Secure Remote Work Enabled by Cloud and Zero Trust Architectures

CACI

EVER VIGILANT

Secure Remote Work Enabled by Cloud and Zero Trust Architectures

Contents

Summary

The rapid pace of digital innovations and modernization means that much of today's world revolves around a digital landscape. This is even more true in the last 18 months as the Covid-19 pandemic has dramatically increased remote work. Professional or personal sensitive data is often stored online from banking information and passwords to coding and commands for war technology and more. Threats to that data also occur online – hacking, malware and viruses, and phishing are becoming common issues for both organizations and individuals.

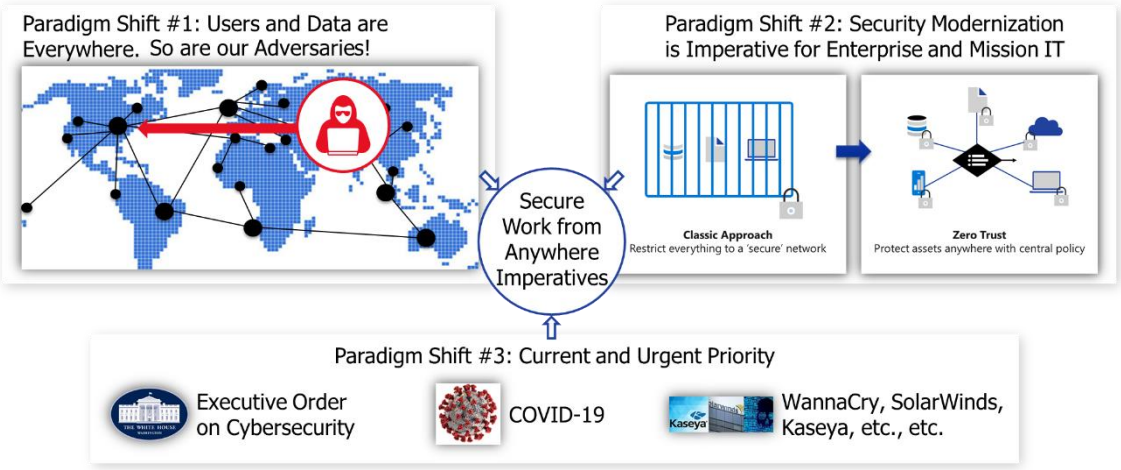
The President's Executive Order on Improving the Nation's Cybersecurity in May 2021 recognized the need for vastly improved cyber protections across the U.S. Government enterprise – citing a need to move more quickly to the cloud, moving to zero trust architectures, continuing to strengthen identity and access management, improving supply chain risk management, as well as strengthening cybersecurity incident response.

As a result, there's a critical need for solutions that address enterprise and workforce cyber threats in the context of today's diverse and geographically dispersed workforce. With this exponential increase in remote work, advancing cyber threats, and an increase in sensitive data being stored and utilized online, it is imperative that cloud-enabled and zero trust architecture solutions are implemented to create and maintain a modern, resilient, and secure workplace.

The Challenge

The current digital landscape is rapidly and drastically changing. Three significant paradigm shifts are driving the need to reimagine and fortify how information is being stored, protected, and accessed.

1. **Mission imperatives and uncontrollable events** – such as the Covid-19 pandemic – have pushed data and users outside the perimeters of the enterprise. This has significantly increased mobile/ remote work, and drastically altered and changed the attack surface at the very time we see increased adversarial activity, as demonstrated by daily attacks against our infrastructure. U.S. Government agencies need secure mobility solutions in the form of lightweight, purpose-built, and trusted communication apps to enable mobile and remote work at the speed of the mission, without compromising security.



2. **Traditional security architectures** have proven too inflexible and expensive to support the enterprise and mission operations of a distributed workforce. The classic security approach of hardened perimeters and layered defenses is being replaced with zero trust architectures that monitor and protect all the assets and data, all the time, and wherever they reside. And again, the challenges of managing an attack surface of organic, in-house IT are exceeding the talent of the work-force – necessitating more rapid migration to the cloud, reimagining security to embrace zero trust architecture principles, and embracing automation as a way to strengthen protection of assets and data.

3. **There is an unmatched urgency and immediate priority** to strengthen the enterprise while embracing the tectonic shift in workforce and mobility. The President's Executive Order on Cybersecurity recognized the need for vastly improved cyber protections across the U.S. Government – citing a need to move more quickly to the cloud, as well as stronger security architectures. To address the need requires reimagining the approach to remote work and security architectures and even how the U.S. Government partners with industry.

The Solution

Mitigating these problems and substantially decreasing the risk involved with an online, remote, and mobile workforce requires changing from current, traditional methods and implementing new processes. Threats evolve and adapt and security needs to as well or the enterprise is left vulnerable.

1. **Mitigate new threats that come with remote work and mobility through zero trust architecture.**

   A systematic approach to securing network, data, and information informs users of decisions that allow for safer security practices. U.S. Government agencies need to create discrete, granular access rules for specific applications and services. This creates multiple layers of authentication that makes it harder for people to access information that is not intended for their viewing.

