Acceptto®

Passwordless Continuous Authentication™

# eGuardian® Platform

> In a world where identity is persistently attacked, your credentials have already been compromised, or soon will be.

System vulnerability has skyrocketed, as have costs, with little done to mitigate friction as solutions fall short of enterprise needs: Two-factor authentication is temporal, produces friction and fatigue, and can be easily intercepted during transmission; current multi-factor authentication (MFA) security solutions lack context and rely on too few attributes; even your biometrics can be reduced to a few binary traits. While a fingerprint, face, or retina scan appears to be distinctive and safe, it too can be spoofed with ease.

> Enterprise struggles to balance both objectives of IT Operations—service level and speed—and Risk Mitigation—confirming who has access to what.

Enterprises must manage three main considerations when it comes to cybersecurity: vulnerability, friction, and cost. Vulnerability increases when utilizing insecure binary authentication methods, while friction accrues as the use of these methods become overbearing and inconvenient. Accumulating costs come with both vulnerability and friction: the cost of deploying and maintaining authentication solutions, of help desk, of breached data, of multi-vendor non-unified solutions, and of lost productivity due to authentication troubles. The unfortunate truth is that the efficacy of controls deteriorates over time. Therefore, a technology that treats authentication as a ***continuum***, instead of a binary event, is critical in defending against threat actors' increasingly advanced tactics. This is the only way to maintain the delicate balance between the two competing objectives of IT Operations: service level-speed and secure access management.

> Acceptto's Passwordless Continuous Authentication™ models and analyzes user behavior to infer whether an access attempt is legitimate pre-authentication, during authentication, and post-authorization—all while reducing friction and costs.

Acceptto is the first of its kind in delivering continuous authentication of your identity. There are no other solutions on the  market that validate your identity post-authorization. Our AIML approach utilizes context and behavior to create an enriched user profile within each application landscape, negating the need for vulnerable and costly passwords.

## Next Generation Authentication

Unfortunately, when you combine authentication with people, people do what's easiest: they recycle credentials. Cybercriminals harvest credentials (a trivially easy task, be it through phishing, malware, or simply via the 15 billion credentials readily available on the dark web), get into systems, and escalate privileges. Even worse, they disseminate what they've aggregated, and the tools they employ are scalable. Threat actors can spray passwords across multiple hundreds of domains of choice, and breach the system with perfect access to all resources thereafter. Then there's the rise of insider attacks. What you can't see, you can't respond to. What is necessary is real-time detection and faster mitigation. The longer we view authentication as a binary event, the higher the risk. Hence, the increasing need for a data-driven model for post-authorization anomaly detection.

Acceptto has a modern data science approach to passwordless authentication and anomaly detection, bringing Next Generation Authentication (NGA) to the forefront: a modern system design and architecture with streaming at its core, treating authentication as a continuum.

> In a nutshell, traditional authentication is the guard for the company door, while Acceptto NGA is the security cameras roving over all the company hallways, recording throughout the day and night, ushering unwelcome intruders to the door.

Acceptto NGA enforces behavioral verification, consequently detecting imposters using stolen credentials by carrying out anomaly detection and commonality analysis. Combined with a data stream, the system remains evergreen, bypassing the deterioration of efficacy that comes with mainstream controls. The detection of imposters at a low latency suddenly becomes possible through the AI model performing predictions on the data stream.

The modularity and interoperability of Acceptto solutions enables integration with existing enterprise UBA & IAM to enrich the risk profile and maximize both the impact and return of investment while reducing cost.

eGuardian®

**20M+**
Users

**20**
Patents

**97%+**
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.

### 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.

### Zero Trust Identity (CIAM)

You need to know that your customers are who they say they are; customers don't want to jump through hoops to prove it and they want you to keep their credentials safe.

### 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 @AccepttoCorp Acceptto Corporation