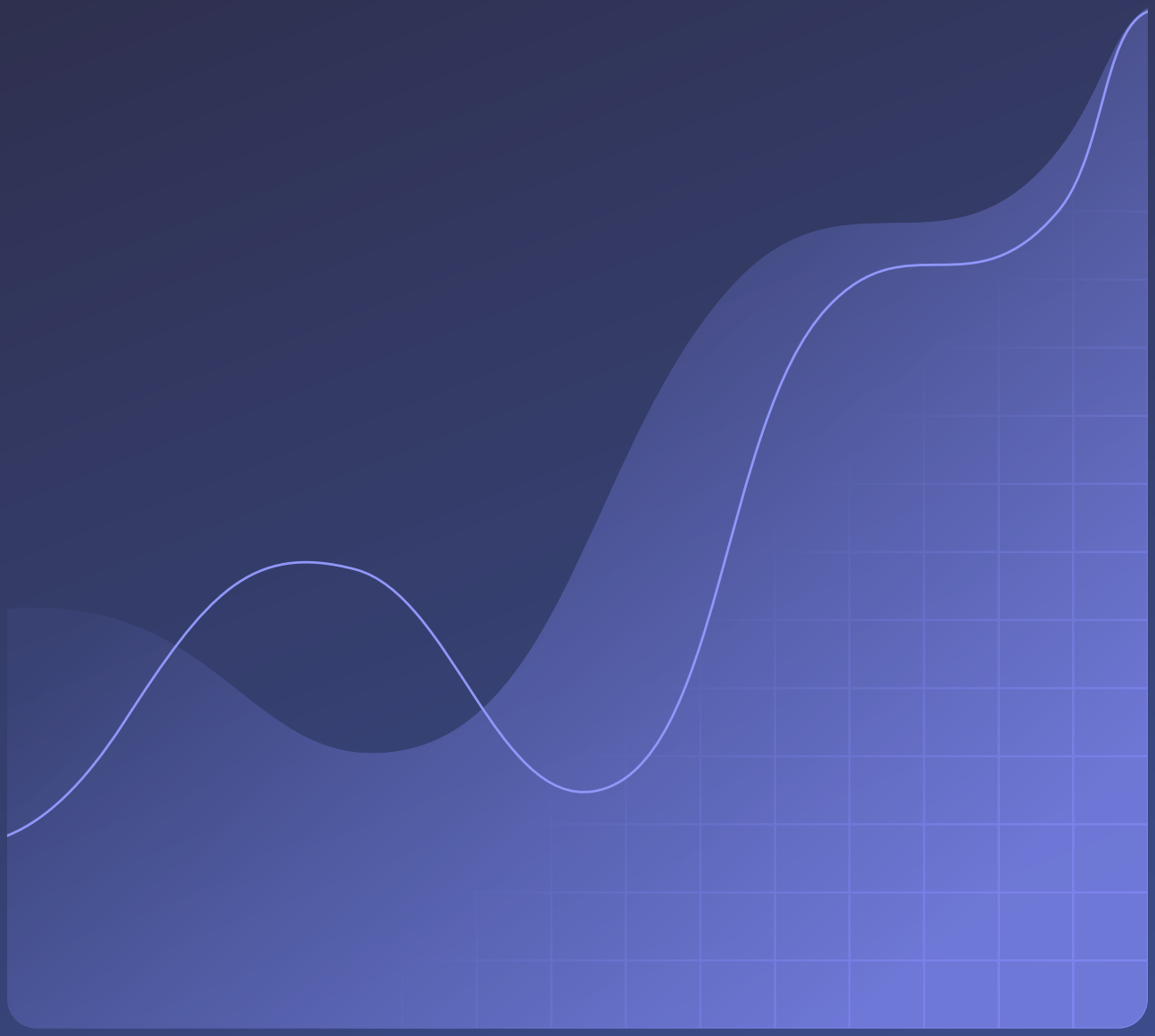
DASHLANE

CASE STUDY

How a Fully Remote Tech Company Secures Access While Minimizing IT Burden



Wonolo

Company description

Wonolo is a technology company that created and maintains an on-demand job marketplace platform.

