User Identity and Access Management: A Bridge to Government IT Modernization

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

1. The Need for Government IT Transformation

Government agencies face unique cybersecurity challenges in today's world, including a large legacy information technology base, processes not built for the digital age and a prohibitive legislative budgeting cycle. The same IT systems that enabled progress in fulfilling agency missions for decades, ranging from entitlement programs to regulatory controls to public health and safety initiatives and beyond, are now consuming IT budgets to maintain legacy applications and aging on-premise infrastructure. This burden is reflected in major expense categories that are common across governmental organizations and departments: software maintenance, upgrade costs for hardware, IT staffing, and helpdesk support. According to the General Accounting Office, 78 percent of the federal IT budget is set aside to maintain legacy IT.

Meanwhile, as security vulnerabilities proliferate, citizens, employees and contractors face access and usability challenges when trying to navigate the multiple systems required to get to public services and entitlements, or to simply do their jobs. Problems include:

- Employees and contractors need to access multiple disconnected systems with different profiles and passwords
- Citizens need to apply and register for their entitlements, make recurring contributions, and/or update and maintain their account information
- IT and program administrators need to assign granular access privileges as well as set up, activate and decommission users

Because of these challenges, government agencies are looking for creative new approaches to overcome the obstacles preventing adoption of the latest technologies driving transformation in the U.S. economy.

Agencies working to replace legacy IT, such as the Federal Communications Commission, are seeing dramatic results. Under the leadership of Chief Information Officer Dr. David Bray, the FCC transformed a complex legacy IT system comprised of more than 207 different components into an award-winning technology stack in less than two years. This included rolling out new cloud-based IT applications and services that achieved results in half the time and at one-sixth of the originally projected cost.

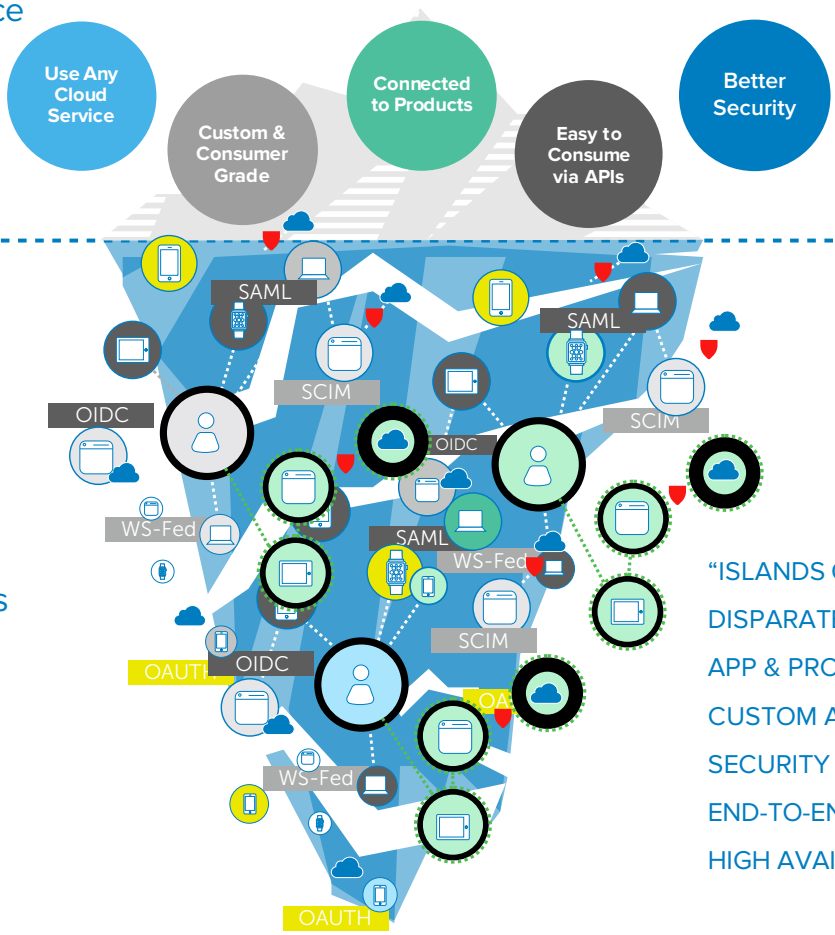
"Wanting to get out of this sort of trap of maintaining legacy, one of the things we've been doing at the FCC is—like at other public sector organizations—to move to the cloud as quickly as we can."

— Dr. David A. Bray, CIO, FCC
September 2015, i-cio.com

2. Complexity in Legacy Identity and Access Management Infrastructure

In the current environment, government infrastructure is highly complex and requires IT to carry the bulk of the burden. A rapidly growing base of users with differing needs, workstyles and lifecycles needs to be supported by complex, expensive and brittle legacy solutions that require time-intensive processing with limited automation and scalability. This burden has also halted innovation in government, where the modern explosion of apps, devices and resources available in the market is unusable by employees, hindering productivity.

