typingdna

# Working from home

## The new reality

The current COVID-19 pandemic has brought a significant shift in the traditional office settings, highlighting the need for better workforce management, security, and agile implementations — ushering in changes across facets of the organization.

To adapt to the new normal, many companies will follow major players such as Twitter, Shopify, and Facebook, announcing plans to make remote work a permanent option. This marks the beginning of a new era that will reshape organizational structures, with leaders racing to embrace change and improve remote interactions. Despite working from home, giving employees secure access to corporate assets and resources remains critical, as does ensuring they produce at optimal levels.

> *"91% of HR leaders (all in Asia/Pacific) indicated that they have implemented 'work from home' arrangements since the outbreak, but the biggest challenge stems from the lack of technology infrastructure and lack of comfort with new ways of working." - Gartner*
>
> *Google reported 18 million phishing and malware scams related to COVID-19 every single day.*

## A remote workforce requires enhanced security

During the pandemic, more and more employees were forced to work from home. In turn, security has now become the backbone of corporate success. For instance, Google reported 18 million phishing and malware scams related to COVID-19 take place every single day.

Since the beginning of the pandemic, cyberattacks have increased — particularly in the banking and financial sectors. A ransomware attack forced the world's third-largest fintech provider to put servers offline and investigate a cybercrime that allegedly made millions of dollars in wire transfers vanish. The ransomware action was deliberately orchestrated while the corporation migrated thousands of employees to a work-from-home setup.

The Federal Deposit Insurance Corporation (FDIC) identified scams targeting the pandemic, with cybercriminals deliberately sowing distrust in the banking system. This, in turn, caused people to withdraw large sums of money from their accounts, bringing a severe hit to the banking system.

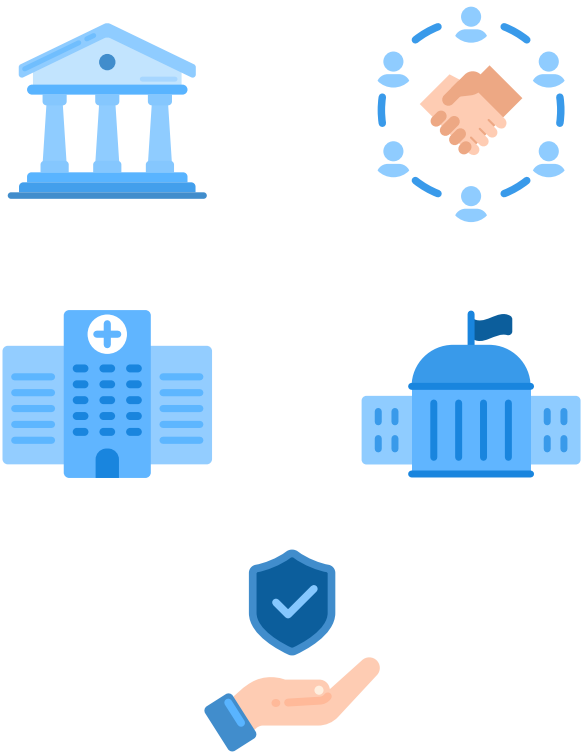
Today, 80% of data breaches are linked to weak or reused passwords. This is a clear indicator that strong security will always go beyond a single point of vulnerability with MFA. Additionally, 34% of respondents said they share passwords or accounts with their coworkers. Primarily, this is due to their desire to improve collaboration. According to the data, one out of every three American workers may be sharing passwords — leaving organizations unable to determine who can access company assets.

## Highly affected industries

Remote work is now a requirement in many industries. Many of them were forced to implement a work-from-home policy for the first time in 2020. Looking ahead, sectors that handle critical client information face the biggest challenges of protecting vulnerable data from prying eyes or leaks.

Globally, bank staff that is working from home is at risk. Cybercriminals are on the lookout for sensitive data that will help them breach an enterprise's network.

As such, security and risk management (SRM) leaders — especially **in highly sensitive industries such as banking, financial institutions, insurance, health care, BPO, and government** — have the critical mission to enhance remote access security with MFA and state-of-the-art access management to combat existing threats.



### Attack vectors in a remote workforce scenario

**Employee endpoint devices** may be vulnerable as some employees share devices with other household members or work on their own personal devices. IT departments will not directly maintain the laptops, desktop PCs, and other devices that remote workers use, further complicating the matter.

Data leaks or interception often occur on unprotected networks. This risk is augmented by remote employees using unsecured or **vulnerable WiFi networks** — e.g., home WiFi networks with weak passwords. To illustrate, the Mirai botnet, one famous attack, infected millions of vulnerable home network devices then used to launch a massive DDoS attack.

**Insider threats** originating from within the organization involve a current or former employee or associate who has access to sensitive information or privileged accounts within an internal network and who misuses that access. Some examples of insider threats include malicious insider, careless insider, and privileged account takeover — all of which are able to compromise a company's network.

## Challenges in securing remote workforce access

### Security hardware tokens

With a distributed large workforce, it's hard to deploy hardware tokens due to significant costs associated with shipping and lost devices. A remote workforce security policy requires IT departments to implement all changes from a distance, preventing them from setting up hardware devices and managing them.

### MFA with SMS OTP

SMS OTP has been a security alternative, though its flaws have been revealed in various circumstances. Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts has proven that SMS and mobile authenticators helped block 76% of targeted attacks.

SMS OTP is still regarded as one of the successful options to integrate into an MFA solution. Nevertheless, large corporations are dependent on their current hardware infrastructure. The need to use a smartphone for mobile push notifications can be problematic when users don't have corporate phones. As much as 15% of the North American workforce might not be willing to use their personal phones for work purposes. This makes the traditional SMS OTP codes to log in into corporate accounts an expensive solution due to lacking the needed infrastructure.

### Touch biometrics via smart devices

This behavioral biometrics authentication technology has become more and more popular over the last few years, popularized by the high adoption of touchscreens in smart devices. In case you're unfamiliar, touch biometrics is a passwordless solution used as an authentication method. The swiping behavior can provide an EER—or the threshold level between False Acceptance Rate (FAR) and False Rejection Rate (FRR) ranging from 4% to 0.4%. Still, smart devices bring challenges in a distributed workforce set up, requiring a corporate device that, in many cases, needs to be acquired, shipped, and set up—each step associated with high costs.

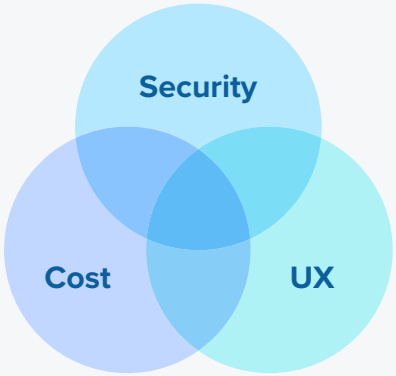
> *Through 2021, enterprises that rapidly expand remote access without implementing MFA will experience five times as many ATO incidents as those that use MFA.* Gartner

### MFA considerations - Easy to adopt and deploy

The ideal MFA solution offers flexible controls, scalability as the business grows, out-of-the-box configuration, and a seamless user experience for employees. The challenges among classic MFA solutions vary depending on the organizational setups. Adding MFA — a simple upgrade that works off-the-shelf with your VPN, ZTNA, or CASB of choice — can exponentially increase both the remote workforce's security and productivity.

A survey conducted in June 2020 with participants employed in 17 different countries revealed that 65% of organizations had VPN solutions in place pre-pandemic, but only 37% had MFA.

An MFA authentication flow should be customizable based on the company's needs and integrate with cloud-based software and premises, all while enabling successful user adoption. A detailed list of critical MFA deployment factors to consider can be found here.




## MFA with typing biometrics

By being easy to deploy and adopt, typing biometrics in an MFA solution answers the above requirements. Recent technological improvements have allowed the development of algorithms to learn how people interact with a device. Typing biometrics, or capturing the way people type on their keyboards, is a newly emerging technology facilitated by AI progress and computational power. Every individual has a unique typing pattern — meaning it's possible to identify people based on the way they type.

As part of the typing biometrics authentication process, the initial enrollment consists of capturing the typing pattern and attributing it to the user. Every time a new authentication is made, the stored hashed pattern is verified against the initial one. Once it's matched in the background, the user is logged in. Combined with other factors, an MFA implementation with typing biometrics helps organizations avoid drawbacks — such as costly tokens or user experience disruption.

## Three steps to an authentication


### Enrollment

When new users sign up for your service or turn on the 2FA, we record the typing pattern and build the user profile.

### Verification

When they try to authenticate, we record the typing pattern again and match it to the user profile.

### Access

The right users are authenticated and can further ineract with your service while you are confident in their identity.

When adding typing biometrics to other authentication factors such as email OTP, the result is a robust and stealth account protection that can be implemented on many levels and further be part of a risk-based authentication (RBA) system. Unlike fingerprint or iris scans, typing biometrics has proven challenging to reproduce. Also, major drawbacks such as long log-in times or cumbersome user experience can be avoided by implementing typing biometrics in a multi-factor authentication system.

TypingDNA's cloud-based technology is available via an API that lets companies easily integrate it into any IAM system and fine-tune it to meet their unique requirements. It's the easiest way to protect your company's most sensitive assets while your team is working from home throughout the world.

# About TypingDNA

TypingDNA is a behavioural biometrics company based out of New York City. We specialize in providing keystroke dynamics technology (also known as typing biometrics) in order to recognize users based on the way they type.

This AI-based technology makes it easier to prevent fraudulent activity, such as account takeovers, in a non-obtrusive way that doesn't require any special equipment. TypingDNA works with financial, retail, and educational organizations around the world, and is backed by VCs like Gradient Ventures (Google's AI Venture Fund) and Techstars.


**contact@typingdna.com**

**typingdna.com**

**@typingdna**

**@typingdna**


typingdna