

CASE STUDY

**AFGE Automates MFA
Challenges With
Help From Twosense**





“

MFA is something everyone loves to hate, but it's necessary and people get it," he said. "With **Twosense** we are able to make that necessary evil a little less evil."

-Taylor Higley,
Director Information
Systems

A SECTION

Introduction

The American Federation of Government Employees (AFGE) is the largest federal employee union and represents 700,000 federal and D.C. government workers nationwide and overseas. With full IT responsibility for over 300,000 members and 400+ employees, keeping private information secure is essential. As early adopters of two-factor authentication, AFGE implemented 2FA everywhere from desktops to SaaS applications. However, with the adoption of that 2FA policy, challenges emerged and there was a realization that the number of prompts has a real financial and productivity cost. Taylor Higley, Director of Information Services decided that it was in the organization's best interest to begin looking for a more agile and scalable IT infrastructure to best serve its users.



CONTINUOUS AUTHENTICATION IS BIOMETRIC!

Continuous authentication is **private**, we do not store any PII. We don't even need to know what the user is doing, just how they're doing it.



OVERVIEW

With the specific goal of finding a smarter way to implement identity security, AFGE began discussing how continuous authentication would solve their problem. Intrigued by Twosense's passive biometric approach to identity automation, AFGE reached out after seeing Twosense on the Okta Integrated Network (OIN).

Higley said, "Twosense stepped in at just the right time with everyone working remotely and was able to help AFGE implement more secure multi-factor authentication policies without sacrificing the user experience."

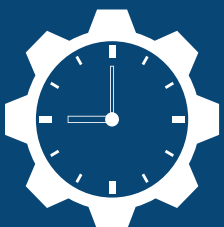
Better Security & Better Experience!



SECTION

The Story of AFGE

When it came to identity, AFGE originally had a traditional on-premise infrastructure. Password reset requests, one of their top 10 issues, became a real headache for IT and employees who were routinely locked out for at least 20 minutes at a time. As a result of highly frustrating and complex identity security issues, AFGE began the transition from Microsoft Active Directory Federated Services (ADFS) to Okta. What differentiated Okta was the ability to contact support and get quality help when needed. Okta provided AFGE with an on-demand identity and access management service. However, even after implementing Okta, MFA difficulties remained.



The true cost of employee interruptions

On average, employees lose 18.96 hours per year to IT security procedures, and that does not take into consideration the roughly 15 seconds per MFA check completed successfully. Twosense automates the challenge-response of multi-factor authentication on behalf of its users by using machine learning to drive passive biometrics that can guarantee a user's identity.



SECTION

The Better Way To Engage MFA

GET INTO A FLOW

Recent studies indicate that it can take roughly 30 minutes of uninterrupted focus on a task in order to achieve a state of flow, and once in a flow subjects saw a significant increase in productivity.

However, when a flow state is interrupted it can take on average 25 minutes to get back into the original task, plus up to an additional 30 minutes to regain the flow state so they can be fully productive again. This poses a significant challenge to teams that are required to complete multiple MFA challenges throughout the course of their day.

NEXT STEP

Before implementing Twosense, AFGE already had strict multi-factor policies in place. Users were prompted to complete a multi-factor challenge each time they stepped away from their workstation, which could be ten times a day. Every Okta-protected application also required a multi-factor check.

To address employee frustrations with repeated MFA challenges, Twosense was implemented as a layer between AFGE's existing SSO and MFA solutions. By using machine learning to drive passive biometrics, Twosense was able to automate MFA challenges and guarantee each user's identity continuously throughout the day. This continuous authentication process responded to 78% of MFA challenges across AFGE's entire user base, resulting in significantly fewer interruptions throughout the day and increased productivity.

When asked about the result of implementation, Higley said "People are getting significantly fewer prompts." While he can monitor the number of MFA challenges automated and time saved in the Twosense dashboard, he hasn't needed to communicate them beyond the IT department.

"Employees across the organization all the way up to the Board of Directors have noticed fewer MFA challenges, and that's incredibly valuable."

