VERIDIUM
TRUSTED DIGITAL IDENTITY

10 REASONS WHY YOU SHOULD **GO PASSWORDLESS NOW**

"COVID-19 has amplified the awareness and use across the world of passwordless authentication technologies for remote access."

Ismet Geri, CEO, Veridium

White Paper

WHAT IS WRONG WITH PASSWORDS?

In the working world, we all struggle with productivity. This is why it's especially frustrating as a digital user to lose valuable time every day (many times per day!) on activities whose sole purpose is simply to give us access to the systems and applications we are required to use to do our jobs – from logging on to workstations and web applications, to communication tools and VPNs, etc.

What's more, most environments and applications require passwords – different passwords – that must be regularly changed with ever-growing levels of complexity. Having to remember a single password is difficult, multiple passwords impossible. As digital users, we waste time on a regular basis on self-administered password resets or helpdesk calls because we managed to get ourselves locked out. It's frustrating and time-consuming, not to mention expensive (on top of lost productivity).

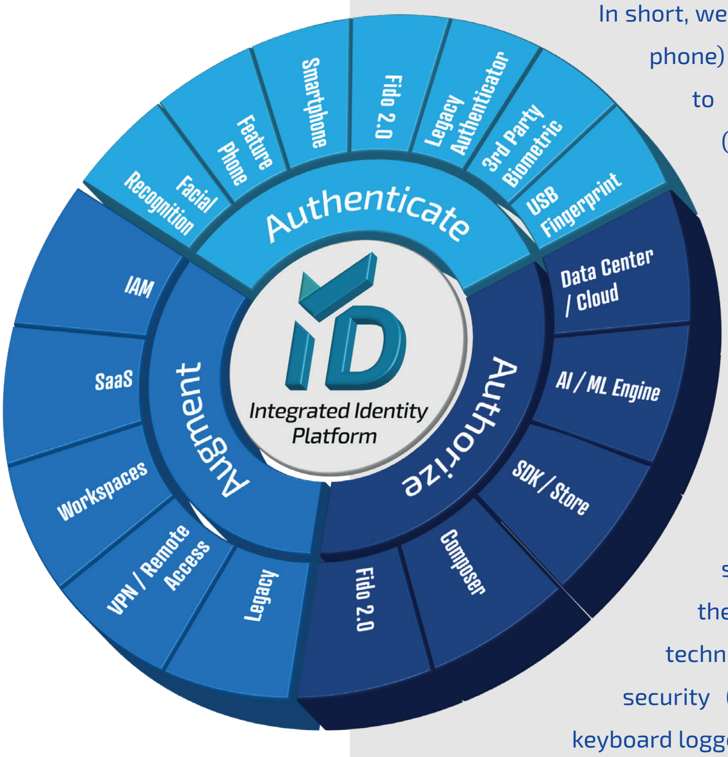
Believe it or not, the Security and IT teams are frustrated too. Often on a shoestring budget and with too few personnel, they are charged with the thankless task of ensuring security in an ever-evolving digital ecosystem, including "zero trust" architectures, made worse by passwords. As a result, they require password complexity, make us change passwords periodically (typically every 30-45 days), and add 2-factor authentication (2FA) or 2-step verification or both into the organization's IT stack.

At Veridium, we recognize that passwords create a huge challenge to both end users and Security and IT teams. In short, they are inconvenient, costly, and insecure (so much so that organizations must add more and more technologies to increase the security around passwords to achieve "strong authentication").

WHAT DOES STRONG AUTHENTICATION LOOK LIKE TODAY?

For most organizations, strong authentication takes the form of time-based one-time password (TOTP) technologies. This is often a hardware token, a soft token (delivered via a mobile app), or "on-demand" (via an SMS). In the soft token world, strong authentication means a password (something you know) plus something you have as the second factor (your mobile phone) – and, ideally, an additional security layer related to the second factor (your smartphone PIN code) (something you know, but technically not an authentication factor in and of itself). TOTP technologies are expensive and cumbersome for organizations to implement and maintain and for end users to use. Plus, they still carry security risks.

We've seen over the years (in smartphones) the adoption of built-in biometric sensors: fingerprint and facial (even iris) recognition. This means that our biometrics can be used to open our smartphone as an alternative to our PINs for a simple device access UX with a level of security. (It's difficult for bad actors to fake our fingerprints or faces to unlock our phones.)



At Veridium, we extend the use of built-in biometrics even further. In short, we take the one device you always have (your mobile phone) and use the biometric capability that's built-in to deliver passwordless multifactor authentication (MFA) for any application that uses challenge-response authentication – be it a desktop app, a WEB app, or a mobile app.

