The Key to Digital Transformation: Privacy-by-Design Solutions

Michael Hughes
Chief Business Officer, Duality Technologies
Ronen Cohen
VP, Global Product Strategy and Regulatory, Duality Technologies

The Key to Digital Transformation: Privacy-by-Design

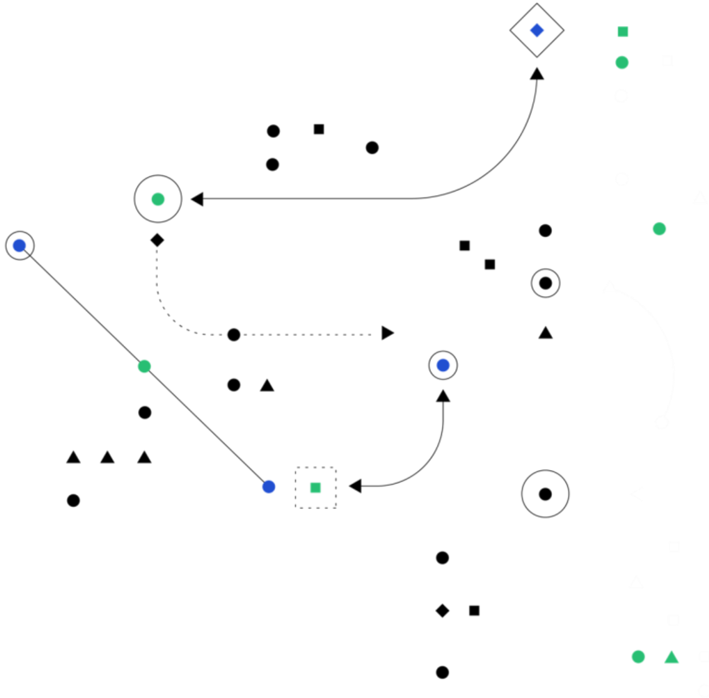
Michael Hughes

Chief Business Officer
Duality Technologies, Inc.

Ronen Cohen

VP Product Strategy
Duality Technologies, Inc..

Agenda



1. Introduction
2. UK National Data Strategy and Privacy
3. Case Studies
4. Q&A

Duality **unlocks data collaboration**, empowering organizations to maximize the value of data and models

Privacy, Security, Data Governance Built-in means working with sensitive data is easy, fast, secure and compliant

We **unlock AI on sensitive data** while maintaining privacy and security

DARPA
The Department of the Treasury 1789
U.S. Department of Homeland Security
NIH National Institutes of Health
ico. Information Commissioner's Office
LLOYDS BANK
LSEG
MasterCard
Deloitte.
CDA Cyber Defence Alliance
aws
Microsoft Azure
Google Cloud
IBM
ORACLE
CACI EVER VIGILANT
Globant
carahsoft.
intel
Scotiabank

The National Data Strategy & Privacy

3 Key Priorities from the UK National Data Strategy

Unlock the value of data across the economy.

Transform government's use of data.

Build a world-leading data economy.

Achieving these goals requires sensitive data

Improve data access, skills, infrastructure, and foster trust in the data ecosystem.

Unlock the value of data across the economy.

