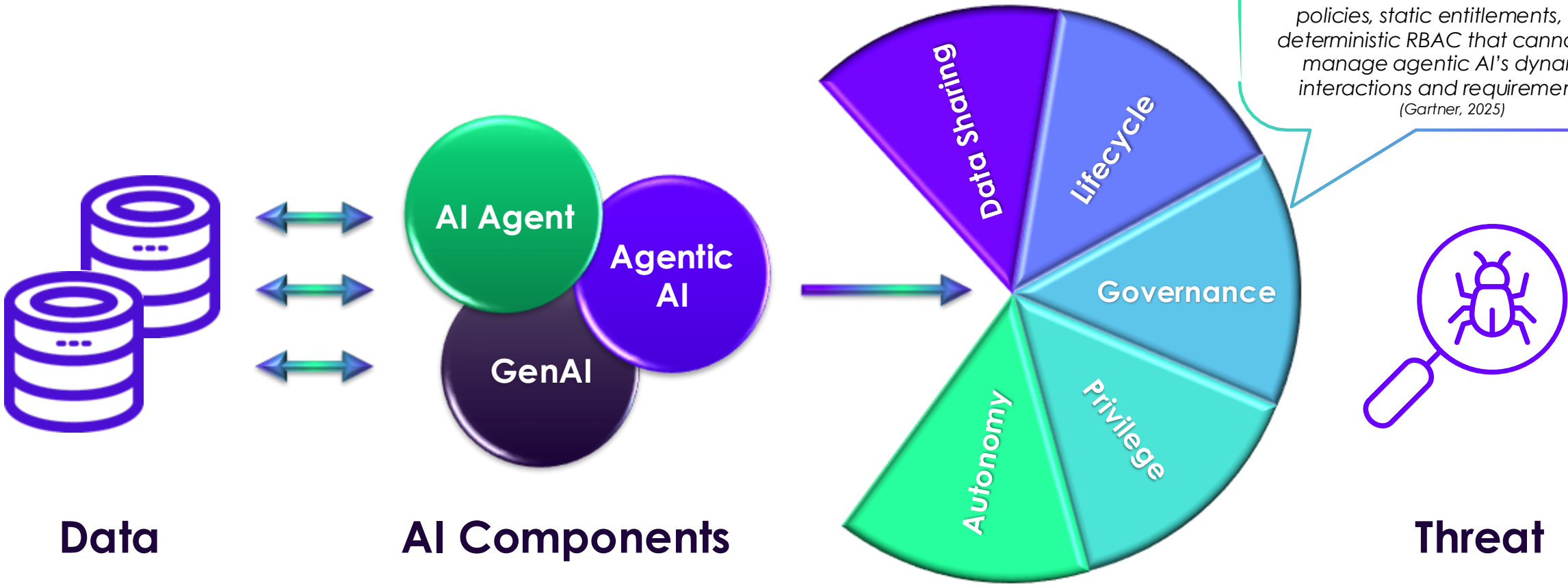
Gartner Perspective:

"Through 2028, over 50% of AI initiatives will halt, becoming unmanageable, because of unresolved agentic identity challenges."

(Gartner, 2025)

Unpacking the Risks:

Agentic Identity and AI Security



Agentic AI Challenges Traditional Identity Security

Gartner Perspective:

"Conventional IAM relies on fixed policies, static entitlements, and deterministic RBAC that cannot fully manage agentic AI's dynamic interactions and requirements."

(Gartner, 2025)