IDENTITY MANAGEMENT: MEETING THE NEEDS OF MODERN COMPUTING PLATFORMS

In this Q&A, Ted Girard, vice president of public sector for Okta, discusses how modern cloud-based identity systems can address the unique challenges of identity management in edge, cloud and IoT environments.

As government agencies move to the cloud, how do their needs and requirements change around identity?

Their needs change drastically. Cloud and modern compute platforms are driving the need for modern identity architectures. Prior to cloud, identity systems were typically bolted on as part of the application stack, hosted in the agency's data center and protected by complex perimeter security systems that included firewalls, VPNs and intrusion detection systems. With cloud, the data center perimeter becomes perforated as data and applications extend beyond it. The security perimeter is no longer the firewall; it is the user. In this new era, identity must move beyond the application stack and be its own independent and neutral platform.

Governments increasingly operate multi-cloud and hybrid environments. How does this impact identity and what should agencies be thinking about?

Agencies can now pick a host of cloud services — the best email platform, the best content management system, etc. — for their own specific missions. These services usually come from different cloud vendors. Agencies also are choosing multiple cloud infrastructure providers along with their own data center or private cloud. These trends drive home the need for identity management

to be its own independent and neutral platform that supports whatever applications the agency requires.

How can modern identity solutions improve the user experience for government employees and citizens?

In the past, the greater the security needed, the greater the friction that was imposed on the user. With modern identity solutions, organizations can dial up the security while simultaneously reducing impact on the user. Users also want to log in any time. Modern cloud-based identity systems deliver a 99.9 percent uptime service level agreement with zero planned downtime. That is never the case with legacy on-premises systems, which always have downtime.

WITH MODERN IDENTITY SOLUTIONS, ORGANIZATIONS CAN DIAL UP THE SECURITY WHILE SIMULTANEOUSLY REDUCING IMPACT ON THE USER.

Do emerging technologies like IoT and edge computing impact government identity strategies? How?

Absolutely. IoT in particular is a challenge. Rather than just data being at risk, dams, crops and power generation are now at risk. A government identity strategy has to address these factors as part of risk assessment and mitigation. In this environment, specific methods of multifactor authentication, application authorization and API authorization (authorization to the data) become particularly relevant.

How can modern identity solutions help governments share more data (to improve service and efficiency) while complying with increasingly complex privacy laws?

The ultimate goal of any modern identity solution is to allow the right data access to the right person at the right time, from anywhere and on any device. However, it's not the only goal. The service provider must also prove to be trustworthy. This trust typically comes in the form of third-party attestations and authorizations that are continuously monitored and adhered to. These accreditations and authorizations include ISO27018, ISO27001, FedRAMP, AICPA SOC2, CSAStar, HIPAA and GDPR.

Learn more at **Carah.io/Okta-Edge**

Redefine Security with Modern Identity

Deliver seamless user experiences to citizens and employees without compromising security.

> **"** Identity was one of the biggest hurdles we had to cross, but we also wanted to provide a good experience to QPP users. Okta helped us achieve both those goals. **"**
>
> – David Koh, Engineer, USDS

Okta helps CMS transform the American healthcare system by securing and streamlining Identity.
Read more at: **https://carah.io/Okta-CMS-Study**