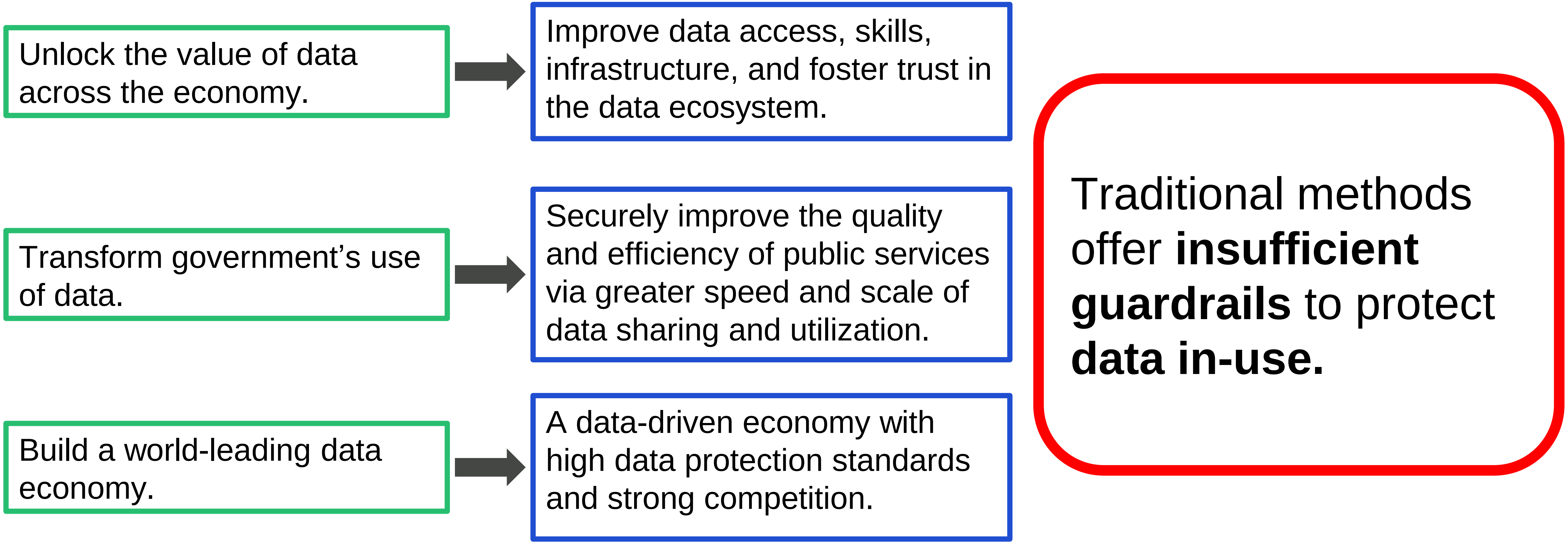
Securely improve the quality and efficiency of public services via greater speed and scale of data sharing and utilization.

Transform government's use of data.

A data-driven economy with high data protection standards and strong competition.

Build a world-leading data economy.

Traditional means of using data prevent success



Unlock the value of data across the economy.

Improve data access, skills, infrastructure, and foster trust in the data ecosystem.

Transform government's use of data.

Securely improve the quality and efficiency of public services via greater speed and scale of data sharing and utilization.

Build a world-leading data economy.

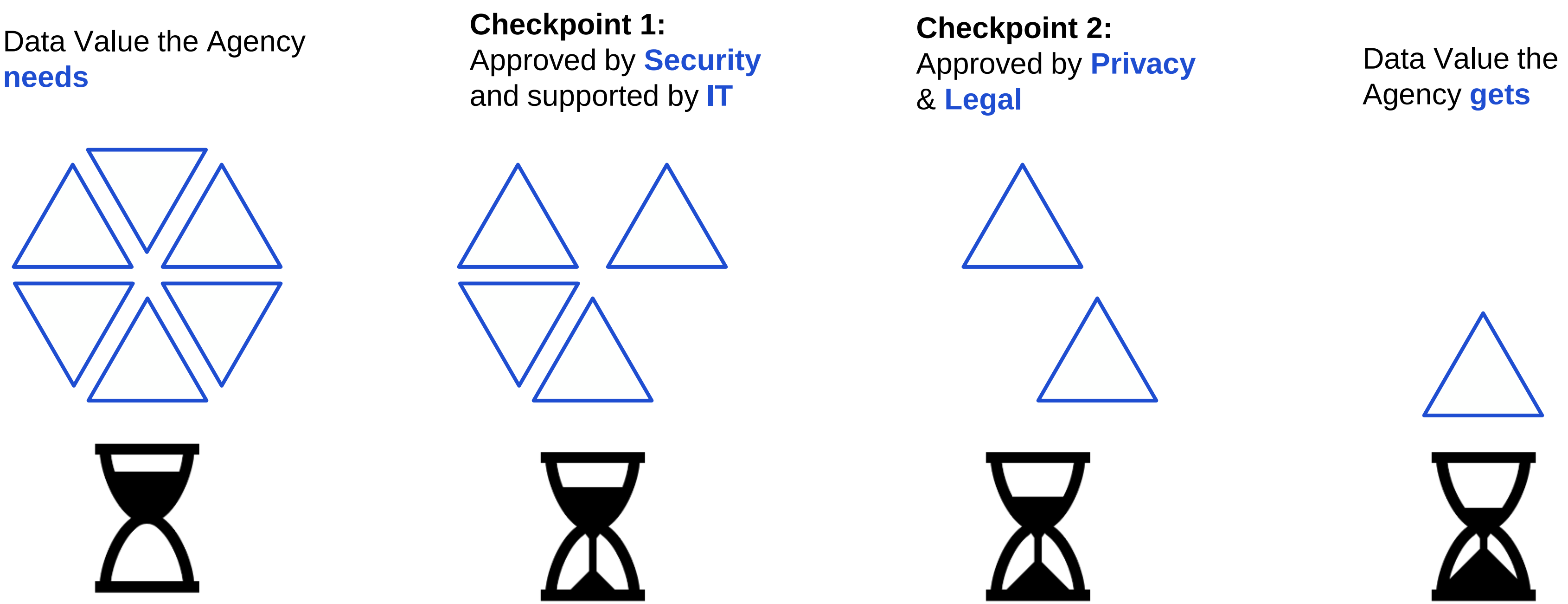
A data-driven economy with high data protection standards and strong competition.

