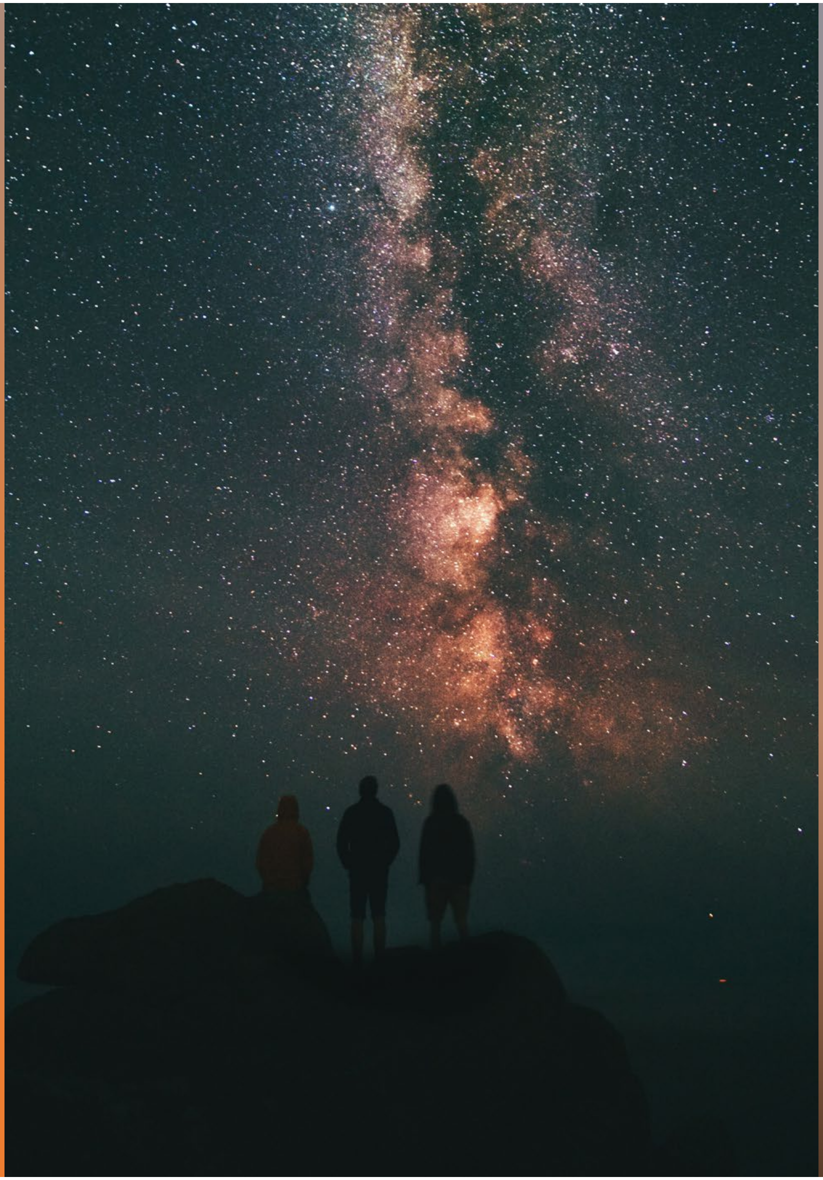
Booz | Allen | Hamilton



Exploiting Data at Mission Speed through Artificial Intelligence

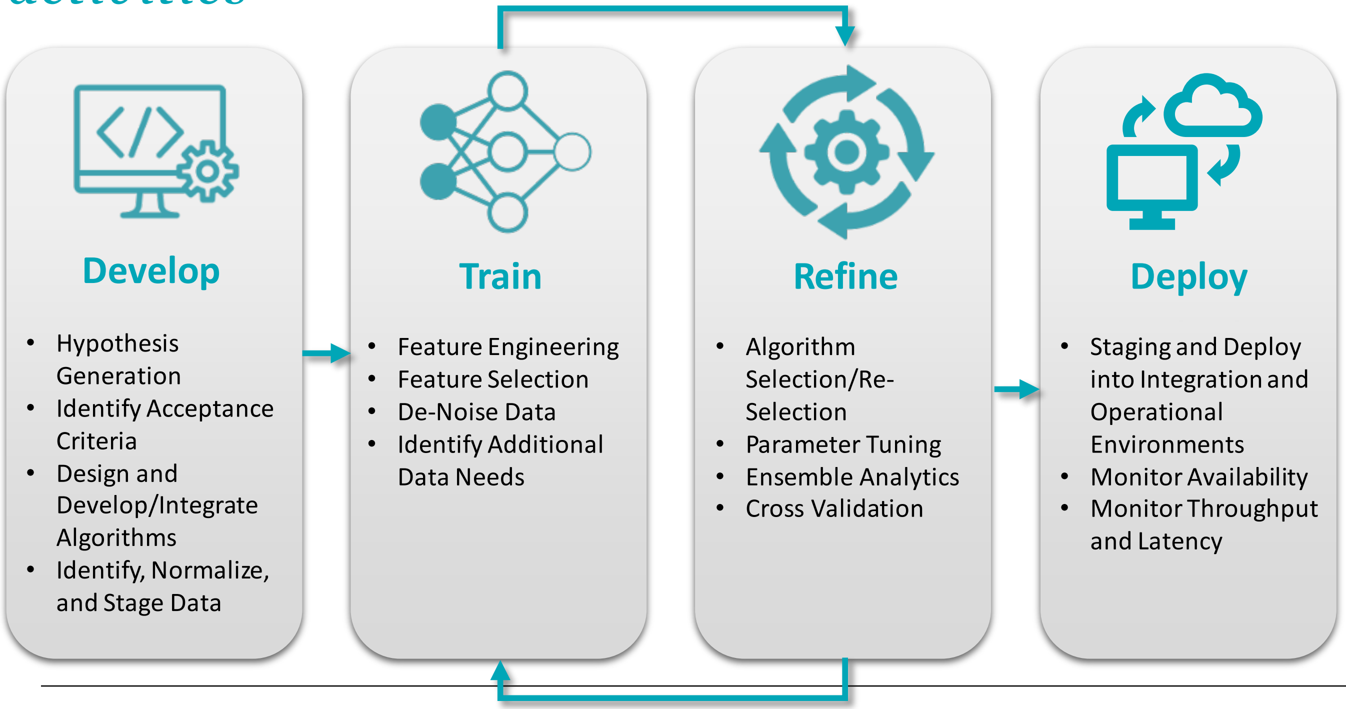
Virginia Cevasco

GSAW 2020

FEB 2020

ARTIFICIAL INTELLIGENCE (AI) IS THE ABILITY OF MACHINES TO PERFORM TASKS THAT WOULD NORMALLY REQUIRE HUMAN INTELLIGENCE

AI relies on large volumes of historical data and sophisticated mathematics to identify patterns