

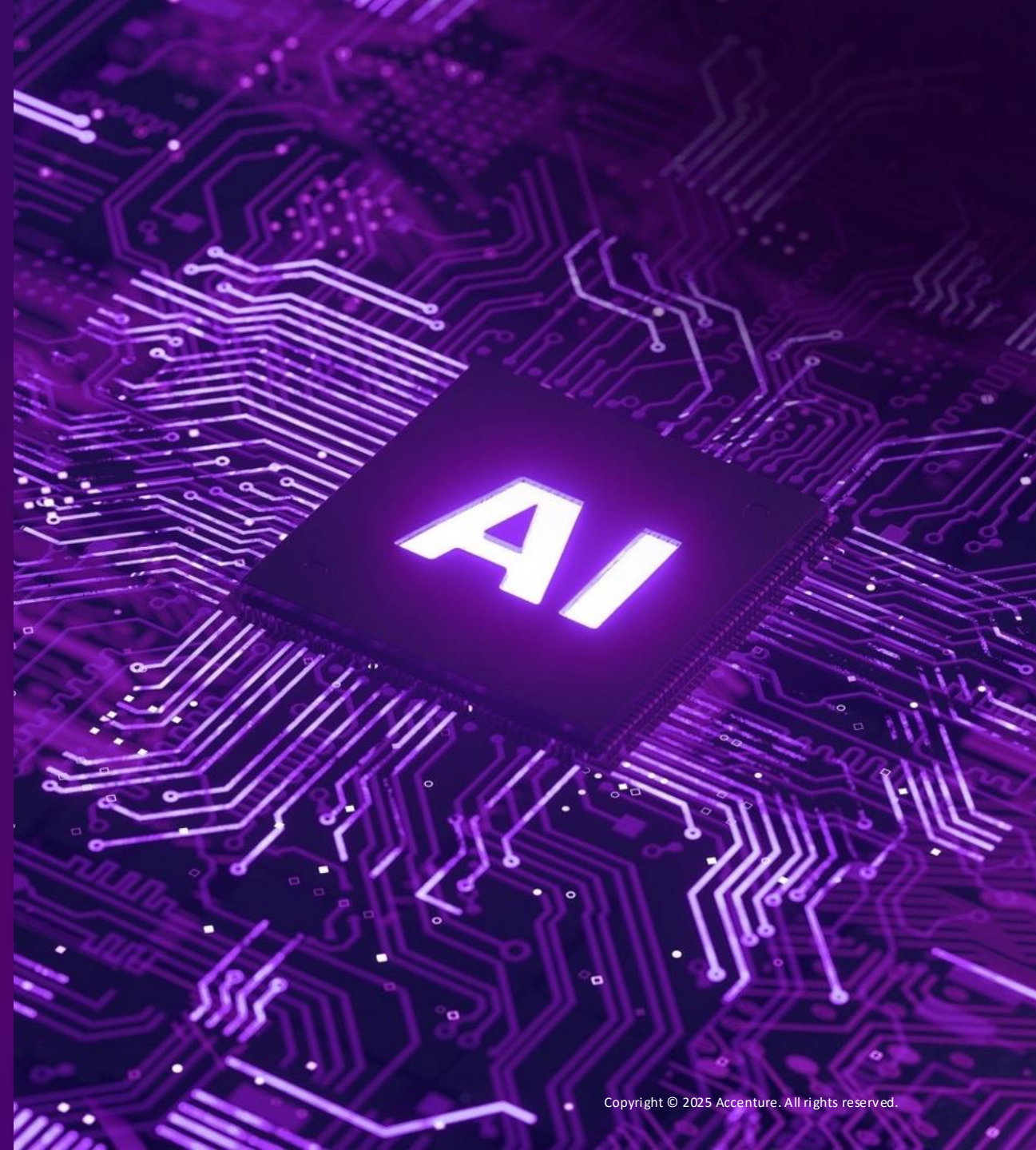


# Accenture Cybersecurity

## The Convergence Imperative: Board Readiness for Advancing AI Intelligence

NACD Chicago

September  
2025



# Meet Your Speakers



**Daniel Kendzior**

Global Security AI  
Reinvention lead



**Periklis  
Papadopoulos**

Senior Strategist,  
Accenture Security



# Agenda

01

**Risk Landscape**  
*10 Minutes*

Evolving threat landscape  
in an AI-first world

02

**Managing AI Risks**  
*5 minutes*

Control considerations for  
enterprise resilience

03

**Reinvention w/ AI**  
*5 minutes*

Mindfully adapting  
Security with AI

04

**Board Actions**  
*5 minutes & Discussion*

Recommendations for effective  
oversight and governance



Accenture Cybersecurity

# How is Gen AI Re-shaping the Cyber Threat Landscape?



# Cyber threats are evolving faster than enterprise defenses can adapt.

With unprecedented speed and scale, AI is enabling attackers to bypass legacy systems and overwhelm security teams. Traditional defenses are no longer sufficient.

31%

of technology leaders acknowledge that AI is outpacing their security capabilities.

86%

of companies lack the maturity to counter today's AI-enabled threats.

69%

of organizations lack the foundational data and AI security practices needed to safeguard critical models, data pipelines and cloud infrastructure.



# Technology Threat Landscape in 2025

Accenture Cyber Intelligence (ACI) identified the following major cyber security trends impacted by advances and use of GenAI/AI through 2025.



## 1 Nation-State Threat Actors

**Generative AI enables nation states** to automate the creation of disinformation campaigns, tailor propaganda, and simulate authentic-looking documents and communications.



## 2 Data Theft

More and more, **threat actors are targeting user accounts of ChatGPT and other LLMs**, which often don't employ MFA, to steal data. Organisations creating their own internal LLMs, especially to create virtual private assistants, are attractive targets.



## 3 Social Engineering and Deepfakes

**Generative AI can be used for crafting sophisticated phishing emails** and to create realistic personas for social engineering. Deepfakes and voice cloning enable threat actors to bypass controls. Fake AI platforms posing as GenAI tools deliver malware.



## 4 Ransomware

To optimize code and automate aspects of the attack path, threat actors have been **leveraging AI-enabled ransomware**. They can then automate the exploitation and the process of encrypting all the company files.



## 5 Insider Threats

**AI analytics help detect insider threats by monitoring user activity** and highlighting unusual behavior. Additionally, they can automate risk scoring and prioritize investigations, enabling faster response to potential threats.



## 6 AI Supply Chain Compromise

**AI supply chain compromises exploit trusted third-party models, libraries, and datasets**, introducing hidden vulnerabilities that can cause widespread damage across multiple AI systems. This includes risks like data poisoning that can corrupt AI training and behavior.



# AI-powered attacks on organizations are increasing

## More Attacks

More individuals enabled to run cyber attacks due to AI-powered tools

**72% surge in cyber risks over the past year (2024).**

- Cybercriminals and nation states attack tools have easy access to sophisticated AI-powered.
- Notable increase in use of deepfakes to bypass identity measures and gain unauthorized access to enterprise networks.

## More Effective

Rapid development of large scale, multimodal, precise, automatized attacks

**42% of organizations experienced a successful social engineering attack in the past year.**

- Accelerated reconnaissance through AI enables faster and more targeted attacks.
- Increased effectiveness shown for AI driven attacks with a higher penetration and victim rate, such as deepfake phishing attacks.

## More Damaging

AI is enabling threat actors to unleash more damaging attacks...

**creating bigger risks to enterprises and organizations.**

- Organizations are not yet equipped to detect and respond at the speed and scale of AI-powered attacks that can result in significant financial, operational, and reputational impacts.

# Deepfake technology is an evolving, highly-sophisticated tool in a Threat Actor's social engineering toolbox

## Key Personas targeted through deepfake attacks



### Frontline staff (property & contact center workers)

Attackers can impersonate customers, leading to scenarios where associates are manipulated into granting unauthorized access

**Example: Ransomware group pretended to be IT manager for MGM Grand**



### C-Suite & Board Members

Attackers can mimic executives leading to fraudulent communications that could authorize significant financial transactions or influence strategic decisions.

