Is AI the silver bullet government has been waiting for to implement zero trust?

Trust nothing and no one; continually verify the identity of every person, device, or system requesting access to a network resource; and ensure they're given least privileged access to it.

That's the concept of zero-trust security. The idea has been around for more than two decades, but there has always been a seemingly endless set of hurdles hindering its adoption. This is especially true for government agencies where technology and infrastructure complexity is more the rule than the exception, and factors such as compliance and the consequences of a cybersecurity failure are unlike any seen in the private sector.

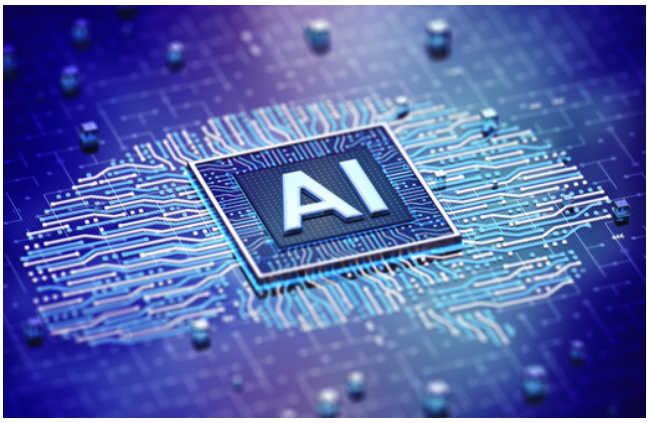
The recent bloom of artificial intelligence (AI) dangles before us the enticing promise that finally the technical hurdles may be behind us. Is AI the solution we've all been waiting for that can finally break through the barriers to zero-trust adoption?

While the simple answer may be "yes," the more complete answer isn't that simple. AI has already become an indispensable cybersecurity tool, and it's rare to find a security operations center (SOC) that isn't relying on it for faster and more robust threat detection and remediation.

However, zero trust isn't a technology problem and so it can't be solved by technology alone. Beyond the tools and engineering, there are many human-related elements needed for successful adoption of AI models in support of zero trust and broader cybersecurity fundamentals. It requires significant organizational change management, for example, as it substantially changes the way humans conduct their day-to-day duties and how agencies conduct their business. And that's just the start.

Why modern government is important

Government agencies in the U.S. must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.



Zero trust: A double-edged sword

It is true that AI can evaluate far more variables and apply more detailed rules and policies than any non-AI-based system could ever hope to. Its ability to adapt automatically to dynamic environments and unanticipated circumstances is unparalleled. Without AI, it would be impossible to make the millions of instant decisions that must be made every second for a zero-trust environment to function as envisioned.

However, government agency program executives and operators need to fully understand and appreciate that any use of AI comes with as many risks as benefits. Trusted AI capabilities have become essential to help guard against risks such as decision bias or privacy or compliance violations. Blackbox risks—a lack of transparency into the AI model or its training data—may be among the most concerning for government officials looking to apply AI to zero trust. It can be difficult to know if a system or software application even uses AI, let alone the rules it uses to make decisions. Can you delegate critical security decisions to an algorithm when you may not fully understand how it makes those decisions?

Of course, AI has also been weaponized by adversaries and attackers. It can be used to breach security through impersonation or by more sophisticated discovery and exploitation of system weaknesses. The current wave of generative AI adoption may offer some insight. In a June 2023 survey of 652 senior cybersecurity professionals, 45 percent of Chief Information Security Officers (CISOs) said they believe generative AI will make their organization more vulnerable to attack; 75 percent reported an increase in attacks over the past 12 months; 85 percent attributed this rise to bad actors using generative AI.[1]

It's true that AI can be a double-edged sword. But the same can be said for almost any technology. Simply networking a computer introduces a host of risks. Even encryption—arguably one of the most valuable tools in an organization's cybersecurity toolkit—can be used for ransomware attacks or for masking what data is being removed from a network. So, while its risks must be accounted for, AI is still more friend than foe, and it's certainly not something that can be ignored.

[1] Louis Columbus, "How generative AI will enhance cybersecurity in a zero-trust world," VentureBeat, November 27, 2023.

Distracted by the shiny new toy

Amid the excitement about AI's potential, it can be easy to lose sight of what really matters in a zero-trust effort. AI appears to be the silver bullet we've all been waiting for, and therefore has tempted many to focus on the technical mechanics of implementing zero trust.

We can't emphasize enough that zero trust isn't a technology. Some define it as a security model or architecture. We call it a business philosophy and an organizational transformation. You can implement all the available tools and technologies with an ideal architecture and still not get it right.

In our experience, it's rarely the technology that's the complicated part, even in government environments, with their tangled web of aging legacy systems, cloud-based solutions and cybersecurity and compliance challenges. It's almost always the organization that's the real challenge—the "business" side.

The complexity of roles and the access policies tied to those roles can vary widely across agencies. Business processes and the flow of information required to support them can differ significantly agency to agency. The location of people and the resources they need access to matters. Terminology can vary widely. Something as simple sounding as having a common vocabulary can be the difference between project success and failure. Does everyone agree on what is meant by an "application"? Is agency leadership in agreement that users can be denied access to mission resources even in stressful operating environments if something doesn't seem right from a cybersecurity perspective?

Asset value can be trivial at one end of the spectrum and vital to the security of the nation at the other. Access has a similar spectrum; in the event of permissions mismatch, what might be a frustrating inconvenience for one employee could be a catastrophic event for another.

As they say, "change is hard." Organizational change means cultural change, too, and that means people and emotions. Ultimately, the success of any zero-trust initiative depends on employees choosing to embrace it. They can either be a tremendous asset eager to share their input and experience to help the change succeed, or an obstacle whose resistance can dwarf any technology hurdle.

None of these are pure technology issues, and nothing that AI in any form (at least yet) can help address. Armed with even the best AI solution, no technology provider or system integrator, therefore, can hope to help you successfully implement zero trust without a complete and detailed understanding of your agency's business and mission and the ability to foster consensus for change. It's a prerequisite for providing a roadmap and recommendations for how AI and zero trust can benefit your organization and advance that mission—instead of becoming a hindrance to it or something that creates unexpected and unwelcome surprises.

Change is in the air

Even without zero trust, security organizations within government must transform. With quantum computing threating to undermine existing encryption solutions and with AI being weaponized by adversaries, the world of cybersecurity is significantly different today than it was a year ago and promises to be different yet again a year from now. Reexamining existing security processes and technologies and developing the agility to respond to emerging challenges are organizational necessities, and a sound reason beyond advances in AI alone to begin implementing a zero-trust approach—and any other solutions that advance your organization's mission.

How KPMG can help

KPMG has worked with federal, state, and local governments for more than a century, so we know how agencies work. Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer zero-trust methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter. In addition, KPMG has significant experience implementing zero trust in both the private and public sectors and can bring those experiences to every government client.

Contacts

Tony Hubbard
Principal, Government Cyber Security Leader
KPMG LLP
202-486-4945
thubbard@kpmg.com

Tyler A. Carlin
Director, Advisory
KPMG LLP
571-243-5655
tcarlin@kpmg.com

read.kpmg.us/modgov

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia