THE COST OF
MFA FRICTION
WHITEPAPER

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, AFGE

A BETTER WAY TO MFA

Since March 2020, cyberattacks against work-from-home employees have increased by 667%, with most successful attacks coming from compromised user identities, not software. In the era of COVID-19, work from home has become commonplace, with very little indication that teams will be returning to office spaces full-time.

While there are indisputable benefits to remote work, having a distributed team increases vulnerability to cyberattacks, and bridging that gap means adding additional friction to already frazzled employees. As a result, organizations around the world are taking a critical look at their security infrastructure to find ways to increase their protection without making the user experience intolerable.

SECURITY VS USER EXPERIENCE

As cybersecurity continues to rapidly evolve, companies are faced with critical decisions regarding the state of their security posture. Over the last year, Twosense has conducted hundreds of customer interviews with the sole purpose of solving the fundamental problems associated with MFA. Twosense has created a solution that removes the human variable from identity security and acts as a layer that can be deployed into any infrastructure.

This software works on the user's behalf to run continuous authentication via passive biometrics. This means companies don't have to ditch pre-existing systems because Twosense works with what is already in place to increase the overall effectiveness, without negatively impacting the user's experience. This means fewer interruptions, higher productivity because of happier employees, and significantly reduced IT costs.

MFA FRICTION: THE NUMBERS

IT departments and cybersecurity experts have long struggled with a dilemma; the more security procedures they put in place, the worse the user experience. The better the user experience, the more vulnerable an organization becomes. This balancing act means that compromises must be made on one side or the other.

MFA policies are a prime example; when organizations implement stricter MFA policies, the user experience is the first thing to suffer. Multifactor authentication is the most potent tool a security team has to prevent credential-based attacks, and it is unacceptable that fear of excessive MFA friction has caused organizations around the world to loosen their security policies and remain vulnerable to breaches.

The "MFA friction" IT departments are trying to avoid is easy to quantify in terms of time and money wasted. Research tells us that employees lose roughly 18.96 hours per year to IT security procedures. The most commonly used MFA systems can be configured so strictly that some users have reported being locked out for 8 hours at a time. Even a successful MFA check takes an average of 15 seconds to complete. That number may seem small, but some users are required to confirm their identity 20+ times each day. The total amount of time wasted by these challenges across all users in an organization can be shocking. All told, organizations are spending roughly $423 per employee per year on IT security procedures."

With more secure MFA policies, there is also a measurable increase in helpdesk tickets, of which 40% are related to authentication. While it can vary, the average IT Help Desk Ticket Call costs $15.56 per call. For many organizations, up to 8.4 calls a day are related to authentication challenges. These authentication challenge based IT Help Desk Tickets calls can end up costing $130 per year per employee.

When you take all of these factors into account, you can see that the average organization is experiencing a significant increase in security costs to the tune of $553 per employee per year.

Curious to find out how much Twosense can save you? Take $533, which is the total dollars per year, per employee lost to IT security procedures and dollars per year, per employee for IT Help Desk Tickets related to authentication and multiply by the total number of employee's!

THE COST OF INTERRUPTIONS

In addition to the time and money wasted, there are abstract costs to constantly interrupting employees. Cal Newport's book Deep Work goes into detail about the need to remove interruptions from knowledge workers' days. He defines deep work as "professional activities performed in a state of distraction-free concentration that push your cognitive capabilities to their limit. These efforts create new value, improve your skill, and are hard to replicate." This state is also known as "flow" and was popularized by the well-known psychologist Mihaly Csikszentmihalyi in the 1970s. He described it as "stretching your mind to its limits, concentrating, and losing yourself in an activity." One of the distinguishing characteristics of flow is that it's accessible to everyone, and should be a priority for IT management across the industry.

Flow state has been shown to increase productivity by an astonishing 500%, but it is as fragile as it is powerful. Studies indicate that it can take roughly 30 minutes of uninterrupted focus on a task in order to achieve a state of flow, and when interrupted 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.

Giving employees the freedom to work more deeply also has a distinct effect on employee happiness: the more flow experiences that occur in a given week, the higher the subject's life satisfaction. As Cal Newport says in Deep work, "Human beings, it seems, are at their best when immersed deeply in something challenging."

Gallup's Employee Engagement surveys also provide compelling reasons for organizations to prioritize the happiness of their staff. Organizations with engaged employees experience a variety of benefits:

- Up to 43% less turnover
- 10% higher customer loyalty
- 23% higher profitability
- 18% higher productivity
- 81% less absenteeism

With security controls being reported as one of the biggest contributors to job satisfaction and with employee turnover at an all-time high in 2021, organizations simply cannot afford to interrupt their employees throughout the day.

TWOSENSE INTRODUCTION

Twosense has created a solution that empowers organizations to do what was previously impossible: increase MFA security while also automating the challenge response to preserve user experience and productivity.

The fundamental pillar of the software is passive biometrics: the collection of behaviors or characteristics that are intrinsically part of who someone is. Passive biometrics are distinct from traditional biometrics like fingerprint scanners in that no participation is required by the user. The collection of biometric data is both completely invisible to the user and continuous throughout the day. This approach is also more secure; passwords can be stolen, tokens phished, but behaviors cannot be fabricated.

The biometric data is passed into a cloud-based machine learning system that builds a model of each user's behavior. Whenever a user passes an MFA challenge, each model continues to learn and adapt to changing behaviors. When the model is mature, Twosense can validate the user's identity and create a baseline of trust.

When the user's identity can be guaranteed via passive biometrics, the challenge-response of MFA can be automated behind the scenes. From the user's perspective, MFA interruptions have almost completely disappeared.

It's important to note that the multifactor challenge is not being skipped, it is happening continuously throughout the day. From a compliance standpoint, the user is still confirming their identity just as if they had scanned their retina or fingerprint. This is in stark contrast to "adaptive MFA" policies that completely skip multifactor authentication if the user or target system meets certain criteria.

DEPLOYMENT MADE EASY

The application of this solution is simple and effective.

Twosense can be deployed as either a browser extension (Chrome and Edge) or as a Windows agent. In either case, any organization with managed devices can roll out the solution to whatever users they intend to onboard with minimal time and effort. The only remaining steps are to add Twosense as a multifactor option in a Single Sign On (SSO) solution like Okta or Onelogin, then apply that factor to a policy containing users.

From that point, no other actions are required. Users do not need to install a mobile app. They do not need to enroll in the solution. No training is required; users are only expected to continue behaving as they have been. No active management of the software is required, which means that there is no need to hire dedicated staff and no additional workload added to existing IT or Security staff.

THE TWOSENSE EFFECT

Within two weeks, most users will see 95% of MFA challenges automated; a Twosense logo will appear briefly, then they'll be logged into the correct app. For some users, this can mean the difference between 20 interruptions a day and zero. Without the need to open their phone every time they want to access an application, users can get their work done more quickly and efficiently. With the ability to get in a flow state, employees accomplish even more and are happier with their jobs.

Administrators benefit, too: in addition to automating the MFA challenges out of their own workdays, they can log into the Twosense dashboard to easily report progress on percentage of MFA challenges automated and total time saved to stakeholders. Without the need to compromise between security and user experience, security administrators can also implement stricter MFA policies to improve their organization's cybersecurity posture to prevent threats of spear phishing, account takeovers, and malicious remote access.

A FRICTIONLESS FUTURE

The fundamental problem with identity security is that the user is responsible for interacting with security infrastructure to prove that they are in fact an authorized user. This leaves significant room for human error; recent studies show that roughly 24% or ¼ of data breaches are attributed to human mistakes. MFA is just as susceptible to human error as any other security procedure. This can occur in a variety of ways: laptops being left in taxis, smartphones being forgotten on a restaurant table, or misplaced hardware tokens, all of which can lead to data breaches. Some users even reflexively approve MFA challenges out of habit and end up granting access to attackers.

Twosense's approach to reducing MFA friction removes the user from the process completely. We firmly believe that continuous authentication is the future of cybersecurity. Automating the challenge-response of identity is the first step towards the goal of creating a world where all identity security is invisible to the user and free of human error.

Thanks to machine learning and AI, identity management will become significantly more secure, allowing for much stricter policies without impacting the user's experience at all. That means procedures such as retinal scans, fingerprint scans, or facial recognition will be a thing of the past.

RESULTS

Organizations that implement Twosense MFA automation can finally have both the security policies they know they need and a user experience that keeps employees happy and productive. Time is saved when users don't have to check their phones repeatedly throughout the day, helpdesk tickets are avoided, and users can engage in "deep work" that comes from an interruption-free environment.

Users don't need to be trained or onboarded, and IT departments don't need to spend weeks or even days on implementation. With MFA both maximally secure and invisible to users, they can move on to the next big project.

ABOUT TWOSENSE

Twosense automates the challenge-response of multi-factor authentication on behalf of its users so they can avoid frustrating interruptions. This allows IT departments to implement stricter and more secure MFA policies without sacrificing the user experience. Developed in partnership with the US Department of Defense, Twosense uses machine learning to drive passive biometrics that can guarantee a user's identity continuously throughout the day.

To Learn More Visist www.twosense.ai

415 Madison Ave, 4th Floor,
New York, New York 10017, US

info@twosense.ai
www.twosense.ai