Governments: Cyber secure your boundaryless world

Zero-trust security framework verifies everything, trusts nothing

Lack of perimeter leaves cyber vulnerabilities

In 2020, there were more than 29,000 cybersecurity incidents across the globe, with at least 3,236 of those in public sector.[1] Industry experts estimate the U.S. government faced over $13.7 billion in costs as a result of cyberattacks.[2]

People and data are no longer within the walls of specific places leaving traditional data security methods ineffective. In environments with no perimeters, cybersecurity has to be more flexible and agile to protect data, networks, workloads, and user identities as users interact in cloud, mobile, on premise, and remote environments. This article introduces zero-trust as a powerful architecture to improve governments' cybersecurity. We present the zero-trust framework in ways that will be useful to technical leaders as well as program and financial managers.

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.

[1] "Global number of cyber security incidents in 2020, sorted by victim industry and organization size," Statista, 2021.

[2] "Average annual costs caused by global cybercrime in 2018, by industry sector," Statista, 2021.

It is not a product. Zero-trust is a framework or model to trust nothing and verify everything.

Rethink cybersecurity for digital, no-boundary environments

Governments accelerated their digital transformation efforts in 2020, which amplified the need to rethink cybersecurity. However, only 48 percent of government leaders surveyed well into the pandemic were using cybersecurity technologies and services to enable their organization's digital transformation.[3] As government organizations move more data and applications to the cloud and environments become more dynamic, they must rethink cybersecurity. Zero-trust is an approach to cybersecurity and risk management that government organizations can build to safeguard the environment no matter where data and people are located. It is not a product. Zero-trust is a framework or model to trust nothing and verify everything.

A **zero-trust framework shifts cybersecurity defense focus from network-based, static perimeters to protect users, assets, and resources**. It requires stringent security validation with no implicit trust based on users or locations. For example, if an employee loses their mobile device, zero-trust would provide the capability to know the person who picked up the device does not hold or type on it the way the owner does. When this happens, technology broadcasts the information to the security operations center where humans, with help from technology, assess the situation in real-time and terminate the session.

Adopting a zero-trust framework can achieve a number of valuable benefits that apply no matter where government workers, data, citizens, and other constituents are or what devices or networks they use. Benefits include improving threat detection, minimizing data loss, and lowering risk. Zero-trust also helps organizations enforce security policies and prepare for what might happen next. Most importantly, **zero-trust helps governments maintain public trust**.

Since cyber threats can originate anywhere, we cannot trust the user's **identity**, the **device**, the network, or the **data**. Under a zero-trust architecture, technology spots atypical activity and prevents communication with unauthorized apps, servers, locations, accounts, or human behaviors. These four main components make up a zero-trust framework:

— Strong **identity management** employs authentication and user rights to help ensure access only to authorized people. Zero-trust capabilities many government organizations already use are role-based access control, multi-factor authentication, and access where each user or device is granted the minimum system resources to perform its function.

— Zero-trust also depends on a mobile **device/workload** management strategy that includes application programming, interface security, and frequent security updates as well as an accurate, detailed workforce device inventory. The entire supply chain needs to be secured, including companies, products, and services.

— Zero-trust **protects networks** while devices are connected with a software-defined perimeter service. Microvirtualization provides application-level isolation from the operating system and microsegmentation divides the network and reduces the number of users per network segment. It also maintains cyber visibility into containers and encrypted traffic.

— **Data security** encompasses properly implementing a wide range of technologies and software, including data loss prevention tools and processes, file integrity monitoring, and encryption. Cloud access security broker software resides between users and cloud applications. It monitors activity and enforces security policies to protect data stored in the cloud.

A new executive order lays out its zero-trust framework and cybersecurity best practice steps federal agencies must take.[4] Many states are boosting their cybersecurity legislation and activities to lower their risk exposure after a multitude of threats across the industry. Looking at government organizations' cybersecurity from a zero-trust perspective may be the approach they need.

[3] "Impacts of COVID-19 on digital transformation strategies and the future of work," KPMG and Forrester, 2020.

[4] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021.

Zero-trust is a multi-step process you may have already started

Achieving zero-trust across the digital experience is an art and a science. Citizens need easy access to services. They are not technologists, so it is up to government organizations to assure data and each interaction across the digital experience is secure, which is the science. The art is in providing an experience that is easy and seamless.

Installing an app does not achieve zero-trust, no matter what some software vendors might claim. Designing a zero-trust framework is a multi-step, ongoing process that uses a number of components and, similar to puzzle pieces, each component must fit to create a cohesive cybersecurity environment. The good news is many organizations already have pieces of zero-trust already in place. Multi-factor authentication is a good example. The difference is each piece exists because the organization needs the function, but they are discrete. Now you want a **cohesive framework or architecture designed to trust nothing and verify everything. This is zero-trust**.

