City & County of Denver + Duo

The City & County of Denver deploys Duo to 18,000 users in under three months.

The Organization

The Government of Denver makes up the public sector of the City and County of Denver, Colorado. Denver boasts a population of approximately 750,000 people in a metropolitan area of about 3 million. The city is located at the eastern base of the Rocky Mountains and is the capital of the State of Colorado. Denver's government consists of an elected nonpartisan Mayor and Auditor, and a 13-member City Council. The city has over 30 departments that carry out the day-to-day functions.

"Our deployment of MFA, with multiple authentication options, helped the city achieve a security mindset, a major culture change. The City and County of Denver rolled out MFA to over 18,000 users in less than three months with minimal impact to our IT help desk. Having a simple mobile app option is crucial to higher user adoption."

Paul Kresser
Chief Data Officer

DENVER
THE MILE HIGH CITY

The Organization

The Government of Denver makes up the public sector of the City and County of Denver, Colorado. Denver boasts a population of approximately 750,000 people in a metropolitan area of about 3 million. The city is located at the eastern base of the Rocky Mountains and is the capital of the State of Colorado. Denver's government consists of an elected nonpartisan Mayor and Auditor, and a 13-member City Council. The city has over 30 departments that carry out the day-to-day functions.

- Deployed to 18,000 users in under three months with minimal IT helpdesk tickets
- Easily demonstrate compliance for both PCI-DSS and CJIS requirements
- Minimized risk of a breach by implementing a layer of strong user authentication

The Challenge

The Information Security team at the City and County of Denver manages a hybrid IT environment with many on-premises applications and a growing number of SaaS applications. The organization is in the middle of its digital transformation journey, and recently onboarded a cloud-based ERP application that houses sensitive data. To secure access to corporate applications, the team previously deployed various multi-factor authentication (MFA) tools ranging from traditional hardware tokens to free authenticators. Managing multiple MFA solutions created administrative overhead and an inconsistent end-user authentication experience.

“We maintain large amounts of sensitive and regulated data types and we need to comply with various regulations that require MFA. We had implemented multiple solutions, which created MFA sprawl and we needed to consolidate into a single tool that was easy to manage for IT and simple to use for the wide variety of users we serve,” says Paul Kresser, Chief Data Officer, City and County of Denver.

State and local governments store sensitive citizen data and are increasingly in the crosshairs of cyber criminals. The InfoSec team observed an uptick in phishing attempts that targeted SaaS apps and aimed to steal passwords in order to gain unauthorized access. To address the risk of a breach due to compromised credentials, the team proactively implements a variety of security controls.

“We are constantly under threat of cyberattacks and one of the ways cyber criminals gain access to our networks is by compromising user accounts. We have a layered approach to securing our networks and MFA is a critical layer of our security program,” says Todd Deering, Information Security Architect, City and County of Denver. “When we implement layers of security controls like a spider web, it makes it harder for cyber criminals to be successful. Every layer helps keep the bad guys out of our networks longer and that gives us more time to detect and stop any ongoing attacks. I call it time-based security,” opines Todd.

The Solution

Originally, the team implemented hardware token-based MFA. However, the legacy solution became frustrating to deploy and manage. In response to the growing pain point, the InfoSec team decided to move away from the old MFA and began evaluating top modern MFA solutions.

To choose a new solution, the team looked at two key criteria. The first evaluation criteria was the solution's ability to integrate with a wide variety of systems: SaaS and on-prem applications, SSH, Unix boxes, RDP and Windows devices. The second criteria was to provide a consistent user experience for secure access that was easy for all users from technology workers and administrative staff to law enforcement officers in the field.

The team chose Duo for its ease of use and speed to security. Duo easily integrated with critical applications and demonstrated that the solution could be deployed and rolled out across multiple departments at a rapid pace. And, Duo's flexible authentication options catered to every user. "Having a mobile app that is simple to install and use is reflected by high user adoption," says Paul. "Most of our users authenticate using the push notification. If this option does not work for certain users, we have the flexibility to use FIDO security keys to ensure strong authentication," says Todd.

Accelerated Deployment and Successful User Adoption

An uptick in phishing attempts and the push to remote work meant the InfoSec team had to deploy Duo at an accelerated pace. Duo's extensive documentation on the website, the lift-off guide and expert guidance from Duo Care made it easy for the team to support IT administrators as they rolled out protection for various applications. The team phased the Duo MFA deployment by application, starting with critical applications such as Workday, VPN and Microsoft ADFS.

The team chose to allow users to self-enroll into Duo MFA. "Initially we had concerns around user adoption and help desk overhead. But the rollout was smooth, and we did not receive any significant pushback," says Paul.

To ensure that users adopted the new solution, the team partnered with the HR communications team and ran targeted email campaigns for specific applications. The team leveraged Duo's end-user email communication templates that detail step-by-step enrollment instructions. This helped to successfully rollout Duo MFA to over 18,000 users within three months, which resulted in less than 100 help desk tickets. "Asking users to download a mobile app on their phone for MFA required a culture change and adopting a security mind-set. Additionally, a mobile app that is intuitive translates to faster adoption across the organization." says Paul.

Unique Requirements: Offline Authentication and Compliance

The InfoSec team caters to over 30 lines of businesses and many departments have unique requirements such as:

1. Officers in the Sheriff's department and the staff at the District Attorney's office are not allowed to carry cell phones in jails or court. And internet connectivity is not available at these locations. The team tested and deployed Duo's offline authentication using YubiKeys for Windows machines, enabling users to login to their workstations even when there is no network connectivity.
2. Law enforcement officers and first responders need compliant access to criminal justice information (CJI) while certain administrative users require compliant access to payment card information (PCI) environments. By deploying Duo MFA, the team could easily meet the requirements for both CJIS and PCI-DSS while keeping the access experience consistent for a wide variety of users and applications.

Balancing Security and Productivity

When policies get obtrusive, productivity takes a hit and users often try to circumvent security controls. The InfoSec team analyzes data from Duo's comprehensive authentication logs to identify access trends in their environment. The insights gained from this information help the team make productivity and security decisions, and avoid bad security behavior. Todd's team monitors metrics such as the frequency of MFA challenges per job role. This data is helpful to understand whether the user population experiences MFA fatigue, and fine tune the policies in order to balance security and productivity.

Looking Ahead: A Shared Zero Trust Vision

The City and County of Denver has started on this journey towards zero trust security with Duo. The InfoSec team plans to balance security and productivity by implementing MFA for every single application while ensuring this does not result in "MFA fatigue" for their users. The team also plans to rollout the Duo client for local authentication on every Windows machine.