Securing Contractors' Access to Resources Without Sacrificing Productivity:

A Zero-Trust Approach

As states and local governments grapple with persistent worker and skillset shortages, contractors have become essential for getting the work of government done. To do that work, contractors often require secure access to agency applications, processes and data. However, critical systems and confidential data typically reside in both cloud and on-premises applications, and contractors often connect to agency resources from everywhere with their own devices. As the network perimeter becomes more amorphous, it is more vulnerable to cyberattacks and more difficult to protect.

Zero Trust is a leading best practice to improve and simplify access control and other security processes that help protect an organization's resources. The core tenet of Zero Trust is the concept of least privilege — that is, designing security architecture so each user is granted the bare minimum access needed to perform their job.

Zero-Trust network access (ZTNA) solutions help organizations put Zero-Trust principles into action. Using these solutions, organizations can safely and easily engage with contractors by enforcing least privilege best practices, reducing the time and cost associated with credential provisioning, and ensuring the best possible user experience when contractors attempt to access network resources.

Granting access without giving away the keys to the kingdom

Organizations face the following challenges as they open their organization to contractors and other third parties:

Legacy identity and access management (IAM) applications. Many legacy IAM solutions don't natively support cloud-based access and are difficult or impossible to integrate with cloud platforms, SaaS and other cloud solutions. Organizations may have to administer separate sets of user names and passwords for applications that don't work with the main IAM platform or deliver non-conforming applications via a virtual private network (VPN).

Shared VPNs. VPN solutions extend the network perimeter to the contractor's home or place of work. They can create security holes by granting access to poorly defined groups of users and allowing more access to resources than contractors need. In addition, VPN tunnels are often shared with multiple employees and contractors, which leads to traffic jams and performance issues that impact the end-user experience.

Risky contractor behavior. Excessive privileges and insufficient contractor training can lead to risky behavior. At the same time, organizations need to make the user experience as simple and satisfying as possible to keep contractors productive and engaged.

At-home vulnerabilities. At-home devices such as printers, smart TVs and voice over IP (VoIP) phones — as well as applications that contractors download for their personal use — can introduce vulnerabilities when they're connected to the same network that a contractor uses for work.

Moving toward Zero Trust

The May 2021 Executive Order on Improving the Nation's Cybersecurity[1] mandates that federal government agencies move toward Zero-Trust architecture, and it's likely that state and local government agencies will face similar requirements.

"I think we can easily project that states will be held to the same standards going forward. Even if that weren't the case, given the reliance of government services on data and technology, government at all levels should be moving toward adopting Zero Trust to better protect citizen data and critical systems and operations," says Deborah Snyder, senior fellow for the Center for Digital Government and former chief information security officer for the state of New York.[2]

Unwieldy provisioning processes. Onboarding/provisioning processes are time-consuming, expensive and complex to manage — especially when administrators are responsible for managing hundreds, if not thousands, of employees and contractors. Having to deploy VPNs or provision agency-owned devices further increases the burden on administrators and delays getting contractors up to speed and productive.

Putting a Zero-Trust network access strategy to work

A ZTNA strategy focuses on applying granular access controls and the concept of least privilege so only the right person can access the right resources at the right time.

Advanced ZTNA solutions put this strategy into action via three core pillars: security, performance and availability. Leading ZTNA solutions allow these pillars to rest on a purpose-built, cloud-hosted global infrastructure with hundreds of points of presence. These solutions protect resources wherever they exist, eliminate the need for a VPN, simplify and improve contractor access, and reduce the cost and complexity of onboarding contractors.

Security. This pillar focuses on the technologies, policies and processes used to grant access based on a user's identity and context. Tactics include creating secure boundaries around applications, hiding applications behind encrypted tunnels, monitoring and logging all access requests, and enabling seamless authentication for contractors without disrupting employee directories.

Performance. Contractors should be able to complete authentication processes and access resources as quickly and seamlessly as possible. Performance suffers and wait times grow when too much traffic travels across shared VPN tunnels. A better approach is to enable access directly between the contractor and the ZTNA solution platform's edge. Content and processes can be cached and delivered at the closest point to the contractor, which reduces latency significantly.

Availability. ZTNA solutions must be available 24/7 to continuously protect resources and maintain contractor productivity and satisfaction. A globally distributed infrastructure and intelligent routing help ensure services remain available even if local data centers experience an outage, maintenance downtime or another issue.

When choosing a ZTNA solution, organizations should also look for the following features:

Integration with endpoint/device security solutions. Contractors' mobile phones, remote laptops, printers and other devices are also vulnerable to breaches and misuse. A good ZTNA solution integrates with the organization's anti-virus and endpoint/device security solutions so contractors' devices can be properly authenticated and incorporated into a Zero-Trust strategy.

Centralized management. A centralized console enables administrators to view and manage every user, device and security tool from a single point. If an administrator makes a configuration change to enable (or withdraw) a contractor's access to resources, the change is automatically replicated globally within seconds, providing a seamless end-user experience and allowing administrators to focus on more engaging, higher-value tasks.

Getting ZTNA right

The following tactics help organizations successfully implement a ZTNA solution:

- Start by documenting what hasn't worked (i.e., where and why the organization experienced an attack or a service outage)
- Focus on securing the transactions between users, applications and data instead of focusing security on connectivity and static, network-based perimeters
- Identify one application that contractors use frequently and pilot ZTNA with a small group of contractors
- Consider the entire contractor lifecycle, including off-boarding
- Pull the finance team into the conversation early on to weigh Opex vs Capex options

Seizing the moment

With millions of dollars of aid available through the Infrastructure Investment and Jobs Act (IIJA) and other federal funding, state and local governments have an unprecedented opportunity to tackle their cybersecurity gaps and implement Zero-Trust strategies. The State and Local Cybersecurity Grant Program is an obvious place to start. Although the grant application window for the first $200 million closed November 15, 2022, an additional $800 million in grants will be awarded between FY2023 and FY2025. Organizations should reach out to trusted vendors and consultants now to see how they can seize the moment and prepare for the next grant application windows.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] CDG interview with Deborah Snyder. May 2022.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Cloudflare.

Produced by: gt CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Sponsored by: CLOUDFLARE®

Cloudflare is the security, performance, and reliability company on a mission to build a better Internet for state and local governments. Today it runs one of the world's largest networks that powers anything connected to the Internet. **https://www.cloudflare.com/**