GMG ArcData LLC

Zero-Trust Access Management: Privacy-First Passkey Solution for 8,000 Department of State Users

A scalable, mobile-responsive, zero-trust passkey solution for the Department of State, providing secure access for over 8,000 users without storing personally identifiable information.

Call for change

1. Increasing Security Demands in a Complex Environment

With the Department of State managing sensitive information across a global workforce, securing access to digital resources has become a critical priority. Traditional access management systems are vulnerable to breaches and increasingly sophisticated cyberattacks, necessitating a move towards a zero-trust security model. Department users, accessing wellness and other content remotely, require a solution that ensures both security and privacy, safeguarding personal and departmental data against unauthorized access.

2. Privacy Concerns in Wellness Programs

As part of the Department's efforts to promote employee wellness, providing access to wellness content must be done with strict adherence to privacy standards. Users need assurance that their personally identifiable information (PII) will not be collected or exposed. Without a robust solution, the risk of data leaks could undermine trust in the program and limit engagement. This creates a critical need for a system that allows seamless access while preserving user anonymity and privacy.

3. Scalability for a Global User Base

The Department of State supports over 8,000 users, many of whom work in different time zones and environments. A solution that can scale efficiently to accommodate varying usage demands is essential. Traditional systems may struggle to provide this flexibility, leading to potential disruptions in access. The need for a cloud-based, mobile-responsive solution capable of supporting a global workforce is key to ensuring consistent access and user satisfaction.

4. Modernizing Identity and Access Management

As the Department of State adopts more digital tools and services, outdated identity and access management (IAM) systems can create bottlenecks and vulnerabilities. There is a growing need for a modern, automated solution that can manage user access dynamically while meeting security protocols like zero-trust. A passkey-based solution eliminates reliance on traditional passwords, offering stronger protection against breaches and simplifying the user experience.

Modernizing IAM & Addressing Privacy Concerns

GMG ArcData developed and implemented a zero-trust, passkey-based identity and access management (IAM) solution for a Department of State bureau, enabling over 8,000 users to securely access wellness content without compromising their privacy. This mobile-responsive solution eliminates the need for traditional password systems, instead relying on a passkey method that provides users with secure, seamless access to content. By integrating open-source technology and leveraging commercial cloud infrastructure, the solution is designed to automatically scale to meet fluctuating demands while ensuring top-tier security. Importantly, the system does not collect or store personally identifiable information (PII), preserving the privacy of all users.

In line with zero-trust principles, the solution ensures that no user or device is automatically trusted, and all access requests are continuously verified. This approach significantly reduces the risk of unauthorized access or breaches, even in a global workforce environment. The solution is designed for easy integration with existing systems and can be expanded to support additional use cases in the future. By implementing this state-of-the-art passkey solution, GMG ArcData has enabled the Department of State to enhance user privacy, improve security, and offer a scalable, future-proof IAM system.

Making a Difference

GMG ArcData's implementation of the zero-trust passkey solution has made a significant difference for the Department of State by enhancing the security and privacy of over 8,000 users, while simplifying their access to wellness resources. By eliminating the risks associated with traditional password systems and ensuring that personally identifiable information (PII) is never collected or stored, the solution empowers users to engage with wellness content without fear of compromising their privacy. This innovation not only bolsters the Department’s cybersecurity posture but also fosters trust and confidence among employees, enabling them to focus on their health and well-being with peace of mind. Through this forward-thinking approach, GMG ArcData has contributed to creating a safer, more secure digital environment for the Department’s global workforce.

About GMG ArcData LLC

Since its inception in 2019, GMG ArcData, an SBA certified service disabled veteran and minority-owned small, disadvantaged business (SDVOSB), helps government, commercial, and not-for-profit clients accomplish their goals by providing innovative solutions and evidence-based advisory services through applying software engineering, data analytics, first principles-based problem-solving, and user-centered design principles to enhance decision-making, performance, and organizational situational awareness. GMG ArcData is led by hands-on principals with MD, PhD, and PMP and over 65 years of combined experience in the private and public sectors and the military. The company is HIPAA and 42 CFR compliant.