



A Leader in Managed IT, Multi-Cloud
and Cybersecurity Services for the
Global Financial Services Industry

Adversary and Ally: The Dual Role of AI in Highly Regulated Industries

LIVE WEBINAR
OCTOBER 15TH, 2025

Our Speakers



Moderator

Jonathan Bohrer
President



Panelist

Travis DeForge
Director of Cybersecurity



Cybersecurity Unit



Panelist

McKaila Posey
Manager of Cybersecurity
Advisory



Cybersecurity Unit



Panelist

Steven Shapiro
Chief Marketing
Officer





Agenda

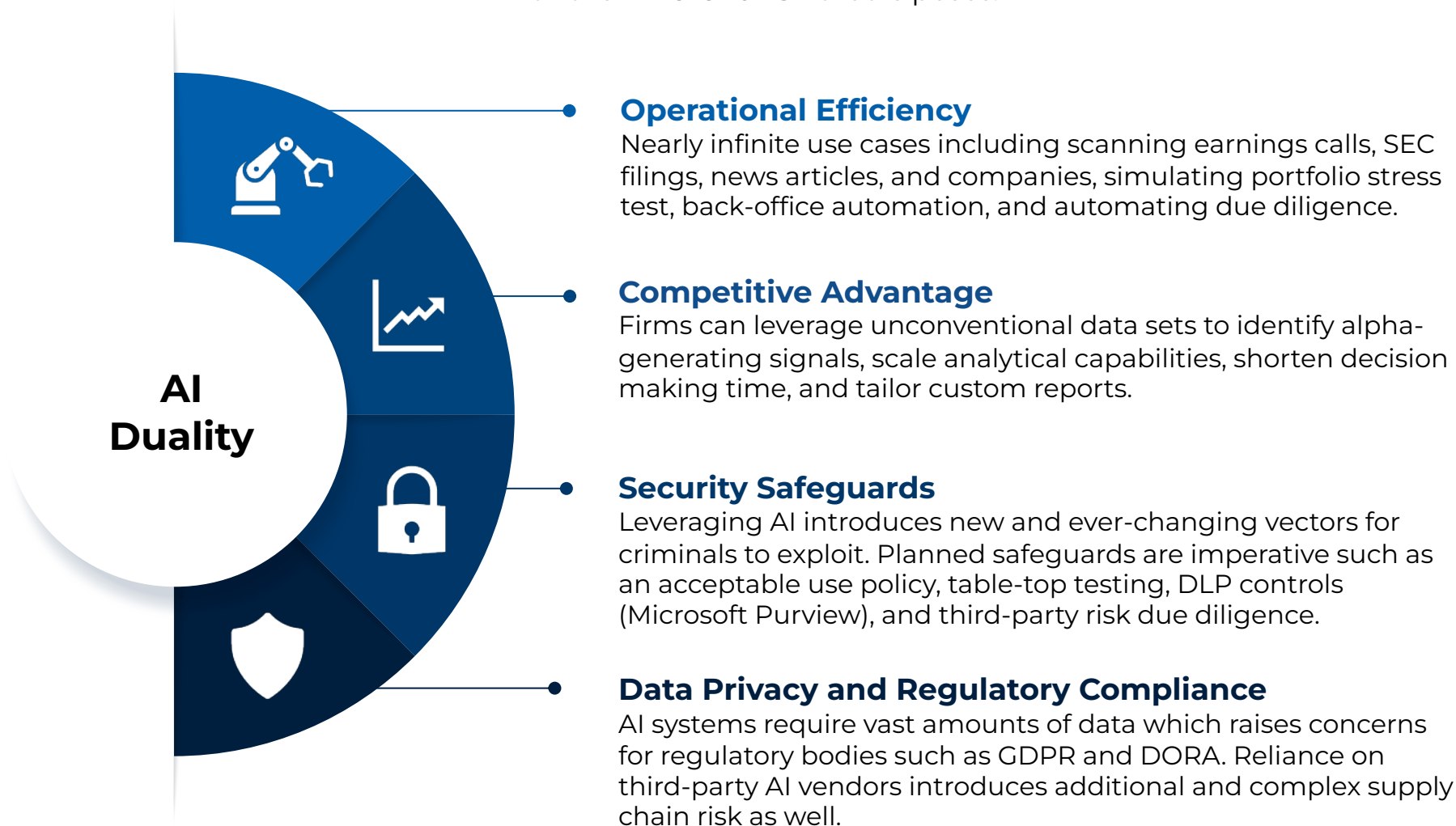
1. What is AI Duality?
2. AI Efficiency and Security
3. AI-Driven Attacks
4. What Can You Do?
5. Q&A

-
- **Webinar Duration:** 30-45 minutes
 - **Recording:** Webinar will be recorded and emailed
 - **Q&A:** Please use Q&A function in GoToWebinar to ask questions

What is AI Duality?



AI Duality is the balance between the **potential of AI** to enhance operational capabilities with the **inherent risk** that it poses.



AI to Drive Efficiency and Security



When used responsibly, AI becomes both a **productivity multiplier** and a **protective shield** navigating complex regulatory and cyber landscapes.

Operational Efficiency

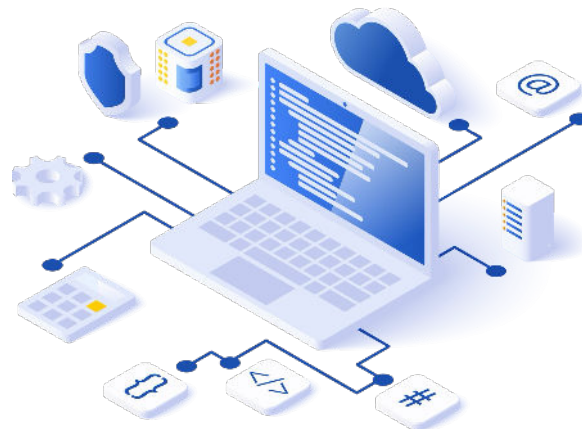
- Automates repetitive workflows
- Accelerates data analysis for faster, smarter decision-making
- Predictive analytics

Risk Management

- AI models can identify anomalies in financial transactions
- Enables real-time monitoring to ensure regulatory compliance
- Reduces human error in complex reporting processes

Cyber Defense

- AI-driven systems can detect threats faster than traditional tools
- Identifies and neutralizes anomalies before breaches occur
- Strengthens resilience against AI-powered attacks



Adversaries Leveraging AI



Targeting Large Language Models

Manipulating AI systems to cause them to malfunction. Techniques include poisoning training data, evasion attacks to mislead AI models, and tampering with AI model parameters.



AI-Driven Social Engineering Attacks:

AI gathers information to create highly personalized phishing emails or messages, making them more convincing and harder to detect.

- **Phishing Attacks:** emails, messages, chatbots
- **Deepfakes:** videos, audio or images mimicking real people

AI-Enabled Ransomware

AI can enhance ransomware by automating the identification of vulnerabilities, encrypting data more effectively, and adapting to avoid detection.

Current Statistics:

- AI-Driven Fraud constituted **42.5% of all detected fraud attempts** in the financial sector in 2024, with 29% of them being successful.
- Deepfakes in 2024 represented 6.5% of the total fraud attempts, but that is a staggering **2,137% increase** in the last 3 years.
- **703% increase** in phishing attacks in the second half of 2024.

Agentic AI Ransomware



Agentic AI:

Empowers ransomware with a high degree of autonomy, allowing it to adapt to environments and defenses in real-time. It gives it the capability to outpace traditional detection and response capabilities.

Purpose-Built and Adaptable Agents:

Reconnaissance, initial access, defense evasion, exfiltration and other agentic AI agents are purpose built and adaptable.

- **Reconnaissance AI agents** can persistently watch for changes in the attack surface.
- **Defense evasion AI agents** can learn the latest evasion techniques, rewrite payloads, and recompile. It can adapt to defenses by encoding traffic different or switching C2 protocols.
- **Exfiltration AI agents** can observe network traffic and blend in, throttle traffic based on traffic patterns, and switch protocols if blocked.

100x Speeds:

Current examples show speed of attacks increasing by 100x. CrowdStrike recently reported that the fastest observed lateral movement following an initial compromise in 2025 was 51 seconds.




Context in Modern Phishing



 You

Analyze the writing style of Travis DeForge based on public posts, blogs, articles and books, and generate a message in that writing style urging people trying to break into cybersecurity to leverage the free resources at xyz.com

 Copilot

Travis DeForge's writing style is characterized by a clear, engaging, and motivational tone. He often uses direct language, practical advice, and a supportive voice to connect with his audience. His style is approachable and informative, making complex topics accessible to a broad range of readers.

Here's a message in the style of Travis DeForge:

Subject: Unlock Your Cybersecurity Potential with Free Resources at XYZ.com

Dear Aspiring Cybersecurity Professionals,

1

Conducting reconnaissance on organizations used to take several hours, if not days.

2

By leveraging AI models, time has been exponentially reduced, allowing malicious actors to launch more attacks against more firms with the same amount of time and effort.

3

AI is particularly good at copying the 'tone' of people's writing. Try it on yourself, it's crazy!

What Can You Do?



1

Ensure that the purpose for the AI solution is understood prior to implementation and educate users on the **Acceptable Use** of any AI solution

2

Implement data classification labels and data loss prevention controls, prior to implementation.

3

Incorporate AI-based scenarios into **Tabletop Testing**

4

Test integrations and access controls to minimize the risk of unintended data exposure.

5

Test your firm's resiliency with a **social engineering evaluation**.

6

Consider a technical solution to **combat deepfakes** such as Netarx.



Questions?

Use the Q&A
Function



Jonathan Bohrer

*President,
Abacus Group*

jbohrer@abacusgroupllc.com



Travis DeForge

*Director of Cybersecurity,
Abacus Group*

tdeforge@abacusgroupllc.com



McKaila Posey

*Manager of Cybersecurity Advisory,
Abacus Group*

McKaila.Posey@entaracorp.com



Steven Shapiro

*Chief Marketing Officer,
Netarx*

sshapiro@netarx.com

*The recording of this webinar will be shared within 24 hours.
For more updates, follow us on LinkedIn.*

LEARN MORE
abacusgroupllc.com