By definition, Veridium's passwordless MFA solution provides strong authentication; in our case, the authentication factors are the mobile phone ("have") and the biometric ("are"), bolstered with device behavior (context-based analytics) and behavioral biometrics ("are"). Our solution can remove from the IT budget not only the cost of password management, but also the TOTP technologies. All this while improving UX and increasing security (e.g., by eliminating phishing, brute force, and keyboard logger attacks) and increasing productivity.

WHY SHOULD WE GO PASSWORDLESS NOW?

Password vulnerabilities make organizations prone to many types of cyberattacks, which are increasing in frequency, ingenuity, and danger – and costly. In fact, studies have shown that:

80% of global organizations experienced data breaches in 2020 (with $4m being the average cost of a breach)

75% of global organizations experienced phishing attacks

85% of breaches involved a human element

- 61% involved compromised credentials
- 10% showed traces of ransomware, more than double the frequency from last year

10 REASONS TO GO PASSWORDLESS

*Having worked with organizations around the world, Veridium has identified the following **Top 10 Reasons To Go Passwordless** to counter the hydra-headed password problem:*

1. **ENHANCED IT SECURITY:** Passwords are the major attack vector to gain access to systems and data. Removing passwords removes many types of attack vulnerabilities.
2. **GREATER FINANCIAL SECURITY:** The probability of future data breaches is greatly reduced – which means reduced risks of fines, ransomware, lost revenues, and other types of loss.
3. **INTELLIGENT AUTHENTICATION:** Fraud is a massive problem - thus the growing need to have a high degree of certainty of the user's identity. Intelligent and behavior-aware digital authentication is a must have for any passwordless MFA solution.
4. **EASIER COMPLIANCE WITH LAWS AND REGULATIONS:** Different data protection and security rules across the world and in different industries exist and are growing. Going passwordless across all your systems makes it much easier to comply with the different standards.
5. **IMPROVED USER EXPERIENCE:** Users aren't required to remember complicated passwords or periodically renew their passwords (or comply with various other password-specific security policies), nor utilize cumbersome, legacy OTP security tokens.
6. **SCALABILITY:** Works with any application, desktop, WEB or mobile; there's no need to manage multiple logins so users can be given access to more systems as needed, without additional password fatigue or complicated registrations.
7. **THE HYBRID WORKPLACE IS ENABLED:** Employees can easily switch between the systems and data they need whether in the office, on the go, or at home - i.e., passwordless MFA facilitates a secure WFX organization.
8. **REDUCED HARDWARE COSTS:** There's no longer the need to purchase security devices such as smart cards and tokens for your workforce and customers.
9. **REDUCED SUPPORT COSTS:** The help desk can focus on more important things than resetting user passwords over and over again.
10. **SIMPLIFIED POLICIES:** It is not necessary to establish, maintain, and enforce complex password rules and policies.

Let's dig a little deeper into each topic to understand the issues and showcase the solutions to improve your own cybersecurity.

1. ENHANCED IT SECURITY

Your systems and data are increasingly under cyberattack. Recent surveys from the UK Government and Verizon show that relying on outdated password security measures for protection puts your organization, your workforce, and your customers at serious risk. In short, your data, systems, revenue, and reputation – all – are in danger.

The UK Government's ***Cyber Security Breaches Survey 2021*** discovered:

"Four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses (65%), large businesses (64%) and high-income charities (51%)."

Passwords are the major attack vector to gain access to systems and data. Removing passwords removes numerous vulnerabilities:

61% **of breaches involved credentials**

85% **of breaches involved a human element**

Source: ***Verizon 2021 Data Breach Investigations Report***

The Verizon 2021 Data Breach Investigations Report reveals that "financially motivated attacks continue to be the most common, likewise, actors categorized as Organized Crime continue to be number one."

Veridium improves security for organizations by addressing the password problem head-on: by removing passwords altogether. By eliminating the use of knowledge-based authentication, our solution means:

- **Users cannot share credentials**
- **Phishing attacks cannot capture passwords (since they are not exposed)**
- **Brute force attacks are eliminated (bad actors can't guess a password that doesn't exist)**
- **Keyboard loggers cannot capture password information**

Passwordless authentication is seeing a surge in interest from all types of organizations, public and private, regardless of where they sit along their digital transformation journey. The global pandemic has amplified the need for simple and secure access for employees, customers, and partners.

Passwordless authentication should be the norm.

2. GREATER FINANCIAL SECURITY

"Among the 39 per cent of businesses and 26 per cent of charities that identify breaches or attacks – one in five (21% and 18% respectively) end up losing money, data or other assets. One-third of businesses (35%) and four in ten charities (40%) report being negatively impacted regardless, for example because they require new post-breach measures, have staff time diverted or suffer wider business disruption."

Source: The UK Government's ***Cyber Security Breaches Survey 2021***

Data breaches are a major headache for organizations for many reasons. Employee credentials are targeted so that attackers can gain access to systems and create mayhem at a time of their choosing. Once the door is open, it's often easier to gain access to system-after-system as those which are not outward facing often have weaker security. It's simple for criminals to turn data breaches into profits for themselves through fraud and ransom demands.

Customer credentials are also pure gold for cyber-attackers. Gaining access to customer passwords is a route to their personal and financial information. Credit card and bank data can be harvested for rapid financial gain. Email IDs, addresses, social security numbers, and health records provide the means for full identity theft.

"Credentials remain one of the most sought-after data types. Personal data is a close second. Considering that personal data includes items such as Social Security numbers, insurance related information, names, addresses, and other readily monetizable data, it is little wonder that attackers favor them as they do. They are also useful for financial fraud further down the line, not to mention their resale value."

Source: ***Verizon 2021 Data Breach Investigations Report***

Authorities around the world are introducing and enforcing financially punitive data protection laws in response to the increase in data breaches. For example, the UK GDPR and DPA 2018 set a maximum fine of £17.5 million or 4% of annual global turnover – whichever is greater. The corresponding EU GDPR fines are the greater of €20 million or 4% of annual global turnover.

Some of the biggest GDPR fines in 2020-21 (so far) include:

amazon	Google	H&M	TIM	BRITISH AIRWAYS
€746 m	€50 m	€35 m	€27.8 m	€22 m

Source: *Enforcement Tracker*

In the EU, one of the mitigating factors (which can reduce fines) is:

"Precautionary measures – The amount of technical and organizational preparation the firm had previously implemented to be in compliance with the GDPR."

Going passwordless with Veridium removes the most common attack vector in data breaches. Veridium provides modern authentication for any application, delivering passwordless MFA. Eliminating user passwords via a single step MFA solution provides organizations with greater security.

"Our digital society can't rely on passwords anymore. It's about security, it's about fraud, it's about trust – ultimately, it's about reputation. Think of employees who deal every day with phishing and credential reuse attacks, and consumers who deal with accounts taken over and their passwords reused on their digital channels. This needs to end. It really is a no-brainer."

Ismet Geri, CEO, Veridium

3. INTELLIGENT AUTHENTICATION

With increasing and constantly changing numbers of digital users (employees, partners, and customers), along with their evolving access needs and use cases, it's almost an impossible task to keep track. Where and how they will log in also evolves as the hybrid workplace becomes established. Redundant or duplicate employee or customer accounts may linger in dusty corners of your systems.

Security vulnerabilities are amplified as a function of the more accounts your organization has and the more they become outdated or out of sync with what's needed. Many organizations lack complete visibility over how many accounts they have or where they can be used. This is especially problematic for privileged accounts, which have greater access and powers. Hacked privileged accounts can have far-reaching consequences.

Better visibility and a deep understanding of credential usage is needed. This is now possible with the use of biometrics and AI to analyze behavioral patterns (e.g., when, where, and how people use their devices). This data greatly enriches the information the organization has to ensure the user behind the device is the right user. It is hard for bad actors to circumvent or replicate these types of controls.

Veridium delivers intelligent, passwordless MFA through device analytics and behavioral biometrics. These capabilities are powered by machine-learning. Individuals can be further identified through their actions in the digital space, including their interactions with devices and patterns of behavior. Machine learning can be used to map these data patterns and flag irregularities

4. EASIER COMPLIANCE WITH LAWS AND REGULATIONS

Different data protection and security rules are appearing around the world. There are generic rules that apply to all organizations within a jurisdiction (such as country or economic grouping, like the EU). There are also laws and regulations that apply only to specific industries. Further complexity comes when these rules intersect or clash or where multiple rules apply because of the global nature of an organization's business.

For example, GDPR data protection rules apply in the EU. Post Brexit, the UK incorporated these into its own laws – but they could diverge over time. NYDFS, New York Department of Financial Services, has developed the Cybersecurity Regulation (23 NYCRR 500), which places cybersecurity requirements on financial institutions. CCPA, the California Consumer Privacy Act of 2018, gives consumers more control over the personal information that businesses gather about them. FINMA, the Swiss Financial Market Supervisory Authority, has introduced tight regulations. LGPD, Lei Geral de Proteção de Dados, provides the data protection rules in Brazil. The list goes on… and is growing.

Going passwordless across all your systems makes it easier to comply with different standards and to prove this compliance. The localization of users during authentication facilitates regulatory compliance even in virtualized and distributed environments.

Going passwordless across all your systems makes it much easier to comply with different standards and to prove this compliance. The localisation of users during authentication facilitates regulatory compliance even in virtualised and distributed environments.

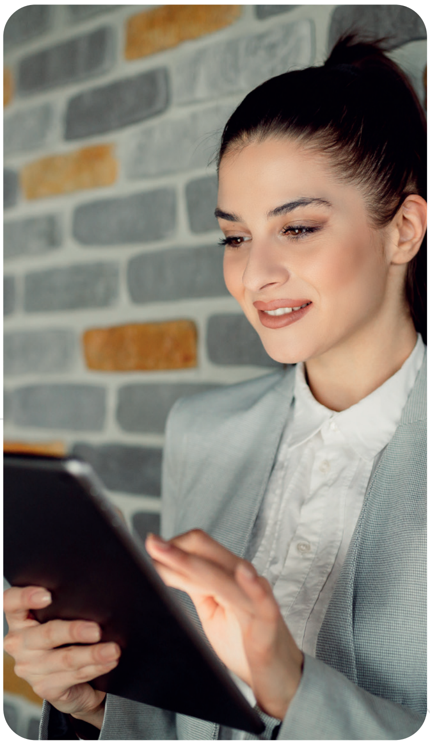
Today, strong authentication is legally required for access in many different countries. Regulations like FINMA mandate strong authentication and location awareness. All these efforts are focused on protecting the digital user's personal information, be it identity or financial or health-related (a.k.a. PXI). This means you must honor this request and deliver the results at the same time.

On the other hand, with some specific regulations, like PSD2, organizations must ensure that the right person is accessing the right data. In this you also must have strong authentication. PSD2 requires an audit trail covering the whole process to make sure the forensic process is maintained properly. Veridium's authentication solution facilitates regulatory compliance.

5. IMPROVED USER EXPERIENCE

"Users have traditionally been told to remember passwords, and to not share them, re-use them, or write them down. The problem with this is that the typical user has dozens of passwords to remember – not just yours. To cope with this overload, users resort to workarounds, such as reusing passwords, insecure storage or predictable passwords."

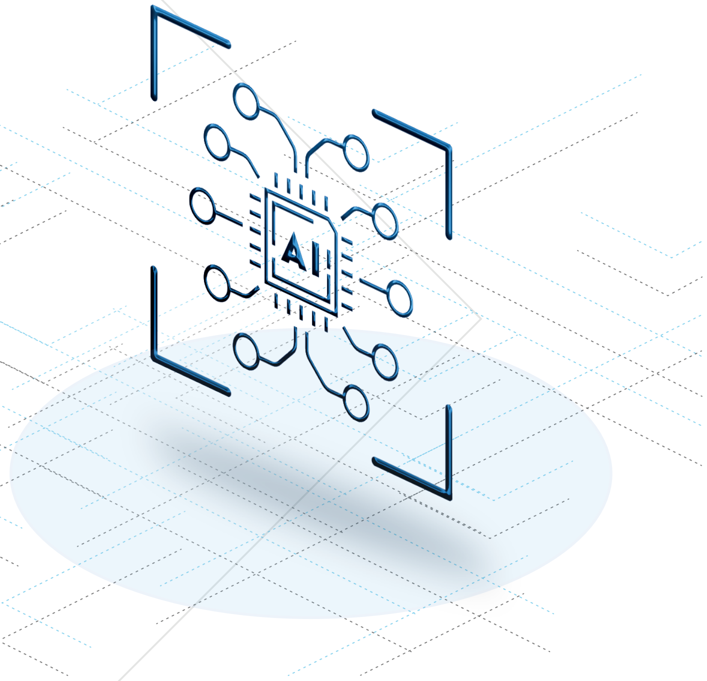
Source: ***UK National Cyber Security Centre***



The password paradox is that the harder IT departments try to make passwords stronger – the more likely users are to forget their passwords or ignore password security policies.

Where password friction increases, UX for employees and customers notably deteriorates and the efficacy of security measures fails. The answer is to remove passwords completely.

Veridium's passwordless MFA solution is fast and simple to use. There are no passwords to remember – so no slow, cumbersome, painful logins. No password resets. No need for password changes. No calls to the helpdesk. Going passwordless means a better experience for the user and time and resources saved for everyone involved.



