KPMG zero-trust security for government

Enabling the mission by transforming security through innovative IT solutions, robust change management, and a strategic shift in security principles and architecture

Zero trust (ZT) is more than a technology or compliance effort. It's an organizational transformation—a strategic cultural shift that enables government agencies to effectively and reliably achieve their missions in a world where technology has become both an indispensable asset and a significant vulnerability.

We help government organizations realize their ZT objectives with strategies, technologies, and organizational transformations that improve the effectiveness of cybersecurity capabilities, reduce control complexity, and lower the costs of regulatory compliance.

KPMG zero-trust offerings

Zero-trust integration office

A successful ZT implementation demands an effective vision and strategy. We can help by analyzing gaps between your current and desired states, synchronizing capability implementations, coordinating activities across ZT pillars, and establishing a strategic communications approach with stakeholders. We can also help you perform advanced data collection to increase efficiency, reduce stakeholder strain, and accelerate implementation timelines.

ZT assessment, gap analysis, and roadmap

ZT strategy and governance

ZT metrics and reporting

ZT organizational change management

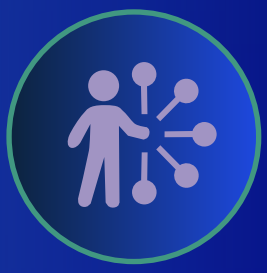
Application discovery

ICAM transformation

We take a holistic approach to identity, credential, and access management (ICAM). We can help you automate manual processes, reduce user friction with just-in-time provisioning, centralize access decisions and authorization matrices with streamlined roles and attribute-based authorization, and leverage platform reporting capabilities to strengthen segregation of duties and access request policies.

ICAM strategy and governance

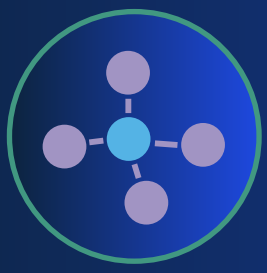
ICAM policies and procedures development



ICAM implementation and integration

Zero-trust networking and architecture

Fine-grained network segmentation is a key component of a ZT architecture. We can help you bring your network boundary protection to the application level to increase granularity of control, enhance network visibility, reduce the organizational attack surface, and improve control of network traffic to reduce adversarial lateral movement on the network.



Macrosegmentation, microsegmentation, and software-defined perimeters

ZT network access and secure access service edge capability implementation

Secure applications and APIs

Why KPMG

KPMG LLP (KPMG) has worked with federal, state, and local governments for more than a century.

We have over 1,500 dedicated cybersecurity professionals worldwide and alliances with leading ZT and cybersecurity technology providers. We have significant experience implementing ZT in both the public and private sectors, and have been recognized by Forrester, IDC, and ALM Intelligence as a leading global organization of professional services in cybersecurity[1, 2, 3].

We're a multidisciplinary organization with business, technology, data and AI, risk, audit, and change management professionals working together as a global organization. We bring our cybersecurity acumen, well-honed methodologies, government operations experience, and cross-sector and cross-disciplinary knowledge to every engagement to help you navigate the complexities, nuances, and transformative nature of a ZT journey—and deliver results that matter.

1. ALM Intelligence Pacesetter Research, April 2022.
2. Philip D. Harris, "IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment," October 2023.
3. "The Forrester Wave, Cyber Risk Quantification, Q3 2023," Forrester, 2023.

Contact us

Talk to our team about how we can help you adopt a successful zero-trust approach to security.

Tyler A. Carlin

Director, Advisory
KPMG LLP

240-306-5097

tcarlin@kpmg.com

Nate Deshong

Director, Advisory
KPMG LLP

843-327-6641

ndeshong@kpmg.com

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

Learn about us: **kpmg.com**