Traditional methods offer **insufficient guardrails** to protect **data in-use.**

Today’s processes to access and use data strip away value and waste time

Processes using…

- **Deidentification**
- **Tokenization**
- **Synthetic data**
- **Differential Privacy**
- **Governance alone**



Data Value the Agency **needs**

Checkpoint 1: Approved by **Security** and supported by **IT**

Checkpoint 2: Approved by **Privacy** & **Legal**

Data Value the Agency **gets**

PETs Create Efficiencies and Improve Quality

When security, privacy, and governance are by design.

Software using PETs…

- **FHE**
- **Confidential Computing**
- **Federated Learning**
- **Secure MPC**
- **Governance with PETs**

Data Value the Agency **needs**

Guardrails: Platform already approved by **Security, Privacy, Legal** and supported by **IT.**

Data Value the Agency **gets**

“If your organisation shares large volumes of data, particularly special category data, we recommend… using PETs. PETs enable safe data sharing and allow organisations to make the best use of the personal data they hold”

- John Edwards, UK Information Commissioner

[ICO urges organizations to harness the power of data safely by using privacy enhancing technologies]

Meeting Data Priorities in Public Health

Health care ecosystems are **too complex and critical to endure lengthy checkpoints** or data centralization efforts.

Benefits of better data access

- Better research, outcomes, and policies,
- Reduced administrative burdens, and streamlined operations

But…

Challenges include

- Protecting sensitive data while using it
- Engendering public trust and confidence

Meeting Data Priorities in National Security & Defence

Unlocking data offers a **broad asymmetric advantage** and supports a **defence-in-depth** strategy.

Benefits of better data access

- Better decision making
- Streamlines operations
- Reduces costs by up to 90%

But…

Challenges include

- Leveraging highly sensitive data and analytics while maintaining security standards
- Balancing transparency with secrecy

Meeting Data Priorities in Government in General

Data is critical to providing services and supporting social needs

Benefits of better data access

- Better policy decisions, service delivery, and optimized public spending

But…

Challenges include

- Handling sensitive information transparently
- Collaborating across departments to support citizen needs

The data doesn’t matter unless you can use it

Public / Private Collaboration

ico.
Information Commissioner's Office

BACKGROUND

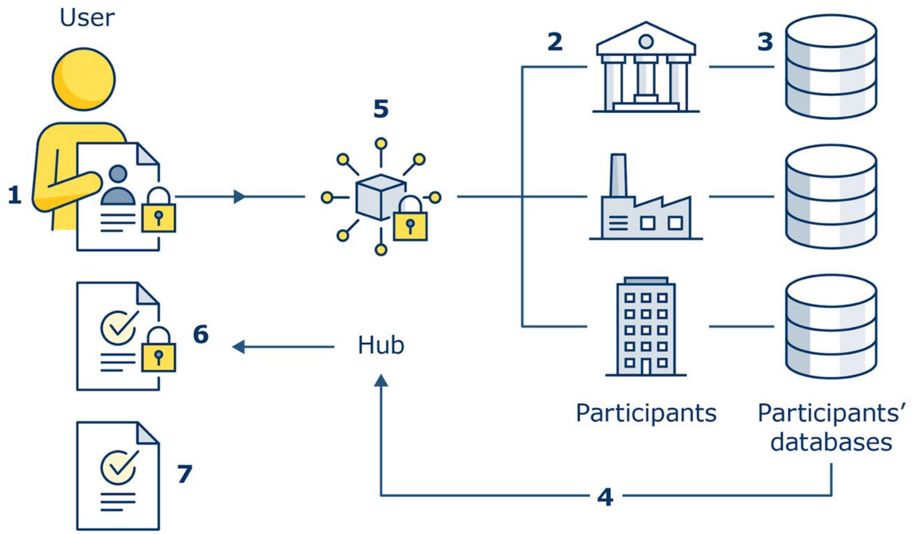
- LEA and private sector partners need to share PII to detect and prevent financial crimes, and investigate networks
- Certain data cannot be shared until suspicion threshold is reached – which may never happen

SOLUTION

- Each participant deploys **encrypted queries** to hide subjects of investigation / customer info
- Insights can be shared **without moving data**

RESULTS

- **Ability to share data – even "pre suspicion"**
- **Responses in minutes** rather than weeks
- **Improved attribution and case building**
- Ability to collaborate **in compliance with GDPR**



"If your organisation shares large volumes of data, particularly special category data, **we recommend that… you start considering using PETs**."
~John Edwards, UK Information Commissioner

“Zero Footprint” OSINT, CAI, PAI Investigations

BACKGROUND

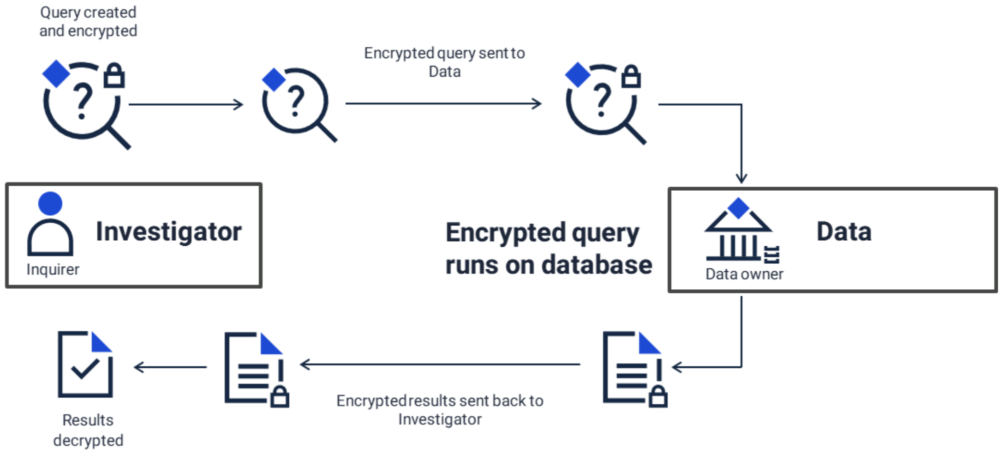
- Law enforcement agencies (LEA) are hesitant to leverage cloud data for investigations due to privacy and security concerns
- LEA do not want to move data from cloud to premises due to high cost and data quality impacts

SOLUTION

- Deploy privacy-protected queries and models to **without exposing investigation targets or moving data**

RESULTS

- Enhanced **data quality**
- Significantly **reduced cost**
- Ability to maintain **operational security**
- Maximizing operational value by doing **entity resolution**


Query created and encrypted
Encrypted query sent to Data
Investigator
Inquirer
Encrypted query runs on database
Data
Data owner
Encrypted results sent back to Investigator
Results decrypted

Secure AI in Healthcare

Dana-Farber Cancer Institute

BACKGROUND

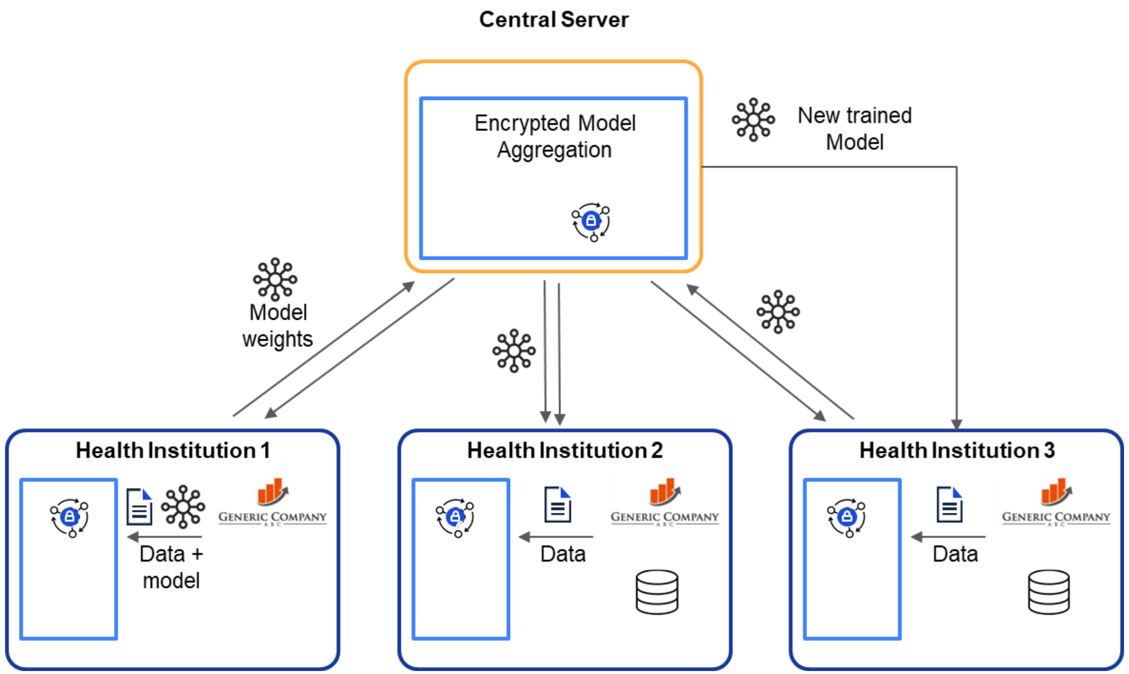
- Dana Farber Cancer Institute seeks to tune and optimize cancer classification model
- Required data from other health centers to enhance outcomes
- Today’s processes are manual, lengthy, and burdensome

SOLUTION

- Engage in federated learning and analytics **without moving data or exposing model weights**

RESULTS

- Enhanced **model to drive patient outcomes**
- Significantly **reduced cost**
- Time savings of **over 90%**



Duality

Secure AI in Cybersecurity

BACKGROUND

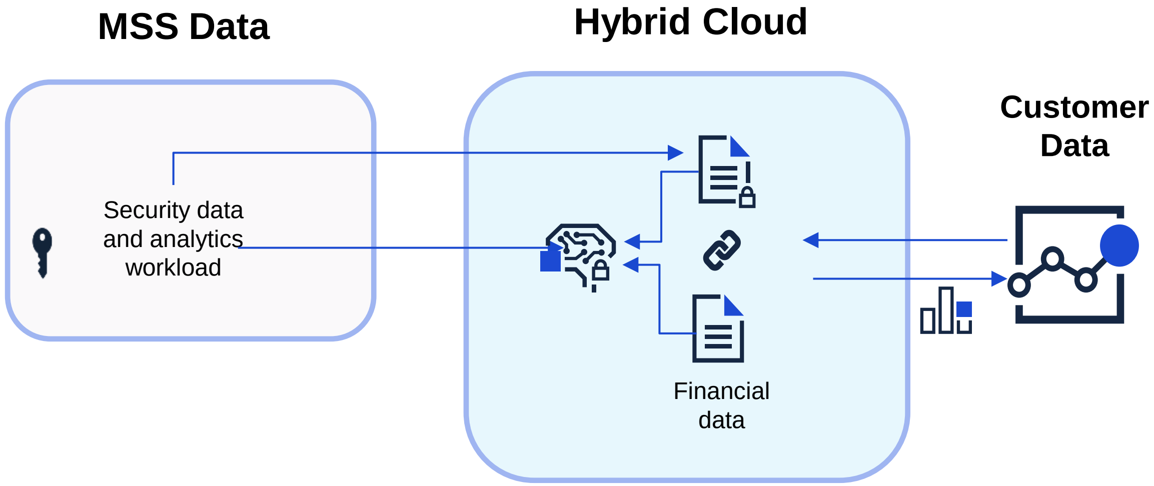
- Customer would like join its data with MSSP client security data for training models

CHALLENGE

- Customer wants way to optimize modeling **by using sensitive data assets that cannot currently be shared**

RESULTS

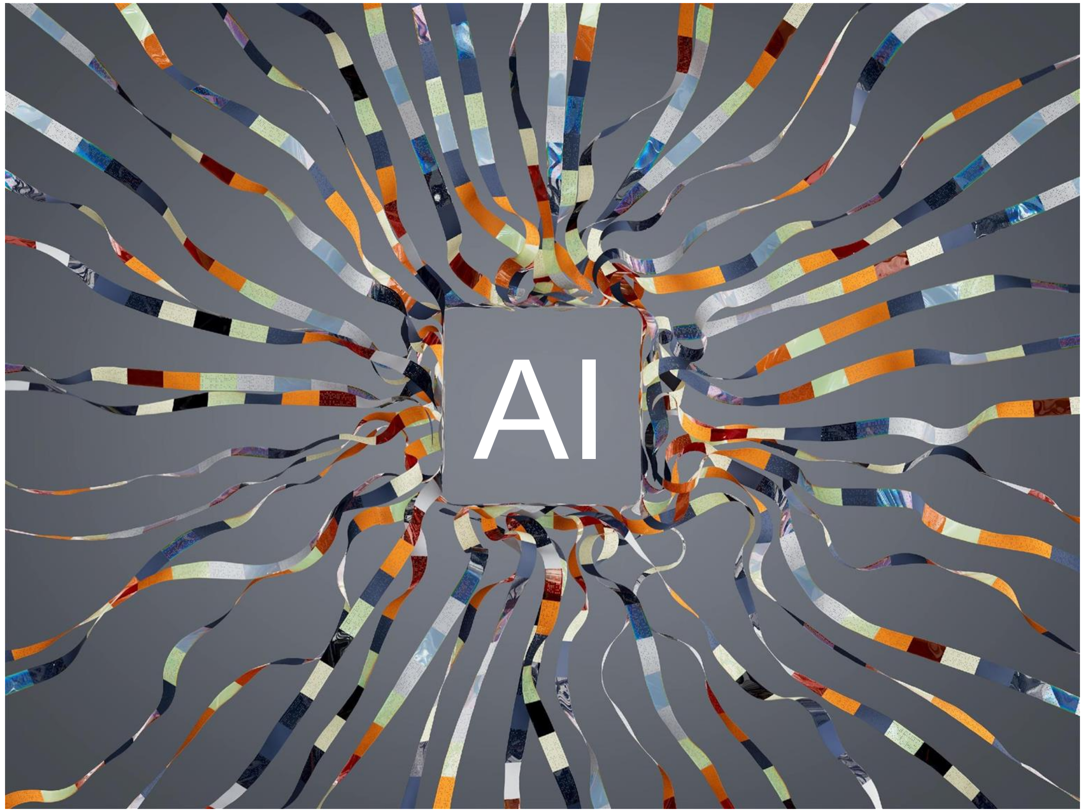
- **Enhanced data and models** by leveraging external sensitive data
- MSSP **links its data** with its Customer’s data **while preserving privacy**
- Customer can **train, tune, and deploy models on linked data while encrypted**



© 2024 Duality, All Rights Reserved | Proprietary

The (near) future: Utilizing Generative AI in Government

- PETs allay concerns of government users around data and prompt sensitivity
- PETs can be used to protect prompts and tune specialized models on sensitive data
- Data and prompts do not need to be revealed to third parties, including LLM providers



Q&A

Interested to learn more?