AI-DRIVEN CYBERSECURITY: SAFEGUARDING CRITICAL INFRASTRUCTURE IN THE AGE OF INTELLIGENT THREATS

INNOVATION WEBINAR

October 27, 2025

3:00 to 4:00 p.m. ET

Free & open to the public!

NARUC CPI Innovation Webinar

Moderator: **Hon. David Veleta**, IURC

Ronan Murphy, Forcepoint

Sharla Artz, Xcel Energy

Michael Holko, PA PUC

About NARUC

- Founded in 1889, the National Association of Regulatory Utility Commissioners (NARUC) is a non-profit organization dedicated to representing the state public service commissions who regulate the utilities that provide essential services such as energy, telecommunications, power, water, and transportation.
- NARUC's members include all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands.
- Our mission is to serve the public interest by improving the quality and effectiveness of public utility regulation.
- For more information, visit: www.naruc.org

About NARUC CPI

- The NARUC Center for Partnerships & Innovation (CPI) builds relationships, develops resources, and delivers training to assist state commissions contending with complex current and emerging issues.
- CPI is funded by cooperative agreements with the U.S. Department of Energy (DOE) and the National Institute of Standards and Technology (NIST).
- CPI conducts work across five key energy areas and many topics within each: generation; transmission; distribution; customers; and critical infrastructure preparedness, response, and resilience.
- Among other events, CPI hosts a monthly innovation webinar series on a wide range of timely topics.
- For more information, visit: www.naruc.org/cpi

Upcoming Events

Virtual Events:

- **NCEP Webinar Series: State Agency Roles in Load Growth**
  - **Balancing Speed and Engagement:** November 17, 2025, 2:00 to 3:00 p.m. ET.
  - **State Agency Collaboration:** December 15, 2025, 2:00 to 3:00 p.m. ET.

Upcoming In-Person Events:

- **NARUC Annual Meeting and Education Conference**, Seattle, WA, November 9 – 12, 2025
- **NGA/NARUC Energy Security Workshop** – Dec 9 – 10, Atlanta GA

See the full list of events and access registration links at: www.naruc.org/events/event-list/

Today's Speakers

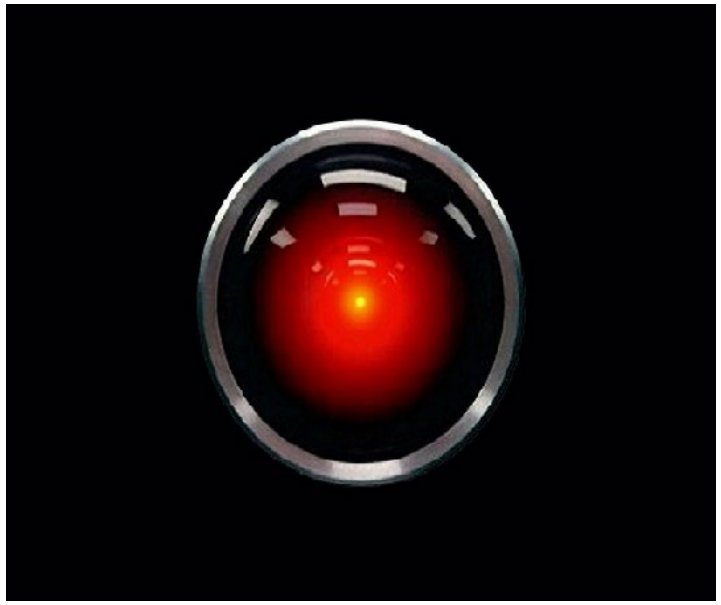
WELCOME

10-27-25 NARUC Meeting

Artificial Intelligence and Impact to Utilities and Regulators

Michael Holko
Director of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission

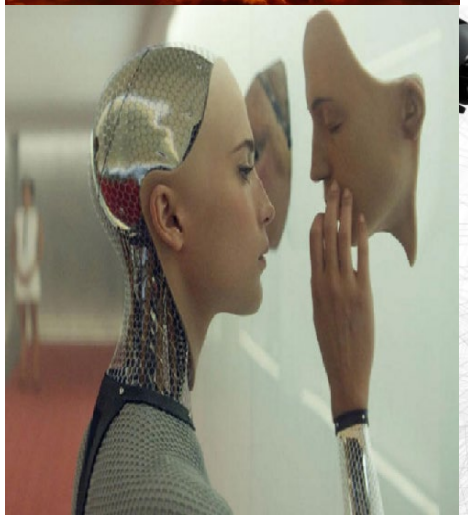
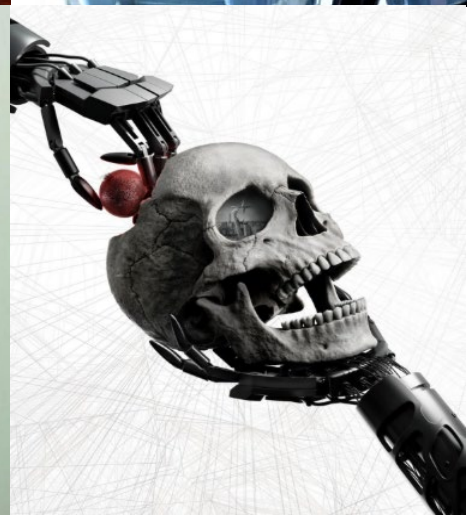
Agenda



- Welcome
- Why We Fear Artificial Intelligence
- Artificial Intelligence Overview
- Artificial Intelligence Benefits to Utilities
- Artificial Intelligence Threats to Utilities
- What Regulators Need to Know
- Biography and Contact Information

Science Fiction Themes



- **Nuclear Holocaust/End of the World**: Movies like The Terminator, War Games, Colossus, etc. where AI become self-aware and starts a nuclear attack or a robotic war to wipe out humanity.
- **Rogue Creation**: TV shows like Battle Star Galactica and Westworld warn us about how robots could turn on their human creators.
- **Manipulative Operating System**: Movies and TV shows like Her, Star Trek, and Person of Interest where an AI operating system becomes so emotionally and intellectually advanced that its human companion's reality is altered and manipulated.
- **Sociopathic**: Movies and TV shows like in 2001: A Space Odyssey, the AI HAL 9000 turns against its human crew with chillingly calm logic after perceiving them as a threat to its mission.
- **Singularity**: Movies and TV shows like the Matrix, Ex Machina, and Black Mirror where AI surpasses human intelligence and can improve itself, suggests that humanity will eventually be superseded, making our existence irrelevant.

News and Social Media Influence

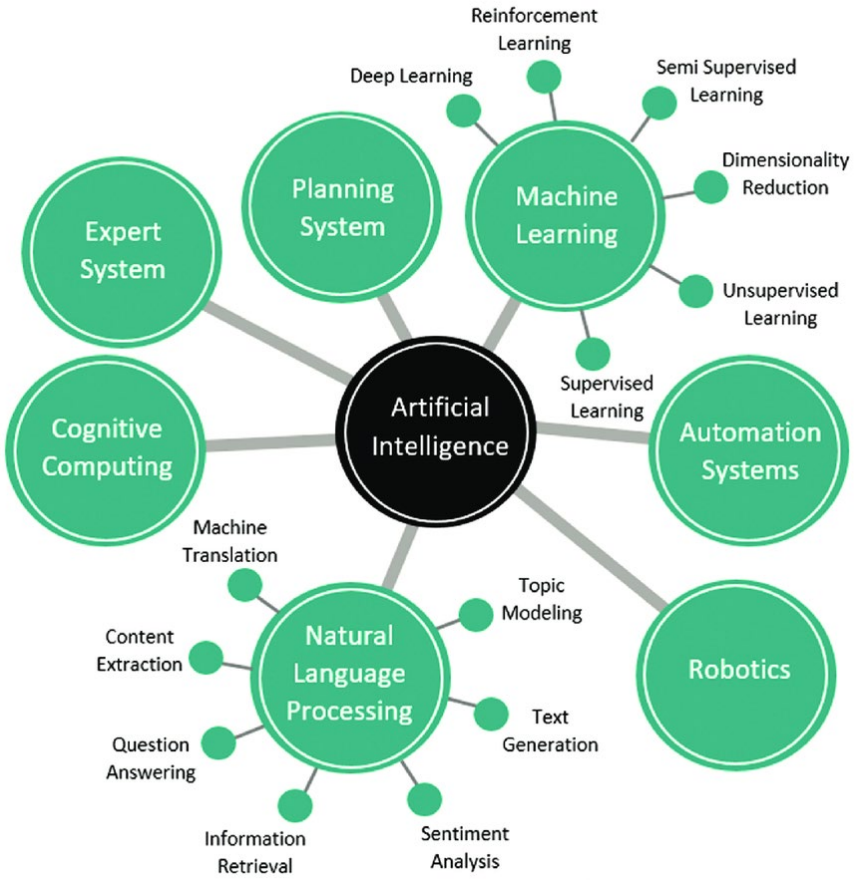
- **Sensationalism**: Headlines that inflate technological threats to grab attention. Stoking anxieties about job losses and threats to humanity. Journalists and social media bloggers frequently highlight worst-case scenarios, such as massive job losses or data breaches, without providing the necessary context or mentioning the potential for new opportunities created by the technology.
- **Fear Mongering**: Media often focus on AI's potential dangers rather than its positive applications.
- **Misuse of AI Technologies**: AI-generated fake news and deepfakes created by people become sensational news and the media uses a few instances of misuse of the technology to highlight the most terrifying possibilities of the technology which increases public distrust in AI.
- **Misrepresenting Capabilities**: Media and social media often embellishes AI capabilities. This creates a public perception of an "all-powerful" technology that is much more advanced and threatening than it truly is.

Artificial Intelligence Overview

Artificial intelligence (AI) is a field of computer science dedicated to creating machines that can perform tasks that typically require human intelligence. Rather than following explicit, step-by-step instructions like traditional software, AI systems are designed to learn and adapt from data.

In simple terms, artificial intelligence works by training a computer to analyze vast amounts of data to identify patterns and make predictions. This is often done using machine learning, where algorithms process data to find correlations and relationships.

Artificial Intelligence Overview



The process for most modern AI, particularly machine learning, can be broken down into three key steps:

- **Collect and Prepare Data**: An AI system's learning begins with a massive and diverse dataset, which can include images, text, numbers, or videos. For example, to teach an AI to recognize a cat, you would provide it with thousands of labeled images of cats and other animals.

- **Train the Model**: Using a learning algorithm, the AI processes the data to find and learn patterns. It finds the underlying features that distinguish a cat from other animals on its own. The more data it is given, the better it becomes at recognizing the patterns.

- **Predict and Improve**: Once the AI is trained, it can make predictions or decisions based on new, unseen data. It continuously refines its own internal settings to minimize errors and improve accuracy over time.

Traditional AI vs. Generative AI

Feature	Artificial Intelligence (Traditional AI)	Generative AI
Primary Goal	To analyze, categorize, and interpret existing data to solve specific problems and make predictions.	To create entirely new content, such as text, images, music, or code, based on learned patterns from its training data.
Core Function	Predictive analysis, classification, and automation of tasks. It makes decisions within predefined rules.	Content generation and creative tasks. It produces unique and original output rather than simply identifying existing patterns.
How it Works	Uses various techniques like supervised and unsupervised machine learning to find structure in data. It often follows a more transparent, interpretable decision-making process.	Uses large, complex models, like deep learning with neural networks, to learn the underlying structure of data and generate new data that has similar characteristics.
Common Uses	Spam filters, fraud detection, recommendation engines (e.g., Netflix), and predictive analytics.	Writing articles, creating images from text prompts, composing music, and generating code.
Data Needs	Depending on the task, it can be efficient even with smaller, more specific datasets.	Often requires massive, diverse datasets to learn how to create high-quality, novel outputs.
Key Limitation	Its output is limited to what it has been trained to recognize or classify. It cannot produce original content beyond its existing data.	It can "hallucinate" or create false but plausible information, and its creative output lacks true human understanding or intent.