and generate insights. AI can perform manual, time-consuming tasks at high capacity, giving humans more time to focus on value-adding activities



Develop

- Hypothesis Generation
- Identify Acceptance Criteria
- Design and Develop/Integrate Algorithms
- Identify, Normalize, and Stage Data

Train

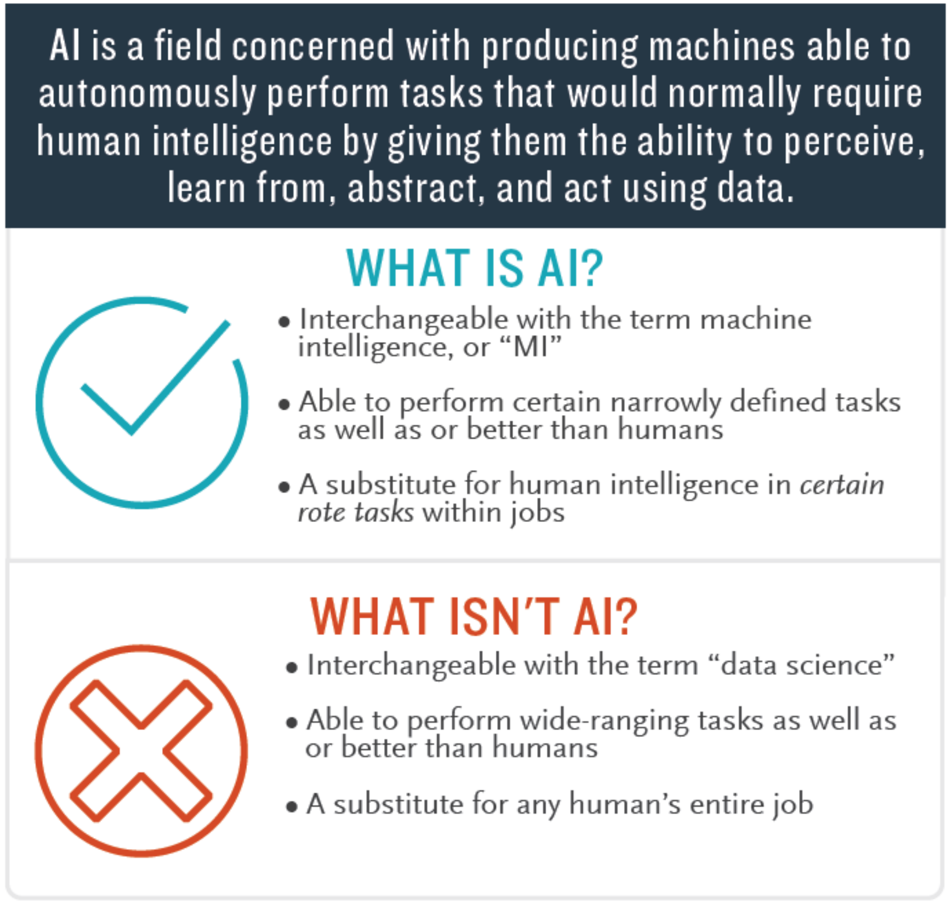
- Feature Engineering
- Feature Selection
- De-Noise Data
- Identify Additional Data Needs