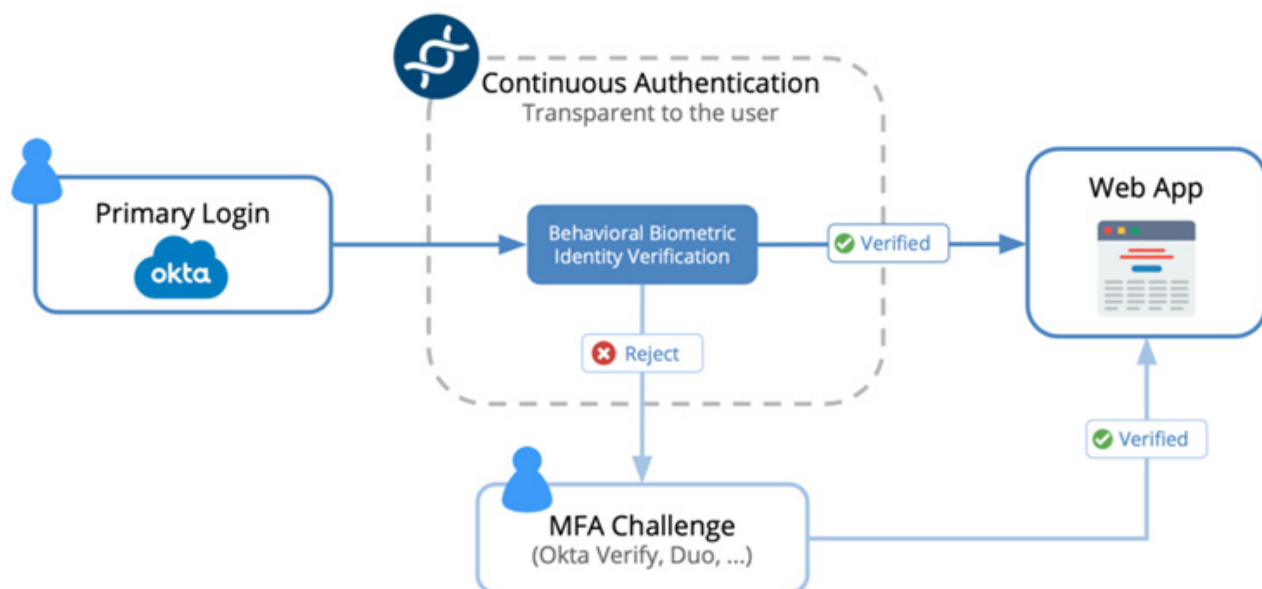




SECTION

Why AFGE Chose Twosense

AFGE wanted a solution that would easily slot into their pre-existing SSO and MFA security infrastructure, and ease MFA pain without any reduction in security posture. Twosense software is part of the OIN and designed to work with Okta, making it easy to implement same day. AFGE only needed to deploy the Twosense Chrome extension to managed devices via group policy to start seeing results. The entire process took less than 30 minutes.



Deployment

Once deployed, the Twosense browser extension continuously monitored AFGE users' behavior such as keystrokes and mouse movement and synchronized with the cloud to continuously update each user's trust score.

Automation

Each time a user attempted to access an SSO-protected application, Okta requested verification from Twosense. If the user was verified, Okta granted access. Otherwise, Okta fell back to the default MFA settings before granting access.