Artificial Intelligence Benefits to Utilities

Electric Utilities

- Grid Management: AI helps monitor grid data in real time, enabling it to balance energy load, reroute power to prevent outages, and integrate intermittent renewable energy sources like solar and wind power.
- Predictive maintenance: Using data from sensors, AI can forecast when equipment, such as transformers and power lines, is likely to fail. This allows utilities to schedule proactive repairs and avoid unplanned, costly outages.
- Demand forecasting: AI analyzes historical data, weather patterns, and customer behavior to accurately predict energy demand, which helps optimize energy generation and distribution.

Gas Utilities

- Leak Detection: AI systems analyze real-time data from pipeline sensors to detect anomalies in pressure and flow that may indicate a gas leak. This enables faster response times to prevent accidents and protect the environment.
- Predictive Maintenance: By analyzing data on pipeline integrity, corrosion rates, and equipment health, AI can predict when components might fail. This allows for proactive repairs that minimize downtime and increase safety.
- Infrastructure management: Gas utilities can use AI to model and optimize pipeline routing and infrastructure placement.

Water Utilities

- Leak and Main Break Detection: By analyzing data on water flow and pressure, AI can identify patterns that signal a leak or predict a potential main break, allowing utilities to respond proactively and conserve water.
- Water Quality Monitoring: AI analyzes data from sensors to detect changes in water quality and identify potential contaminants, such as harmful bacteria, in real time.
- Process Optimization: In treatment plants, AI can optimize energy consumption by adjusting pump runtimes and determine the optimal dosage of chemicals for water disinfection.

Artificial Intelligence Benefits to Utilities

Holistic Security Overview

- IT/OT Convergence: AI unifies data from both IT and OT networks, providing a single, comprehensive view of the security landscape. This bridges the communication gap between security teams and improves coordinated responses.

Automated Response and Resilience

- Automated Incident Response: AI-powered Security Orchestration, Automation, and Response (SOAR) tools can automatically contain a threat by isolating endpoints or blocking malicious activity, reducing incident response time.
- Simulations and testing: Using digital twins, AI can simulate cyberattacks in a virtual environment to test security measures without disrupting real-world operations.

Enhanced Threat Detection

- Anomaly Detection: AI algorithms establish a baseline of normal network activity to instantly flag unusual behavior in both IT and OT systems, such as unauthorized commands on a SCADA network.
- Forecasting attacks: AI analyzes threat intelligence and historical incidents to predict potential attack vectors, enabling utilities to proactively reinforce defenses.

Improved Operational Technology (OT) Defense

- Asset Visibility: AI automatically identifies, and maps all connected devices across the OT environment, removing blind spots and securing every endpoint.
- Zero-trust security: AI continuously verifies access requests from both users and machines, enforcing strict, least-privilege access to critical systems.

Strengthened Physical Security

- AI-powered Surveillance: AI video analytics monitor physical assets like substations, detecting unusual behavior, unauthorized access, or abandoned objects, and alerting security in real time.

Artificial Intelligence Threats to Utilities

- **Automated and Enhanced Reconnaissance**: AI enables attackers to scan for vulnerabilities across vast IT and OT networks at machine speed.
- **Sophisticated Social Engineering**: Generative AI creates hyper-personalized phishing emails that are difficult to distinguish from legitimate messages. AI can analyze publicly available information to identify key personnel and third-party suppliers to target.
- **Deepfakes**: Deepfake voice and video can be used to impersonate executives or engineers, tricking employees into unauthorized actions.
- **Advanced Operational Technology (OT) Attacks**: Attackers use "adversarial machine learning" to subtly manipulate data fed into OT systems, causing them to fail or malfunction.
- **Malware**: AI-driven malware can learn to evade traditional detection methods, infecting critical control systems unnoticed.
- **Data Analysis**: AI can analyze system data to precisely time an attack for maximum disruption, such as a targeted equipment failure during peak demand.
- **Combined Attacks**: AI can combine with other technologies like drones to target physical infrastructure, such as substations, from a remote location.

What Regulators Need to Know

Regulatory Oversight and Governance

- **Establish Clear AI Governance**: Regulators need to confirm that utilities have a formal AI governance framework in place. This framework should establish policies and ethical guidelines for the responsible development and use of AI, as advocated by national frameworks from organizations like the National Institute of Standards and Technology (NIST).

- **Identify Decision-making Boundaries**: AI models can be complex and opaque, making it difficult for stakeholders to understand their decisions. Regulators should ask utilities to disclose how AI is being used in critical, customer-facing decisions, such as rate adjustments or service disconnections.

- **Ensure Accountability**: In the event of a system error or failure, regulators must ensure that clear lines of accountability have been defined. It should be clear who is responsible for the performance, ethics, and safety of AI-driven systems.

What Regulators Need to Know

Customer Equity and Bias

- **Prevent and Audit for Bias**: If trained on biased historical data, AI can inadvertently perpetuate or amplify existing inequities. Regulators should ask utilities how they are auditing their AI models and training data to prevent discriminatory outcomes in pricing, resource allocation, and customer service.
- **Ensure Transparency**: Utilities should be able to provide clear, accessible explanations of how AI is used and how customer data is protected. This builds public trust and transparency, especially regarding automated decisions that affect customers.

Cybersecurity and Data Management

- **Mitigate New Threat Vectors**: AI can expand a utility's attack surface and introduce new risks, such as data poisoning and model manipulation. Regulators should question utilities about their cybersecurity strategies, especially regarding the protection of both IT and OT systems from AI-enhanced attacks.
- **Protect Sensitive Data**: Utilities collect vast amounts of customer data through smart meters and other technologies. Regulators need to verify that robust cybersecurity protocols and data governance policies are in place to prevent data breaches, protect customer privacy, and ensure compliance with regulations.

What Regulators Need to Know

Operational Reliability and Safety

- **Monitor Autonomous Systems**: AI in critical infrastructure is increasingly autonomous, capable of making decisions about grid management or other utility functions. Regulators should ensure that utilities maintain a "human-in-the-loop" oversight process for autonomous systems to prevent unintended consequences.
- **Validate Safety-Critical models**: When AI is used for safety-critical functions like predictive maintenance, regulators should demand validation of the AI models. This ensures that the AI can be trusted to perform its intended function without risking catastrophic failure.
- **Evaluate Cost-Benefit**: Utilities should justify the financial investment in AI initiatives to regulators, detailing how the technology improves efficiency, reliability, or service. Regulators can scrutinize the ROI to ensure ratepayer costs are justified.
- **Address Workforce Changes**: The adoption of AI and automation will likely change roles for the utility workforce. Regulators may want to understand how utilities plan to retrain and upskill employees, as well as ensure that AI is augmenting, rather than replacing, skilled workers.

Biography and Contact Information

Michael C. Holko was appointed as the first Director of the Office for Cybersecurity Compliance and Oversight (OCCO) by Chairman Gladys Brown Dutrieuille in September 2018. OCCO is the Pennsylvania Public Utility Commission's office responsible for working with the regulated utilities to ensure they have adequate measures in place to help prevent and/or mitigate damage from cyberattacks on their critical infrastructure.

As the Director of OCCO, Mr. Holko is responsible for advising the Chairman, Commissioners, and Executive Director on policy and procedural issues; improvements involving cybersecurity oversight functions of regulated utilities; draft proposed cyber-related regulations; and oversee the preparation of orders, rulemakings, policy statements, Secretarial Letters and memoranda related to cybersecurity policies and procedures of those regulated utilities.

Michael Holko, Director, Office of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission
400 North Street, 3rd Floor North
Commonwealth Keystone Building, HBG, PA 17120
717-425-5327 | miholko@pa.gov

Forcepoint

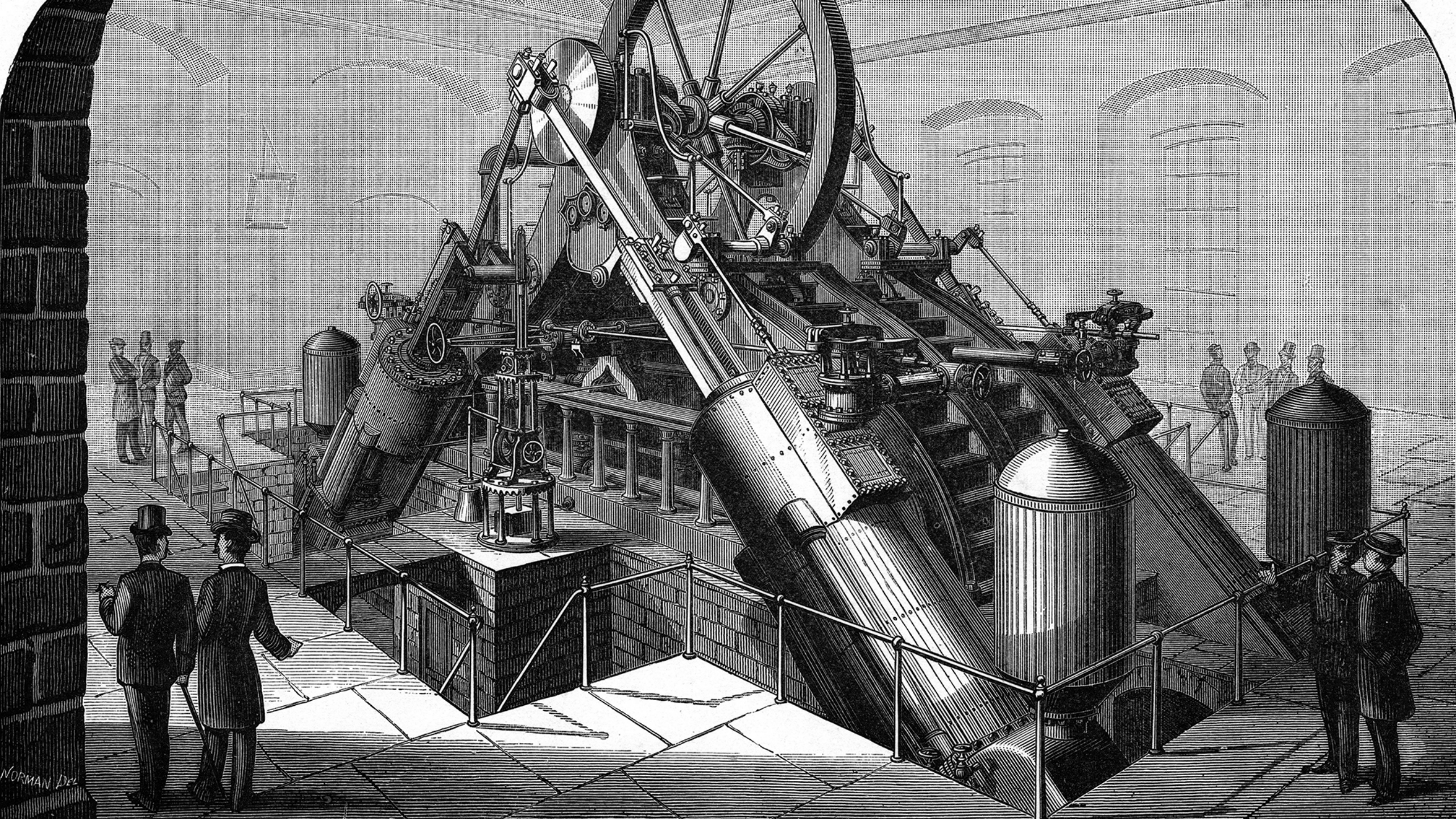
Data Security Everywhere

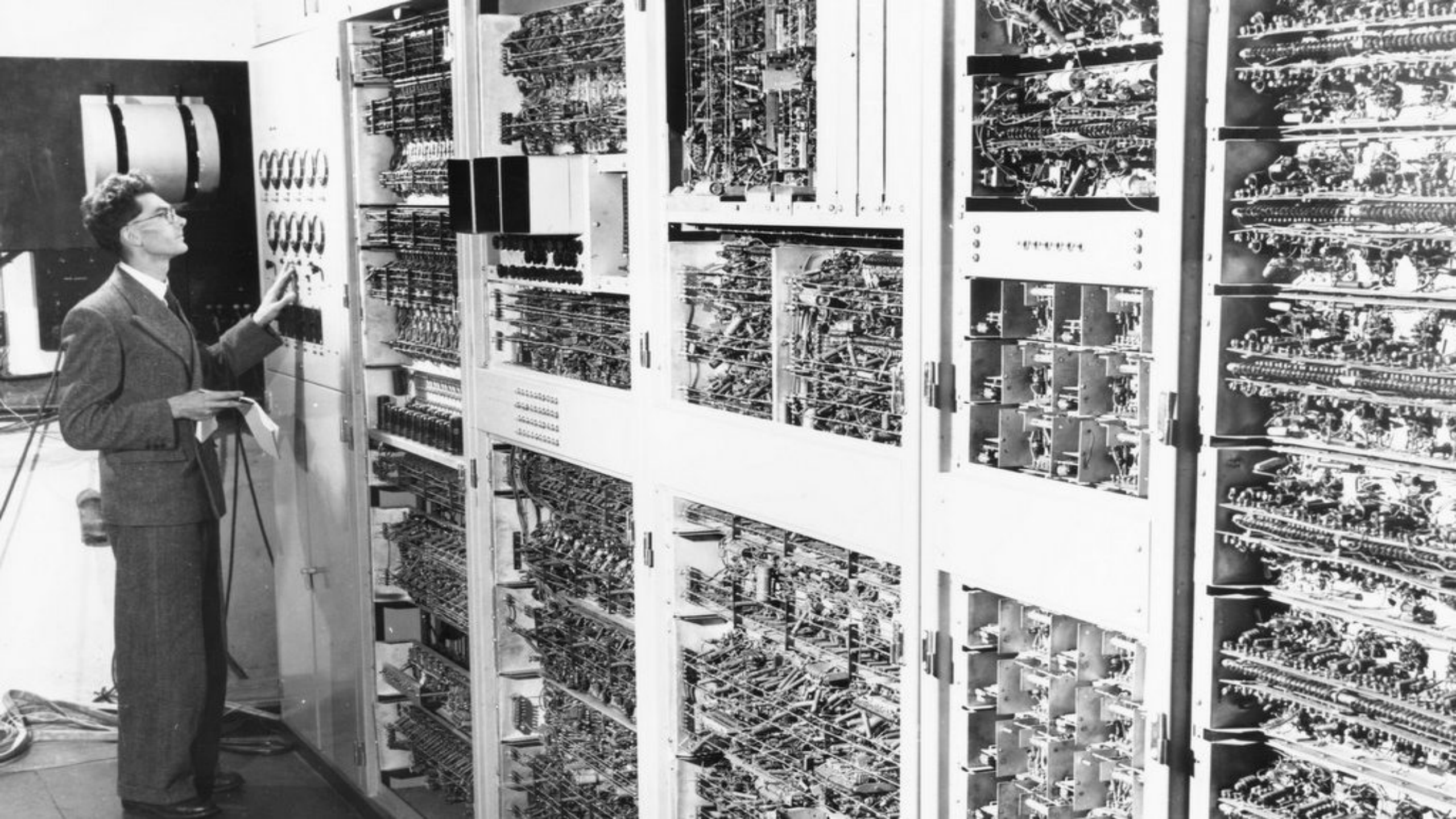
Know. Dynamically Adapt. Simplify.

Ronan Murphy
Chief Strategy Officer

THE AI REVOLUTION

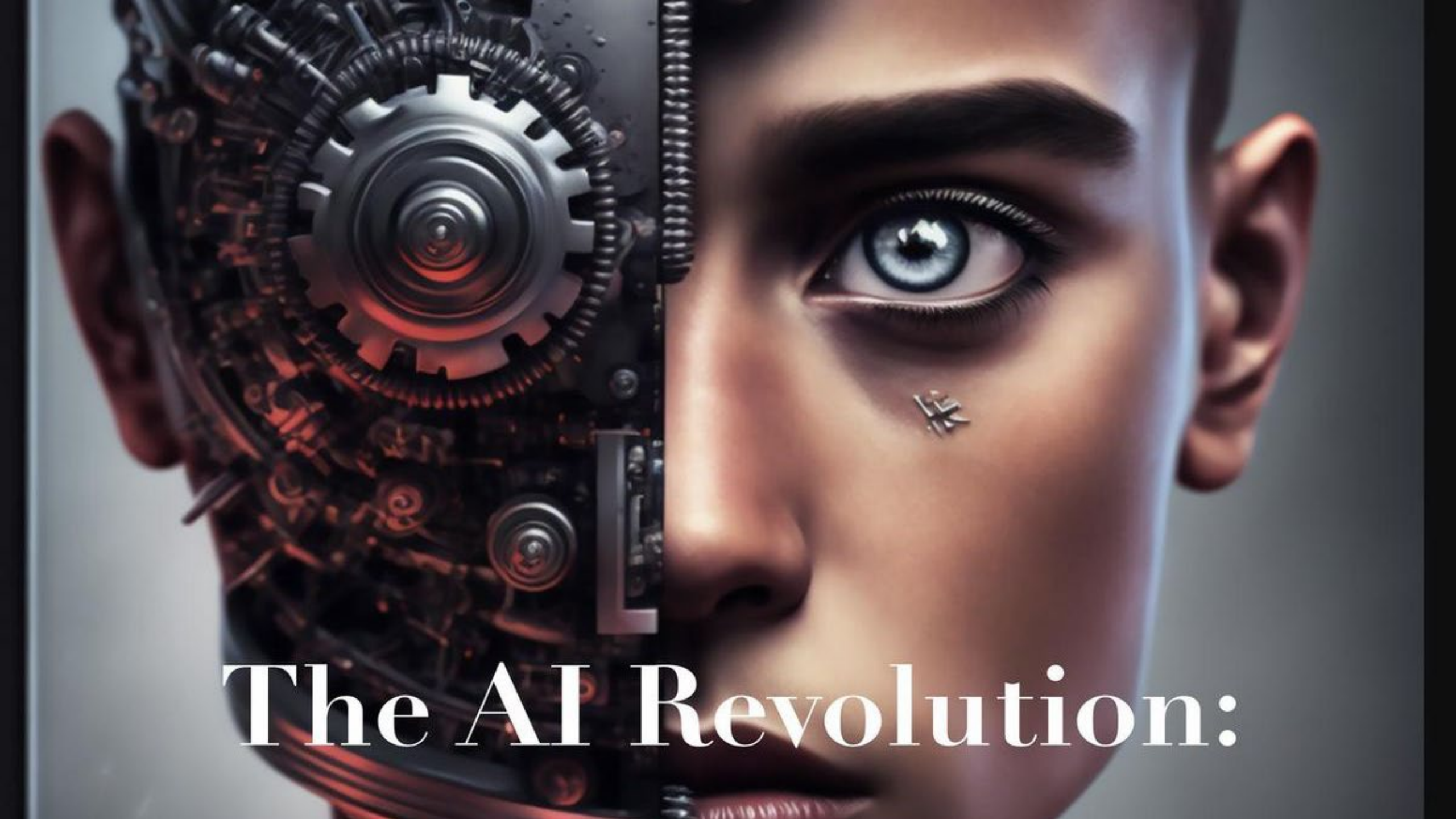
Ronan Murphy


NORMAN DEL



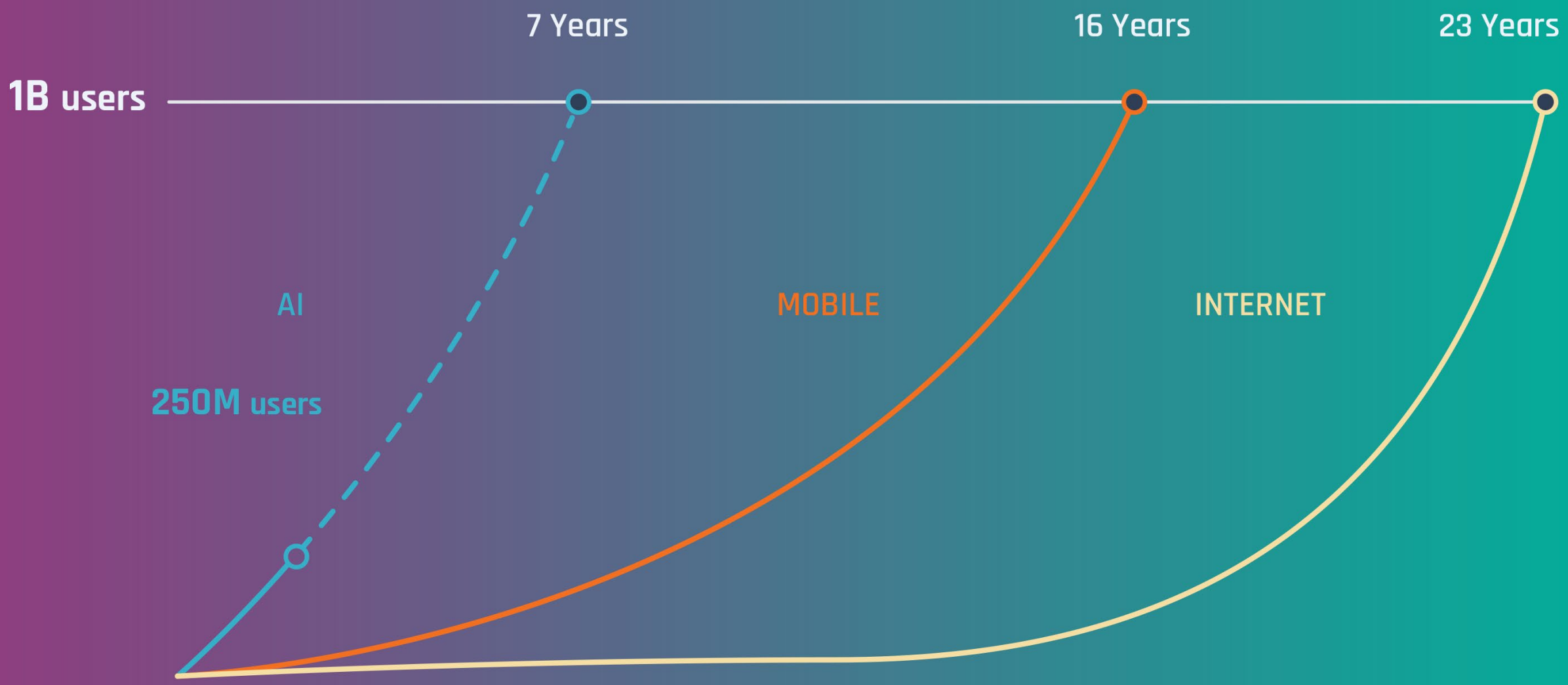

Hello world!
Welcome to Apple
Find It
Product Information
Customer Support
Technology & Research
Developer World
Groups & Interests
Resources Online
About Apple
Apple Sites Worldwide
Switzerland
Taiwan
Turkey
UK & Ireland
United States
Introducing CyberDrive
Register today for a free CD-ROM.
EMATE 300
Mobile, Affordable, & Smart
MOVIES FROM MARS
What's Hot
Preorder Mac OS 8
Now you can preorder Mac OS 8, described by Macworld as "the most comprehensive update to the Mac OS in years, sporting a bold new
Be the First to Know
Learn about new Macintosh software releases the moment they become available. Check Hot Mac Products to hear about programs like Speed
New Tab
Google
Images
Web
YouTube
Chicago, IL - Google