Refine

- Algorithm Selection/Re-Selection
- Parameter Tuning
- Ensemble Analytics
- Cross Validation

Deploy

- Staging and Deploy into Integration and Operational Environments
- Monitor Availability
- Monitor Throughput and Latency



AI is a field concerned with producing machines able to autonomously perform tasks that would normally require human intelligence by giving them the ability to perceive, learn from, abstract, and act using data.

WHAT IS AI?

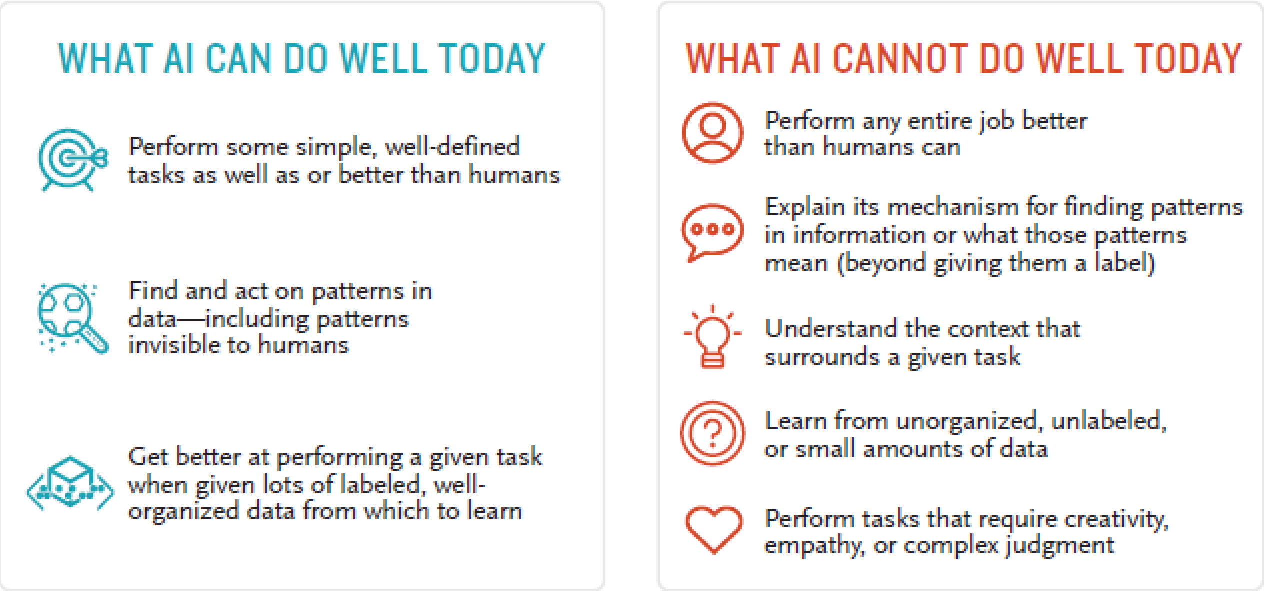
- Interchangeable with the term machine intelligence, or "MI"
- Able to perform certain narrowly defined tasks as well as or better than humans
- A substitute for human intelligence in *certain rote tasks* within jobs

WHAT ISN'T AI?

- Interchangeable with the term "data science"
- Able to perform wide-ranging tasks as well as or better than humans
- A substitute for any human's entire job

AI IN EXECUTION IS AN ELUSIVE GOAL

- Only an estimated 13% of AI projects make it to production [1]
- Ground system developers struggle to move AI from lab to production on the scale necessary to exploit the wealth of new data
- AI deployments often rely on custom-built models that integrate with legacy processes and tools, severely limiting the flow of decisions and actions between collection systems and agencies.