Expectations
of digital experience

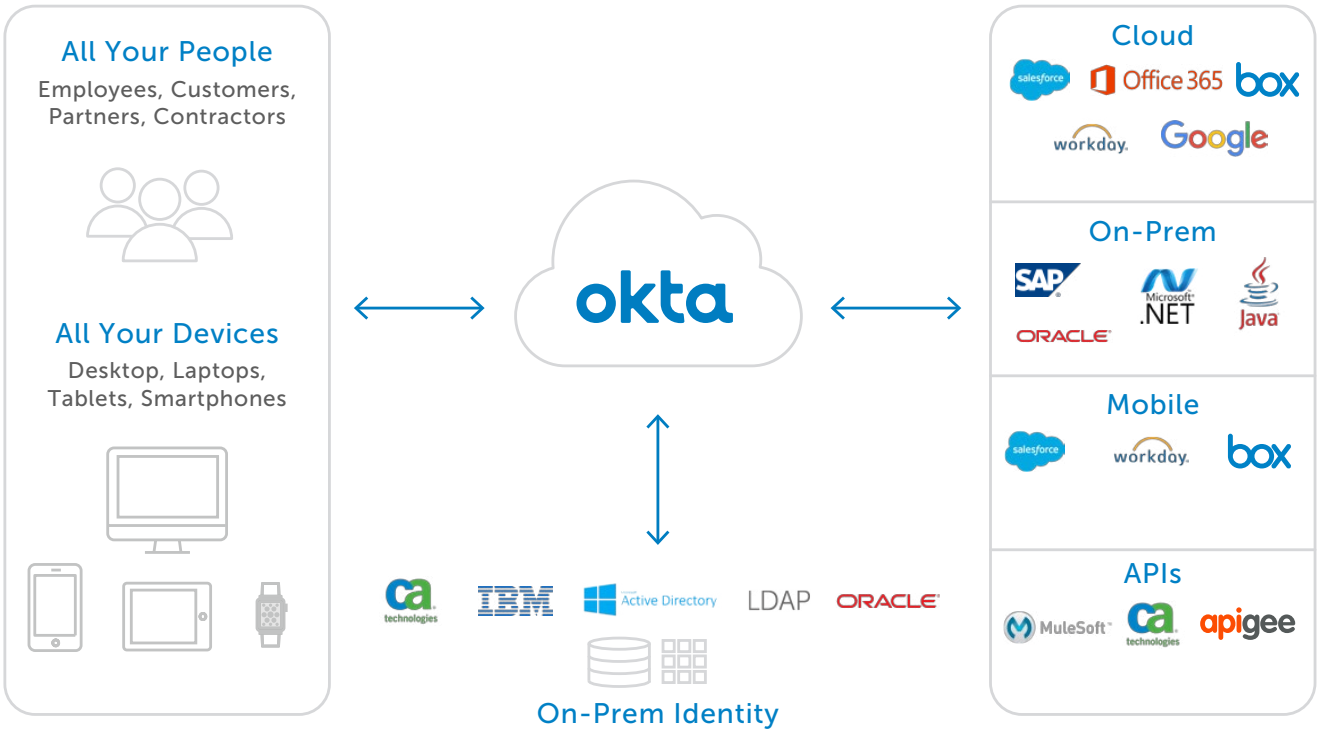


Reality of building
digital experiences

"ISLANDS OF IDENTITY"
DISPARATE DEVICES
APP & PROTOCOL EXPLOSION
CUSTOM APPS & SERVICES
SECURITY IN THE CLOUD
END-TO-END VISIBILITY
HIGH AVAILABILITY

But transformation is achievable. The security architecture changes as major applications are migrated to the cloud. Human capital management systems like Workday contain personally identifiable information (PII), and productivity applications like Office 365 contain sensitive company data. The approach to protecting data needs to shift from securing the network perimeter to securing access to these applications.

A modern cloud-based IT architecture with one modern identity platform empowers enterprises to increase efficiency in managing the identity lifecycle for all applications, provide contextual access management to cloud applications and company data, deploy the best applications for productivity, and support secure collaboration with partners and vendors beyond the firewall.

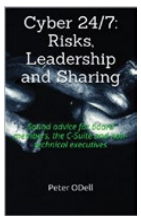


3. User Challenges & Security Concerns

Addressing the User Experience

With legacy IT, there are a variety of commonly reported pain points impacting users and the professionals that manage and maintain it, including:

- Repetition and friction for the user in accessing a myriad of different properties
- User concern regarding whether their PII is secure
- Poor user experience resulting in low adoption and satisfaction levels
- Siloed usage data for IT, with difficulty aggregating and understanding UX analytics



"Single sign-on is a win-win. Unified identity integrates apps and greatly improves the user experience. From an IT admin perspective, the ability to watch an individual's usage across systems can tell you what's working well and poorly."

— Peter O'Dell, IT Security Analyst and Author
Cyber 24/7: Risks, Leadership and Sharing

To break free from today's legacy IT constraints and achieve digital transformation with its promise of agility and savings, agencies need migration plans that provide change management, sustained service delivery, security, and continuous improvement that is visible to constituents.

By putting IT users first, identity and access management (IAM) delivered as a cloud service offers a bridge to span the legacy-to-cloud gap without compromising security.

Technology is transforming employee productivity and allowing government systems to be user-centric. Employees can be productive on their terms, unleashing critical innovation. Cloud is enabling IT to focus on adding value to the business.

Ensuring Security is Top Priority

There are new and complex challenges to safeguarding agency data. The days when applications and file servers sat safely behind a firewall, only being accessed from corporate-owned devices, are gone. Hackers are becoming more resourceful by taking advantage of the shift of applications to the cloud, where employees connect to them from all types of personal devices.

To secure the data within today's cloud and mobile applications, CISOs must move beyond yesterday's tools and look to the next generation of cloud-based security solutions. Even in today's distributed cloud environment, you can mitigate the risk of phishing and account takeover attacks, access comprehensive application records quickly, and offer bullet-proof encryption of agency data.

"I think today the better bet is get to the cloud as quick as you can because you're guaranteed almost to have better security there than you will in any private thing you can do."

— U.S. CIO Tony Scott
October 2015, cio.com

Okta is a FedRAMP approved vendor and HIPAA-compliant

4. A Modern Identity and Access Management Solution

New initiatives using next-generation technology require a rethinking of the foundation of agency IT to leverage the latest cloud technologies for performance, cost savings and security. This new foundation needs to optimize for addressing all modern use cases on a single platform. It needs to enable individual department stakeholders and IT to choose the best applications and technologies to build out digital experiences with the greatest ROI.

Agility is a must. Delays lead to projects never getting off the ground because opportunities and technology move too quickly. Take full advantage of identity and access management as a platform to enable change, provide IT automation and control, and create a simplified experience for all employees. By extending the breadth of IAM capabilities to all scenarios, this platform can provide the basis for digital transformation in the agency.

Capabilities	Benefits
Cloud-based solution	Reduce on-premise infrastructure
Pricing based on active usage of services	Lower monthly cost
Single sign-on across websites and applications	Improved end user experience Single set of credentials Reduced helpdesk tickets Increased citizen/customer participation
Extensive pre-built and maintained integrations	Flexible, vendor-neutral integration to any application or API
Customizable, consumer grade UX built on native experience	Consistent interface and ease of use
Unified directory	Simplified access to user attributes from multiple sources, including AD/LDAP for profiles and lifecycle states
Built-in, real-time security and compliance reporting	Automated reporting and documentation to meet business and legal requirements
Intelligent and automated lifecycle management across all devices	Streamlined, low-cost user and access management for onboarding and off-boarding
Multi-factor authentication (MFA) with a comprehensive set of modern factors but simple for end users	Increased security for authentication
Administrators can manage all users, apps, groups, devices and factors from one console	Increased control over users, devices

Case in Point: IAM in Action at AFGE

To better serve its 450 employees and 300,000 members, the American Federation of Government Employees (AFGE) led its cloud transformation with a new identity solution that could provide its users with a much-improved experience accessing the organization's 350 internal and 5 external apps.

AFGE's password reset requests, consistently a top issue, had become a real headache for IT as well as employees, who were routinely locked out for at least 20 minutes at a time. In addition to reducing password requests by 80 percent, AFGE was able to reduce connectivity issues and support requests, ease their administrative burden, and integrate Microsoft Office 365 to enhance business productivity and deliver collaboration apps via the cloud.

AFGE

"Internally, we had a lot of different log-ins for numerous systems, and nobody enjoyed the situation. Our public-facing web at AFGE was entirely custom. It didn't give us the ability to integrate with other applications and required a lot of heavy lifting for our internal team."

— Taylor Higley, Director of Information Systems, AFGE

Learn more about the AFGE journey here.

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects organizations to their partners, suppliers and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe, trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Secure, Audited Infrastructure and Processes

AICPA SOC 2 · CSA STAR ATTESTATION · ISO 27001 Certified · ISO 27018 · HIPAA · FedRAMP

For more information, visit us at www.okta.com or follow us on www.okta.com/blog.


okta