HPE Innovation Day

AI and cybersecurity: balancing risk and reward

Simon Leech

Director, HPE Cybersecurity Center of Excellence

Hewlett Packard Enterprise | NVIDIA

Imagine the scene

[1] https://arstechnica.com/information-technology/2024/02/deepfake-scammer-walks-off-with-25-million-in-first-of-its-kind-ai-heist/

“Data is the new currency for the digital economy. The key to extracting value and insights will come from AI.”

Antonio Neri

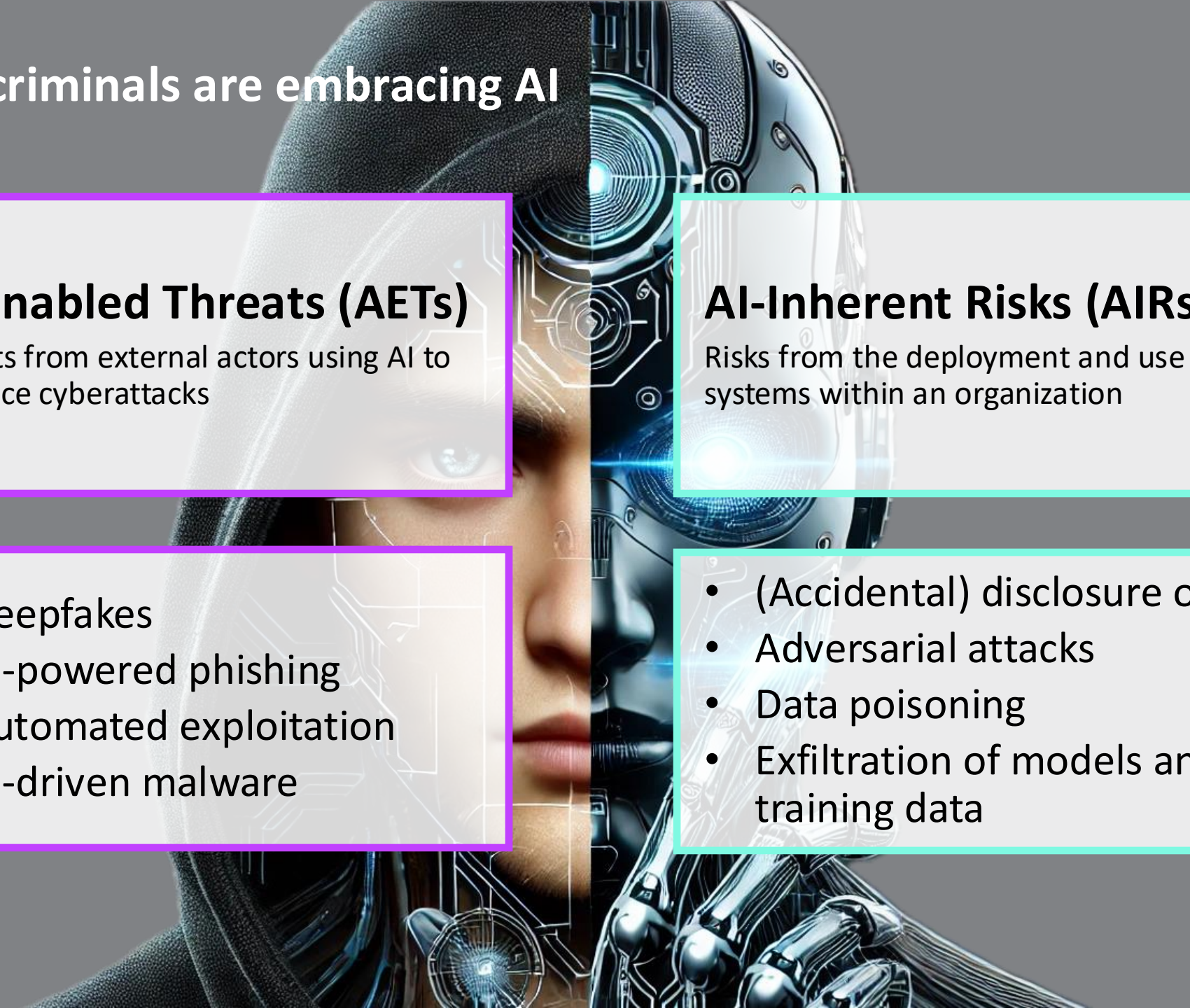
President & CEO, HPE

“Why do I rob banks? Because that’s where the money is!”