WHAT AI CAN DO WELL TODAY

- Perform some simple, well-defined tasks as well as or better than humans
- Find and act on patterns in data—including patterns invisible to humans
- Get better at performing a given task when given lots of labeled, well-organized data from which to learn

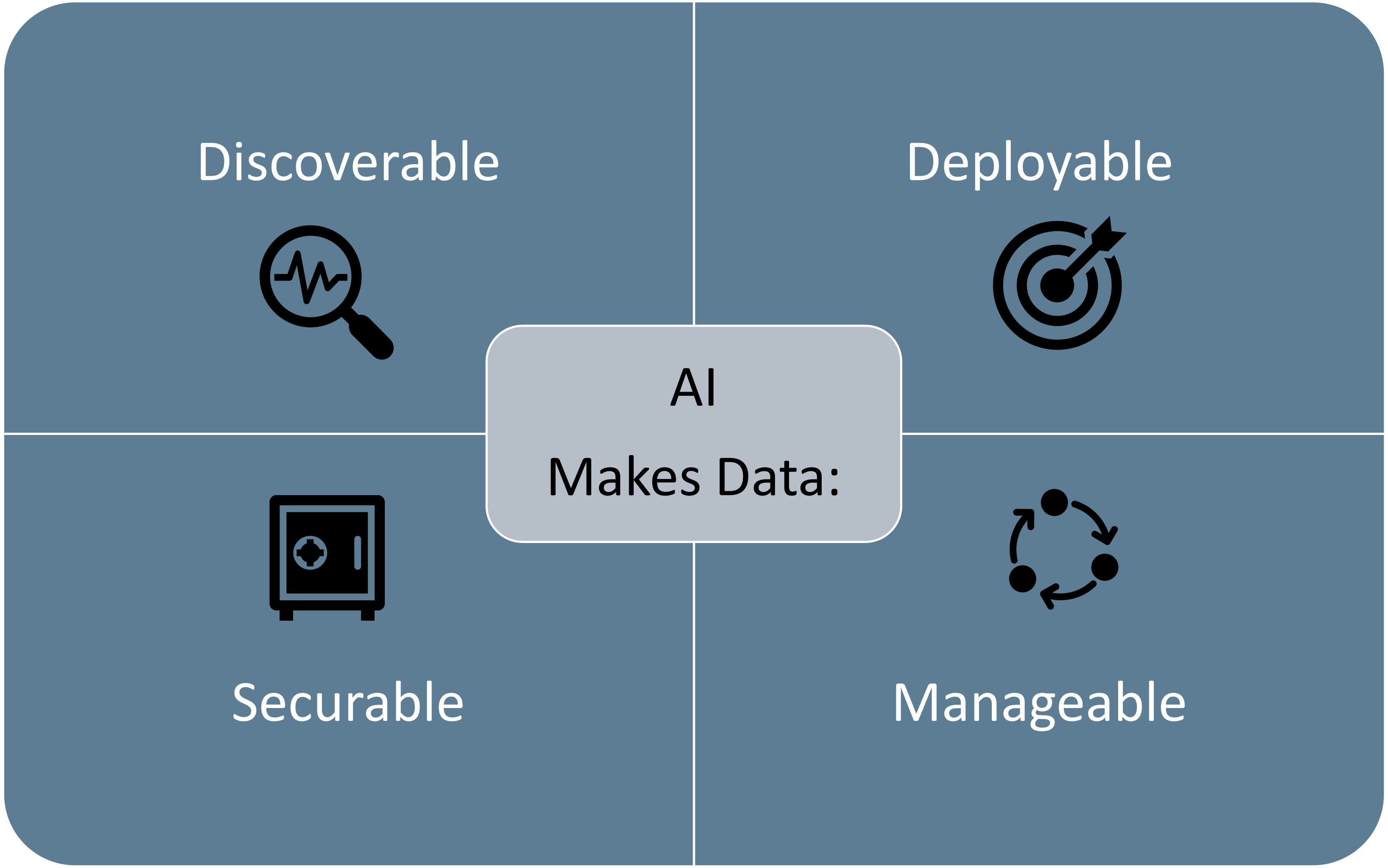
WHAT AI CANNOT DO WELL TODAY

- Perform any entire job better than humans can
- Explain its mechanism for finding patterns in information or what those patterns mean (beyond giving them a label)
- Understand the context that surrounds a given task
- Learn from unorganized, unlabeled, or small amounts of data
- Perform tasks that require creativity, empathy, or complex judgment

- Lack of definitions to discover, deploy, manage, and secure AI models introduces inertia and distrust
- Consistent, open standards and plug and play interoperability introduces velocity, choice, and innovation to meet critical mission needs

[1] https://venturebeat.com/2019/07/19/why-do-87-of-data-science-projects-never-make-it-into-production/

AI HOLDS TREMENDOUS PROMISE TO MAXIMIZE THE VALUE OF CURRENT COLLECTIONS.



AI

Makes Data:

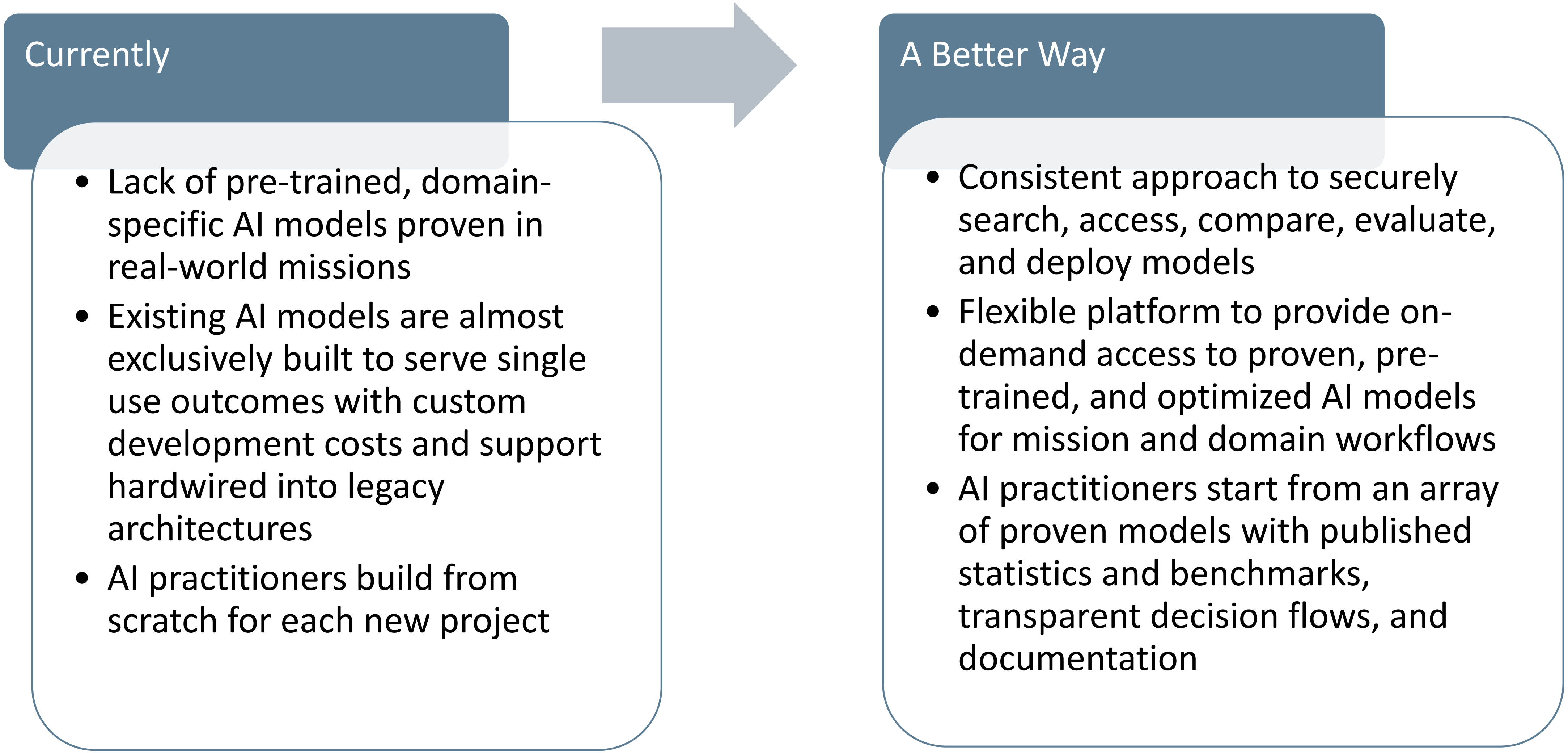
Discoverable

Deployable

Securable

Manageable

AI MAKES DATA **DISCOVERABLE**



Currently

- Lack of pre-trained, domain-specific AI models proven in real-world missions
- Existing AI models are almost exclusively built to serve single use outcomes with custom development costs and support hardwired into legacy architectures
- AI practitioners build from scratch for each new project

A Better Way

- Consistent approach to securely search, access, compare, evaluate, and deploy models
- Flexible platform to provide on-demand access to proven, pre-trained, and optimized AI models for mission and domain workflows
- AI practitioners start from an array of proven models with published statistics and benchmarks, transparent decision flows, and documentation