EXIT



The AI Revolution:

AI Is already the fastest growing Technology in our history

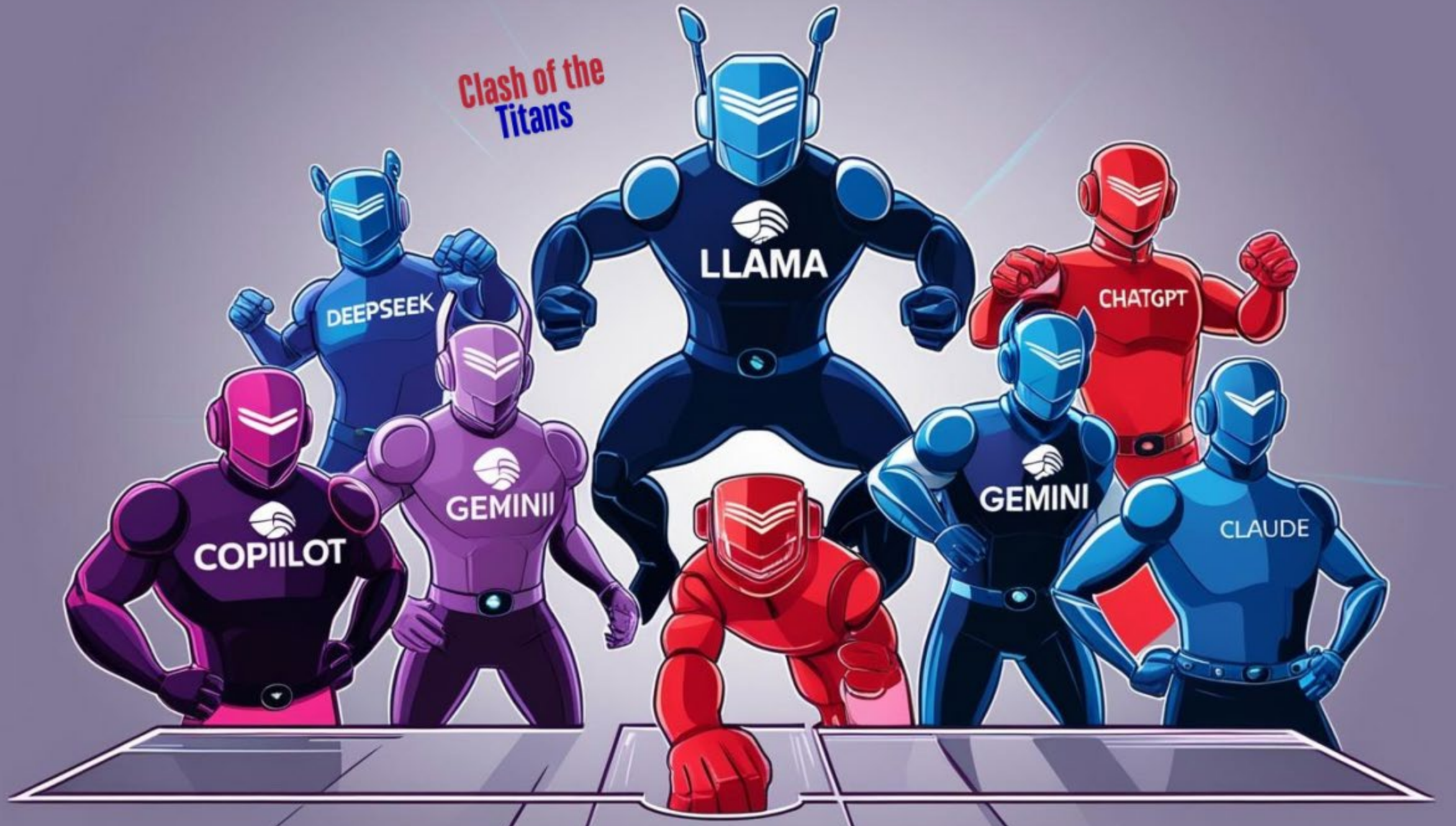


Improved Decision Making

Efficiency based on Automation

Productivity Gains

Personalized Services & Experiences




deepseek


RISK
MANAGEMENT


Copilot
Your everyday AI companion
Copilot


OpenAI
Gemini

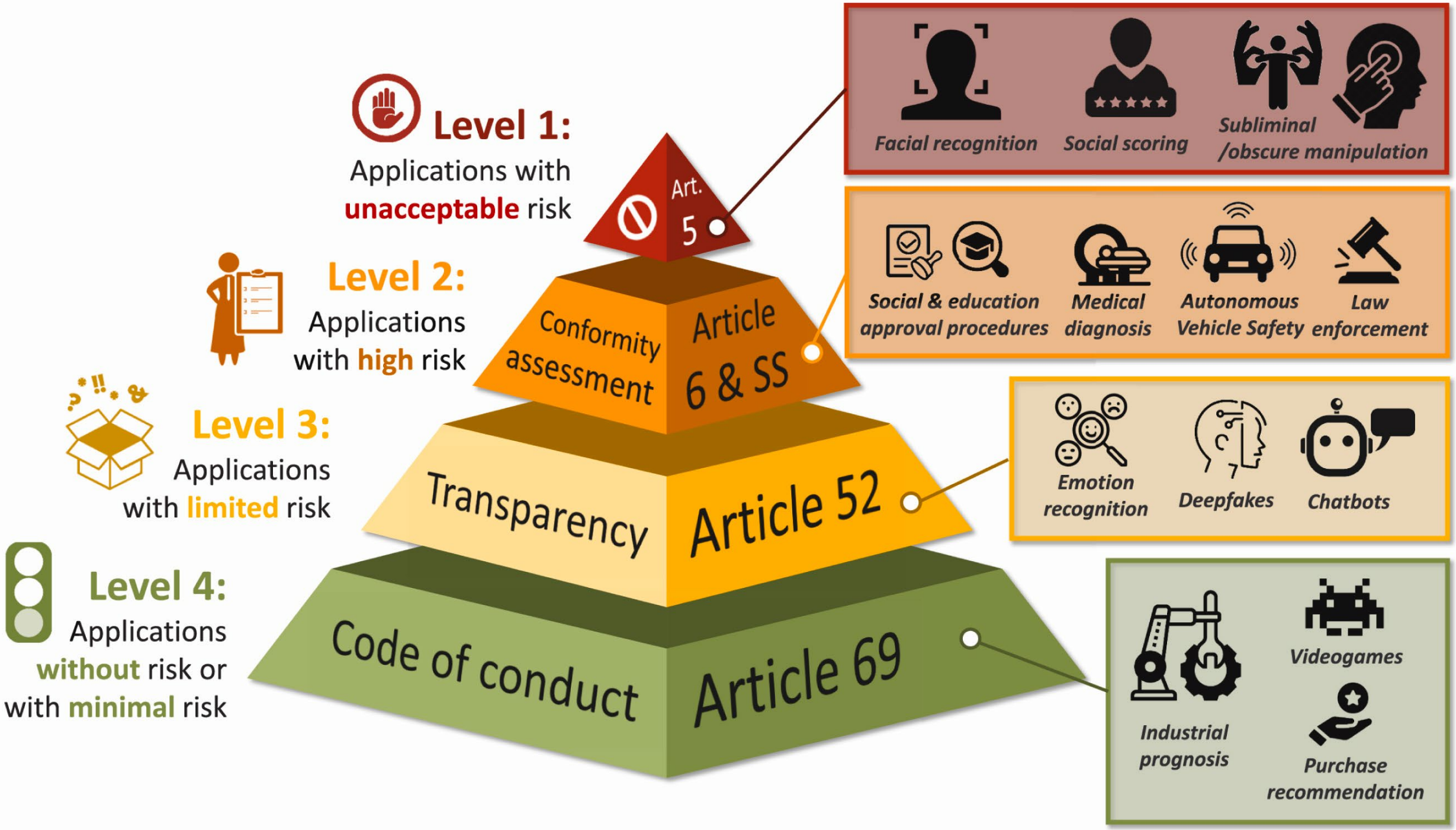
Legit Discovers “AIJacking“ Vulnerability in Hugging Face

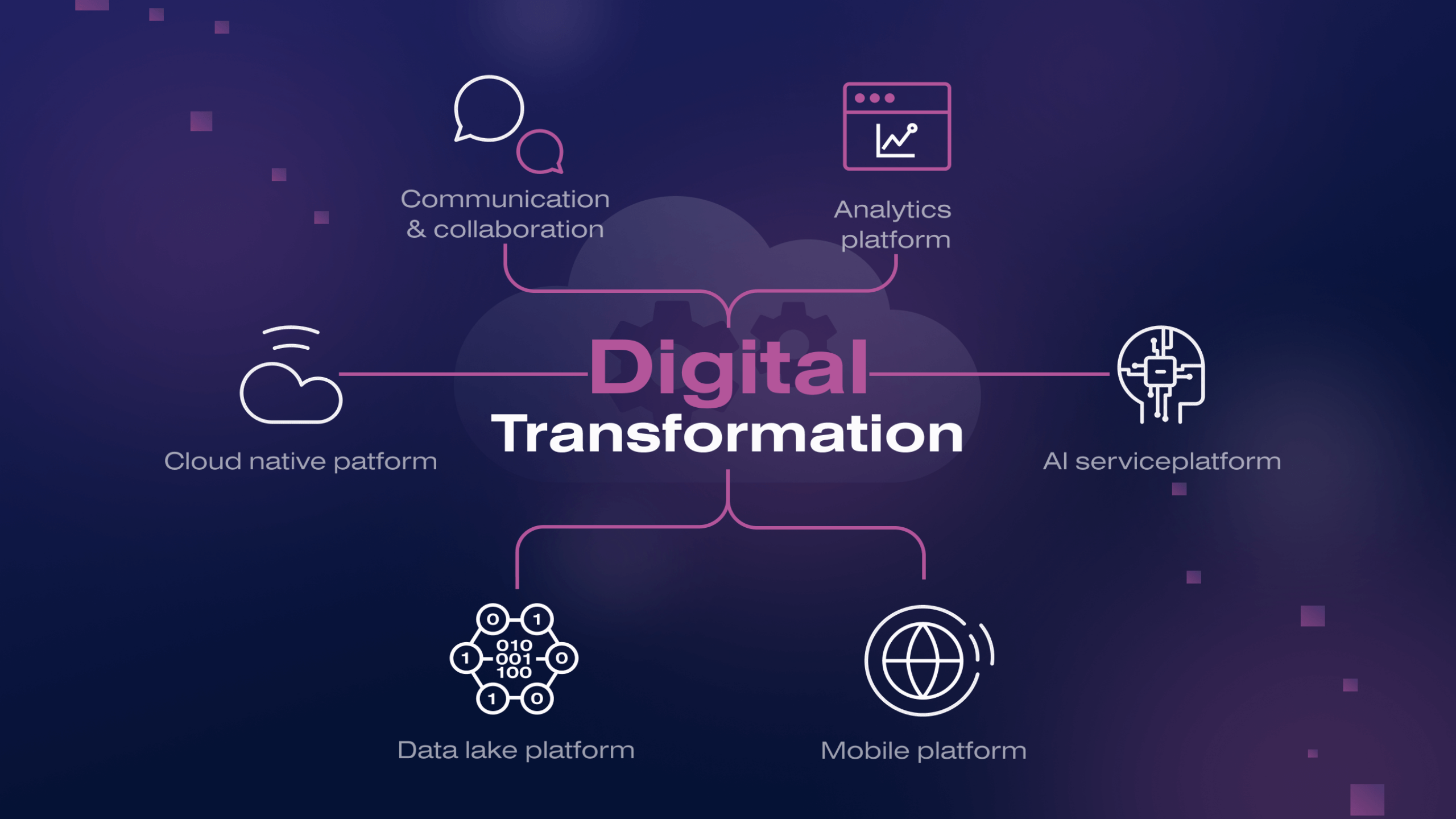

NATIVE AI
EMBEDDED AI
DATA RISK
CISO


AI
AI
AI
AI
AI
AI
AI
AI
COMPANY
DATA
AT RISK


NEURAL
DATA
BRAINS
WEB DATA
DAIA
DATA
DATA
FOR DTA AVAILEBANITY
FOR AI TRAINING
DATA
DATAS


The
EU
AI Act
Welcome to
the European Parliament


Level 1:
Applications with unacceptable risk
Level 2:
Applications with high risk
Level 3:
Applications with limited risk
Level 4:
Applications without risk or with minimal risk
Art. 5
Conformity assessment
Article 6 & SS
Transparency
Article 52
Code of conduct
Article 69
Facial recognition
Social scoring
Subliminal /obscure manipulation
Social & education approval procedures
Medical diagnosis
Autonomous Vehicle Safety
Law enforcement
Emotion recognition
Deepfakes
Chatbots
Industrial prognosis
Videogames
Purchase recommendation