Willie Sutton

1930s bank robber

How cybercriminals are embracing AI



AI-Enabled Threats (AETs)

Threats from external actors using AI to enhance cyberattacks

- Deepfakes
- AI-powered phishing
- Automated exploitation
- AI-driven malware

AI-Inherent Risks (AIRs)

Risks from the deployment and use of AI systems within an organization

- (Accidental) disclosure of IP
- Adversarial attacks
- Data poisoning
- Exfiltration of models and training data

Strategies for balancing risk and reward

Consuming AI

Using Gen AI for improved decision making with efficient governance

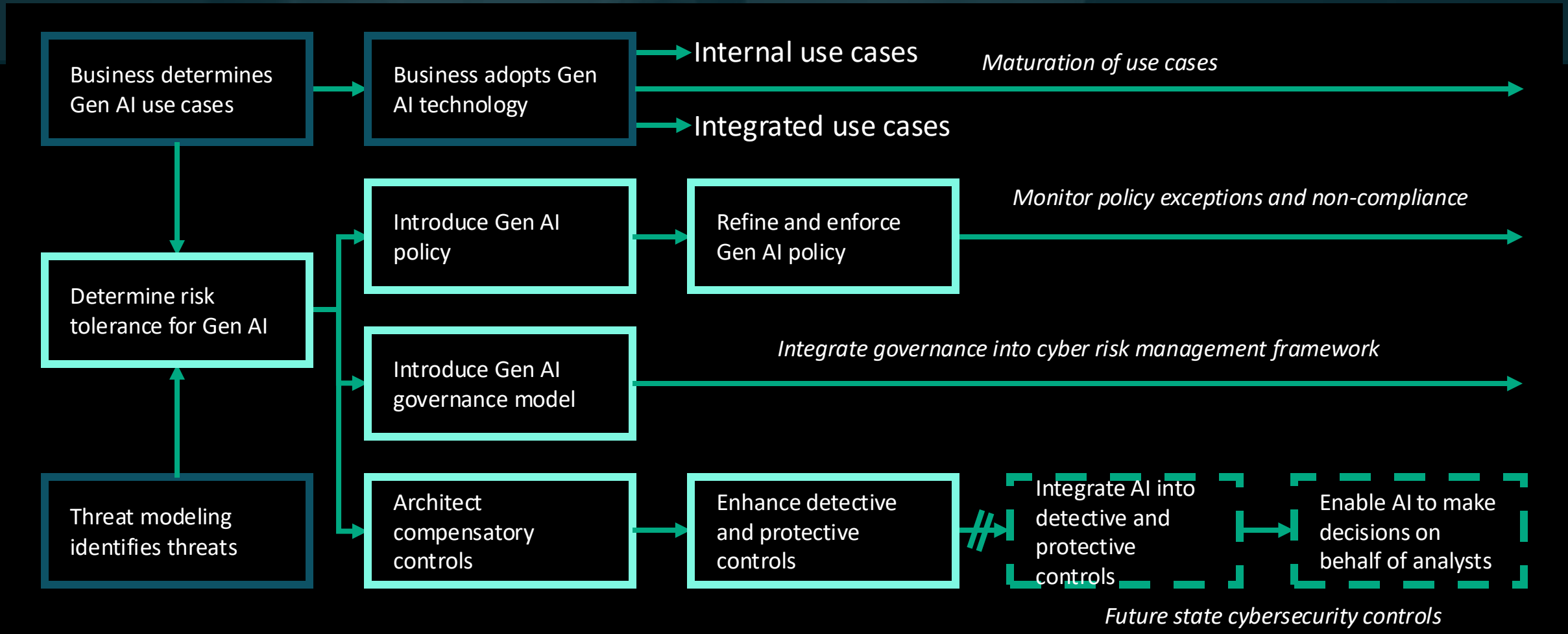
Building AI

In-house developed models for greater control and improved security

Protecting with AI