6. SCALABILITY

Employees feel like there's a daily battle to stay productive. Just to do their job, they need to log in and access a broad range of different environments, systems, and apps – in a variety of ways. To perform their work, employees will often need to sign in and out of their desktop, cloud applications, communication and collaboration tools, Office 365, G-Suite, HR Tools, Corporate Intranets, VPN, partner systems, web and mobile apps, SAP, Oracle, Salesforce etc.

Often the way they need to access these systems will be different when in the office, when working from home, or when on the road. Each environment and each application typically needs a different username and password.

It can be difficult to remember even one user ID and password combination, let alone dozens. So, employees, like consumers, tend to use and reuse the simplest passwords.

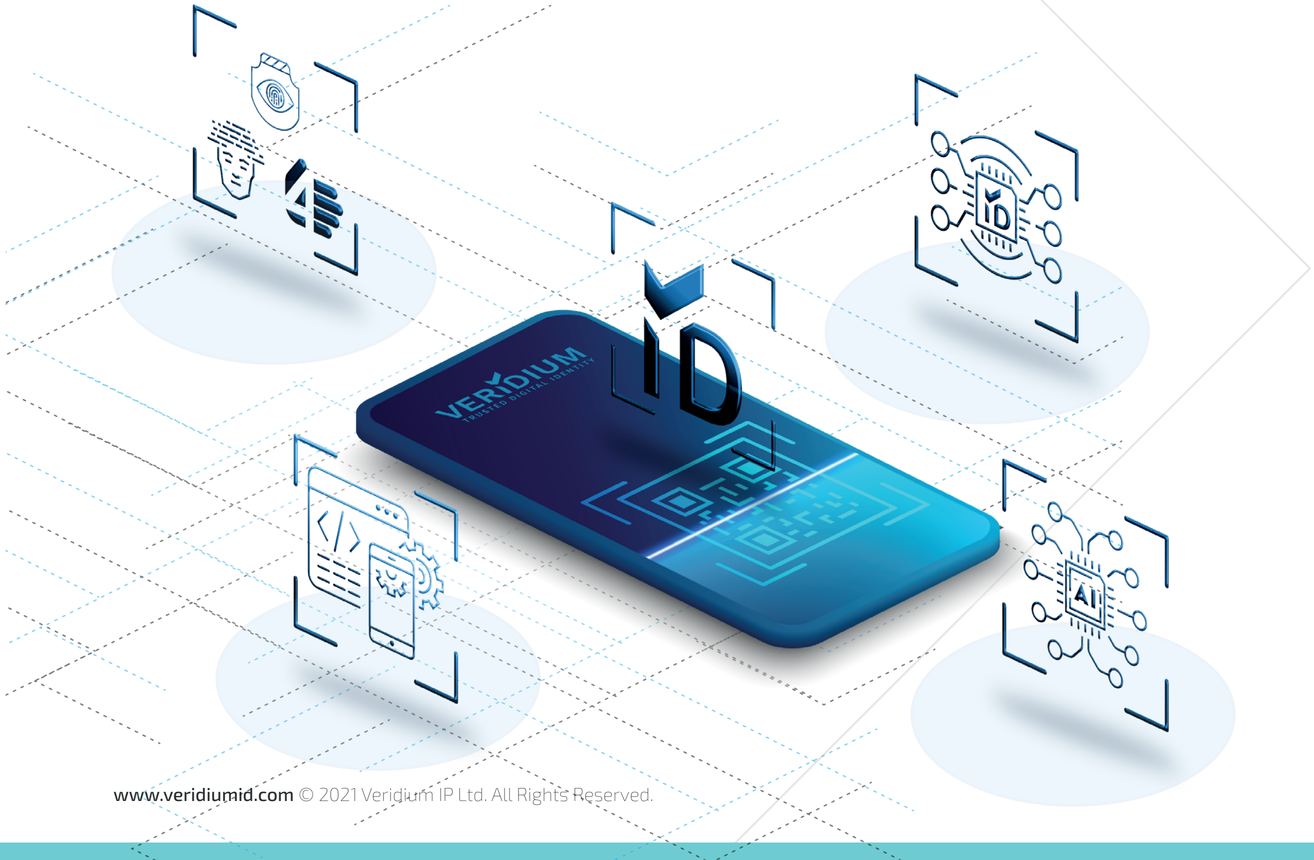
Single Sign-On (SSO), which allows one login process to access multiple systems, can seem an attractive way to reduce the complexity but it can also increase vulnerability. Making things simple for the user also means attackers just need one key to get into all the rooms in the house too. Going passwordless removes issues around increasing the scale of your operations. It means the volume of admin can be reduced, the complexity of policies and procedures is removed, and the pressure to keep increasing the size of the IT team to deliver scalability is reduced.

