

# RunBuggy Secures Internal Resources with Secure Workforce and Secure Customers

## About RunBuggy

RunBuggy is an open marketplace that connects car shippers and haulers in real time. Dealers, car auctions, lenders, fleets, OEMs, and individual sellers connect directly to drivers ready to transport vehicles and get real-time tracking without having to use expensive load boards and custom software to find and manage the transportation. Drivers get work assignments and secure, quick payouts via a mobile app they can use on the go. Since 2019, RunBuggy has moved hundreds of thousands of cars, generating tens of millions of dollars in revenue, and is experiencing triple-digit year-over-year growth.

## Challenge: Level up security and accessibility for employees, enterprise customers, and drivers

RunBuggy's accelerated growth has been driven by an increase in enterprise customers—dealers, car auctions, fleets, and OEMs—transporting hundreds of thousands of cars. This impacted the company's security needs in two ways: 1) enterprise customers have high security requirements for accessing their systems, and 2) ramped-up hiring meant the company needed a scalable solution to manage and review the devices the 100-percent-remote workforce uses to access company assets. Add into this mix the drivers themselves, who have wildly disparate levels of technology expertise and often access the RunBuggy app on the go from mobile devices.

"If we're not secure enough, we won't be allowed to access enterprise customers' systems," said RunBuggy CTO Sasha Jovicic. "So our security directly impacts our ability to interact with

**Region:**

USA

**Industry:**

Software

**Size:**

- » 200+ team members, 100 percent working remotely
- » Around 17,000 active drivers

**Solution:**

Beyond Identity Secure Work, Beyond Identity Secure Customers

**Integrations:**

Okta

**Results:**

- » Reduced driver onboarding time to under one minute
- » Increased assurance employees are accessing resources via approved secured devices

F500 customers.” At the same time, RunBuggy needed to make it as easy as possible for drivers to access the mobile application. The company needed a way to level up security for its employees, its enterprise customers, and the drivers—some of whom were using flip phones before using the RunBuggy app—while at the same time making it as easy as possible for everyone to access the resources they need.

## Solution: Simple, secure logins for both customers and employees

RunBuggy was in the process of adding security such as single sign-on (SSO) functionality for its workforce when Jovicic heard about Beyond Identity’s passwordless solutions. Going passwordless fits the company’s innovative, problem-solving DNA. “Our goal is to be innovative and ahead of everybody,” Jovicic said. “We needed a process that would increase security yet not impact the usability for the end users.”

RunBuggy began talking with Beyond Identity about the company’s needs, initiating a proof of concept (POC) on an aggressive schedule. Based on the POC results, RunBuggy deployed Secure Workforce first, and three months later deployed Secure Customers.

## Results

### ***Direct impacts on revenue and margins***

Reducing the complexity of the driver onboarding process translated not only to ease of use for drivers; the increased app usage also translated directly to increased volumes and margins.

### ***Simple, secure driver onboarding drastically reduces support calls***

Another dramatic result RunBuggy has seen since deploying Secure Customers is the decrease in support needs from drivers. RunBuggy’s enterprise customers, who often have hundreds of drivers, provide each of them with login credentials. In the original process of onboarding drivers, Jovicic said 99 percent of them needed attention from the RunBuggy side. Since the company transitioned to Secure Customers, once a transporter has entered a driver’s information, they only have to click one link before they can get to work. “That part of simplifying onboarding was huge for us,” Jovicic added.

The company was initially concerned about using a new technology with customers that were less tech-savvy, but Jovicic said the feedback has been very positive.



***“We used to get a lot of support calls, sometimes once a week, from drivers who couldn’t remember their passwords. But we’ve virtually eliminated those kinds of calls, which has reduced the burden a lot on our customer support.”***

Sasha Jovicic, CTO, Runbuggy

## ***A zero-trust model for accessing internal resources***

As RunBuggy expanded, the company wanted more visibility into the devices in their environment. “We are striving for a zero-trust model,” said Senior Director of Security and Audit Max Graupner. “We need to know who you are and what device you are using when you access company resources.”

Secure Workforce went beyond the company’s existing sign-on solutions, which included multi-factor authentication (MFA), by combining authentication events with the actual device posture at the time of authentication. This was important for RunBuggy’s fully remote employees and outsourced customer service representatives. With the Beyond Identity credential, the company can enforce security measures when devices are added and, before any user is granted access, rule out threats before they ever have a chance to arise.

## ***Scalable yet flexible device management***

RunBuggy’s rapid growth also meant the company needed a solution that would scale with them. Beyond Identity’s Secure Workforce simplified the sign-up and sign-in process while integrating fully with its Okta SSO. In addition, if a company-issued device breaks, RunBuggy can now let an employee temporarily use their own device while a replacement is shipped out, as long as it meets the device posture requirements. This preserves the integrity of the company’s zero-trust security without losing valuable time.

*“Beyond Identity has exceeded my expectations,” Jovicic said. “Our deployment time frame was aggressive, but we had great support from the engineering and product teams from Beyond Identity who made it happen. It’s also seamless for my customers, and we are getting all positive feedback.”*

## **Beyond Identity**

Beyond Identity is fundamentally changing the way the world logs in—eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user’s identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out [www.beyondidentity.com](http://www.beyondidentity.com).

**GET A DEMO**

[beyondidentity.com](http://beyondidentity.com) | [info@beyondidentity.com](mailto:info@beyondidentity.com)

**BEYOND  
IDENTITY**