What's the best way to zero trust?

Forget about zero trust

By now, you're undoubtedly well aware of zero trust security. Its praises have been sung for more than 20 years. Your inbox is likely full of emails explaining its importance and there's no shortage of guidance to help government agencies navigate the path to this holy grail. Yet across government, progress on zero trust has varied.

The concept is simple enough: continually verify the identity of a person, device, or system requesting access to a network resource, and then ensure they're given least privileged access to that resource. The concept, however, is where the simplicity ends.

The typical government IT infrastructure is a tangled web of aging legacy systems, cloud-based solutions, mobile apps, and so on, and that complexity plays a key role in the challenge. But it's only one of many. Most government IT or data security professionals face a wall of impediments, and yet another article extolling the benefits of zero trust or touting a new zero trust solution isn't likely to make a dent in that wall. For many, zero trust may seem more of a pipe dream than a realistic target.

As counterintuitive as it may sound, perhaps a better way to start on zero trust is to forget about it, at least for the time being. Given the realities that government organizations face, there are many things you can do now to lay the groundwork for zero trust that can help turn that pipe dream into an attainable goal.

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.

Develop a realistic roadmap—and realistic expectations

In an ideal world, zero trust would take two-to-three years to implement. In the real world, however, it may be more like a three-to-five-year journey at best—especially for large federal agencies. In that time, budgets can fluctuate. Leadership can change. Legislative mandates can appear. New security threats can emerge. Therefore, your priorities almost surely will reshuffle; something new is always being pushed to the top of the list. This is perhaps the biggest impediment to zero trust that agencies face, a complexity those in the private sector rarely will experience.

Another issue is that zero trust isn't really a project; it's an enterprise transformation. As with any transformation, there's no real beginning, middle or end. How do you sell that to the executives, directors or legislators who control your budget?

It starts with a three-to-five-year roadmap with specific and realistically achievable milestones that account for the dynamism of your priorities and budgets. Many of these milestones won't be specific to zero trust but they will be things that can make implementing zero trust easier, such as reducing tech debt and modernizing legacy systems or building in network segmentation. The roadmap should also specify milestones where long-term savings can be expected to appear that make the effort economically appealing (and not just appealing from a security perspective).

Measure, measure, measure

Any zero-trust implementation will open up a firehose of data—it's that information, after all, that is used to determine if access should be granted or denied, and to help refine access policies going forward. Putting all that data together will allow you to know early when something is just not right. Without careful data collection and analysis, data breaches could go undetected for long stretches.

It's more than detecting vulnerabilities, however. Zero trust is not a product or service that can be purchased. Simply completing a list of procurements and their scheduled installations is not enough to say the work is done and that zero trust has been achieved. Achieving a transformation program at the scale of the enterprise typically requires an implementation plan with specific outcomes and an associated scorecard in order to track and reinforce the goals, measure progress against plan, and report progress. The scorecard needs to identify metrics that contribute to zero-trust outcomes. To the extent possible, automating the collection of data in advance to support this scorecard is an important step.

Consider the human element

Beyond the typical resistance that can accompany any proposed change to the way people work, there can be especially pointed opposition to role-based access control (RBAC). Rather than simplifying access, it seemingly creates a new layer of technical "bureaucracy" between employees and the tools of their job. This can hinder their ability to complete their work when the privileges they've been granted don't align perfectly with their real-world responsibilities. Such misalignment can exist at all levels of government where it's not uncommon for an individual to wear multiple hats and even carry several government identity cards that cover their different roles and responsibilities.

Can RBAC handle such real-world complexity? Can it match the simplicity of the multiple identity card solution? The answer, of course, is "yes." It can offer an even simpler solution to it—provided it's designed from the outset to account for such complex roles and access policies. This is a critical step that can and must be completed before you begin any zero-trust implementation.

It's essential, therefore, to get all stakeholders engaged early in the process. The proper design of roles and privileges depends on their input—they are the sole keepers of the knowledge of what's required to make the system work. But overcoming the resistance goes beyond this largely technical task. It requires stakeholder buy-in to the underlying premise behind zero trust.

All must believe that this change is for the better and not something to be resisted, but this isn't necessarily an uphill battle. Ask any stakeholder this: "If you could do something that would make your life simpler and make our network more secure, wouldn't you do it?"

Add trust to zero trust

What about when stakeholders can't buy in—not "won't" but "can't"? While a mismatch between access and responsibility might be a frustrating inconvenience for the Internal Revenue Service, it could be a catastrophic event for an air wing. Balancing competing risks—preventing appropriate and essential access versus allowing inappropriate access—may lead some to conclude that zero trust is far too dangerous for them. Here, too, the right way to adopt zero trust may be to not adopt it—or perhaps more accurately, to put some trust into zero trust before you do.

