DELL TECHNOLOGIES

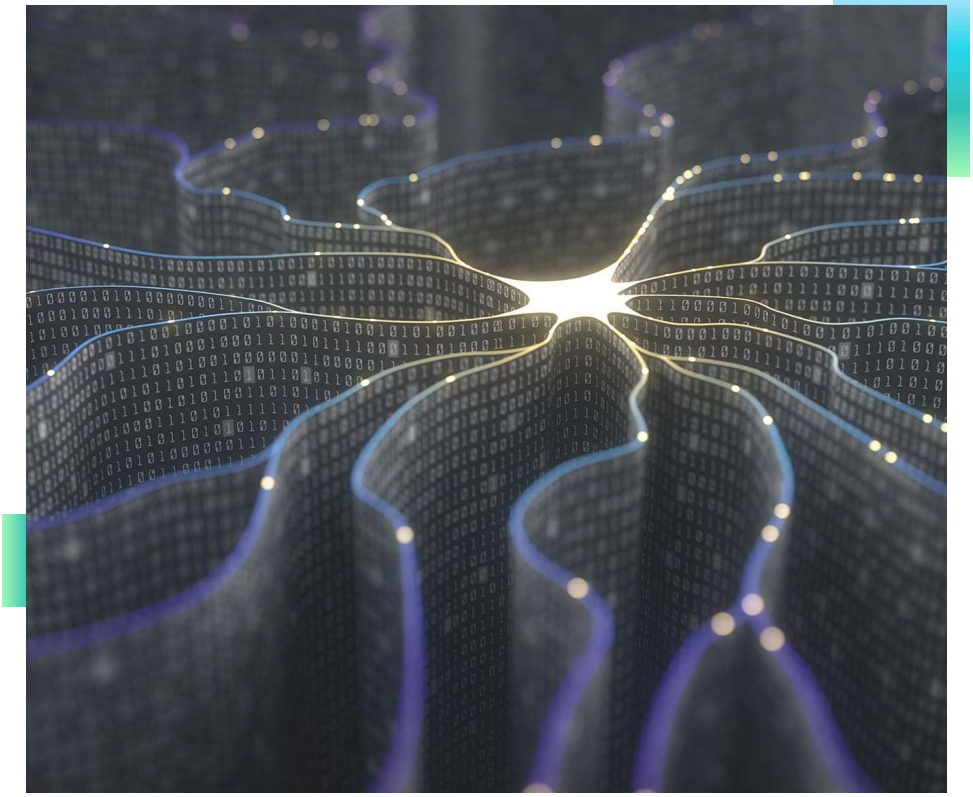
Unlocking the value of artificial intelligence

AI is transforming government operations, and new developments promise to bring even greater improvements

Lev Katz
Dell Technologies

The way people work with artificial intelligence has been following an evolutionary process. We began with machine learning, followed by large language models and the recent meteoric rise of approaches such as generative AI and retrieval augmented generation. Now we're seeing the emergence of small language models and agentic AI workflows that focus on specific areas.

Rather than replacing the previous phase, each development builds on the prior phase, and they all work together.



However, there's no inherent value in AI itself. The value lies in what insights AI can unlock and what people can do with those insights.

AI-assisted knowledge can lead to faster and better decision-making, which has profound implications for areas as varied as citizen services, military operations and cybersecurity. Imagine a tool that could suggest a course of action or a solution to a complex problem in a way that complies with government regulations and policies. AI can do that.

Conversing with generative AI

The government has such an incredibly large amount of data that people can never review it all. By using AI to analyze that data, agencies can see what has occurred and predict what might occur to make more informed decisions. Much of AI's strength is rooted in its ability to combine a wide range of information sources—including text, images, video and audio—into a robust framework for human-machine interactions.

Among other opportunities, AI has important applications for border control. When people come into the U.S., they could interact with an AI bot that asks the appropriate questions and understands the answers so it can gather all the necessary information about that citizen or non-citizen and alert law enforcement if necessary.

Imagine if new government employees could talk to a computer just as they would converse with a human. Instead of reading through a manual that may not be user-friendly, an employee could have a conversation with generative AI and ask, "How do I perform this task?" and receive an easily understood answer.

Protecting the data that fuels AI insights

As AI continues to evolve, it brings new capabilities and new security challenges. Addressing those challenges requires adhering to zero trust principles and layering security throughout the IT environment. A zero trust framework gives agencies the ability to restrict users' access to only the data and workflows they need to do their jobs. In addition, when AI is being used to analyze data, that data should be encrypted at rest and in transit.

Data is gold, and the data that is used to train and tune AI models is very important to its owners, who want to keep close tabs on it. Unfortunately, many public cloud environments are not ideally suited to ensuring the protection of the large datasets that are needed to train AI models. As a result, we have seen a massive increase in on-premises cloud hosting. Some agencies are choosing to create their own data centers that no one else has access to so they can maintain a high level of security, whether they run the centers on their own or contract with a knowledgeable vendor.

Such developments are a natural adaptation to a technology that touches on nearly every aspect of government operations. Given AI's massive potential, it's no surprise that it is transforming agencies' ability to reap the benefits of IT modernization. ■

Lev Katz *is vice president of the Infrastructure Solutions Group at Dell Technologies.*

"AI-ASSISTED KNOWLEDGE CAN LEAD TO FASTER AND BETTER DECISION-MAKING, WHICH HAS PROFOUND IMPLICATIONS FOR AREAS AS VARIED AS CITIZEN SERVICES, MILITARY OPERATIONS AND CYBERSECURITY."