White Paper

Passwordless/touchless solution selection guide

Protect your enterprise & your people

ENTRUST

SECURING A WORLD IN MOTION

Why Passwords Still Exist

Security experts have been talking about killing passwords for years. In fact, in 2004, Bill Gates said this at the RSA Security Conference: "There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down, and they just don't meet the challenge for anything you really want to secure."

Now, 17 years later, technology has raced forward and we are using—passwords. Yikes.

According to a 2019 Verizon study, the problems with passwords are only increasing, as they're the root cause of more than 80% of all data breaches—each of which costs an average of $4M to $8M, depending upon which study you believe. We're also spending an average of $70 every time an enterprise employee calls a help desk to reset a forgotten password.

The 2020 coronavirus pandemic only worsens the case for passwords. Enterprises are developing and deploying new procedures in an attempt to mitigate the spread of disease. This includes a thorough examination of any activity that requires workers to touch surfaces. Entering passwords on keyboards or touchscreens falls squarely in this area of risk. This has led enterprises to expand their searches from simply "passwordless" offerings to "passwordless and touchless" solutions. Beyond passwords, many organizations are looking to replace smart cards and other physical authenticators in their quest to go "touchless."

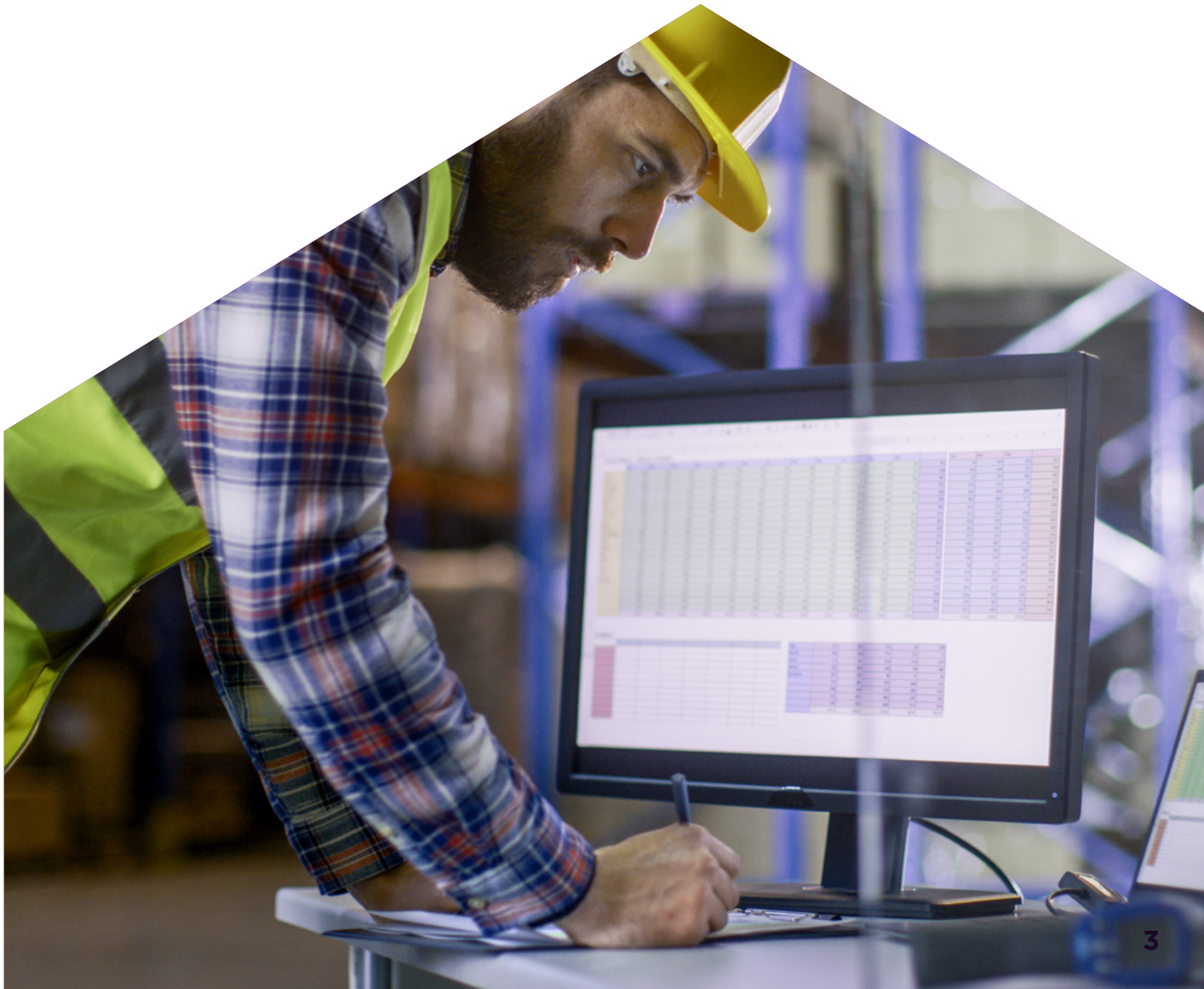
80% of hacking related breaches are caused by compromised credentials.