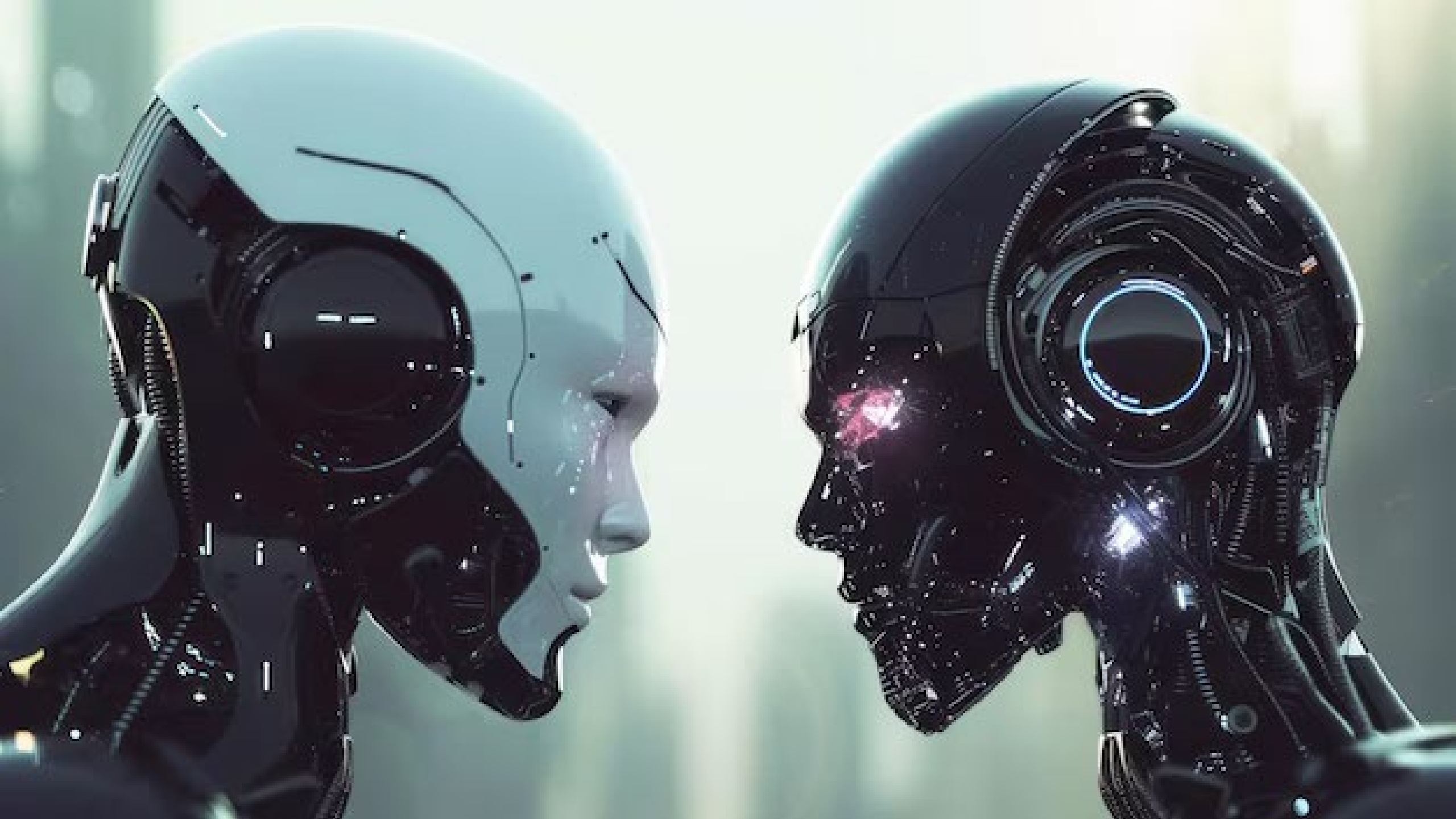

Communication
& collaboration
Analytics
platform
Digital
Transformation
Cloud native patform
AI serviceplatform
010
001
100
Data lake platform
Mobile platform

If your data isn't ready for AI, you're not ready for AI

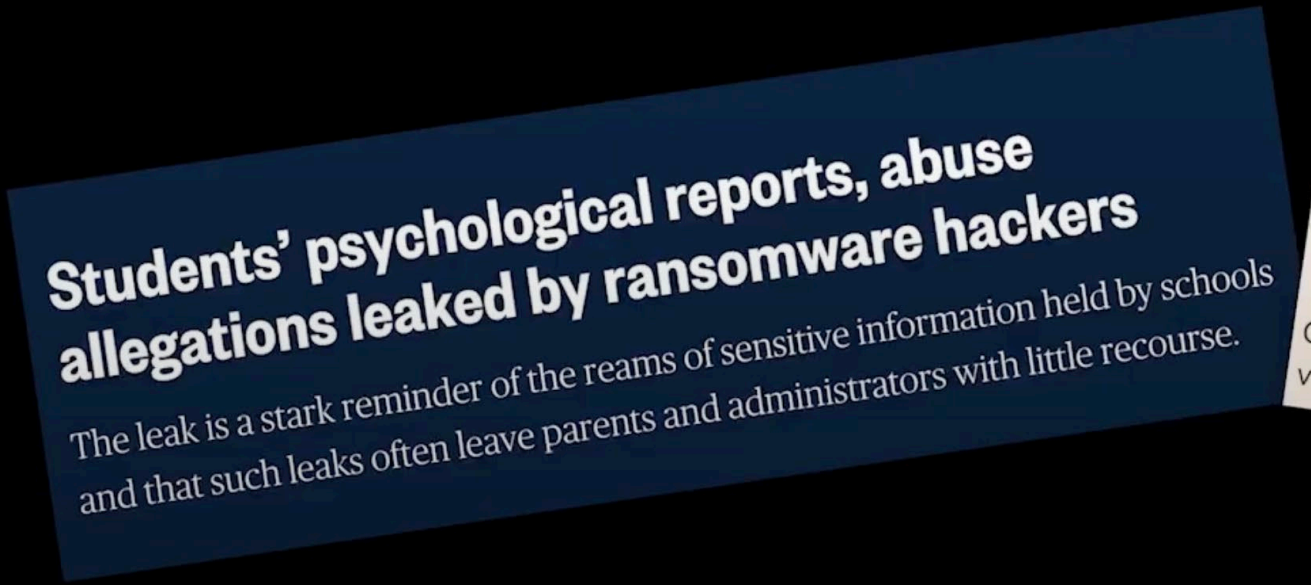

aps Lock
PROTECT YOUR DATA
Ctrl
A
S
Z
X


$6
trillion
$10.5
trillion
2022
2025


Ai



DATA IS WHERE DAMAGE HAPPENS

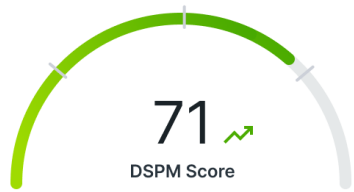


Forcepoint

- Dashboard
- Insights
- Data Sources
- Assets
  - Files
  - Users
  - Emails
- DDR
- Policy
  - Compliance Hub
  - Data Register
  - Controls Orchestration
  - Incidents
- Administration
  - Pattern Matching
  - Live Events
  - Detectors
  - AI Mesh
  - Access Controls
  - Webhooks
  - Email Configuration

Collapse

Dashboard



By Data Source

One Drive	18
Google Drive	34
Sharepoint	59
One Drive	78
Google Drive	96

5 More

Users oversharing data

Emilia Aniston	324
Joel Johnson	256
Sandra Parker	201
Sam Willson	178

354.6K
Total files

102.6K
Critical files

210.7K
Regulated files

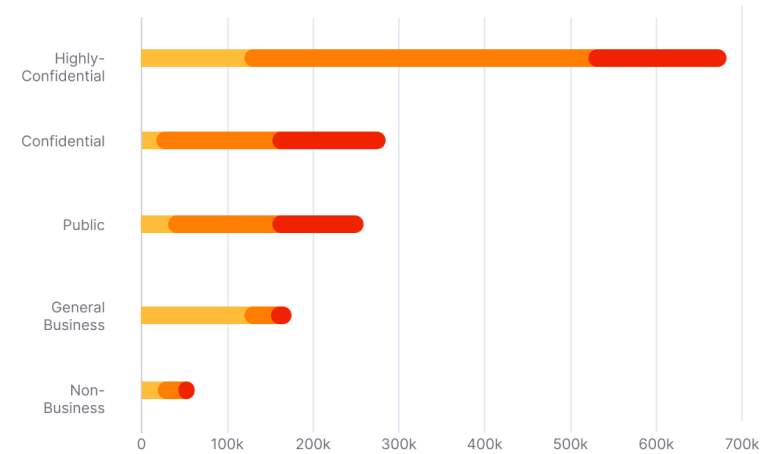
Quick fixes

Overshared critical data 54.1K

36.5K	Public access detected	Make private
10.1K	Shared with Third Parties	Review access
10.1K	Scope too broad internally	Specify teams

Risks files distribution

Group by: Data Sources | Classification | Compliance | Categories



Open Incidents

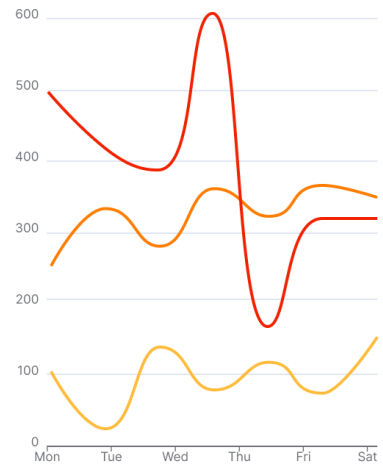
High Severity

Compliance	968
Least privilege	561
Misconfiguration	361
Overshared	230
Policy violation	143