Industry

Tech

Company size

215 employees

The goal: Effectively protect remote, globally distributed employees with a holistic solution

As a job marketplace platform company, Wonolo serves as a connector between individuals looking for fulfilling work and businesses seeking quality talent. More than 1 million workers have used Wonolo's technology platform to find jobs in different industries, with more than 3 million jobs posted to date.

Wonolo's own employees work remotely from across North America and the globe. Without a physical office, the IT team needs to handle everything remotely, from deploying and managing tools to ensuring visibility into potential threats.

The company had a robust security program in place that protected multiple layers. The IT team and the company leadership understood the importance of a password manager, and they had a solution deployed. However, the existing password manager had limited features. Wonolo also wasn't getting the full value from it because employee adoption was a struggle.

"Security is always evolving, and we've always tried to make sure we're changing along with the technology," explains Waynn Lue, Vice President of Engineering at Wonolo. "We knew the need for a password manager early on. So we didn't need to be sold on the value of a password manager, but we needed to ensure we got high adoption across the entire organization as we rolled it out."

The IT team didn't have the complete visibility they wanted into credential risks across the organization. The lack of visibility can expose any company to risk, but even more so a remote workplace that handles a lot of sensitive user data.

Wonolo needed a new credential management solution that could:

- Protect their remote workforce cost-effectively
- Enable teams to securely distribute access to shared accounts
- Minimize IT burden on the small team for tasks like password recovery

> "Being able to take a heavy lift off our team doing password recovery was incredibly important, as was empowering our users to utilize self-service options."
>
> **Maranda Kelley**, IT Manager, Wonolo

The solution: A user-friendly credential manager that ensures 100% adoption and provides visibility into risk

Wonolo's existing solution only provided visibility into risky passwords at the individual user level. As they evaluated potential vendors, the IT team's priority was to gain a better understanding of their credential risks across the organization.

Other top selection criteria included:

- Organization-wide password health scores
- Easy, zero-touch deployment
- Simple tool management to minimize IT lift
- User-friendly features to help ensure strong adoption
- MFA enforcement capabilities

Dashlane checked all those boxes—and more. Wonolo was swayed not only by Dashlane's comprehensive and robust security capabilities, but also by the strong brand reputation.

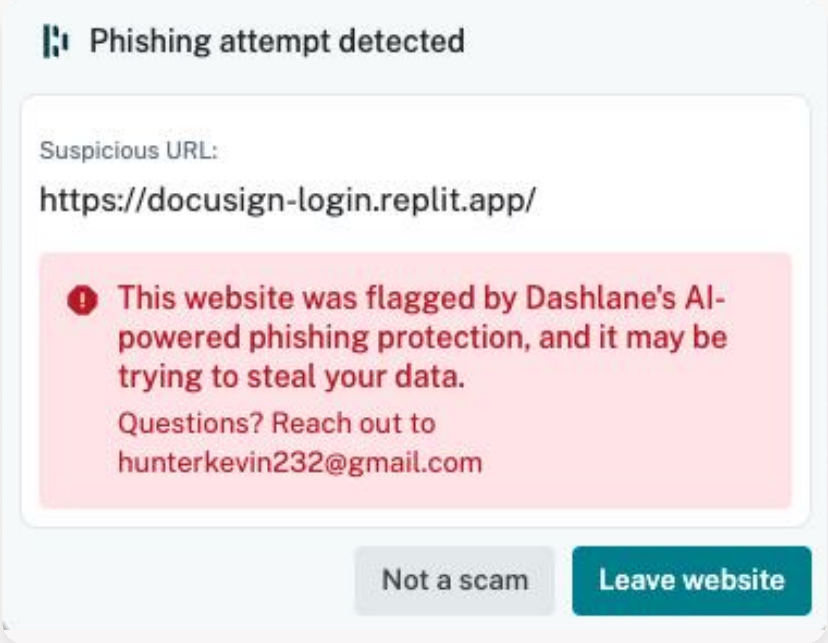
> "We looked at other vendors like LastPass, but because Dashlane had such a better history with security and device encryption, it was a big selling feature. We wanted to make sure we were choosing the best option."
>
> **Maranda Kelley**, IT Manager, Wonolo