The VeridiumID platform integrates with your Identity Access Management (IAM)/ID Management (IDM). VeridiumID is an integrated authentication platform that delivers passwordless MFA to any application or service thanks to its support for open standards and seamless integration capabilities or through custom API integration for legacy applications.

It's a software solution to deliver MFA.

It protects enterprise applications and services including:

- **Windows Desktops (Physical or Virtual)**
- **SaaS & Web Applications**
- **Networking & VPNs**
- **Legacy Applications**



7. THE HYBRID WORKPLACE IS ENABLED

"In the post-pandemic future of work, nine out of ten organizations will be combining remote and on-site working, according to a new McKinsey survey of 100 executives across industries and geographies. The survey confirms that productivity and customer satisfaction have increased during the pandemic."

Source: *McKinsey "What executives are saying about the future of hybrid work", May 2021*

McKinsey & Company

We have seen a gradual shift over the last 2 decades around flexible working practices. Allowing employees to 'work from home' for a few days a month became an acceptable business practice for many organizations. The beginning of 2020 saw a dramatic shift, overnight for some organizations, as the COVID-19 global pandemic took hold. Employees were often unable to go to their workplace or meet in person. Businesses scrambled to find ways to keep their workforces working. Organizations had to race to enable secure access to business systems for working-from-home employees – and sometimes this was, by necessity, achieved in a rushed and sub-optimal way.

As the world unlocks (or at least lurches from lockdown to lockdown), organizations and employees have realized that collaboration can be achieved, work tasks performed, informed decisions made, and business conducted, with employees continuing to work from home for an increased proportion of the time.

To be a credible alternative the hybrid working model needs effective workforce authentication to provide safe and secure access to the workplace. This is best delivered with easy passwordless multi-factor authentication (MFA).

Veridium makes the secure hybrid workplace a reality. Passwords are removed and access is given via a range of flexible authentication options. Accessing all systems and apps is done using common, familiar methods and processes. There's no requirement to remember numerous passwords with different rules and refresh periods. Nor is it necessary to carry around multiple access devices such as cards, fobs, and dongles.

There's a growing demand from employees for even more flexible working. At the beginning of 2021 Salesforce said

"THE 9-TO-5 WORKDAY IS DEAD"

and will provide 3 new ways for employees to work - including the possibility of working from home forever.

salesforce

Google, Microsoft, Morgan Stanley, JPMorgan, Capital One, Zillow, Slack, Amazon, PayPal, Salesforce and other major companies **have extended their work-from-home options, according to the largest human resources organization, SHRM, and other sources.**

Square

Jack Dorsey, CEO of Twitter and Square, ***informed his employees at both companies that they can continue*** ***"WORKING FROM HOME FOREVER".***

Veridium's passwordless access leverages modern technologies and protocols, as well as offering custom API integration for legacy applications to deliver strong authentication and provide tight security. A single, consistent user experience can be achieved across devices and networks via familiar personal mobile devices to deliver a passwordless MFA solution. Organizations can opt for users to simply download the Veridium App from their App Store or they can opt to use their own mobile application and incorporate Veridium's mobile app SDK. The IT team can manage digital authentication for all identity stores (Identity Providers) from a centralized dashboard within the VeridiumID Authentication Platform.