**Example: Ferrari CEO Deepfake plot**



### HR & System Administrators

Attackers can impersonate trusted associates, coercing HR staff or system admins to provide elevated access or divulge sensitive information, or bypass MFA requirements

**Example: KnowBe4 malicious job application**



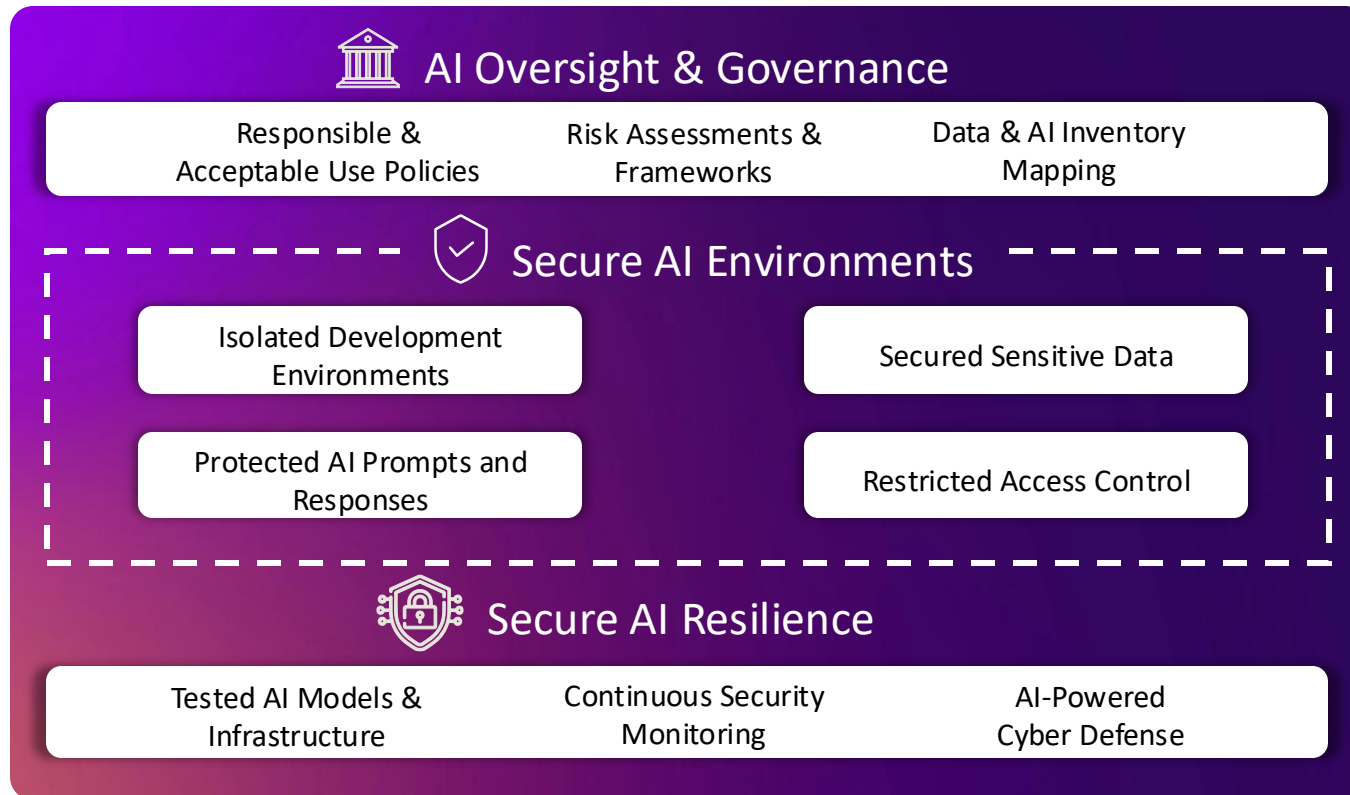
Accenture Cybersecurity

# Managing AI Risks Effectively



# Accenture's Framework for AI Security & Risk Management

The framework collates Responsible AI capabilities to jumpstart a comprehensive governance structure, with accountability.



Define actionable and modular enterprise governance components (principles, policies and standards) for AI systems



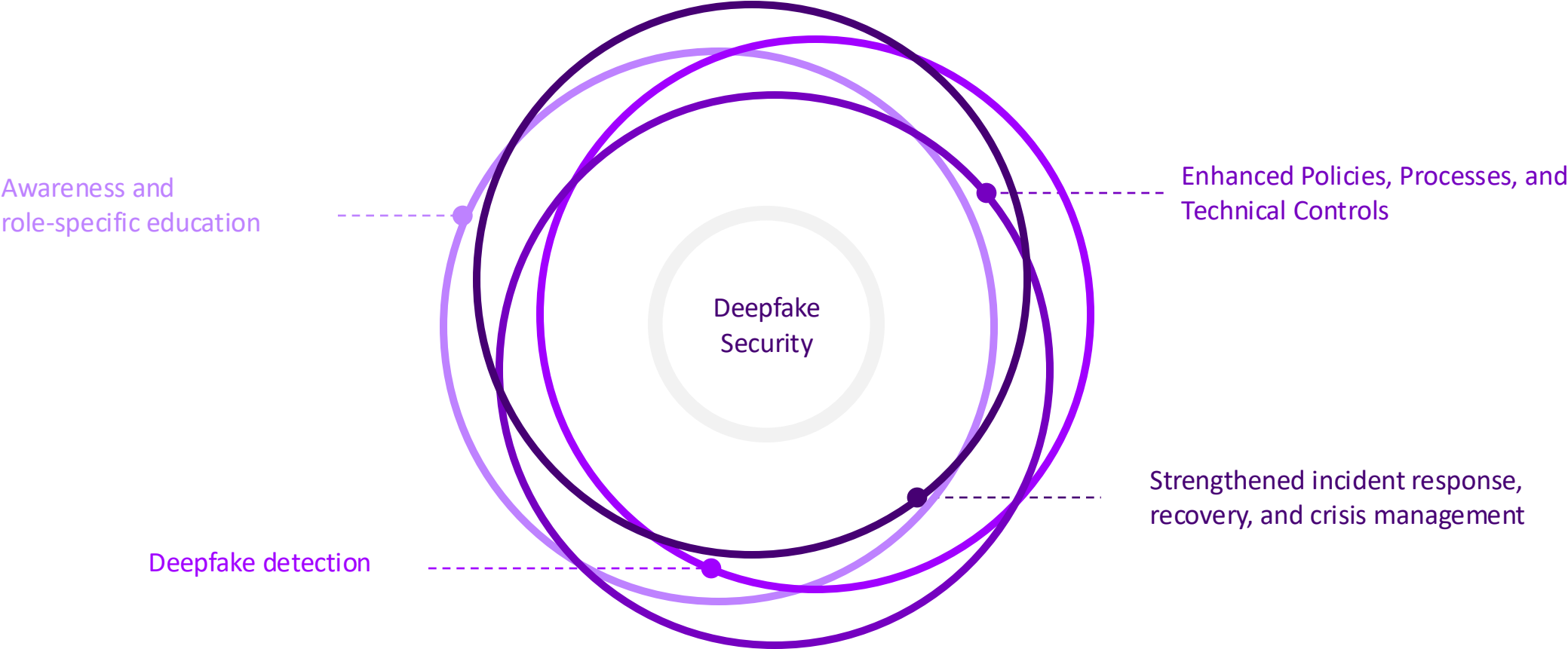
Operationalize and embed controls across enterprise processes, development and data pipelines



Enable monitoring, testing and readiness for AI systems.

# What does good deepfake security look like?

Beyond education and awareness, an effective approach requires defense-in-depth to safeguard the organization against evolving deepfake threats at every stage of the attack lifecycle

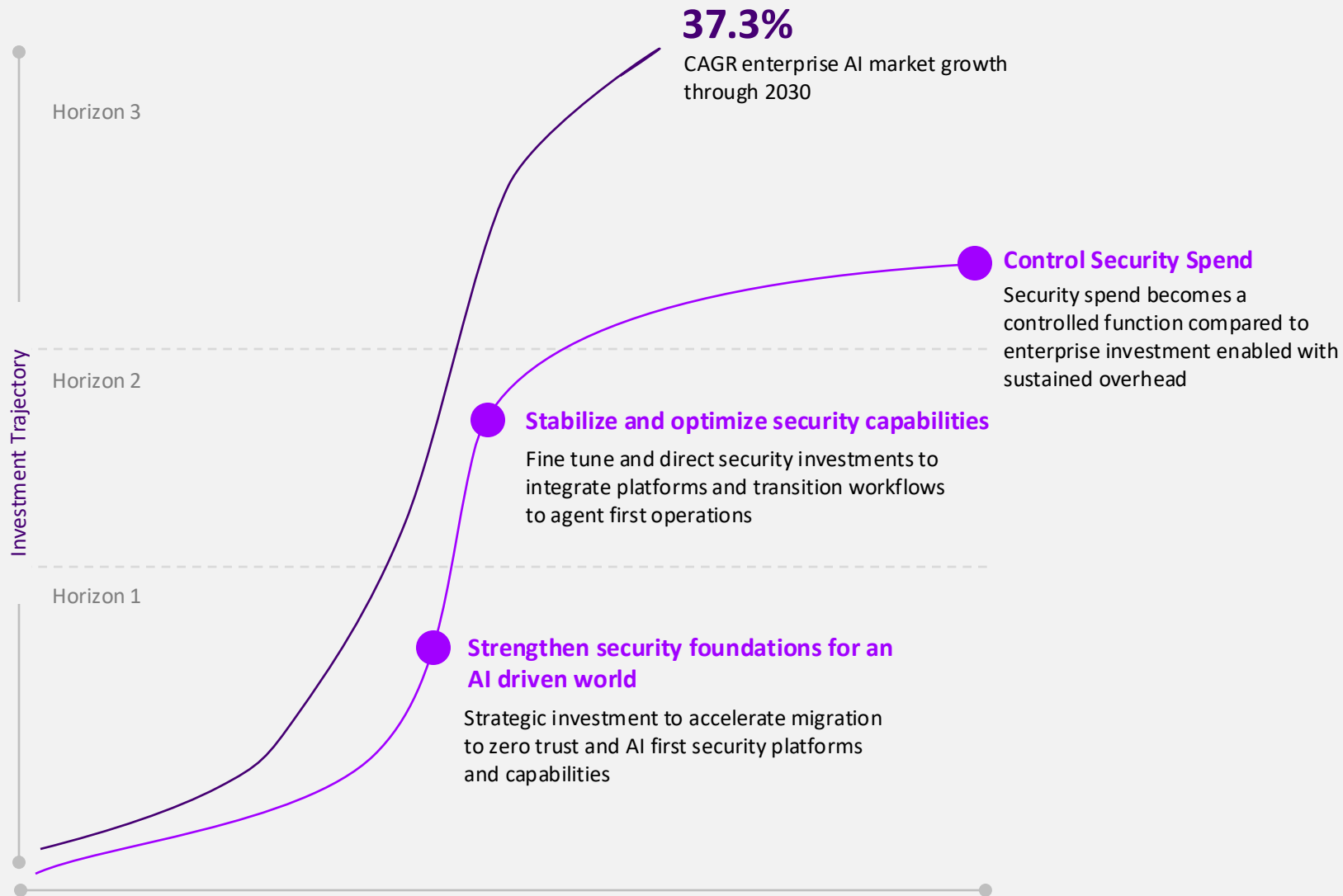


Accenture Cybersecurity

# Leveraging AI for Enhanced Resilience



# The path to sustainable growth



## The situation

- Over the past five years, security budget as a percentage of IT spending has steadily increased, rising from 8.6% in 2020 to 13.2% in 2024
- AI Investment growth is expected to increase at a considerable pace which means security leaders will be required to invest more heavily to stay up to speed and strengthen defenses

## The Path Forward

Agentic first workforce and operating model to enable resilient and manageable spend for security

# New risks New technologies New opportunities

Accenture Cybersecurity's research highlights the benefits of a three-stage and structured transformation program for sustained benefit realization



## The crucible for change – Agentic AI

From enabling Operational Excellence

- Autonomous threat detection & response
- Intelligent policy optimization
- Predictive risk assessment

To Strategic Advantages

- Accelerated transformation timelines
- Enhanced analyst productivity
- Continuous learning & improvement



## From risk exposure to reinvention

Horizon I

Now to 18 Months

**Modernization Leap** by establishing the foundations for secure AI and scaling security for a digital and AI first enterprise

Change Management

Horizon II

10 to 24 Months

**Agentic Activation Leap** by utilizing cross-platform security investments to deliver actionable risk reduction

Governance

Horizon III

36 Months

**Reinvention Leap** delivering operational elasticity and proactive risk management

Human in the Loop



Accenture Cybersecurity

# Actionable Insights for Governance over AI Risks and AI Reinvention



# Board considerations in the fight of AI threats - Immediate Actions



## Encourage proactive AI adoption in cybersecurity

Empower, enable and encourage management to innovate with AI-driven cybersecurity solutions



## Leverage third-party expertise and assess capabilities

Encourage partnerships with third-parties who specialize in AI-driven cybersecurity solutions and understand how they are using AI within their own operations



## Establish regular AI threat briefings

Briefings from the cybersecurity team on the evolving landscape covering the latest developments in AI-driven cyber threats



## Prepare for deepfake scenarios

Conduct dedicated table tops exercises on deepfakes that involve validating the authenticity of information and the organization's preparedness to address and mitigate deepfakes that target the company

# AI and Cybersecurity Questions for Boards

1. How is management reporting on its ability to defend against growing AI powered cyber threats?

2. How is management demonstrating the protection of data as the organization leverages third-party Gen AI applications?

3. How is management changing its approaches to cybersecurity in the face of threat actors increasingly using Gen AI?

4. How is management demonstrating that the organization has the right skills and accountability to manage security risks of AI?

5. How will management ensure that security is embedded into AI approaches across the organization?

6. How is management preparing for new and enhanced AI laws and regulations that raise cybersecurity expectations?

7. How is management leveraging AI to improve cybersecurity efficiency in the face of growing internal and external risks?

8. How is management ensuring strong cybersecurity oversight of its ecosystem partners that leverage AI?

9. How is the Board demonstrating its oversight and challenge of the organization's responsible AI approaches?

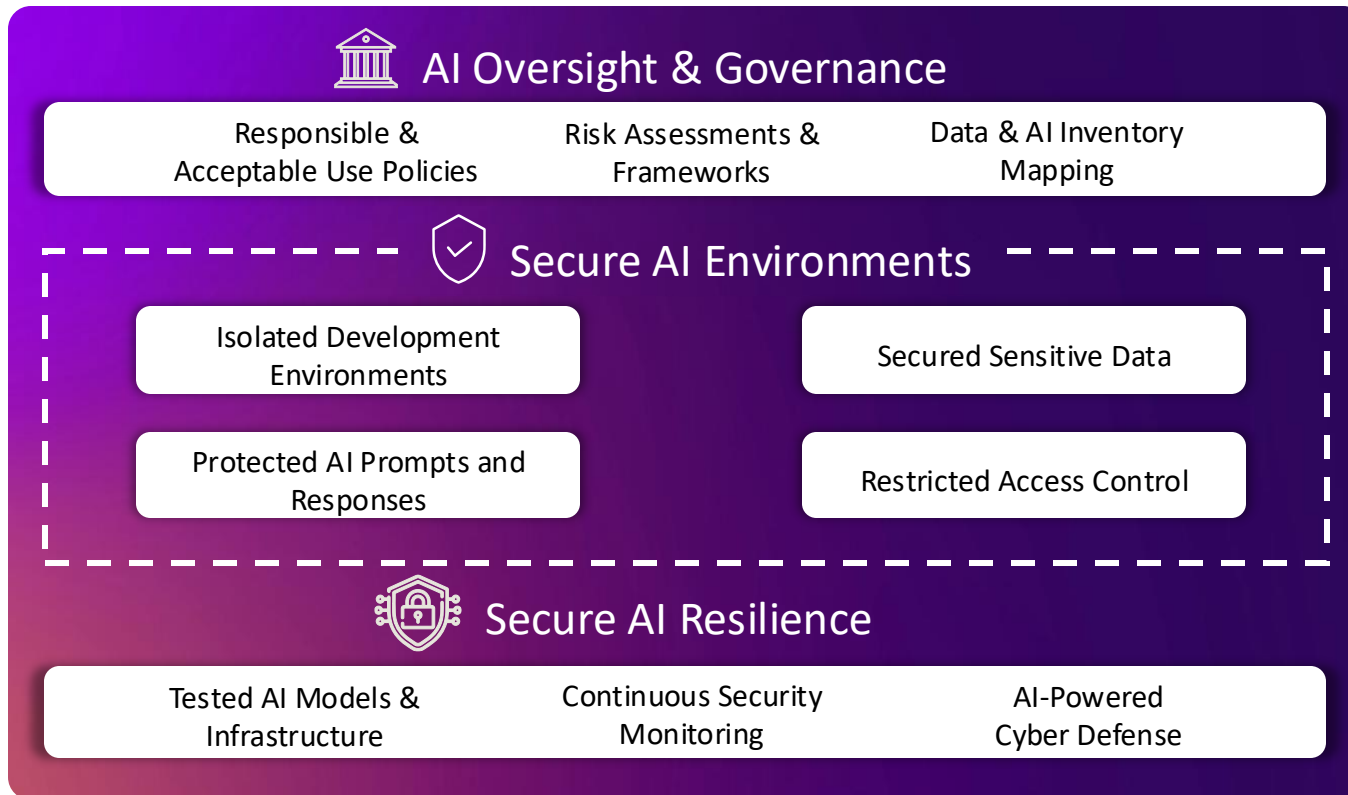
10. How is management addressing security risks rising from the organization's use of Gen AI?



Questions to assist boards with AI Security

# The Path to Scaling AI Risk Management

## Accenture's Framework for AI Security & Risk Management



## Indicative Key Actions



- Develop AI security **governance frameworks**
- Implement **AI discovery capabilities** for oversight, review, and reporting
- Conduct a **deepfake readiness** exercise
- Integrate **training and awareness for responsible AI** usage



- Engineer secure, fit-for-purpose environments for AI research and development
- **Implement policy-driven controls** to protect sensitive data in large repositories and **secure prompts and responses**
- **Implement safeguards for MCP<sup>1</sup> servers**



- Enable **monitoring, detection, and response** for AI systems
- Actively test external/client facing **AI capabilities**
- Implement **deepfake identification, prevention, and response capabilities**
- Establish **AI-driven roadmap** for scaled SOC<sup>2</sup> processes

<sup>1</sup>MCP: Model Content Protocol

<sup>2</sup>SOC: Security Operations Center

# Management & Board Secure AI Responsibilities



## Govern

### Institute Gen AI oversight & governance

#### Management

- Develop and implement Gen AI security governance frameworks for oversight, review, and reporting
- Integrate training and awareness for responsible Gen AI usage through enterprise training, compliance, and oversight

#### Board

- Oversee how management is addressing security as part of the organization's approach to **Responsible AI**
- Review and challenge **reporting on AI security and compliance with internal policies and standards** and evolving regulatory requirements and security standards
- Update the appropriate **board committee charter** to include specific reference to Responsible AI oversight

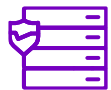


## Protect

### Secure Gen AI environments

- Engineer secure, fit-for-purpose environments for Gen AI research and development
- Design & implement policy-driven controls utilizing AI to restrict access to sensitive data and assets
- Work with trusted partners to shorten the learning curve and minimize AI adoption risk and assess third party vendors for risks associated with their GenAI technology

- Review and challenge how management is embedding and adjusting security controls to create and maintain **secure environments and protect data**
- Review and challenge the organizations use of partners and **third-party vendors** for their effectiveness at managing **AI related risks**



## Defend

### Implement Gen AI security testing and adopt Gen AI-Powered Cyber Defense

- Implement security monitoring, detection, and response for Gen AI capabilities and technologies
- Establish red teaming activities to proactively identify and mitigate potential security risks and vulnerabilities

- **Participate in regular tabletop exercises** using real-world AI scenarios to understand management's response and board interaction
- **Continuously expand the Board's knowledge** and understanding about AI threats and innovations
- Oversee how **security is leveraging AI** to mitigate risks from the growing cyber threat landscape.



**Thank You**

