

# Go Passwordless

Ensure the Security Hygiene of All Your Devices

The enterprise security journey starts with ensuring the safety and health of devices used to access company sensitive data.

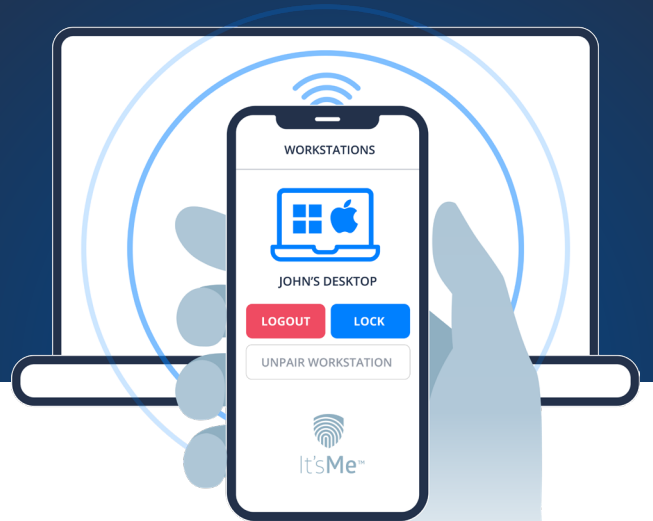
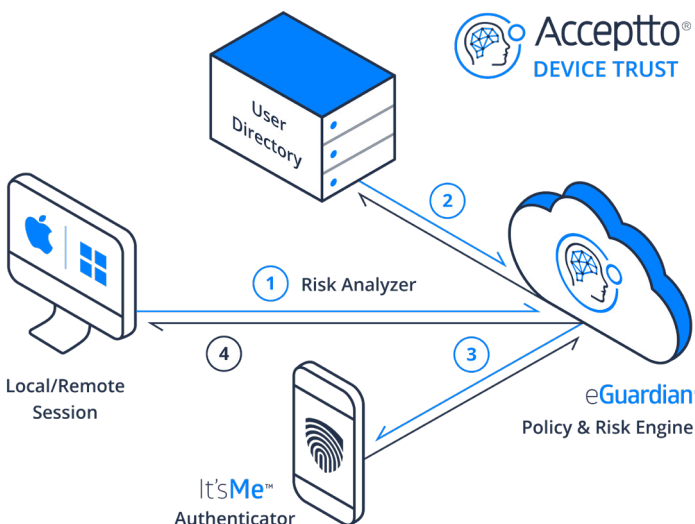
In a world where identity is persistently attacked, your credentials have already been compromised, or soon will be. Stolen and lost passwords are the number one source of breach, resulting in productivity loss, exposed security holes, and costly help desk/support calls. **Acceptto's Device Trust** eliminates this vulnerability entirely by establishing the endpoint root of trust at the far left.

Endpoint stolen credentials, which are widely used for remote logins, need better protection through a unified intelligent MFA.

System vulnerability has skyrocketed, as have costs, with little done to mitigate friction as solutions fall short of enterprise needs. The new perimeter is the cloud, where your user name and password for your endpoint devices can be used for remote access, making the attack surface limitless. An Intelligent MFA in combination with passwordless solution eliminates this vulnerability.

**Acceptto's Device Trust** solution allows enterprises to enable desktop MFA and passwordless authentication, minimizing the attack surface by:

- Making passwords benign or going passwordless altogether
- Measuring the real-time security hygiene of devices
- Delivering remote audit logs and control of user access
- Cutting costs of help desk/support
- Providing administrative risk-based policy orchestration



## Device Trust Benefits

### Identity Governance

Policy orchestration and Continuous Authentication with dynamic entitlement management.

### Cross Device Unified Risk Engine

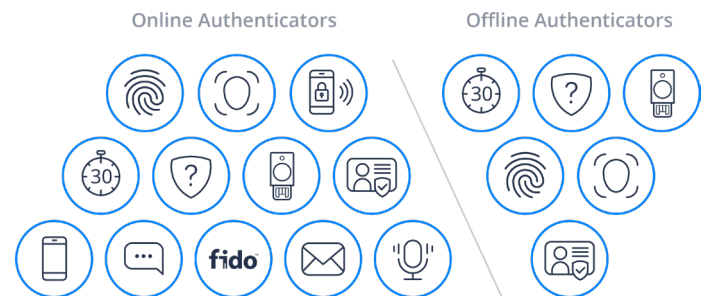
Detect threat and anomalies across all endpoints. Identify risky devices to safeguard the enterprise by applying Zero Trust policies.

### Real-Time Asset Tracking

Identify and track managed and unmanaged devices' whereabouts.

### Enterprise Configurable Authenticators:

Push, Offline TOTP, SMS, Email TOTP, FIDO token, Biometric/Touch-ID, Win Hello, and more.



### Support for Domain, Local and Microsoft User Accounts

Seamless user enrollment supporting multi-forest, disjoint domains, and even no domains per organization needs.

### Unified Mac and Win 10 User Experience

Single UI/UX across enterprise endpoints.

### Automate Identity Lifecycle

Easy account provisioning and lock capability for efficient user onboarding/offboarding.

### Secure Remote and Proximity Unlock-Lock-Logout

Use mobile device for remote and proximity unlock, lock, or logout.

### Identity Binding Across All Domains

Bind any number of cross-domain user identities to a single persona.

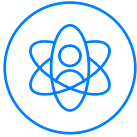
**20M+**  
Users

**16**  
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 helpdesk 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](http://www.Acceptto.com)



[Sales@Acceptto.com](mailto:Sales@Acceptto.com)



[@AccepttoCorp](https://twitter.com/AccepttoCorp)



[Acceptto Corporation](https://www.linkedin.com/company/acceptto)