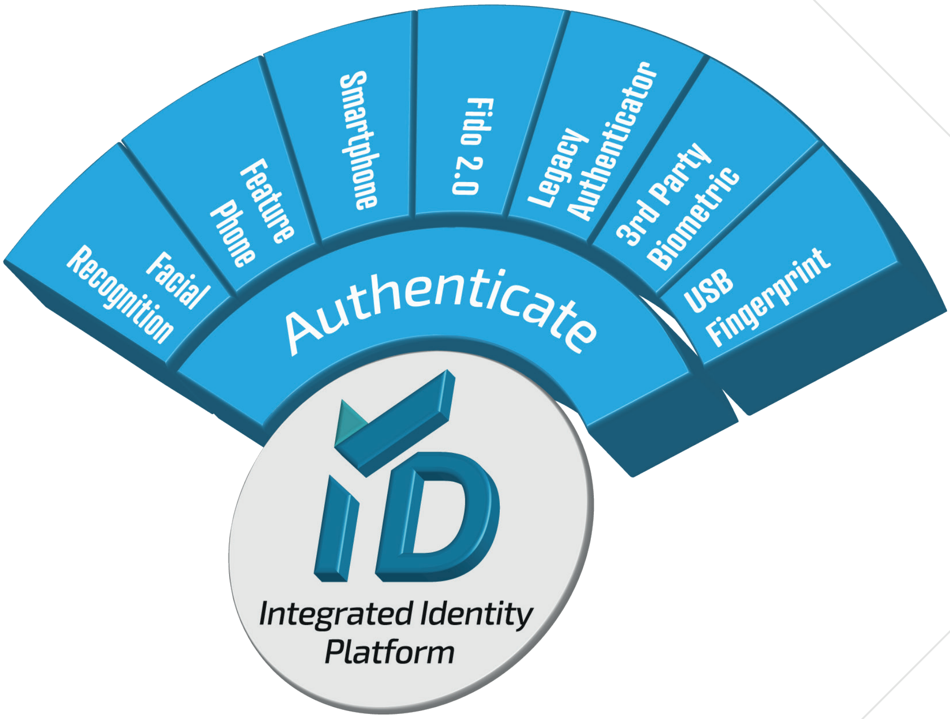
8. REDUCED HARDWARE COSTS

The cost of keeping your organization secure can easily skyrocket. Niche security solutions have multiplied over the years, but are designed to cover only parts of your systems. Implementing solutions to cover your entire workforce, as well as all your partners and customers, can be prohibitively complex and expensive.

Adding hard tokens or soft tokens for security requires your organization to purchase or license such technologies on a monthly or annual basis – and passwords still exist. Removing passwords and utilizing devices which users already have (their smart phones and tablets) to deliver passwordless MFA can simplify users' lives and dramatically reduce costs for organizations.

Veridium can help eliminate the need for all hardware and software tokens, which can cost large organizations millions to purchase, rent, administer, replace, and upgrade.

While you plan and execute your passwordless MFA rollout with Veridium's solution, existing hard or soft tokens can be integrated and gradually retired as needed.



9. REDUCED SUPPORT COSTS

For larger businesses, it's estimated that nearly 50% of IT help desk costs are allotted to password resets and password management costs companies $180/user each year.

In response to increased security threats, IT teams respond to the password problem by mandating greater password complexity (e.g., the use of upper - and lower - case letters, numbers, and special characters). They also impose periodic password resets and prohibit the reuse of passwords and the use of commonly used passwords or ones which have appeared on data breach lists. With multiple systems making up today's hybrid workplace, there are often different sets of password rules which apply to each, causing further confusion for employees.

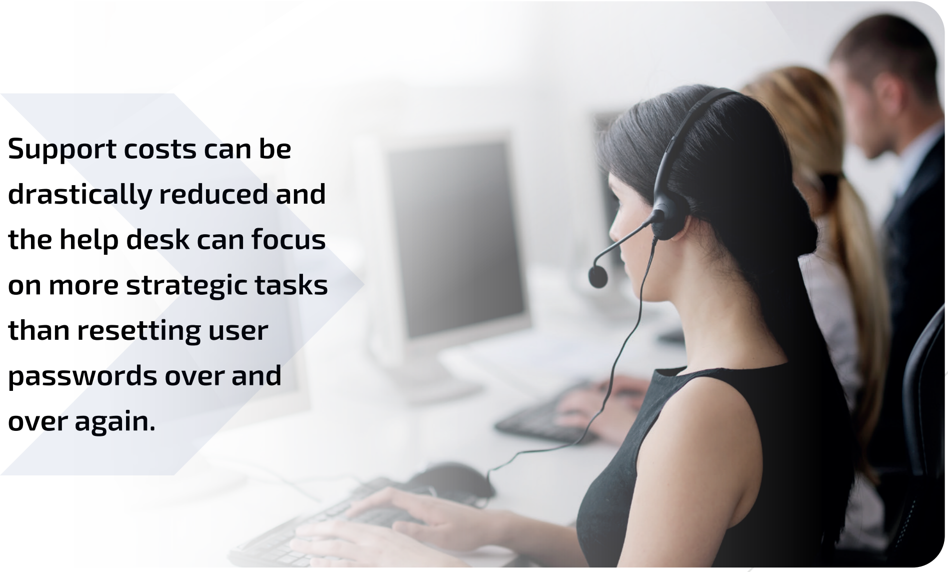
In this game of password cat and mouse, users respond by writing their passwords down on post-its, storing them in documents on their computer or phone, or by sharing them with colleagues. This amplifies the security vulnerabilities.

A study by MasterCard and the University of Oxford found that around one third of online purchases are abandoned at checkout because consumers cannot remember their passwords.

Veridium's authentication solution removes passwords completely from the security equation. Instead of a password free approach (where passwords still exist and are replayed in the background, but hidden from users), Veridium provides a true passwordless MFA solution for tight security and peace of mind for the organization. Support costs can be drastically reduced and the help desk can focus on more strategic tasks than resetting user passwords over and over again.

Drive Costs Down

For larger businesses, it's estimated that nearly 50% of IT help desk costs are allotted to password resets and that:
Password management costs companies $180/user each year.



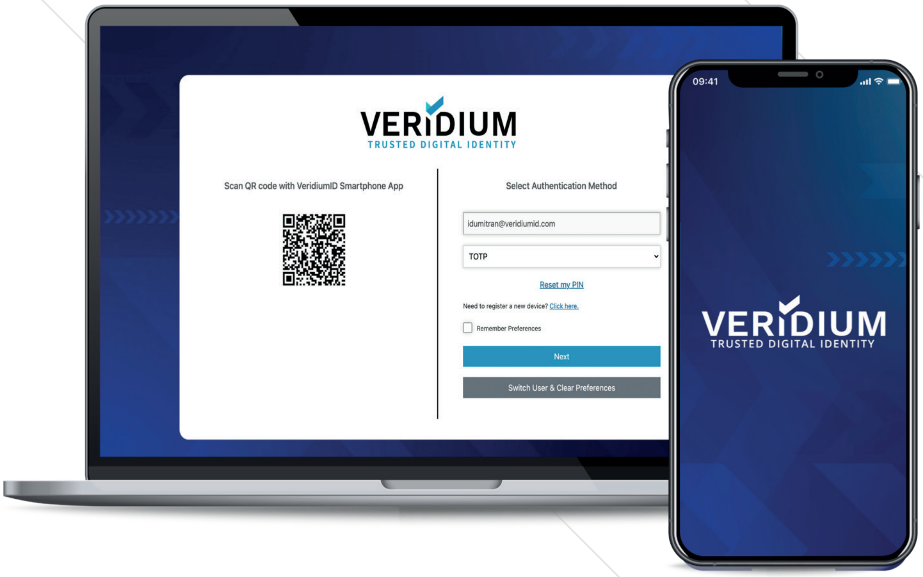
Support costs can be drastically reduced and the help desk can focus on more strategic tasks than resetting user passwords over and over again.

10. SIMPLIFIED POLICIES

Passwords need a lot of administration and documentation. The requirements and rules can rapidly and repeatedly change in order to continually address the evolving nature of cyberattacks and the introduction and tightening of laws and regulations in countries around the world and specific to different industries. These password rules and changes must be documented in policy manuals, guides, and training courses. Often such policies are of interest to regulatory bodies and must be shown to be up to date and rigorously enforced.

Removing passwords from an organization's security framework means a huge amount of administration can be simplified or removed entirely, including the need to establish, maintain and enforce complex rules around password length, composition and reset periods. This means policies can be much simpler and will require fewer updates.

Veridium's passwordless MFA solution means there's no need to expend effort and expense on creating complex and ever-changing password rules which then have to be incorporated into policies and procedures, user education and evidence of enforcement.


Scan QR code with VeridiumID Smartphone App

Select Authentication Method

idumitran@veridiumid.com

TOTP

Need to register a new device? Click here.

□ Remember Preferences

WHY YOU SHOULD CHOOSE VERIDIUM TO HELP YOU GO PASSWORDLESS

At Veridium, we believe that authenticating a digital identity (i.e., validating that the right individual is behind the Digital ID aiming to access a digital service) is *the* pivotal aspect of an IAM system, especially systems premised on "zero trust" principles, but we are also mindful that digital authentication is simply a means to an end. Therefore, we are absolutely determined to disrupt the digital authentication landscape by making every digital authentication fast and secure - irrespective of where an organization sits along its digital journey - using (to the extent possible) passwordless MFA and machine learning technologies to maximize the *automation* of digital authentication (including the use of both behavioral biometrics and device behavior, such as geolocation).

VERIDIUM
TRUSTED DIGITAL IDENTITY

London
100 New Bridge Street
London EC4V 6JA
United Kingdom
+44 1753 208780

New York
1325 Avenue of the Americas
28th Floor
New York, New York 10019
United States of America
+1-857-228-7805

Oxford
The Magdalen Centre
Robert Robinson Avenue
Oxford Science Park
Oxford OX4 4GA
United Kingdom

Bucharest
71 Buzesti Street, 2nd Floor
Bucharest 011013
Romania

Press Contact
info@veridiumid.com
+1-857-228-7805