65% of us reuse our passwords across multiple accounts.

2.7B passwords were compromised in one breach alone.

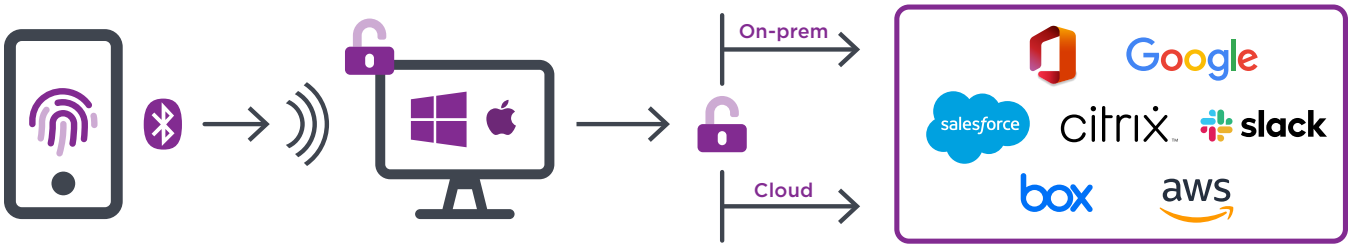
As enterprises search for the right solution, they often encounter confusing product terminology. Many recent biometrics-based solutions claim to offer users a "passwordless experience." Which is true in the sense that workers can scan a biometric instead of physically entering a password. In reality, though, these solutions simply provide a new front-end way to activate passwords that still reside in a central repository. And of course, those centralized credential repositories are a favorite target for hackers. With one successful intrusion, cybercriminals can swipe thousands of credentials and use them to engage in credential stuffing or any other number of attacks. Many biometric scanning technologies also fail to address the "touchless" issue that has become so important.

Here's how you can move on: If you're looking to move on from passwords—and the data and all of the anecdotal horror stories tell you that you should—you need a solution that improves security by shifting from the vulnerability of a centralized credential repository. The truly secure approach is to deploy a new decentralized model, where workers' credentials are safely stored on their mobile devices. From a user experience perspective and for internal efficiency considerations, it's important to choose a solution that offers true single sign-on (SSO) capabilities.



How a True Passwordless & Touchless Solution Works

There are many solutions on the market labeled "passwordless." But a majority of them only deliver a passwordless experience for workers—which is not the same as true passwordless security. Many of these solutions allow users to access a workstation, app, or network by using a fingerprint, eye scan, or voice recognition. With these strictly experiential solutions, passwords only appear to be eliminated—and the "touchless" issue remains largely unaddressed. In most cases, the user's password still exists in a central repository. They're still required for authentication after the biometric scan, and they're still vulnerable to hackers. In other words, it's not an improvement in security, it's just a slightly better user experience. So, these solutions only solve half of the passwordless security equation—and most fail to address the disease transmission issue in a meaningful way.



Decentralized Credential Storage

The secure replacement for passwords—and the one that wows users with a new lack of friction, true SSO capabilities, and a true touchless experience—is based on trusted digital identities. These identities are created by issuing a digital certificate that is stored securely on a user's mobile device. Your IT department can choose to manage certificates internally or through a managed service. Think of these encrypted digital certificates as virtual passports or ID cards that reside on the worker's device. Because they're stored on your users' devices, you're able to build a highly secure decentralized credential infrastructure. There's no central repository for worker credentials.

Public Key Infrastructure (PKI) Technology

The issuance and lifecycle management of certificates requires public key infrastructure (PKI) technology. When a user wants to gain access to a workstation, app, or network, this digital identity is unlocked using a set of encrypted keys. The identity is decoded and confirmed through a secure exchange of keys. There are no passwords to hack or steal and no need to touch a screen or keyboard.

SSO Authentication

Once this encrypted exchange of keys occurs, workers and other authorized users can use self-service onboarding tools to register—then securely access cloud-based apps, on-premises apps, and secure networks anywhere they have an internet connection. A well-designed solution will authenticate users and devices with one-time user registration, eliminating the time-consuming process of re-registering credentials device-by-device and app-by-app. It creates a single sign-on solution that is both secure and frictionless.

How a truly secure passwordless & touchless solution works in an enterprise setting

1. Install a digital certificate on the user's mobile device — this is the virtual ID card.
2. Authorized users self-register — anywhere they have an internet connection — using automated onboarding tools.
3. Workers unlock their devices and access their trusted identity using a biometric, including fingerprints and facial recognition.
4. Once the user is authenticated, Bluetooth connectivity to a Mac or PC delivers passwordless workstation login and single sign-on (SSO) to all cloud and on-premises apps while in close proximity.
5. When users walk away from their workstations with their mobile device, they're automatically logged out of the workstation and their apps. The proximity settings to trigger an automatic logout are configurable and depend on each organization's policy.