AI MAKES DATA **DEPLOYABLE**

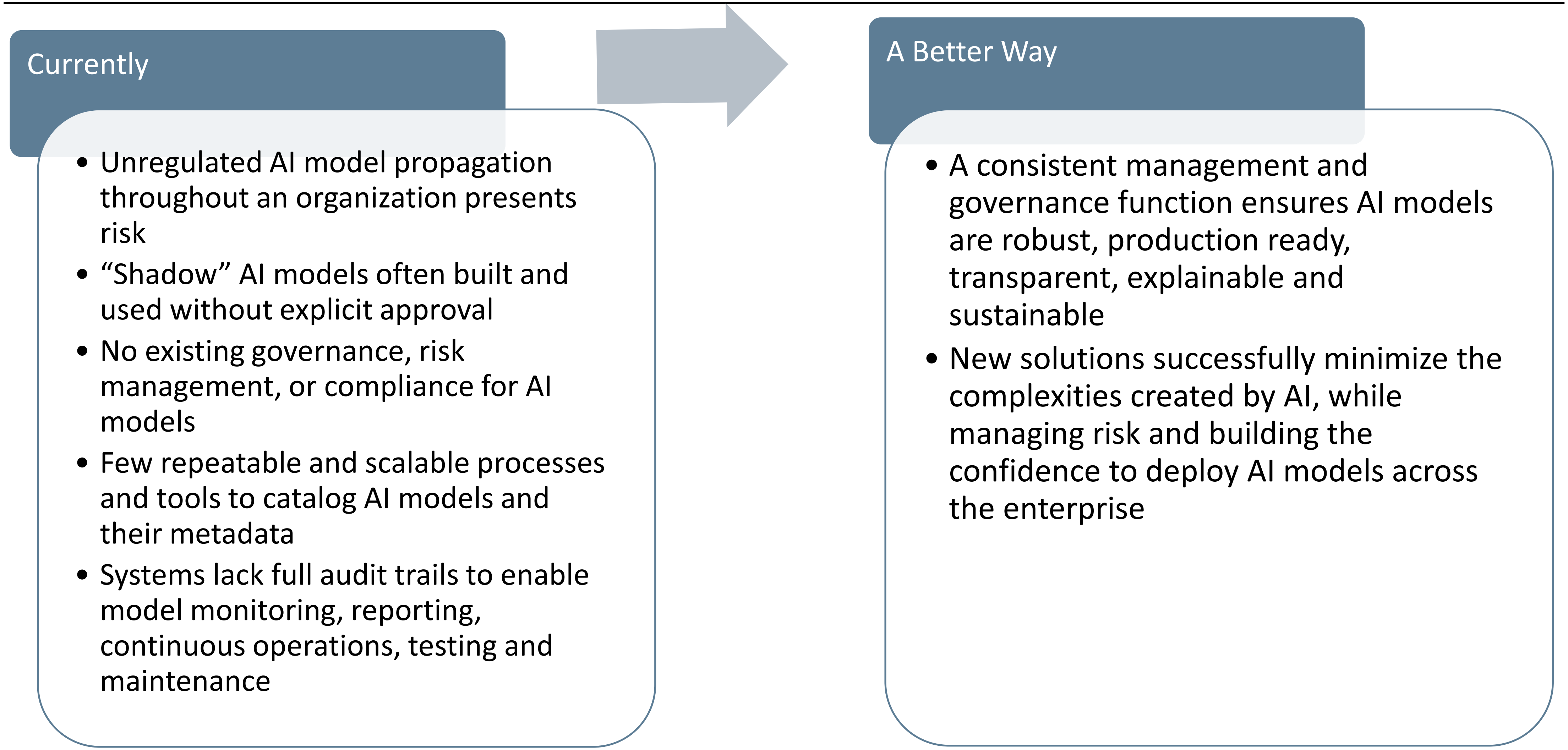
Currently

- Each AI project is deployed differently – usually the result of a pragmatic approach to insert AI into legacy IT infrastructure and existing data paradigms
- Inability to rapidly deploy, manage, and update AI models makes extending AI capabilities to new mission scenarios and adjacent efforts difficult or impossible
- Introducing a new user interface into a complex workflow requires a significant value proposition to even begin to gain analyst attention or start the change management process

A Better Way

- Portability across domain-specific scenarios, deployment environments, and legacy environments through an abstraction layer makes AI models and new technologies available without compromising context or security
- Harnessing lessons learned from AI across multiple highly-regulated domains identifies new ways to abstract complexity and enable consistent, predictable, and secure deployment and integration of AI models into existing mission workflow and tool environments

