

# unqork

BEYOND  
IDENTITY

Unqork shrinks security risk with continuous,  
device-based, passwordless MFA



**REGION:** North America/US

**INDUSTRY:** Software

**SIZE:** Nearly 600 employees,  
mostly in the US

**SOLUTION:**

Secure  
Work

**RESULTS:**

- 95 percent employee enrollment
- 50 percent of employees enrolled within the first 60 days

# UNQORK

## Unqork shrinks security risk with continuous, device-based, passwordless MFA

### About Unqork

Unqork is a fast-growing, \$2 billion unicorn that was designated one of Fast Company's 10 most innovative enterprise companies in 2022. The company's no-code platform enables creators to build complex enterprise applications without writing a single line of code.

### Challenge: Reduce risk as the perimeter grows

Unqork is a remote-first company that experienced incredible growth amid the pandemic—almost tripling in size from 2020 to 2022. This presented a challenge for Global Chief Information Security Officer Marcos Christodonte II, who started with Unqork that spring. How could the company onboard so many new remote employees without increasing the risk of unauthorized access?

He wanted a solution that did not rely solely on the industry standard two-factor authentication (2FA). "Two-factor can provide a false sense of security—although it's a must-do, it's no longer enough," Christodonte said, citing security incidents in his previous experience where users had accepted unprompted push notifications on their phone.

He also wanted to eliminate passwords altogether. Passwords are a security weak point, with approximately 80 percent of security breaches involving stolen credentials. "From my perspective, your passwords will inevitably become

compromised and end up in a public database,” Christodonte said, noting that users will often reuse passwords from personal accounts on their company accounts.

Any solution Unqork deployed also needed to work seamlessly with the existing Okta single-sign-on (SSO) that its remote-first, cloud-first workforce already used.

## Solution: Eliminate passwords while securing endpoints

Christodonte looked at Unqork’s overall architecture from a security perspective and searched for solutions that fit into that architecture while meeting Unqork’s policy requirements in three specific areas.

First, he wanted the ability to eliminate passwords, for security as well as improving the user experience. Second, he wanted device-level authentication. Third, he wanted to couple that authentication with device posture checks, continuously verifying the existence of certain critical security settings or that a particular OS version or patch was in place.

He scheduled proof-of-concept implementations with Beyond Identity and several competitors. “The proof-of-concept with Beyond Identity was very smooth,” Christodonte said. “With some of the competitors it was pretty bumpy. Other solutions also focused more on the UX and UI, and were weaker on device trust, something I weigh more heavily.” He noted some competitors didn’t have an integrated device trust model, instead leveraging third-party integrations. In other cases, competing solutions didn’t have integrations with the endpoint threat detection and response tools Unqork was using.

Ultimately Christodonte chose Beyond Identity’s Secure Work product for its device-level authentication, passwordless user experience, flexible device policies, and solid proof-of-concept. “Secure Work was a robust solution that allowed me to structure policy based on risk, and that was important to me,” he said.

## Results: Enhanced, flexible authentication that employees love

Within five months, 95 percent of Unqork employees were enrolled in Secure Work, half of them within the first 60 days. Employees were allowed to enroll without a specific deadline, so the high percentage of registered users reflects feedback Christodonte saw in company message boards that Unqork users very much enjoy the passwordless experience.

As for implementation, "It was very smooth from start to finish, and Beyond Identity gave timely, thoughtful responses throughout," he said. No specific training for users was required beyond a FAQ. "The platform is very intuitive," Christodonte added. "It's very easy to understand, manage, and update over time." More than 95 percent of Unqork users now actively use the authenticator.

When asked about the impact Secure Work was having on the company, he responded, "Unauthorized SaaS access could lead to a number of bad outcomes, including data loss, data theft, and potential compliance or legal impact. Now we're able to improve on our access security with more enhanced authentication factors, and verify the device, both from an authentication perspective and a posture stance. I can take the controls I care about—the existence of certain security applications and OS versions, for example—and validate them continuously for user application authentication, all while not relying on two-factor and eliminating passwords."

When asked about working with Beyond Identity as a company, Christodonte had this to say: "The solution itself is strong, and from day one the team has been collaborative and open-minded, with strong engagement and customer support. We're looking forward to this strategic partnership."

Ready to Explore Passwordless Workforce Solutions?

GET A DEMO

[beyondidentity.com](https://beyondidentity.com)

[info@beyondidentity.com](mailto:info@beyondidentity.com)

BEYOND  
IDENTITY