Medium Severity

Regulatory risk	750
Security	306
Vulnerability	74

Incidents dynamic



Forcepoint AI Mesh provides highest-accuracy understanding of data

More than just classification, rich context to truly know your data

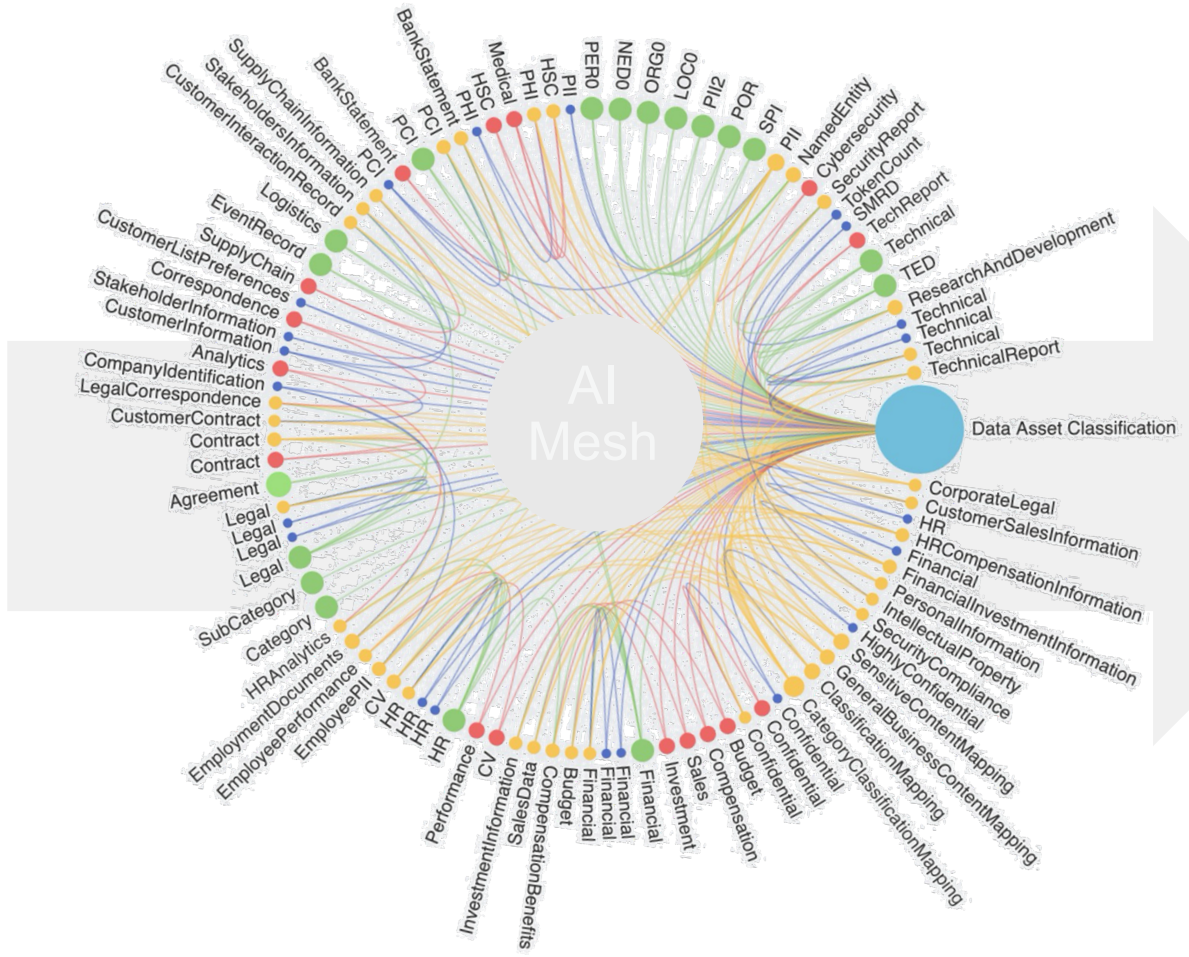
Smaller: SLM 10X smaller than LLM models

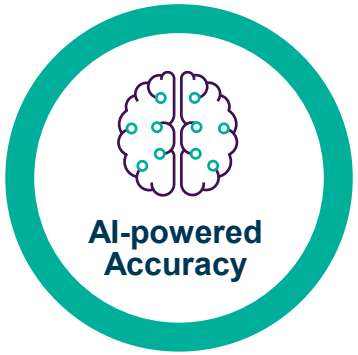
Faster : 200ms classification using regular CPUs

Lower TCO: smaller nodes significantly lowers cost

Trainable: can be tuned to unique classification requirements

Explainable: Simplifies audit of AI for transparency / trust





Detectors · AI Classifiers · Light AI Classifiers · Summarizers

Forcepoint
DSPM

IDENTIFY

SSN, Address, GPS, IP, Loon Number, Account ID. TOxiD, Driver's License, License, Age, Rack, Geeference, Profile, Cookie, Password, Solory, Employed, ..

CATEGORIZE

PII, PCI, GLBA, ITAR, CCPA, PHI, NPI, LGPEDA..

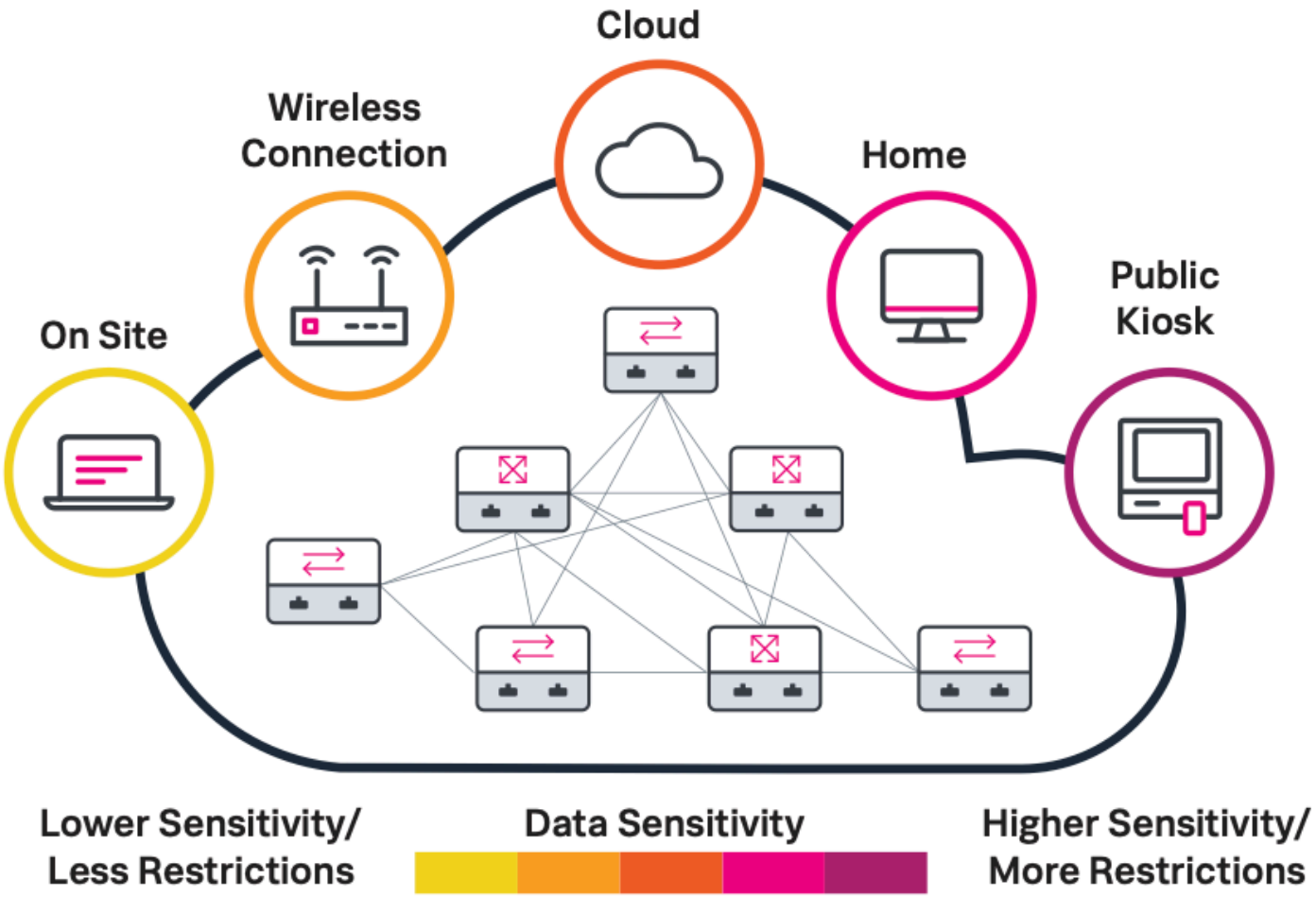
CLASSIFY

Sensitive, Secret, High, Low, Public, Private, Con-

PROFILE

Duplicote, ROT, Similar, Related, Conneected, Correlated

Foundations of Zero Trust Architecture



What a Security Operations Center (SOC) does

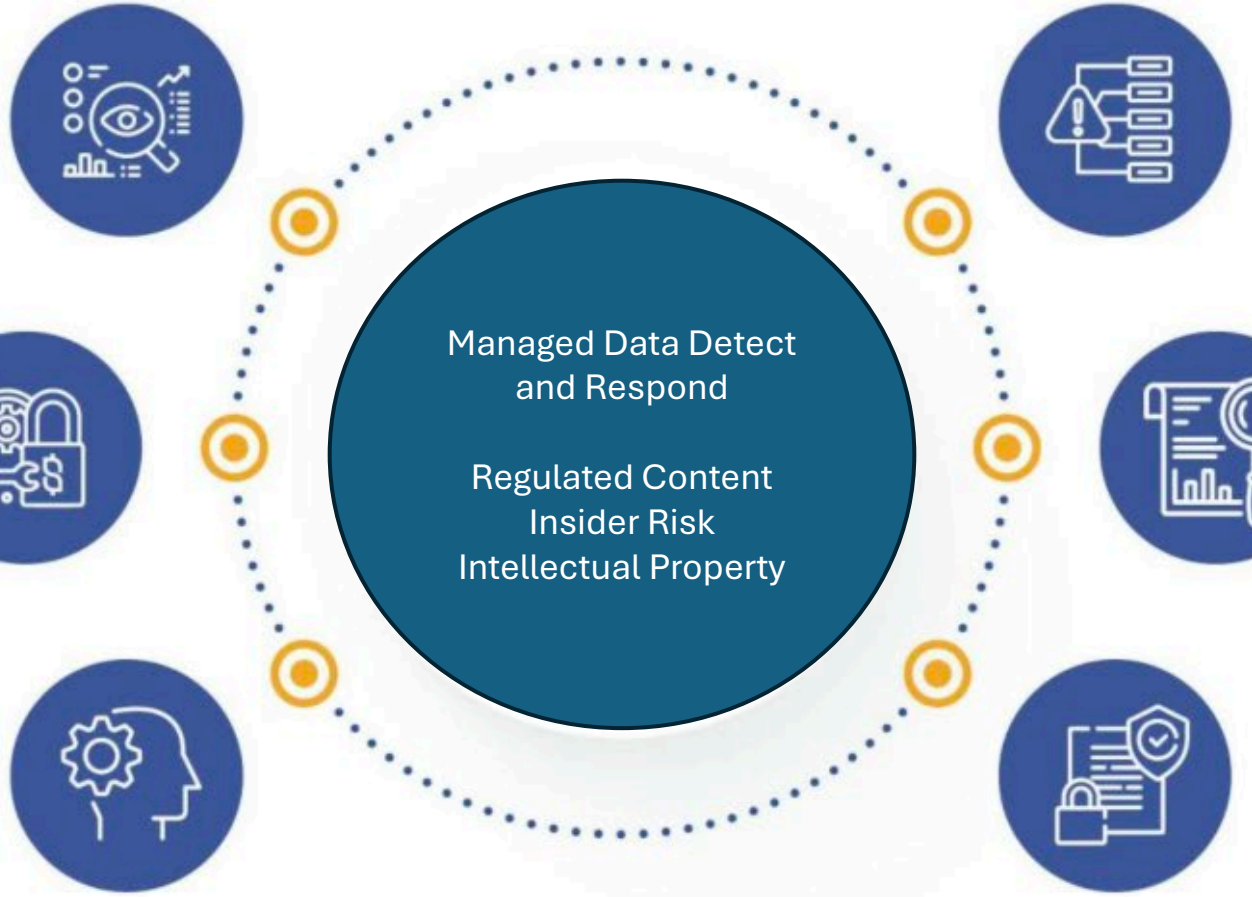
MDR -> MDDR

Continuous monitoring

to provide around-the-clock security awareness and detect anomalies

Incident response

to mitigate damage and keep the organization running after an incident



Prevention and detection

to detect malicious activities and stop them before they can cause any damage

Reporting

to fill in the data repository with all incidents and threats, making it more precise and responsive in the future