After implementing Dashlane, Wonolo gained a more complete view of their employee security behaviors, enabling the IT team to further close risk gaps.

"We had visibility at the user level, where they could understand what weak, reused, or compromised passwords they had in various places," explains Waynn. "Once we moved to Dashlane, it was really beneficial to have that at the organizational level."

When Dashlane launched Credential Protection—a first-of-its-kind suite of proactive credential security features—Wonolo upgraded to get the full power of the Dashlane Omnix™ platform, including:

- **Credential Risk Detection**, which provides visibility across the entire organization, inside and outside the vault, to proactively uncover risks and enable fast mitigation.
- **Credential Risk Alerts & Notifications**, which automate risk response through in-browser alerts and Slack notifications so employees to immediately close security gaps. credential risks immediately
- **AI Phishing Alerts,** which deliver real-time, in-context alerts that serve as a critical last line of defense and empower employees to outsmart phishing attacks.s



The results: 100% adoption, enhanced protection, and boosted security culture

Since deploying Dashlane, Wonolo has achieved complete adoption across its workforce, integrating the tool into their mobile device management program.

New hires must onboard to the credential management platform before they can receive shared credentials, as well as other sensitive data through Secure Notes. The onboarding process is simple and straightforward, with IT staff easily enforcing the tool within Google Chrome. This ensures secure access to all critical data and helps boost the company's overall security posture.

When Wonolo first rolled out Dashlane in 2020, their teams were working remotely due to pandemic restrictions. While initially that was a temporary measure, the company eventually decided to make remote work a permanent model.

> "Moving into a permanent remote environment was a lot easier with Dashlane."
>
> **Maranda Kelley**, IT Manager, Wonolo

The company continues to renew their Dashlane solution every year, as they view the brand as their best option for secure credential sharing, ease of IT management, embedded MFA, and the ability to create groups and granularly manage password sharing at the user level.

"A lot of other password management tools are adopting those features. But based on other vendor demos we've looked at, Dashlane stands out with the ease of use and adoption rates," Maranda shares. "And having access to these features earlier has been incredibly helpful."

Dashlane has enabled Wonolo to roll out MFA across the entire organization. This feature is especially valuable for those teams who have access to highly sensitive data.

“Our head of finance said that’s the most important Dashlane feature from a security perspective, and the head of finance obviously has access to a lot of secure information,” says Waynn. “So it’s been really helpful that she can make sure multi-factor authentication is shared across the people on our team who need access to it.”

Dashlane is an integral part of Wonolo's security culture. The Password Health score, for instance, gives IT an opportunity to educate employees about the importance of security and good password hygiene. This also fosters a sense of responsibility for security across the entire organization.

“It’s been good to have Dashlane because it’s a way for people to use tools to be secure. We’re not just telling them not to do something that’s not secure, like emailing passwords. We’re giving them the tools to be able to do those things securely,” Waynn says. “That has been really, really big.”

The IT team continues to evolve its security approach. And they’re exploring how the new Omnix features can further enhance their security posture and enable both IT and employees to defend against threats proactively.

> “Dashlane has been a really great partner to us. We’ve had really good experience using it, and we’re happy to have it as one of our core tools that every single user has at our company.”
>
> **Waynn Lue**, Vice President of Engineering, Wonolo

See for yourself how Omnix delivers proactive credential security.
Request a demo