



Take the Stress Out of Securing Constituent Engagements

Constituents depend on digital engagements to connect with state and local government. They're going online to pay utility bills, apply for permits, renew vehicle registrations and undertake a range of other activities.

The problem is that many digital services depend on a disjointed mix of underlying identity and access services and capabilities, including legacy applications that are no longer supported, which makes it difficult to ensure those engagements are both seamless and secure. This proves frustrating both for constituents trying to access those services and for agencies trying to minimize the attack surface of their IT environment.

In this report, we will discuss:

- The obstacles to a better digital experience
- The concept of an identity-driven network defense solution
- Best practices in leveraging identity for secure access management



Challenge: Mismatched Expectations, Capabilities

A number of factors can get in the way of ensuring secure and stress-free digital interactions for state and local constituents:

- **Disparate systems** make it hard to manage security in a hybrid world. IT departments may struggle to maintain multitudes of security solutions, and constituents find it hard to conduct business in the absence of a single, seamless online identity.
- **Legacy systems** are inherently vulnerable, and resource constraints mean they are not being kept up to date. Bad actors are well aware of vulnerabilities in backend legacy solutions, yet IT departments may lack the resources to keep these systems patched.
- **The rising volume** of online interactions is problematic. Everyone expects to be able to interact with government online, yet more digital interfaces mean a wider attack surface.
- **There remains a need to balance security** with the user experience. Government has to deliver services online, but this needs to happen in a way that is seamless and simple for every user.

Solution: An Identity-Driven Network Defense

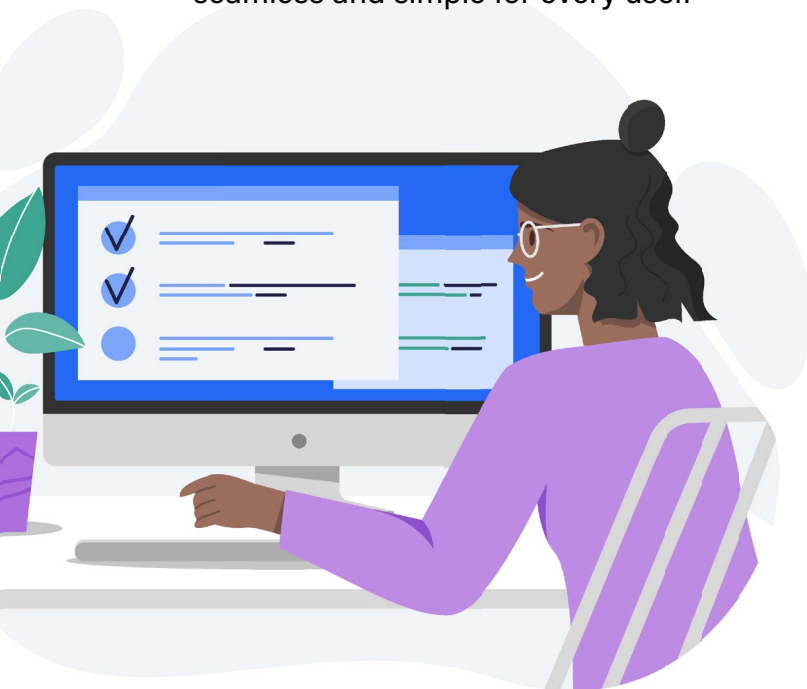
There is power in simplicity. Agencies can replace outdated legacy systems with a cloud-based as-a-service identity and access management platform, which will simplify management for IT teams while also improving the user experience. Key capabilities include:

- **Simplified user identity:** Instead of a local government managing a local database of identities, use social logins to bridge into the constituent's normal identity.
- **Hiding insecure and legacy applications from the bad actors:** With a cloud-based security platform, IT administrators can achieve this with minimal human effort. They'll no longer have to worry about application patches and updates, because they are now hidden from the internet and no longer reachable for exploitation.
- **Enabling dynamic security recommendations:** Leveraging artificial intelligence (AI) and machine learning (ML) capabilities, the platform automates security audits and assessments, empowering administrators with constant, AI-driven recommendations to ensure the ongoing maintenance of a robust security posture.

With data workload protections, elements of zero trust and convenient logins, a modernized solution reduces the complexity of having multiple tools and components and requires less human effort.