2. **Move information and architecture to the cloud and secure mobile communications.**

   The de-facto rollout of Office/Microsoft 365 across the government and maturity of commercial clouds allow agencies and departments to reimagine the end-user experience in the form of feature-rich and pay-as-you-go cloud workspaces that can be accessed securely from anywhere and from any device. They complement lightweight purpose-built secure mobility apps that enable secure communications for the distributed and mobile workforce.

   Separating the digital workspace from the physical end-user device significantly reduces the amount of assets that can be attacked and need to be defended. By moving the digital workspace in the cloud, we can manage it by code, like any other cloud resource, which greatly reduces misconfigurations and user errors. Like any other workload in the cloud, digital workspaces are protected by all the resources and capabilities of commercial cloud service providers – which are additional layers of security for any enterprise, especially small and medium-sized government agencies.

3. **Organizations cannot stand alone – U.S. Government agencies need to develop a strong partnership with private industry.**

   The past 18 months have shown that we need to reimagine the digital workspace experience for the government workforce. On-premise virtual private networks (VPN) and virtual desktop infrastructure solutions are too rigid and costly.

   We need modern digital workspaces that are accessible from anywhere and any device and rely on resources that scale based on the workloads. A fixed architecture cannot scale, which creates a big problem if workloads increase or decrease unexpectedly. If it is provided following a pay-as-you-go model, the U.S. Government pays for only resources that are utilized. Rule-based security configurations also need to be replaced and an adaptive security posture enabled by artificial intelligence and machine learning implemented.

   To be successful in this transformation, U.S. Government organizations need to create and leverage new forms of partnership with industry. Transactional relations are replaced with strategic long-term partnerships that leverage industry's breadth of investments and accelerated pace of innovation to modernize enterprise infrastructure, so they maximize use of cloud services and zero-trust principles while complying with all the existing and evolving standards and compliance requirements.

The CACI Advantage

At CACI, our engineers are innovating the technologies needed to support a secure enterprise cloud architecture and achieving results by creating in-house applications and solutions that complement our customers' current architectures. These solutions fill important gaps in requirements for secure mobility solutions, the implementation of zero trust security architectures, and broad adoption of cloud services.

They are packaged in the form of repeatable services offered in a standard catalog-based setting that can be accessed through different contractual models, including completion- or outcome-based tasks, fixed-unit price (FUP) orders, and as-a-service offerings). These services are elastic and scale on-demand to enable quick access and consumption by our customers in a pay-as-you-use model.

1. **CACI Zero Trust Architecture Playbook**
   Our Zero Trust Architecture playbook provides reusable solutions, templates, accelerators, educational resources, and proof points based on our implementation of zero trust across government agencies. This allows us to support our customers through the process of utilizing a new approach to security and implementing what it critical to effective zero trust architecture. Our playbook in an integral component of CACI's support for multiple government agencies. It accelerates the design and build of new enterprise infrastructure – which uses cloud services and zero trust principles – and in deploying an industry-leading privilege access management tool, which serves as a gateway to and analyzes sensitive information.

2. CACI Steelbox®

Security is not just for laptops and desktops – cellphones, pagers, and tablets all carry private information that needs to be secure. CACI Steelbox is the first secure mobile communications app developed exclusively for U.S. Government. It can be adjusted for users with unique requirements, built on technology approved by the National Security Agency for use in classified environments, and it is compliant with requirements of the Federal Records Act and Presidential Records Act.

3. CACI Cloud Workspaces

Agencies need an end-user experience in the form of feature-rich and pay-as-you-go cloud workspaces that can be accessed securely from anywhere and any device. Our CACI Cloud Workspaces integrates with our other applications and provides an efficient, secure, and user-friendly system that provides just that. We work with Microsoft Azure as well as Amazon Web Services to create an a-la-carte solution tailored to customers' specific needs.

4. CACI Cloud Services Playbook

Built from best practices gained by performing more than 200 public sector migrations, the CACI Cloud Services Playbook (C2SP) is uniquely tailored support that helps customers securely and effectively adopt cloud services and solutions. Whether just getting started, actively designing, migrating, or looking to manage cloud-hosted workloads more efficiently, the fundamentals of C2SP are applicable for all government customers at any level of cloud experience. In addition to the CACI Cloud Workspaces, C2SP also includes a catalog of accelerators and utilities that facilitate the broader planning, implementation, and operation of workloads in the cloud.

For more information, contact:

Patricia Blevins
patricia.blevins@caci.com
(540) 254-1182

Albert Lulushi
albert.lulushi@caci.com
(703) 434-4881

CACI's approximately 22,000 talented employees are vigilant in providing the unique expertise and distinctive technology that address our customers' greatest enterprise and mission challenges. Our culture of good character, innovation, and excellence drives our success and earns us recognition as a Fortune World's Most Admired Company. As a member of the Fortune 500 Largest Companies, the Russell 1000 Index, and the S&P MidCap 400 Index, we consistently deliver strong shareholder value. Visit us at www.caci.com.

Worldwide Headquarters
12021 Sunset Hills Rd, Reston, VA 20190
703-841-7800

Visit our website at:
www.caci.com

Find Career Opportunities at:
http://careers.caci.com/

Connect with us through social media: