ZERO**TRUST**

Accelerating the Journey to Zero Trust:
A Roadmap for Implementing Continuous Authentication

State and local governments are now prime targets for cybercriminals due to the acceleration of remote and hybrid work, reliance on hybrid technologies, and resource and budget constraints that make it difficult to address existing security gaps.

To strengthen enterprise security, governments will have to adopt modern Zero-Trust security approaches. A Zero-Trust framework means an organization should trust no individual or device unless properly verified before being given access to the network and data. Dynamic authentication and authorization are key tenets of Zero Trust.[1] Therefore, to operationalize this model successfully, agencies must implement tools and governance policies to continuously authenticate users.

Here's a roadmap for how state and local agencies can consolidate identity management, segment user access, authenticate every access request, and enforce phishing-resistant multi-factor authentication to improve security postures and implement Zero-Trust security.

Current Authentication Challenges for the Public Sector

Public sector organizations face a range of authentication challenges, mostly driven by the need to accelerate digital transformation. A proliferation of applications, including software-as-a-service (SaaS) solutions, makes it difficult to manage user access to critical and sensitive applications and data.

Michael Makstman, the chief information security officer for the city and county of San Francisco, says government organizations have always dreamed of a single sign-on (SSO) experience for users, but the persistent challenge has been unifying access across a growing number of applications.

"The problem of trying to streamline user access has exploded, and it is more challenging than ever for a large government organization to actually manage access consistently," he says.

New business demands add to these challenges. Remote and hybrid work, for example, require a new way of verifying people, technology and data compared to legacy perimeter security-based approaches.

State and local agencies will likely have to rethink their approach to authentication and gradually move toward an authentication ecosystem that strengthens security while ensuring a frictionless user experience.

"We need to think about a way to do authentication that promotes the user experience, and yet at the same time, up-levels the strength of the authentication itself," Makstman says.

Implementing continuous authentication is one way agencies can accomplish this.

What is Continuous Authentication?

Continuous authentication is a verification method in which an organization validates a user's identity consistently and in real time as they maneuver between systems and applications on their device, or even across multiple devices.

This approach relies on data and analytics to assess risks and determine whether a specific user performing an activity is authorized to do so and that their credentials haven't been compromised. Unlike traditional authentication methods, continuous authentication doesn't just check a user's identity when they log into a session. It consistently verifies the user, identifies anomalies that may indicate a security risk and ends a session if it suspects a threat.

"Every time you access a resource — data, systems or back-end databases — you need to prove you are who you say you are, because at any point during an authentication process or any time you access systems, there might be an attacker who has now moved into your technology landscape," says Jeff Frederick, a senior manager of solutions engineer at Yubico, provider of the YubiKey, a phishing-resistant hardware security key.

As agencies attempt to improve their authentication methods, the following best practices can help them employ continuous authentication to lay the foundation for Zero Trust.

Best Practices for Continuous Authentication

Establish your baseline.

Agencies should use two-factor (2FA) or multi-factor authentication (MFA), at minimum, as a baseline for authentication. They can also transition to passwordless authentication, which may rely on hardware-based authentication methods, biometrics or physical touch for user verification. Not only can passwordless authentication strengthen security, it can also reduce IT time spent resetting passwords.

Though the right approach will vary by organization, it's important for agencies to establish their own baseline authentication infrastructure and associated framework.

Carefully assess multi-factor authentication solutions.

While considering 2FA and MFA solutions, agencies should keep in mind that not all MFA solutions are created equal.

Some forms of MFA, including mobile-based authenticators such as short message service (SMS), one-time password and push notifications, are susceptible to phishing, malware, and man-in-the-middle (MiTM) attacks. Similar to passwordless security, agencies should consider implementing phishing-resistant and user presence-based authentication mechanisms, such as authentication via a hardware security key or token. In addition to security, it's important to consider usability, portability and scalability of authentication solutions. Poor user experiences, low portability and lack of scalability can result in MFA gaps, low user adoption and an increased risk of a breach.

Develop an authentication framework that aligns with your current identity and access management capabilities.

As a starting point, agencies should assess all apps and services — both on-premises and in the cloud — and privileges of all users and admin accounts. Next, they can decide whether to build MFA into every system or just apply it to high-value systems.

From there, agencies should decide on levels of access security for different user types and user roles, or weigh whether deployment is required for all users across the enterprise. For example, they can determine whether to require stronger, risk-based authentication for privileged business and IT users, such as C-level leaders, HR, legal and finance department heads, along with IT, security and network administrators.

Harness the power of analytics and AI.

Behavioral, contextual or activity-based authentication can be useful for detecting anomalous behavior and restricting access.

AI-driven behavioral models can detect anomalies based on things like typing rhythm or mouse movement, as well as factors such as IP address, location and time of day of login.[2] With this intelligence, agencies can fine-tune their approach — for example, revising security policies to dynamically apply two-factor or stepped-up authentication based on real-time changes in their environment.

Start small, but think ahead.

Makstman says agencies can get started by applying continuous authentication to mission-critical applications across the enterprise.

This approach can be impactful because mission-critical applications typically offer access to highly sensitive and confidential data. In addition, agencies should think ahead and require new applications coming into their ecosystem to support modern phishing-resistant authentication protocols, such as FIDO U2F and FIDO2 open authentication standards. This policy will make it easier to integrate new technologies into their authentication ecosystem.

Make authentication a part of equitable service delivery.

As they attempt to implement continuous authentication and Zero Trust, governments should keep equity in mind. Some constituents may not have a mobile phone or computer, may live or work in a geographic location with low cellular connectivity, or may not even have a permanent home address or phone number. Agencies must also serve different ability communities, so inclusive design should be an important consideration when assessing MFA solutions, especially for constituent-facing digital services

"We need to do a lot around equity in the delivery of access," Makstman says.

Working with authentication providers who design their solutions inclusively, testing the user authentication experience with various constituent groups and incorporating their feedback, can help agencies ensure secure access doesn't compromise equitable service delivery.

Creating a Pathway to Zero Trust with Continuous Authentication

With the explosion of cloud-based SaaS solutions, new remote and hybrid work models, and accelerated digital transformation, state and local agencies now need to strengthen authentication.

Continuous authentication is one approach they can adopt to improve identity and access management and protect critical systems and data. By creating a future-proofed authentication framework, aligning their systems and policies to this framework, and making incremental changes to move toward dynamic, risk-based authentication, agencies can lay the groundwork for Zero Trust and develop a more modern, responsive security strategy that empowers them to achieve their mission.

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

Endnotes:

1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
2. https://www.infosecurity-magazine.com/opinions/need-continuous-authentication/

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.**

For: yubico

As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. Yubico is privately held, with a presence around the globe. For more information, please visit: **www.yubico.com**.

IMAGE PROVIDED BY SHUTTERSTOCK.COM