Securing identity

Cloud identity helps agencies manage IT modernization risks and improve the user experience

As the traditional network perimeter disappears and more employees work from home, agencies are turning to cloud-based identity as the best way to secure their expanding enterprise.

Even before the pandemic, agencies were moving to the cloud, transforming their business, and managing threats that were coming from behind their own firewall. They were challenged to balance productivity and security as they support their mission.

Fraudulent identity access, slow user adoption, ongoing operations and onboarding costs, and a delay in providing employees access to applications are just some of the risks that agencies face as they modernize the enterprise.

These risks can be mitigated by using a cloud-based identity and access management approach said Andrew Whelchel, CISSP-ISSAP, CCSP, principal solutions engineer, at Okta. "The right approach is to understand the risk and build a path to mitigate the risk with a cloud identity based approach."

This approach will help quickly integrate and provide application access to employees and contractors, secure applications with zero trust policies, improve the user experience, and reduce administrative costs, he said.

An identity, credential, and access management (ICAM) architecture provides a path for agencies to map capabilities to certain requirements, such as identity and credential management, access management, governance and federation.

"Identity access is key to speeding access and enforcing access policy," Whelchel said. "Cloud identity enables a single plane of access to cloud or on -premises based applications."

Okta wants to "manage access to everything" via ICAM, he said.

"We're not just talking about SaaS applications or custom applications, but everything from APIs to servers to on-premises applications and even workstations."

Cloud-enabled ICAM means that the platform is neutral and independent, scalable and secure, and takes an identity-centric approach to zero trust security, so that "any organization can use any technology" to access applications securely and quickly.

The services that make this possible include single sign-on, universal directory, lifecycle management, adaptive multi-factor authentication, and API access management.

"All of these are core services and part of the Okta identity cloud which enables that cloud-based ICAM," he said.

Identity is central to creating a zero trust architecture. Users have their own attributes and information on their own devices, and additional native data and data from partners can be helpful for understanding risk and context. "Pulled together these things can help drive a context-based risk policy," he said.

> **"Identity access is key to speeding access and enforcing access policy."**
>
> **– ANDREW WHELCHEL, CISSP-ISSAP, CCSP, PRINCIPAL SOLUTIONS ENGINEER, OKTA**

Agencies can create a risk score based of off commonly understood risk elements and the platform offers specific policy information of known risk factors. "These combine together for an authorization engine decision that will drive an access decision," he said. "By access decision, we mean a level of access to different applications, even legacy protocols."

In addition, security, orchestration, automation and response (SOAR) and SIM type applications can grab data from Okta and use it to enrich their own platforms and if there is risk, a user can be temporarily contained.

Most security experts agree that it is easier to secure a single system or a few systems rather than a massive hodgepodge of systems, Whelchel said. This will help them access "the right amount of data to get that authorization and access."

Agencies have to be able to leverage the data where it is, rather than moving it to another location, he said. To streamline this, "provide an access management plane that allows you to keep the data where it is, leverage it and help accelerate the mission that way."