"Regular security audits and assessments help address the lack of centralized visibility and control. Through comprehensive assessments, agencies can gain insights into security vulnerabilities."

Tamer Baker, Zscaler



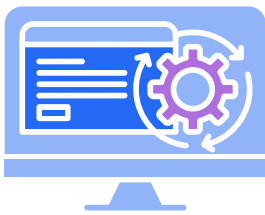
Best Practices in Cyber Upgrades



Use continuous monitoring

Use continuous monitoring capabilities to watch for anomalies across all traffic flows, including constituent interactions and internal logins.

"A robust continuous monitoring program includes real-time monitoring, log analysis and intrusion detection. This helps detect and respond to security incidents promptly," said Tamer Baker, Chief Technology Officer at Zscaler for State, Local, Education and Healthcare. "And you want to have a business process in place to weed out false positives, so your team can focus on things that are important."



Leverage automation

With security delivered as-a-service in the cloud, the vendor handles all updates and patching of its systems and does so with no downtime. The IT team needs only to set policy and can then devote itself to higher-level tasks.

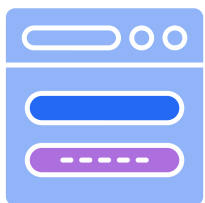
Automation helps monitor and audit the code repositories that support constituent-facing applications. Since 100% safe coding isn't achievable — even with secure coding practices — agencies should also utilize the platform's ability to continuously check the security posture of these applications.



Limit exposure

Take advantage of the ability to hide systems from prying eyes, ensuring applications reside behind a security cloud and are not exposed to the internet.

"If an application is not visible to an attacker, if they can't access it in any way, then it doesn't become a risk," Baker said. "Instead of exposing applications to the internet, you put them behind a security secure cloud so that the attackers never see these systems. Even if they are vulnerable, they won't be exploitable."



Implement a portal

A portal offers a consistent front end for constituent convenience. With an as-a-service solution, the vendor will create the portal to help drive seamless interactions.

"You can have a single front end that is simple even for the user who isn't smart about cybersecurity best practices," Baker said. "They just log in with their social logins and the portal gives them access to the applications they need in a way that's hidden from the bad actors. It's a secure, easy, browser-based experience."

Case Study: A State Agency Builds Trust Through Secure Interactions

To see what this looks like in action, consider a state government agency responsible for providing various online services to its constituents.

Challenge: With the rising volume of online interactions, the agency struggled to maintain security, protect sensitive data and address the diverse needs of its constituents. The agency needed to address these challenges not only to prevent unauthorized access or data breaches, but also to maintain the trust of its constituents.

Solution: The agency implemented Zscaler's comprehensive constituent access security solution to hide applications from the internet while providing secure browser-based access to them, to secure data transmission and storage, and to conduct regular security audits and posture assessments. Through Zscaler, it leveraged an open-standard authentication protocol to deploy robust authentication mechanisms that could integrate with all standards-based identity platforms.

Outcomes: With a comprehensive access architecture, the agency enhanced its security posture and built trust. Engagement with online services increased and satisfaction improved as constituents felt reassured that their personal information was protected. At the same time, strong security measures ensured compliance with industry regulations and data protection standards.

"The agency's efforts in implementing a robust constituent access security solution led to improved security, enhanced constituent trust and a more resilient and secure digital ecosystem for interacting with government services," said Baker.

How Zscaler Helps

With deployments in 23 U.S. states serving over 4 million state, local and education users, Zscaler solutions anticipate, secure and simplify online interactions.

- Zscaler Private Access (ZPA) leverages a web browser for simplified user authentication, while Browser Isolation separates users from actual web applications.
- Privileged approvals allow third-party users, constituents and contractors to log in to a privileged remote access (PRA) portal to gain access to applications and IoT/OT systems.
- Zscaler Internet Access (ZIA) defines safe, fast internet and SaaS access as part of a comprehensive cloud-native zero-trust platform.
- Cloud security posture management (CSPM) policies are built natively into Posture Control by Zscaler, a comprehensive cloud-native application protection platform (CNAPP) that identifies, prioritizes and remediates risk in cloud infrastructure and across multi-cloud environments.

Learn more about [Zero Trust Citizen Access](#).