Passwordless & Touchless Benefits

Early-adopter organizations see a positive impact from passwordless and touchless solutions.

Mitigate threats: When you eliminate passwords, you eliminate password hacks — including credential stuffing, phishing, and man-in-the-middle attacks.

Enterprise control: Users aren't picking bad passwords and engaging in dangerous password management behaviors. The enterprise controls the certificates and encryption keys.

Scale at will: A decentralized approach to credential storage and management means that you can add new users quickly — and almost without limit. All your users need is a smartphone or similar mobile device and you can automatically onboard them in minutes.

Reduced TCO: Passwords require constant monitoring and maintenance. No passwords means no time-consuming password resets or overly-complex password policy administration.

Happier users: Users no longer need to remember and update complex password combinations just to be secure.

Transmission risk: Eliminating the use of passwords and physical authenticators — and reducing dependence on shared devices in favor of a bring-your-own-device (BYOD) culture — minimizes touching of workplace surfaces.

How to Choose the Right Solution for Your Enterprise

There is currently a very short list of solutions that truly eliminate the need for traditional passwords, reduce the need to touch surfaces, and provide high-assurance security.

So, how do you start a search that leads to the best outcome for your enterprise? For starters, consider how you can predict and eliminate unnecessary changeover disruptions. The task of onboarding large or widely dispersed employee populations can be a serious roadblock for many enterprises looking to go passwordless and deploy SSO capabilities. Look for a solution that offers automated tools that securely and reliably allow employees to self-register from anywhere. Burdening your IT or HR departments with onerous onboarding processes is not recommended—and entirely avoidable.

A second key consideration is scalability. If you're expecting to grow organically or through acquisition—and if you plan on continuing to add new cloud apps and broader connectivity with outside ecosystems—you need password authentication that will scale easily.

A third key consideration is your encryption needs. If your workers are accessing or sharing highly sensitive information or conducting high-value transactions, you'll need a system that offers enterprise-grade encryption capabilities. The best passwordless authentication platforms offer clear roadmaps for transaction security and continuous session monitoring.

Here are five additional factors to consider when assessing passwordless and touchless solutions:

1. Avoid device lock-in
This should be at the top of your list. As workforces become increasingly mobile and remote, device flexibility is critical to ensure workers can login to the applications and systems they need—wherever they are working. The rise of the BYOD movement, especially in the post-pandemic world, means that companies no longer have control over the devices their workers use. Ensure the passwordless solution you choose is technology-agnostic—fully compatible with Macs, PCs, cloud apps, and on-premises software. Not only will this minimize disruption to your workforce during adoption, but it also gives your enterprise the flexibility when deploying hardware or software in the future.

2. Enable SSO & true mobility
Especially in the remote work era, it's important to look for a solution that embraces mobile as the new desktop and offers a range of authentication options. As the number of devices workers use continues to grow, SSO capabilities significantly streamline login processes and simplify omnichannel workflows. For workers, this means less friction; for the enterprise, it means optimal productivity. Additionally, the use of NFC or Bluetooth to lock and unlock workstations and applications based on proximity ensures that anywhere-anytime system access doesn't create unexpected security challenges, especially in home office environments. When workers walk away from their workstations, the passwordless solution you choose should allow their devices to recognize the movement—logging the user out until they return.

3. Choose certificate-based identity
Look for solutions that use mobile smart credentials to transform smartphones into virtual smart cards for authentication, encryption, and enterprise mobility management (EMM). Using PKI to place digital certificates on smartphones, tablets, and other user devices mitigates key hacker strategies, such as credential stuffing and exploitations of re-used credentials. When you take a decentralized approach to credential storage, neither of these illicit strategies are viable.

4. Accommodate your digital roadmap
Your current use cases likely include file encryption, digital document signing, and hot desking. As worker mobility expands, passwordless solutions will become more of a necessity. It's important to choose a solution that scales as your needs change. Without a scalable solution, you could end up with one authentication solution for email, one for system login, and another for document signing. This will frustrate users—creating unnecessary complexity and putting additional strain on enterprise workflows.

5. Check vendor credentials
Best-in-class solutions will be offered by vendors whose solutions are approved for use by government authorities and are FIDO2-compliant. FIDO protocols rely on the power of PKI and advanced data encryption techniques to both simplify authentication for workers and elevate security for enterprises. The most proficient vendors will have multi-year histories of offering these services to national governments and global banks.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

RESOURCES FOR YOUR SEARCH

If you're looking for information and insights to help with your evaluation of passwordless authentication technology—or if you'd like to see a demonstration of our platform—you can visit www.entrustdatacard.com/passwordless.

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com