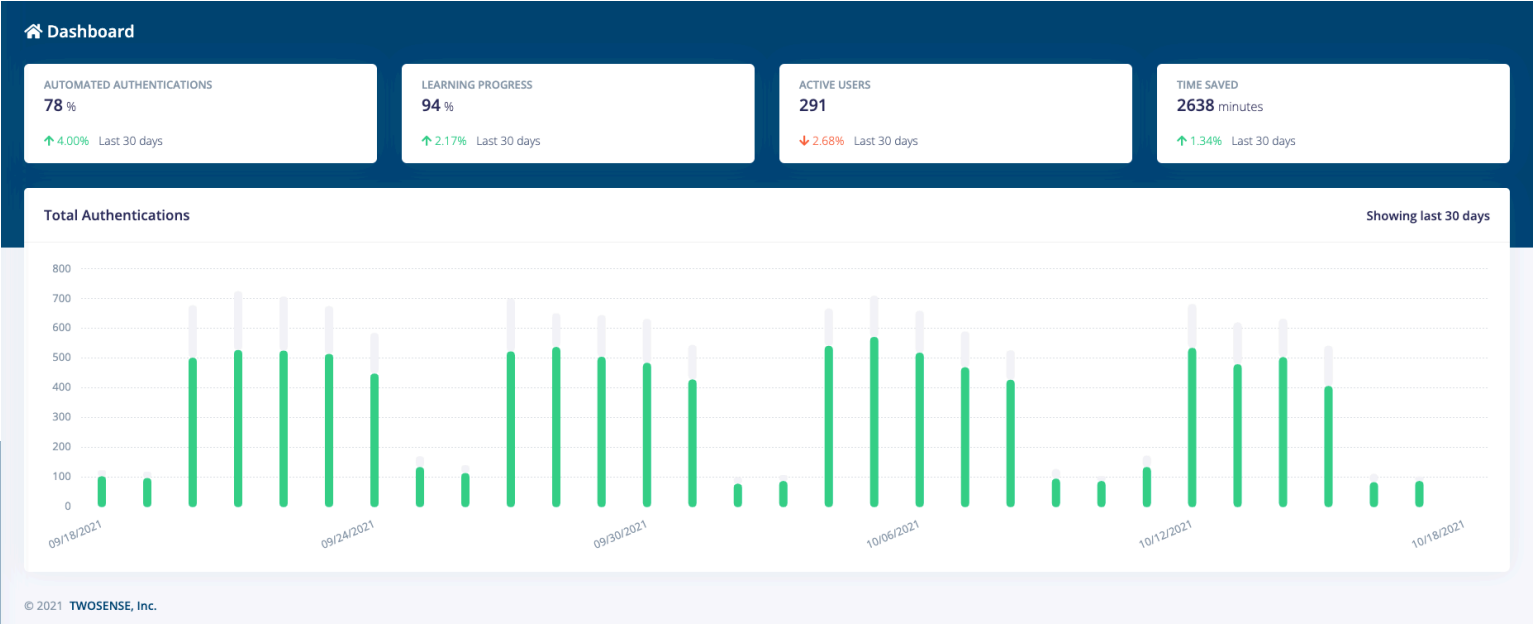


SECTION

The Twosense Effect



The decision to implement Twosense software into AFGE’s security practice resulted in improved productivity due to a decrease in interruptions. According to internal data, AFGE began to quickly see the impact of the Twosense software:



Solution

Device-free MFA led to fewer helpdesk tickets and allowed the IT department to focus its efforts on other important projects while reducing costs. Strict MFA policies also helped to prevent threats of spear phishing, account takeovers, and malicious remote access.

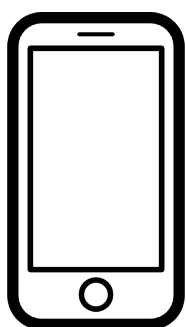
Next Step



When asked about how Twosense software has helped AFGE manage the transition to working remotely, Higley said “Twosense software has been especially helpful for the roughly 200 people that were working on-site who rarely if ever got the Okta MFA prompt. Now, all of a sudden while working remotely they were getting them while working from home or when using a new browser. Twosense was able to ease some of that pain.”

78% ↑

OF MFA CHALLENGES ACROSS
THE ENTIRE ORGANIZATION
HAVE BEEN AUTOMATED.