Planning for an incremental and in-sequence, step-by-step rollout heightens success and can help secure the needed funding. Organizations must **take all of the following actions to adopt zero-trust:**[5]

1. **Establish strong data governance.** Leading organizations understand cybersecurity risks, seek resources to address vulnerabilities, and make risk-based decisions regarding resource allocation. They adopt an enterprise approach that incorporates technology offices such as the chief information officer and also program and functional offices, including personnel and procurement. They prioritize information requiring highest protection levels such as citizens' personally identifiable information (PII) or sensitive agency mission data.

2. **Protect the most critical data.** Assign each data breach category a rating of high, medium, or low importance, with the overall data set receiving the highest rating in any category. The agency's cybersecurity team should use this classification to select the necessary cybersecurity controls. Collaboration is important to establish enterprise-wide cybersecurity priorities that balance risks, impacts, costs, and benefits. Leading organizations focus on mission-critical systems and information.[6]

   Each data category requires certain controls, augmented by targeted and compensating controls tailored to specific cybersecurity risks. For example, misuse of accounts with elevated access rights is one of today's biggest cybersecurity threats. While a common control is to limit access to sensitive PII data to certain personnel, categorizing data appropriately so it resides in specific systems within the organization strengthens control. A cost-effective approach is the principle of least privilege.[7]

3. **Deploy a multi-cloud strategy**. In a multi-cloud strategy, organizations use more than one cloud service provider to flexibly align services and capabilities to meet needs. As they move more data to the cloud and increase remote usage, relying on a single cloud service provider may not be enough to meet demands and provide adequate cybersecurity coverage.[8] In a 2020 survey of 900 technology executives, 51 percent of respondents said they were "prioritizing an all-public, multi-cloud structure."[9]

   Distributing workloads among different cloud service providers broadens an organization's security scope by increasing cloud availability to mission-critical applications. A multi-cloud strategy can reduce service disruptions and failures with readily available backup solutions. In addition, organizations can choose the optimal solution in a given situation and assess the cost/benefit among possible solutions and returns on investment based on pricing models.

   Organizations can increase agility and reduce costs by reusing existing infrastructure, especially with a cloud-native application. Cloud-native technologies provide the capability to build and run scalable applications in modern, dynamic environments, such as public, private, and hybrid clouds. Combined with advanced technology such as machine learning, they allow developers to create high-impact changes frequently and predictably with minimal effort, saving time and money.

4. **Assign cloud gatekeepers**. Organizations can use cloud access security brokers as cloud gatekeepers to oversee information and threat protection from malicious attackers, even beyond the government customer's network perimeter.[10] These cloud-based security solutions can help enforce cybersecurity policies and regulations and mitigate or eliminate risks of attackers targeting cloud blind spots. Agencies also increase assurance of data safety and better control activities throughout their network.

[5] Tony Hubbard, Joseph F. Klimavicz, Steve Wong, Jeffrey C. Steinhoff, "Zero-trust in a Virtual Cybersecurity World," Journal of Government Financial Management, Summer 2021.

[6] "Crown Jewels Analysis," MITRE Systems Engineering Guide, p. 167, 2014.

[7] "Cloud Threat Report 2020: Addressing Security Considerations Amidst a State of Constant Change," Oracle and KPMG LLP, research conducted in partnership with ESG, 2020.

[8] "Agile cybersecurity—by design—for threat-resistant government agencies—The road to new reality for U.S. public sector," KPMG LLP, Fall 2020.

[9] Priya Emmanuel and Paul Glunt, "The sky's the limit for cloud value, but you need a future-ready plan – Have your cloud migration and modernization efforts stalled? New approaches can help maximize value," KPMG LLP, December 2020.

[10] Microsoft Corporation, "Top 20 Use Cases for CASBs," Microsoft Cloud App Security, 2019.

5. **Establish accountability**. Understanding data assets is critical to personal and organizational accountability. It is important to not only implement effective, efficient network controls, but also monitor their use and maintain their effectiveness. Leading organizations continually probe and test cybersecurity capabilities through simulations that attack the data, applications, and services constituting their priority data. They also overlay advanced analytics to automate and discover deeper process insights.

   Accountability includes the wise use of resources. Implementing a zero-trust architecture need not be costly. Repurposing existing cyber tools and capabilities to their fullest potential unlocks significant cost savings and enhances cybersecurity. Identifying effective cyber technologies and leading private and public sector practices foster new and improved cybersecurity approaches. Greater effectiveness and efficiency increase performance and save resources by reducing vulnerability to and the impact of cybersecurity attacks.

6. **Foster a cybersecurity mindset**. All agency organizations and all employees must participate in strengthening cybersecurity. Leading organizations cascade responsibility so all personnel understand the importance of data protection and their specific roles.[11] Routine "cybersecurity hygiene" is invaluable, along with a top-down, bottom-up collective cybersecurity effort by the entire workforce. Top management must be cybersecurity champions, prioritizing it in resource allocation and decision-making.[12] For example, New York City established a cyber command to explore how zero-trust can be "tailored to the City's unique infrastructure and ultimately improve the security posture"[13] across a government with more than 100 agencies and 325,000 employees.

   Cybersecurity regulations, malicious actors, acts of nature, and accidents will not slow down while governments ponder their next cybersecurity steps. Start planning or continue your zero-trust architecture implementation now so your organization is more prepared for what might happen next.

[11] Tony Hubbard, Geoffrey Weber, and Jeffrey Steinhoff, "Protecting Data Assets in a Perilous Cyber World" Journal of Government Financial Management, Fall 2017.

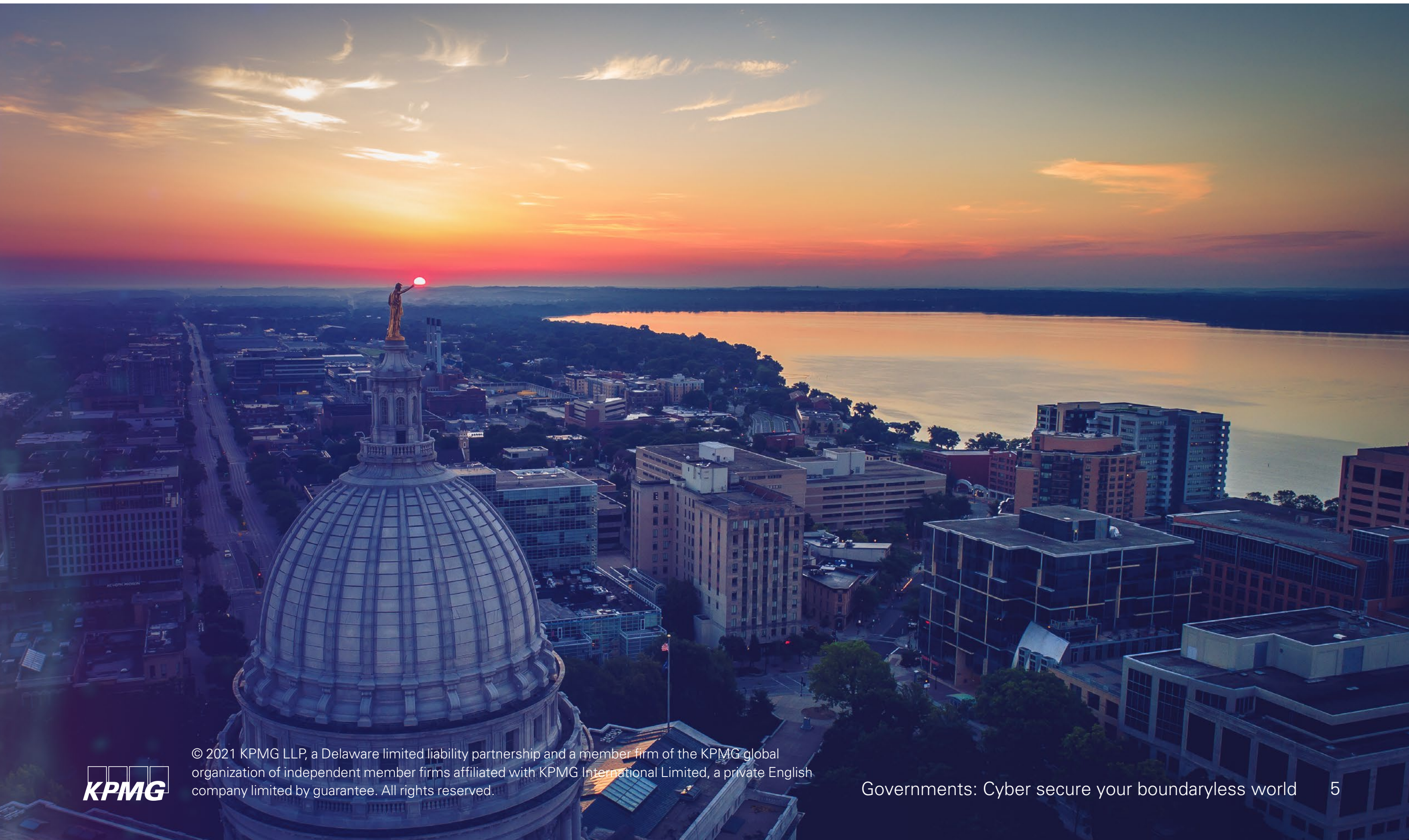
[12] Tony Hubbard, Jennifer Fabius, and Jeffrey Steinhoff, "Harnessing and Protecting Data Assets," Journal of Government Financial Management, Winter 2018–2019.

[13] "Request for Information: Zero-trust Security Management - Moving Beyond the Perimeter," New York City Cyber Command, December 8, 2020.

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.



Contact us

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

Kathy Cruz

Director, Government
Cyber Security Practice
KPMG LLP
916-792-3976
kathycruz@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.