Much of the risk comes from the increasing use of artificial intelligence (AI) to make access decisions. While we have remarkably advanced AI systems, none are yet infallible—think "driverless cars," for example. Yet those same AI systems are remarkably good at detecting anomalies or outliers. This is where human-in-the-loop comes in. If an "out-of-the-box" access request arises, a human's judgment can be injected into the process in the same way that a human can step on the brake when the driverless car fails to.

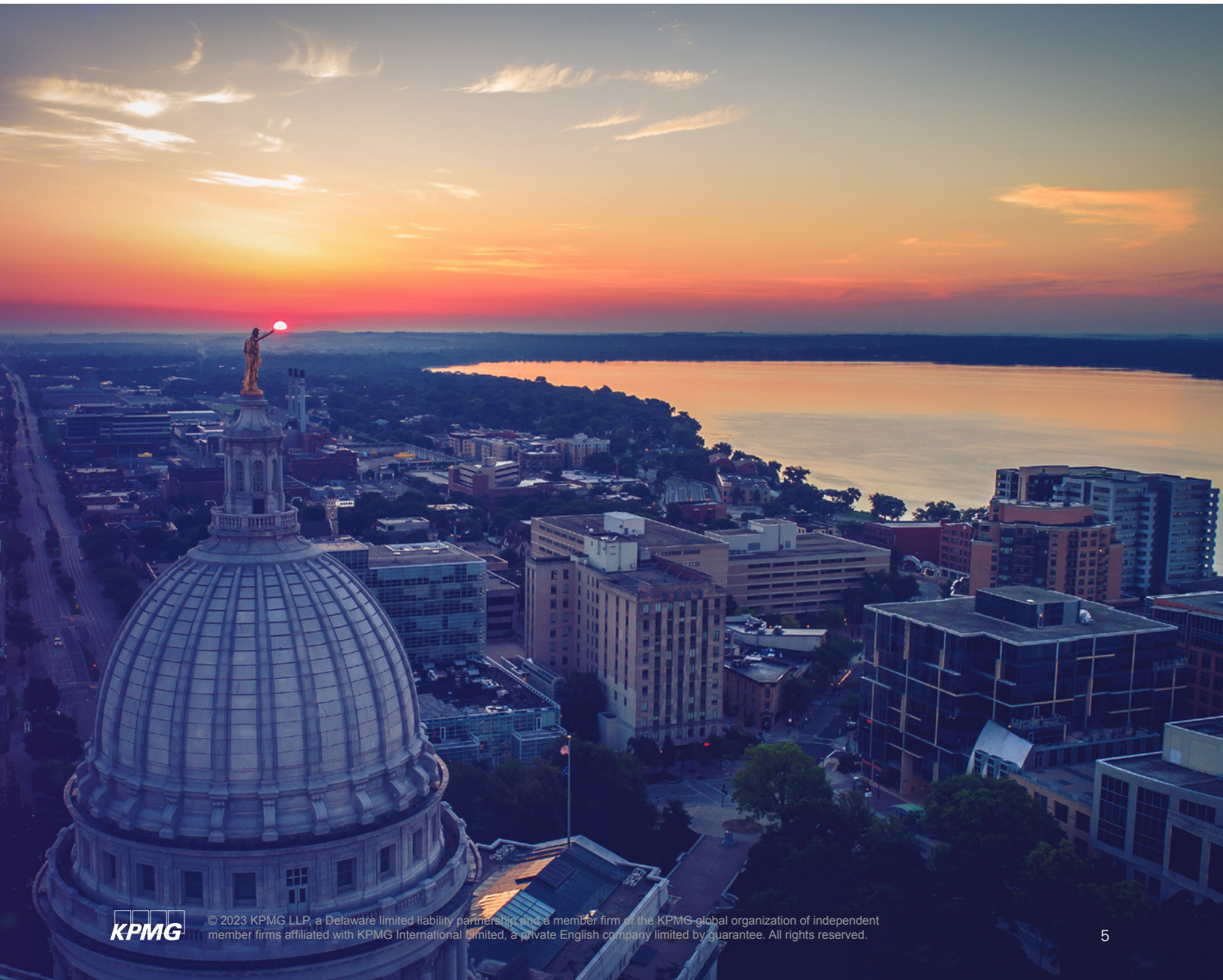
The "bias" of the system can be tuned to either end of the risk spectrum—being predisposed to allow access, for example, while involving a human in the decision to prevent it—based on the consequences of an incorrect AI-made decision.

While much of this involves a technology implementation, human-in-the-loop almost by definition requires an organizational shift. Preparing for these organizational and cultural changes is just as important as any software that might be required.

About KPMG

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 methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.



Contacts

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

Joseph Klimavicz
Managing Director, Federal CIO Advisory Leader
KPMG LLP
703-795-8999
jklimavicz@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