Threat detection, incident response, and vulnerability management automation

Consuming AI
Effective AI governance

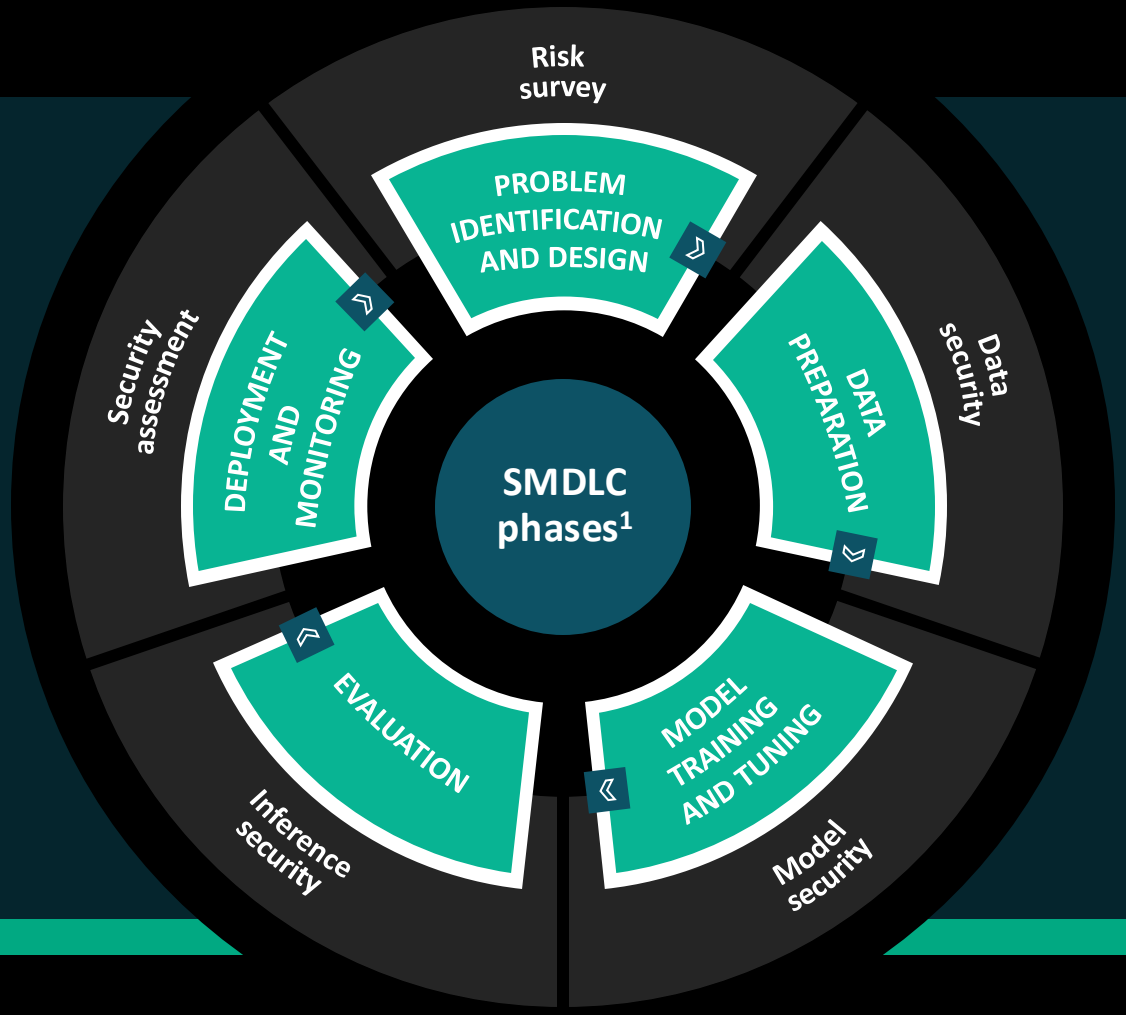


Building AI
Secure model development

Consider security at each step of the model lifecycle

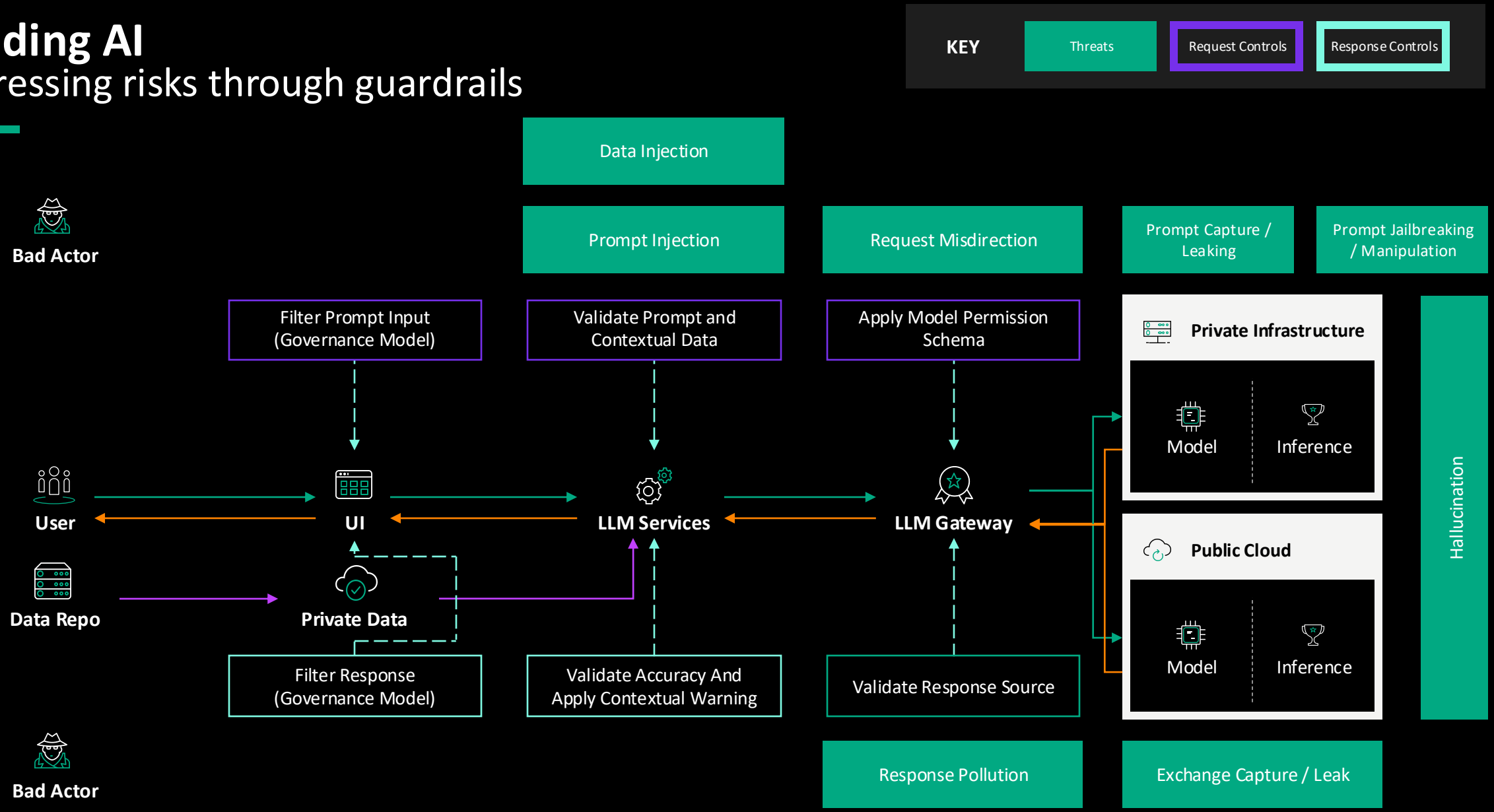
Extend upon existing security principles
- SSDLC, IAM, data security, patch management, security monitoring

Adopt a secure model development framework
- TrojAI's SMDLC
- Microsoft's Secure Development Lifecycle for AI
- NIST's AI Risk Management Framework
- OpenAI's Security Best Practices for Machine Learning



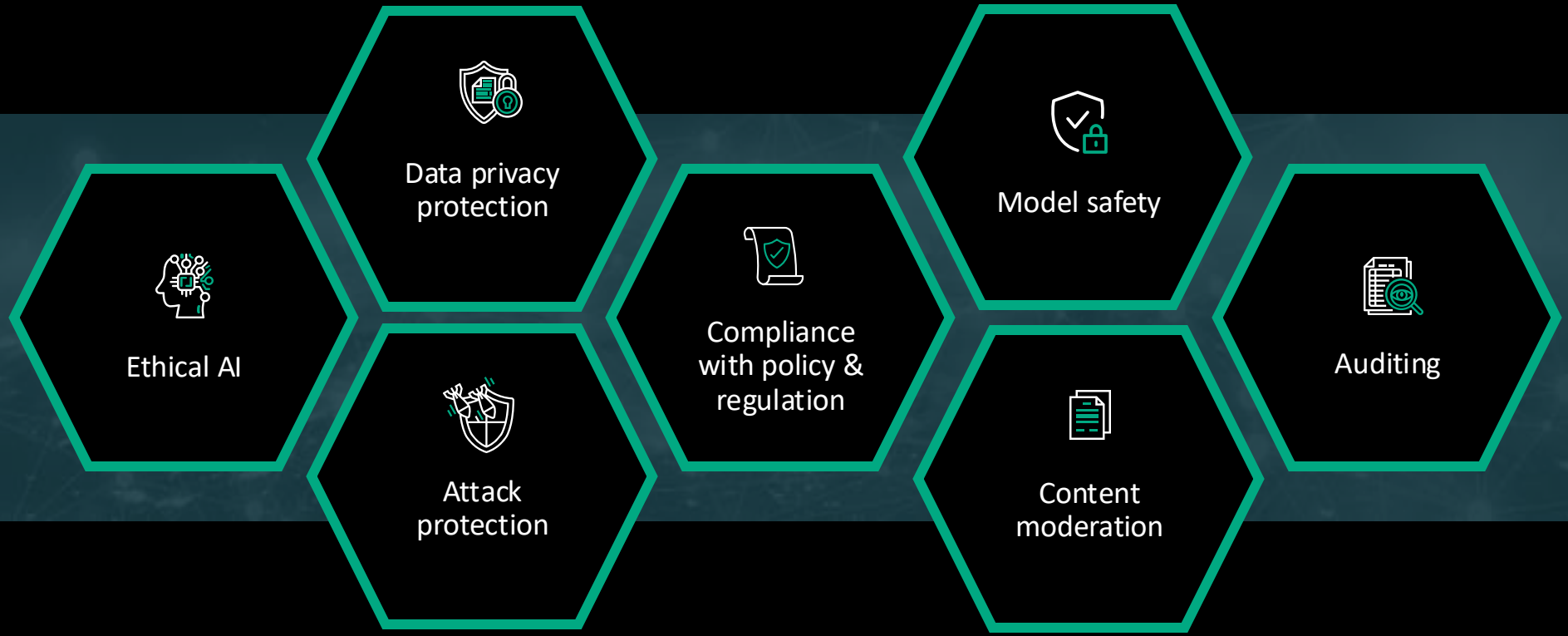
[1] Based upon TrojAI's Secure Model Development Lifecycle

Building AI
Addressing risks through guardrails



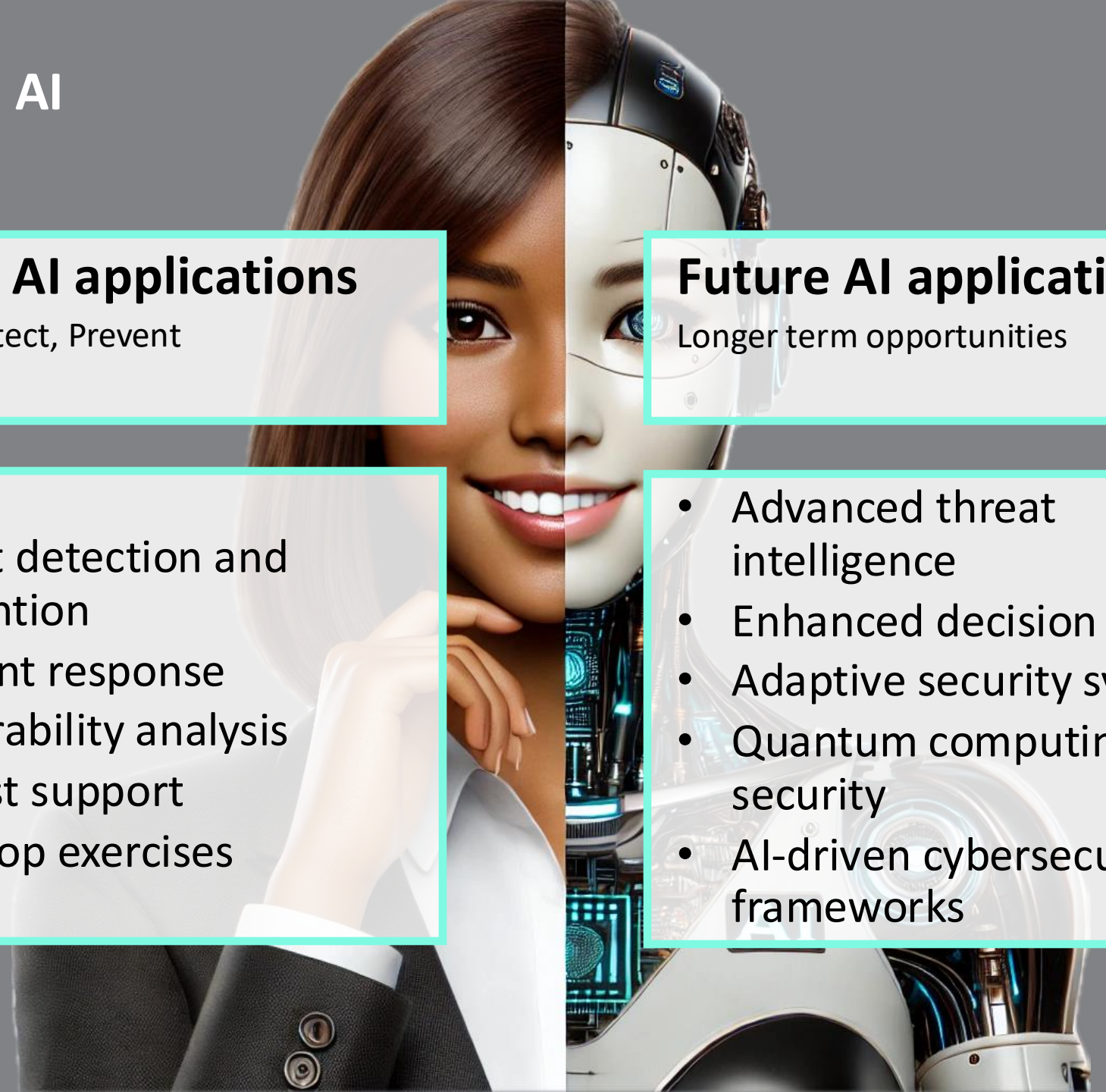
Building AI

AI security and guardrail use cases in AI lifecycle



Data prep | Model building | Model training | Model fine-tuning | Model deployment | Model inferencing | Monitoring

Protecting with AI



Current AI applications

Predict, Protect, Prevent

- Threat detection and prevention
- Incident response
- Vulnerability analysis
- Analyst support
- Tabletop exercises

Future AI applications

Longer term opportunities

- Advanced threat intelligence
- Enhanced decision making
- Adaptive security systems
- Quantum computing security
- AI-driven cybersecurity frameworks

“Artificial intelligence holds **enormous potential** to advance the way people live and work, but we must ensure that we apply these powerful tools **ethically and sustainably.**”

Antonio Neri
President & CEO, HPE

HPE supports

AI ethics for good

- AI privacy-enabled security
- AI human-focused principle
- AI inclusivity principle
- AI robust principle
- Responsible AI

How HPE can help

HPE cybersecurity service offerings for AI-powered cybersecurity

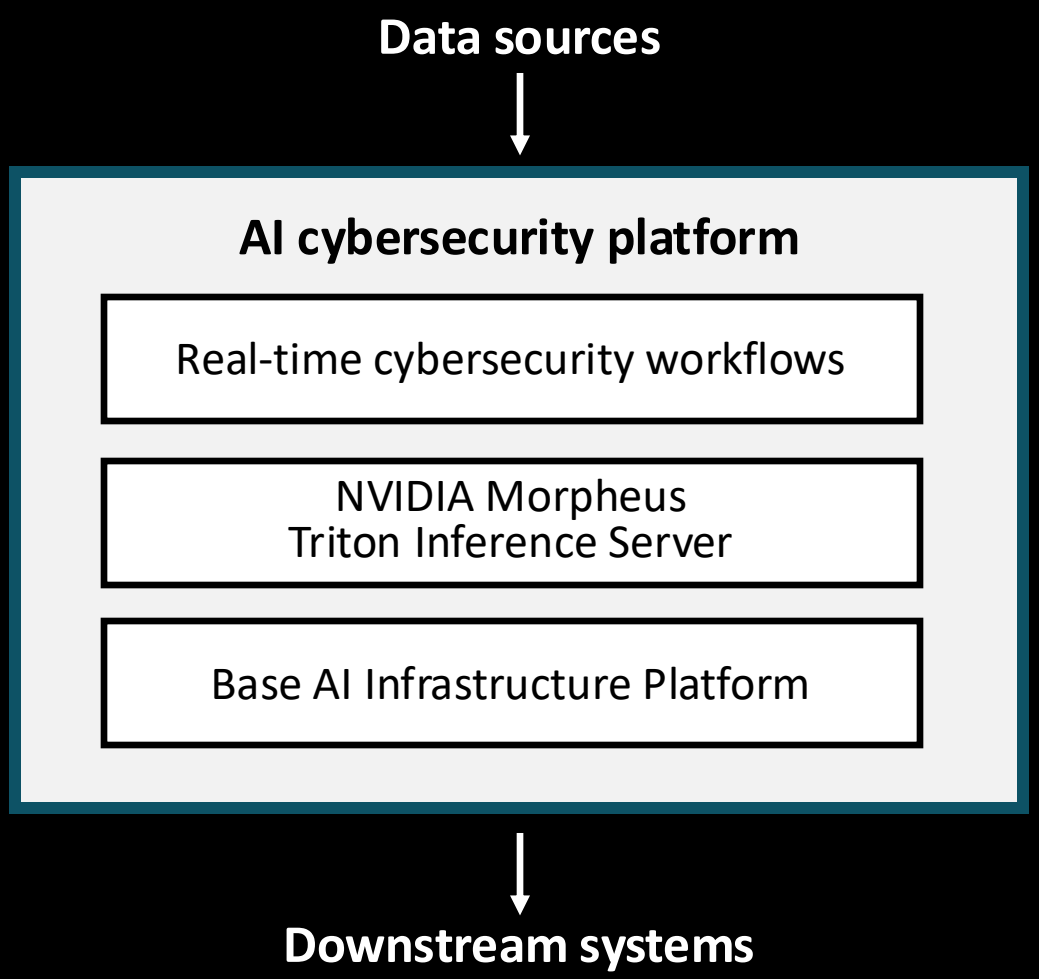
AI Transformation workshop for Security

One-day workshop to identify key security pain points and use cases for AI/ML

AI/ML-powered cybersecurity solution

Customized architecture, design, implementation, and integration of AI-powered cybersecurity solution for security operations

HPE AI-enabled cybersecurity platform overview

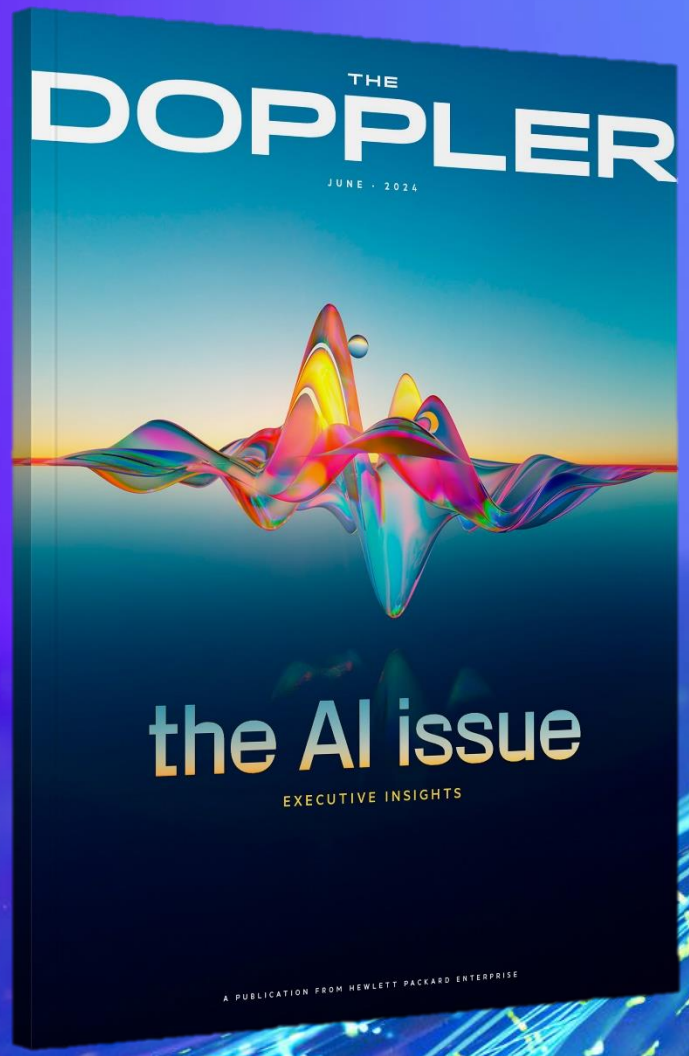


- An integrated solution for data management, ML model training, real-time inference, and visualization of cybersecurity data
- Platform to develop, test, and deploy a variety of cybersecurity use cases
- Leverages Kubernetes base AI platform
- Create end-to-end ML pipelines for cybersecurity
- AI-enabled Cybersecurity Framework solution includes:
  - Training and real-time inference platform
  - Two example workflows using the platform
    - Sensitive information detection
    - Email data-loss prevention

- Organizations that harness AI will step ahead of those that ignore its potential
- AI gives us the opportunity to change the way we secure our enterprises
- We need to address the adoption of AI in a secure and ethical way
- You won’t lose your job due to AI, but you might lose it to someone who knows how to embrace AI

Thank you

sleech@hpe.com



Read The Doppler: AI leadership articles from the front line.

Thank you for joining HPE Innovation Day!

We value your feedback – would you please rate our event?

Hewlett Packard Enterprise | NVIDIA