Acceptto®

PASSWORDLESS CONTINUOUS AUTHENTICATION™

Quick Guide to Passwordless

Why passwordless?

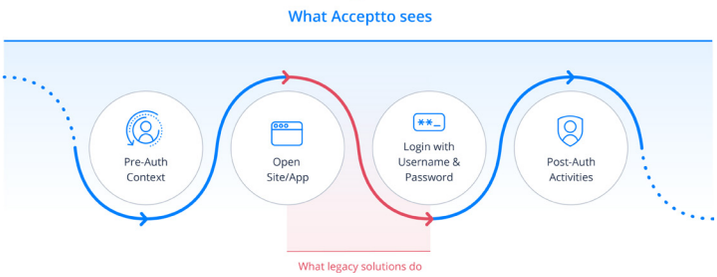
Passwords account for nearly 80% of all breaches in the last five years. Adopting passwordless authentication methods eliminates most breaches and account takeover (ATO) for an enterprise. It will also alleviate friction associated with passwords and drastically cut costs spent on help desk tickets and managing breaches.

Can you really go passwordless?

Some entrenched authentication vendors boldly assert that their solution is “true passwordless”, when upon further inspection, all they offer is a new way to mask passwords from the consumer or workforce. Passwordless is, at times, a buzzword in the identity access management (IAM) world. But we also believe that the journey to begin moving over to passwordless authentication is a step in the right direction, and still provides a step up in security from legacy solutions. Acceptto’s Next Generation Authentication (NGA) has emerged as a more effective, multi-sensory, dynamic, risk-based authentication system, leveraging data science advances that have been compounding for more than six decades. Acceptto is the only platform today that gives an enterprise a fully integrated, adaptive platform for passwordless continuous authentication.

What’s the future of passwordless authentication?

Acceptto’s Passwordless solution is based on a profound truth: The longer authentication is viewed as a binary event, the higher the risk.



Acceptto’s Next Generation Authentication (NGA) provides a simple way to access systems, while ensuring high security over time, throughout the life of each session. Unlike traditional authentication akin to a single guard at the front door, NGA is an embodiment of a staff of digital guardians equipped with multiple security cameras and other sensors protecting all entry points. By harnessing the powerful new capabilities of behavioral modeling and modern data science, the dangers endemic to password-based authentication systems are alleviated while the digital experience for both end-users and system administrators is improved. We have created a platform that combines FIDO’s interoperability with our continuous, data-science approach to risk- based authentication, providing an MFA experience that does not rely on passwords.

Passwordless methods

Magic link: With this method, an email with a personalized link is sent to user, allowing them to log in without the use of a password at any point in the process. This method can integrate with many solutions and devices, but can also be vulnerable--should the email account be compromised, then the magic link is, as well.

Time-Based One Time Passwords (TOTP): TOTPs are expirable codes that can be delivered to the user through SMS, phone, email, application, discrete token, and other routes. The rate at which they expire can be adjusted to shorten the window of time for threat actors to get through. TOTPs differ in both form and substance – no two are the same. Highly unique QR codes advance the level of security by a huge factor, while SMS codes are susceptible to SIM-swapping.

Device as a factor: Device-as-a-factor includes discrete security keys and integrated biometric readers like the Win Hello Face/Fingerprint, as well as Touch/Face ID. Through the use of public key infrastructures and asymmetric key pairs, a device can effectively serve as a compound factor, as it represents something you have and/or know or are. WebAuthn bypasses passwords by encoding a registered device as a factor in itself. This method is convenient and maintains excellent security.

Challenges

Phone as a factor as insufficient.
Phones can be misplaced or damaged. Phone batteries run down. Charter a plan in case of phone malfunction(s) or absence.

Users need time to adjust.
End users generally have more experience working with passwords than without them. The “psychological acceptability” of a passwordless solution requires training and forming new habits.

Meeting compliance regulations.
Consider in advance which compliance regulations your enterprise must meet, such as NIST 800-63, PCI DSS, HIPAA, and more.

Best practices

Phase-in new user experiences.

- Start with a subset of the user population. This provides ample time to troubleshoot unforeseen problems as they occur.
- Provide training for the end-users as changes occur. Keeping users informed encourages them to exercise secure authentication practices.

Configure policies to your specific needs.

- Iterate risk scoring / assurance levels based on your enterprise environment
- Provide as many authenticators as appropriate to ease user adjustment to a passwordless system.

20M+
Users

20
Patents

98%+
Eliminated Account Takeovers

3M+
Daily Secured Authentications

Acceptto Solutions

Intelligent Multi-Factor Authentication
Employees hate using passwords as much as you hate managing password vulnerabilities. More passwords and tokens lead to greater security risk, fatigue, and cost. It's time to get rid of them for good.

Zero Trust Identity (CIAM)
You need to know that your customers are who they say they are; customers do not want to jump through hoops to prove it and they want you to keep their credentials safe.

Device Trust
Acceptto Device Trust solution enables passwordless Desktop SSO for Windows and Mac workstations and measures the security hygiene of devices, tracks who is accessing which company applications, and eliminates costly helpdesk support calls.

FIDO Solution
FIDO Certified program provides assurance of product compliance to roll out FIDO Authentication using Acceptto's enterprise identity authentication security solution.

Why Acceptto

Enable Frictionless Productivity
By using context and behavior-aware risk-based analysis, Acceptto facilitates a frictionless and secure authentication experience for legitimate users and a step-up authentication for suspicious login attempts. We proactively eliminate fatigue while meeting the objectives of IT Operation and Risk Mitigation.

Correlate Audit Logs & Threat Intel in Real-time
Acceptto eliminates the reliance on weak and outdated controls by incorporating multi-modal telemetry into our solution. We utilize contextual, behavior-based credentials that are virtually impossible to replicate, tamper with, or spoof.

Eliminate Account Takeover (ATO)
Acceptto renders credential stuffing benign using passwordless risk-based authentication. Our services drastically reduce the attack surface and eliminate ATO.

Dramatically Reduce Cost of Operations
By eliminating the need for passwords, we significantly reduce help-desk costs, like password resets, governance and compliance, audits, and password tool managers.

Orchestrate Dynamic Authentication
Acceptto offers a powerful but simple set of configurable policies that drive dynamic risk-based scoring of authentication requirements. This, in turn, adapts to user behavior, attributes, and the ecosystem of associated devices and resources.

Integrate and Scale Efficiently
Acceptto provides an out-of-the-box solution for all enterprise cloud or on-premise applications, certified WebAuthn FIDO servers, Mobile SDKs, and REST APIs for scale, extensibility, and visibility into the IT ecosystem. We integrate across web, mobile, cloud, or IoT applications.

About Acceptto

Acceptto secures all your devices, enterprise applications, and credentials, to you.

We are the winner of a number of awards including the **4 Cybersecurity Excellence Awards 2020** and prestigious 2019 SINET 16 Innovator Award. Our expertise and trailblazing perspectives on cybersecurity have been featured in publications like TechRadar, Security Magazine, and digimonica.

Headquartered in Portland, USA with offices in Lisbon, Portugal, and Vancouver, Canada, serving global active customers in healthcare, education, and financial services.

www.Acceptto.com Sales@Acceptto.com @AcceptoCorp Acceptto Corporation