AI MAKES DATA **MANAGEABLE**



Currently

- Unregulated AI model propagation throughout an organization presents risk
- “Shadow” AI models often built and used without explicit approval
- No existing governance, risk management, or compliance for AI models
- Few repeatable and scalable processes and tools to catalog AI models and their metadata
- Systems lack full audit trails to enable model monitoring, reporting, continuous operations, testing and maintenance

A Better Way

- A consistent management and governance function ensures AI models are robust, production ready, transparent, explainable and sustainable
- New solutions successfully minimize the complexities created by AI, while managing risk and building the confidence to deploy AI models across the enterprise

AI MAKES DATA **SECURABLE**

Currently

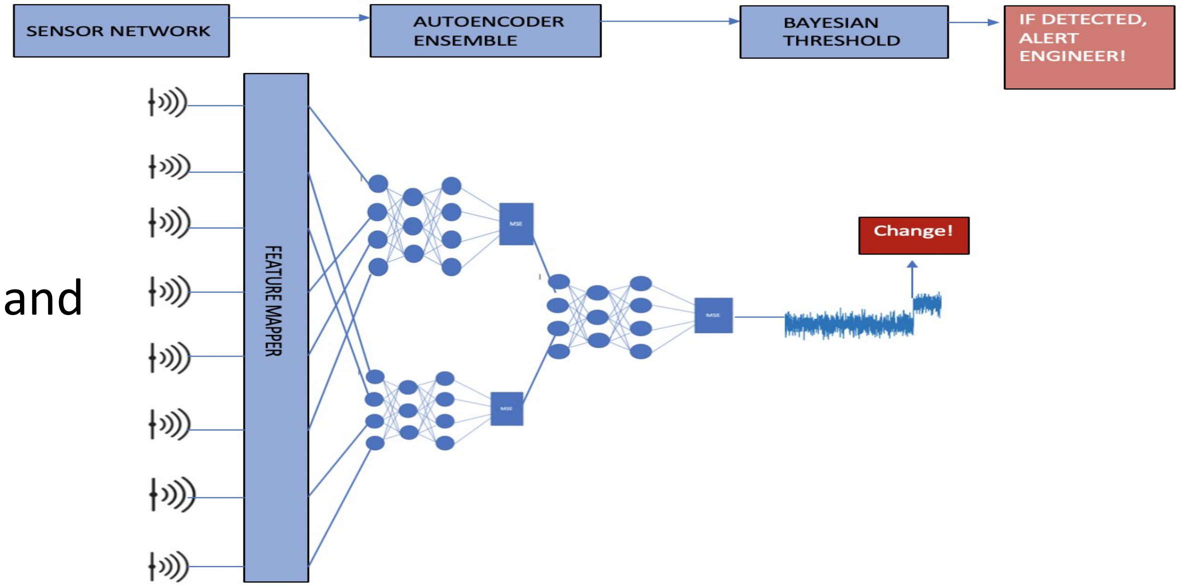
- Trust for AI model decisions depends on more than the algorithm logic. Bad or poisoned data streams, introduced either by accident or intentionally, can result in wrong, even disastrous outcomes
- Research focuses on ethical concerns of AI and potential bias that can exist in how AI models make decisions
- Without proactive defense against adversarial threats in both physical and digital spaces, AI models are vulnerable to physical tampering, hot-flips, poisoning, and model stealing

A Better Way

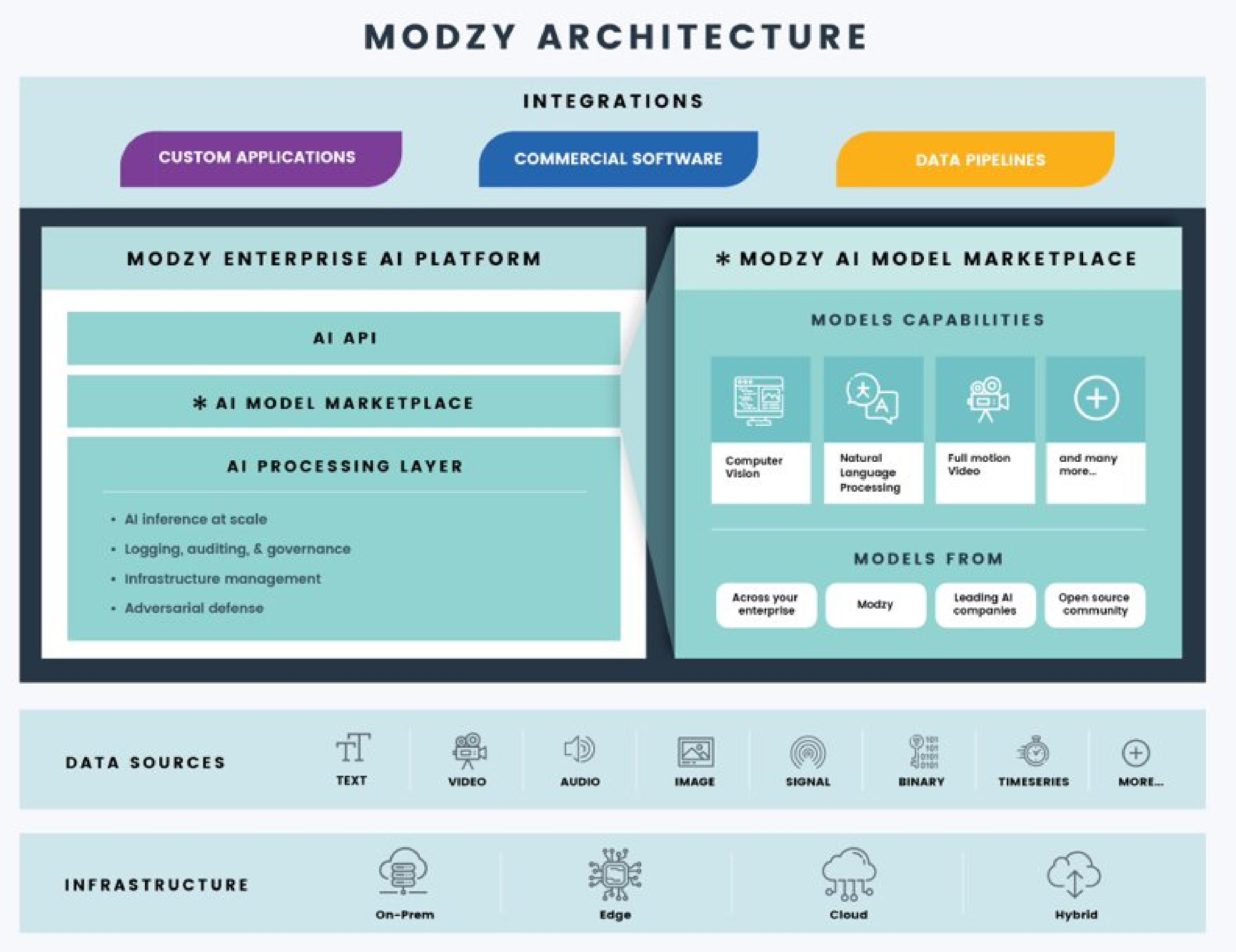
- Recognize and address the advanced persistent threat against AI models that has the potential to wreak havoc and create distrust in AI outcomes
- Apply active and passive adversarial AI capabilities across physical and digital domains, to provide consistent levels of trust and demonstrably reduce the risk to AI

EXAMPLE AI USE CASE – OUTLIER DETECTION

- Streaming outlier detection identifies and alerts on changes to dataset flow in near real time
- Can be applied to many data types:
  - System health and security
  - Fraud Detection
  - Health indicators
  - Resource consumption
- Traditional methods of outlier detection are slow and require many examples to train the model and expertise to define system parameters
- Our innovation uses a Streaming Ensemble of Autoencoders (SEA) in a plug and play, adaptive model
  - Autoencoder: feed forward neural network where input size and output size are the same
  - Architected to perform 5X faster with no data storage and no parameter setting
  - Runs on small devices with minimal computing power.
  - Multivariate, can monitor any number of sensors or input



MODZY: A SECURE SCALABLE PLATFORM FOR AI



- Rapidly deploy AI at scale with embedded governance, Adversarial Defense, and in-depth security
- Pre-trained AI models from leading machine learning companies
- Quickly and easily access, evaluate, deploy, embed and manage the best AI models at scale, and upload new models for management and governance
- Optimized for traditional and accelerated computing such as NVIDIA’s GPU technology, with an open architecture solution available on-premise, in the cloud, or via custom deployments
- Offers API access, built-in governance, adversarial defense, and explainability to solve some of the toughest challenges related to scaling trustworthy AI to the enterprise

CONTACT US

Virginia Cevasco

Director
cevasco_virginia@bah.com
703-633-3917

Jessica O'Rourke

Sr. Lead Technologist
o'rourke_jessica@bah.com
703-633-xxxx

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds; those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no road maps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.

Booz Allen Artificial Intelligence (ai.bah.com)

- 4,000+ analytics practitioners
- 60+ active AI projects
- 400+ cloud migrations
- Partnerships and strategic alliances with other AI leaders like NVIDIA, Hypergiant, UiPath, Amazon, and more
- Decades of experience supporting the Advanced Research Project Agencies, including DARPA, IARPA, and ARPA-E— and currently working with them on 35+ AI programs
- Won the 2019 INFORMS Prize in Operations Research