10,740 ↑

TOTAL AUTHENTICATION
CHALLENGES WERE
AUTOMATED EACH MONTH



2,685 ↑

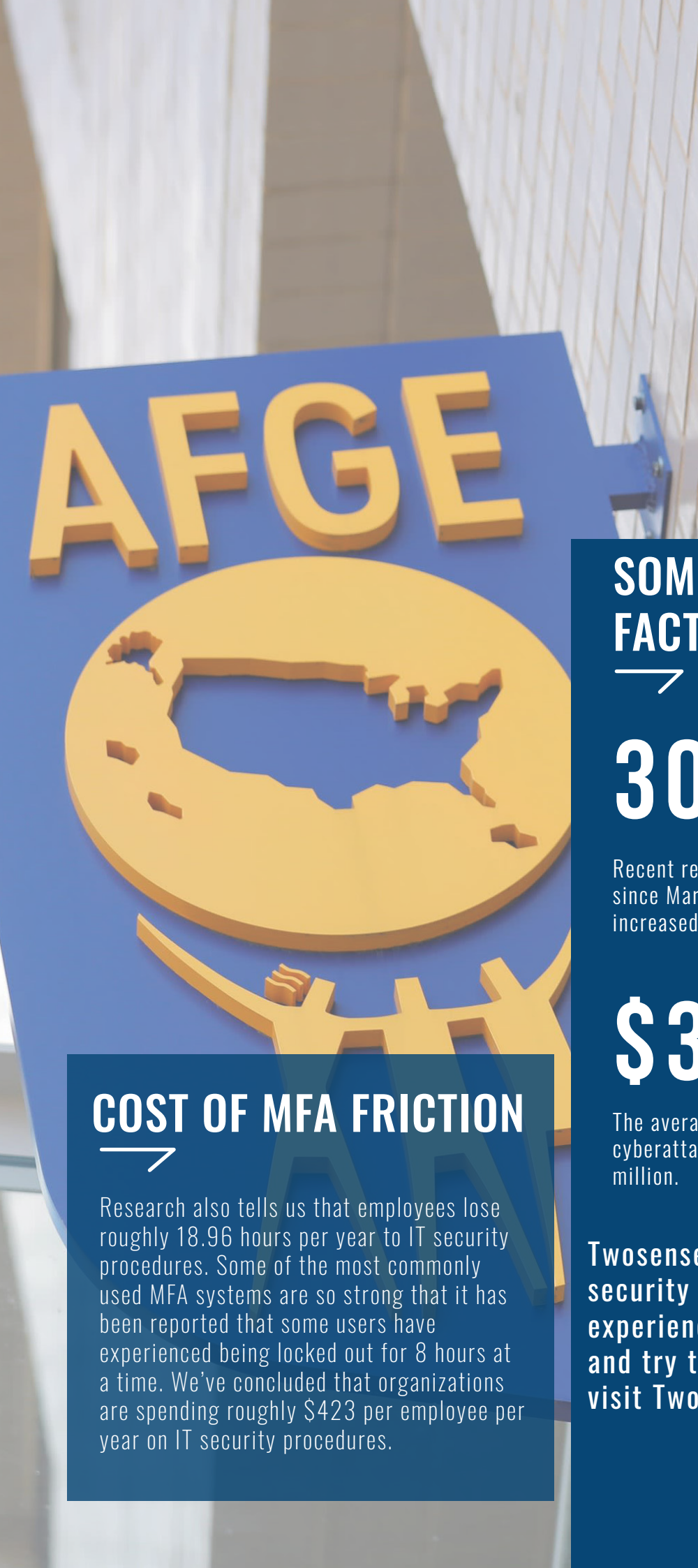
MINUTES SAVED EACH
MONTH



28% ↑

OF ONE FULL TIME
EQUIVALENT



The background of the slide features a large, blue AFGE logo. The letters 'AFGE' are in a bold, yellow, sans-serif font. Below the letters is a yellow circular emblem containing a white outline map of the United States. The entire logo is set against a background of a modern building with a glass facade and white structural elements.

55%

of organizations use MFA. This number continues to rise yearly.

However, implementing MFA with relaxed security policies does not provide the security most CISO and IT Managers know they need.

SOME INTERESTING FACTS



300%

Recent reports from the FBI show that since March of 2020, cyberattacks have increased by 300%,

\$3.86M

The average business cost of a cyberattack sitting at roughly \$3.86 million.

COST OF MFA FRICTION



Research also tells us that employees lose roughly 18.96 hours per year to IT security procedures. Some of the most commonly used MFA systems are so strong that it has been reported that some users have experienced being locked out for 8 hours at a time. We've concluded that organizations are spending roughly \$423 per employee per year on IT security procedures.

Twosense provides both better security and a better user experience. To schedule your demo and try the product for free please visit Twosense.ai.