Threat intelligence

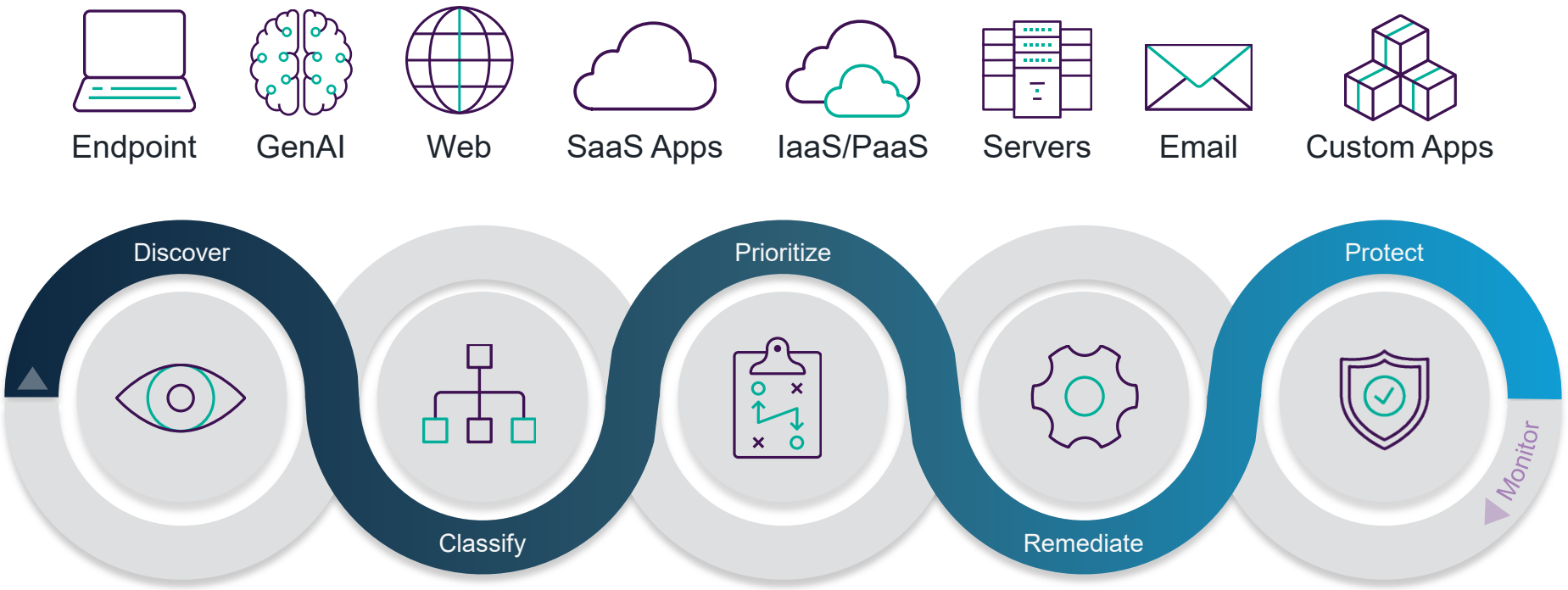
to stay one step ahead of malicious actors by being up to date with specifics on attacker tools, techniques, and trends

Compliance management

help ensure that organizations are compliant with important security standards and best practices.

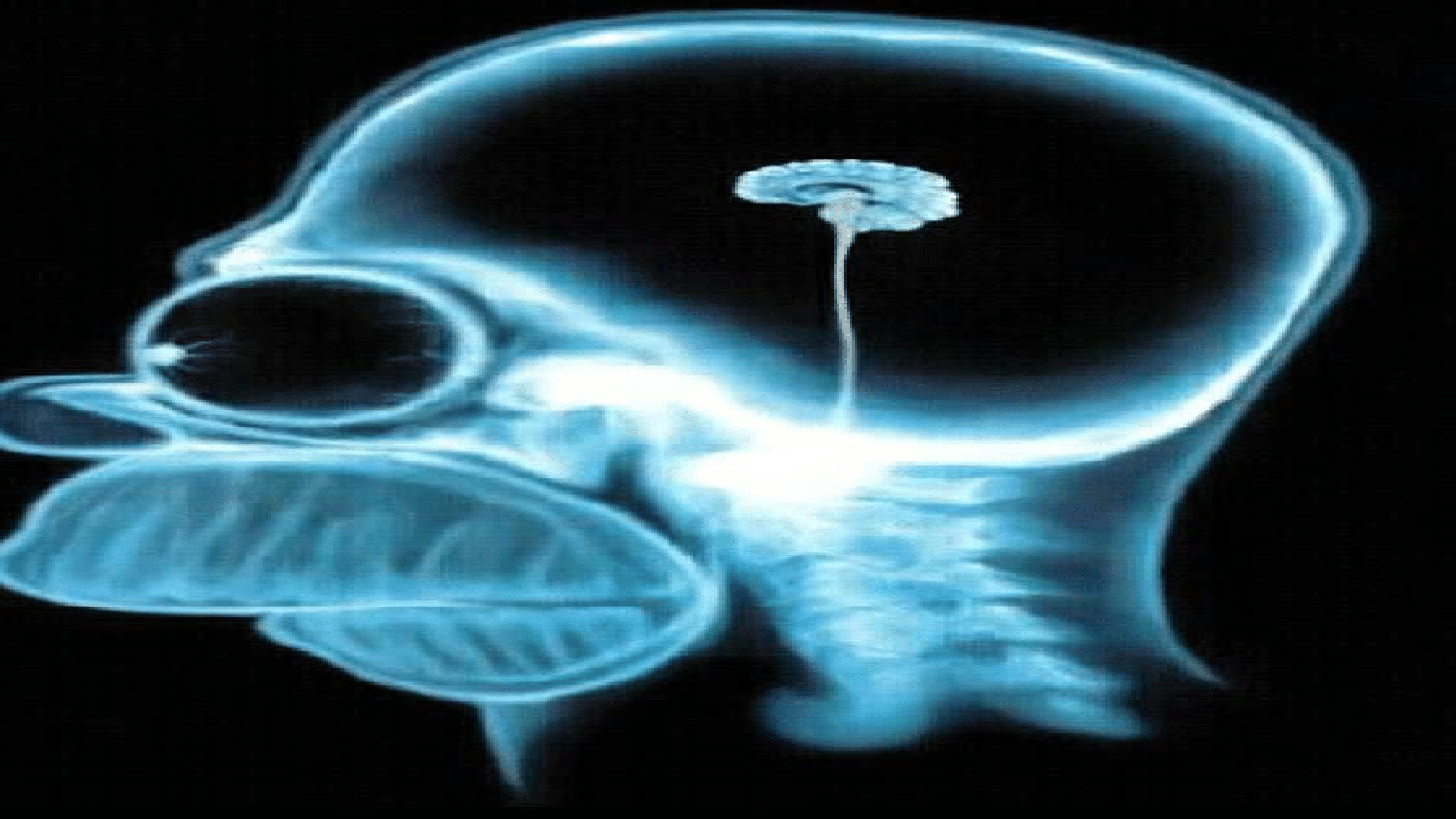
Forcepoint Data Security Framework

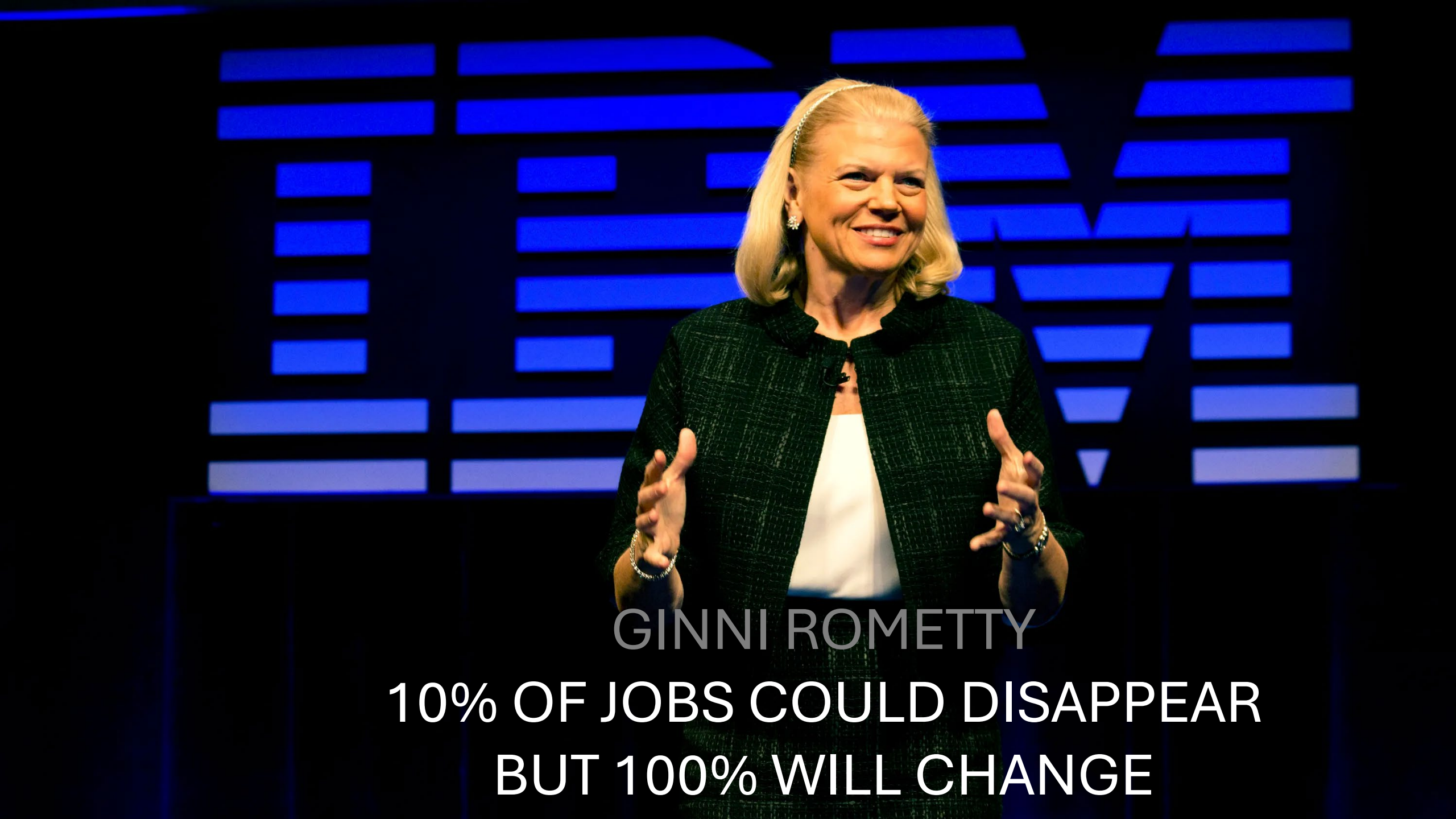
Data Security Everywhere



Data-at-Rest	Data-in-Use	Data-in-Motion
Forcepoint DSPM	Forcepoint DDR	Forcepoint DLP


WHAT NEXT ?



