Zero Trust solutions for state and local government

Manage risk and improve security

Every day, cybersecurity threats to public sector organizations are becoming more frequent and sophisticated. State and local governments are attractive targets because their high-value systems often run on outdated technology or lack modern cybersecurity controls. With rising security threats and ample federal funding available, now is the time to move toward a Zero Trust architecture (ZTA).

Experience the Okta difference

Okta is:

- **Universal.** With over 7,000 integrations, Okta securely connects all apps and multi-cloud environments to a single Identity platform.
- **Complete.** Designed for the evolving needs of government organizations, Okta is a one-stop solution for any workforce or customer Identity use case.
- **Easy.** Developed for every user in mind, Okta's no- or low-code options are simple to build and easy to use.
- **Reliable.** With 99.99% availability and 60 times less downtime than competitors, Okta Identity solutions keep operations running.

Simply put, Zero Trust is a modern approach to cybersecurity that assumes every network is hostile and every request for access could be from a malicious source.

In practice, Zero Trust means you are continuously authenticating, authorizing, and monitoring activity on all networks. A Zero Trust approach gives you better control over access, assets, and users while reducing risk and improving the overall cybersecurity posture of the organization.

While this can seem daunting, Zero Trust is best achieved by building a strong ZTA foundation, where one Zero Trust principle builds on the next. An excellent place to start is with Identity. In fact, the federal Cybersecurity and Infrastructure Security Agency (CISA) considers Identity to be the first pillar in their Zero Trust Maturity Model. As the world's number one Identity platform, Okta's Identity solution empowers you to build a strong ZTA foundation by securely connecting the right people to the right resources at the right time.

Implementing Zero Trust efficiently may be challenging for public sector organizations, especially if your identities are still locked up in legacy silos. When you centralize Identity, strong authentication becomes an easy task for your users and administrators. The fragmented, legacy security postures are not able to continuously authenticate Identity or seamlessly and securely integrate new technology, which is what Zero Trust requires.

Zero Trust begins with Identity, so partner with the trusted industry leader: Okta

When the time comes to update systems, getting internal buy-in on new solutions can be a monumental task. Usually, implementing new technology isn't the issue. Rather, it's the culture shift to a security-first mindset. Public sector organizations can do more and get to Zero Trust more quickly if everyone believes in the direction the organization is headed.

It may seem daunting, but with the right strategy and technology partners, your organization can overcome these Zero Trust challenges. Here are steps you can take to start building a Zero Trust foundation:

1. **Take inventory of current users, existing devices, and data**
   By identifying access points and data classification levels, agencies can determine the type of security needed for different types of data and systems.
2. **Centralize Identity**
   The next step on your Zero Trust journey is centralizing Identity, so you can have a unified view of all users interacting with your agency and more easily authenticate their identities across all systems.
3. **Authenticate the Identity of users**
   Focus on developing a strong, phishing-resistant MFA for both your workforce and the public by authenticating users across all systems and access points to prevent cybersecurity threats.
4. **Integrate device-level signals into the authentication process**
   Any unpatched or compromised devices can introduce unnecessary risk to government systems, but consider providing robust user access to improve both security and the user experience to avoid added security measures from ruining the user experience.
5. **Build Zero Trust into organizational culture**
   Cultural shifts in any organization take time, but developing a culture of security first in every department will help protect the organization for years to come. Organizations can also benefit from building relationships with other stakeholders to receive their buy-in on new solutions and communicate successes.

Building a strong Zero Trust foundation starts with tackling CISA's first Maturity Model pillar — Identity. By leveraging solutions from Okta, you can seamlessly integrate Identity solutions across entire technology ecosystems to unify an approach to Zero Trust. As the world's #1 modern Identity and access platform, Okta provides a single platform view of all your users, groups, and devices so you can strengthen cybersecurity, simplify the customer experience, and build a strong Zero Trust foundation.

Take your first step towards Zero Trust with Okta.

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.