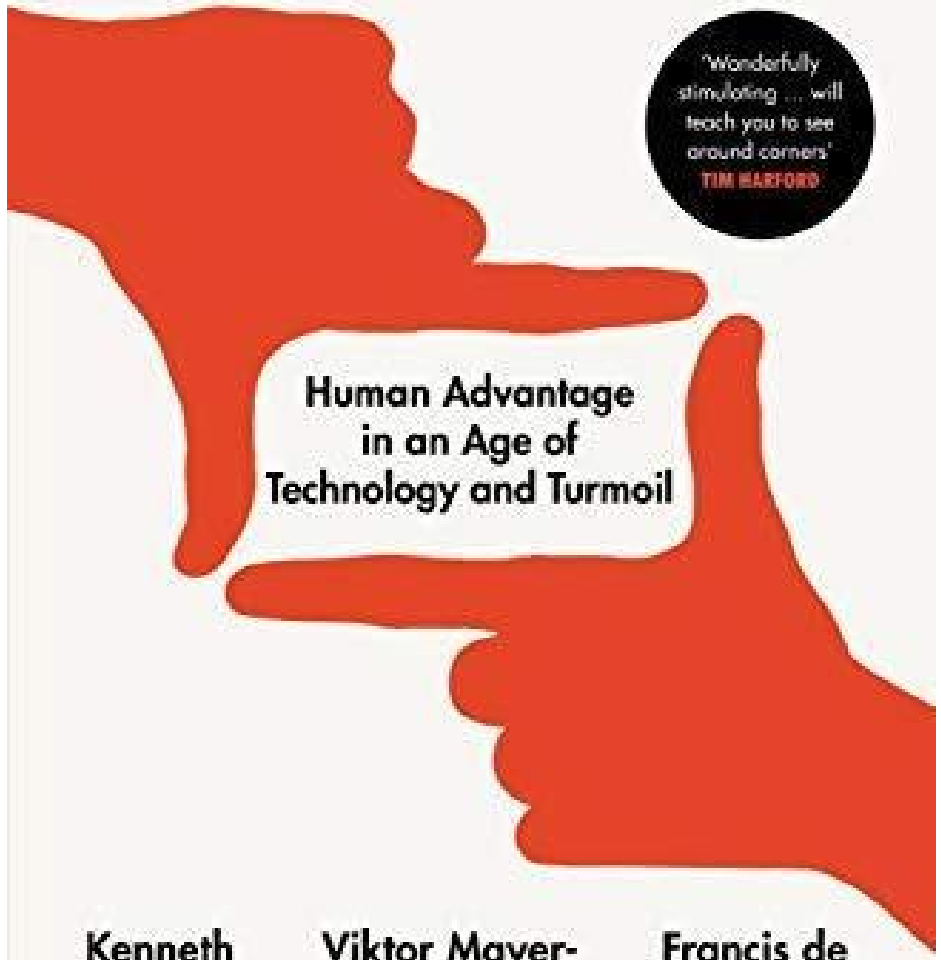

GINNI ROMETTY
10% OF JOBS COULD DISAPPEAR
BUT 100% WILL CHANGE

HUMANS,
ARE STILL
THE BEST LOW COST
ALL PURPOSE NON-LINEAR
COMPUTER SYSTEMS
THAT CAN BE
MASS-PRODUCED
BY UNSKILLED LABOUR.

FOR NOW

2-MILLION-COPY GLOBAL BESTSELLING AUTHORS OF *BIG DATA*

FRAMERS

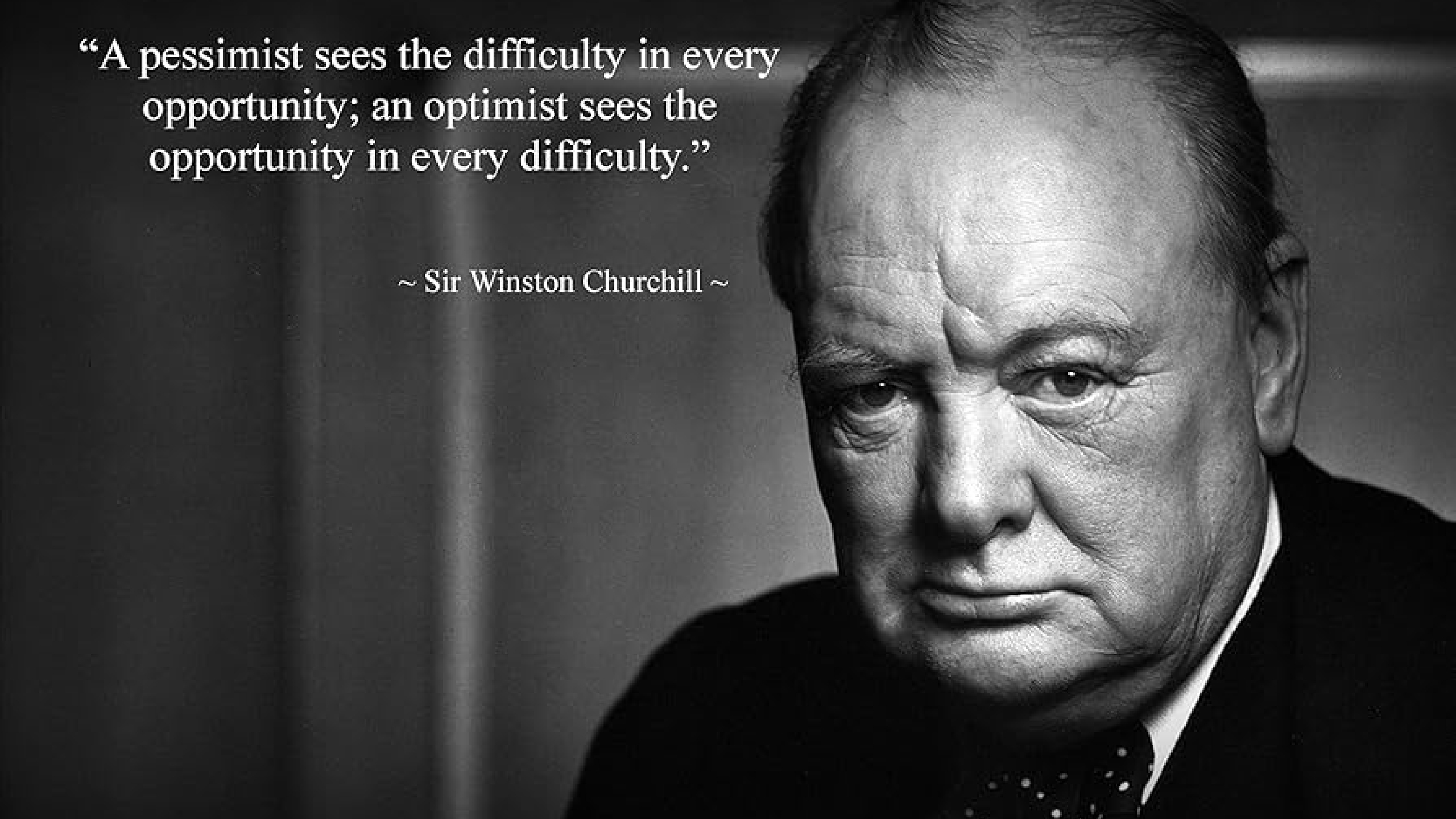


'Wonderfully stimulating ... will teach you to see around corners'
TIM HARFORD

Human Advantage in an Age of Technology and Turmoil

Kenneth Cukier
Viktor Mayer-Schönberger
Francis de Véricourt


Workflow
Automation
Healthcare
Manufacturing
eCommerce
Customer Service


“A pessimist sees the difficulty in every opportunity; an optimist sees the opportunity in every difficulty.”
~ Sir Winston Churchill ~

XCEL ENERGY

MAKING ENERGY WORK BETTER

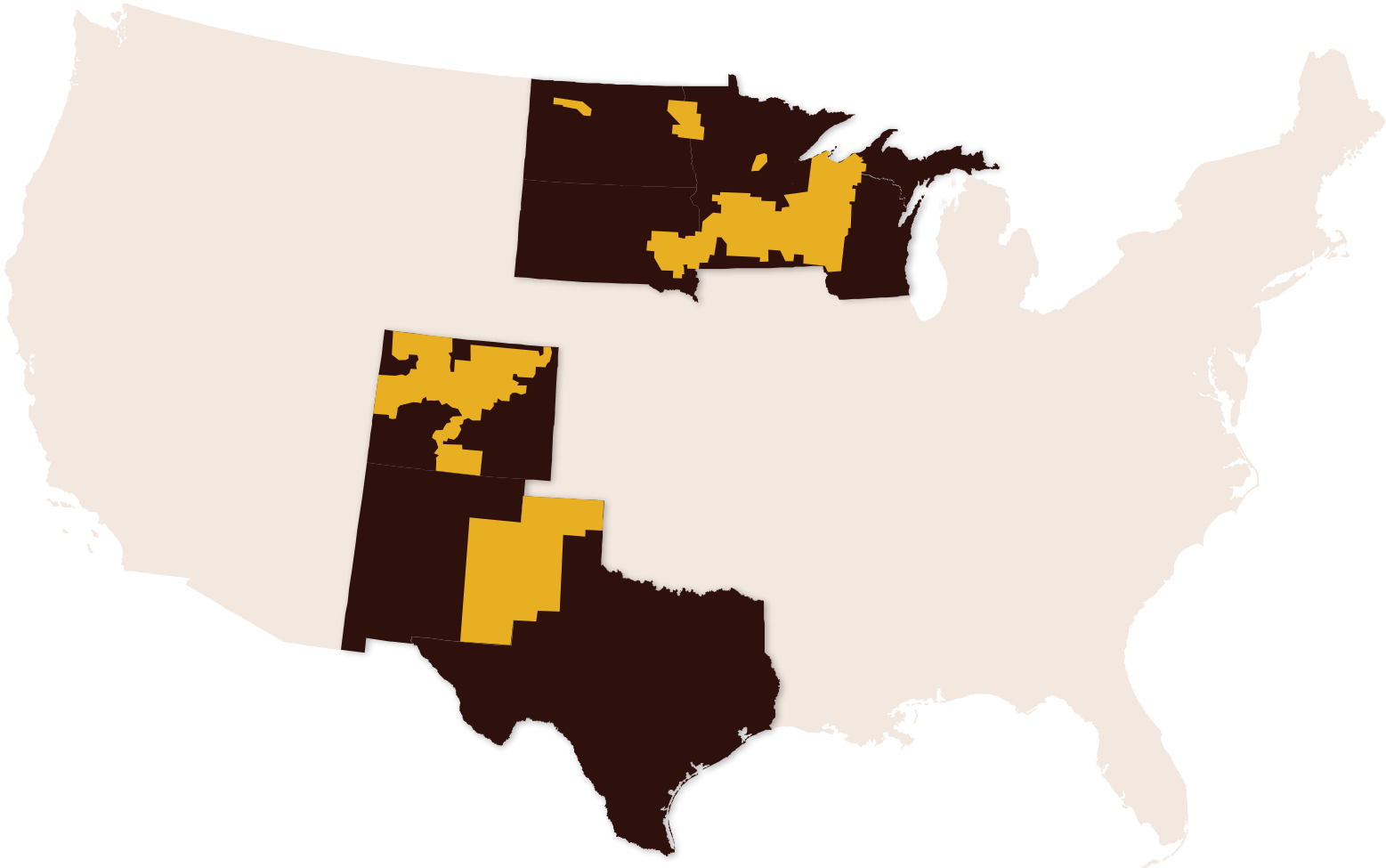
SERVING EIGHT STATES

3.8 million
electric customers

2.2 million
natural gas customers

National leader

- Wind energy
- Energy efficiency
- Carbon emissions reductions
- Storm restoration



Q&A with all Speakers