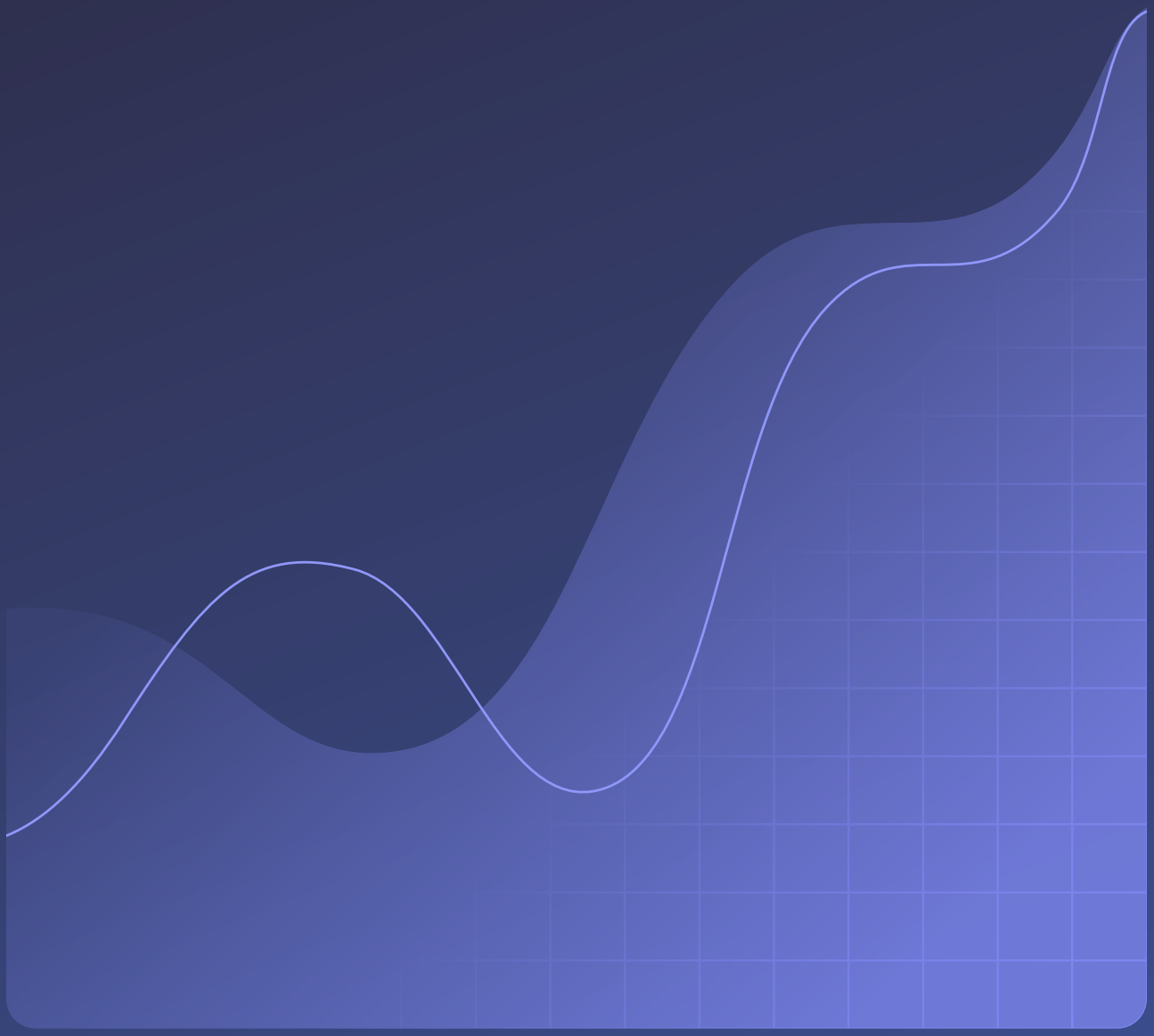
DASHLANE

CASE STUDY

How South Carolina Aquarium Got Compromised Passwords Down to 0 for 200 Employees



South Carolina Aquarium

Company description

South Carolina Aquarium is located in Charleston, South Carolina and welcomes thousands of visitors each year. The aquarium showcases the state's diverse ecosystems while providing education, conservation, and engaging guest experiences.

Industry

Recreation

Company size

200 employees

The challenge: Securing credentials in a high-stakes, always-on environment

As South Carolina Aquarium grew and adopted more digital tools, the organization recognized the need to strengthen its credential management.

Employees were using a variety of unsecure methods—browser-based password storage and personal email accounts—to keep track of credentials. Personal and work credentials were sometimes mixed together, and admins had little visibility and control.

“There was nowhere centralized for passwords,” says Jamie Ratcliffe, IT Manager at South Carolina Aquarium, where he’s worked since 2012. “So we started to really look into securing passwords and other parts of our organization.”

The aquarium’s 3-person IT team supports both guest-facing technologies, such as interactive exhibits, digital signage, and AV show controllers, and mission-critical systems that keep animals safe and healthy. While the team has ensured these systems have redundancy built in, credentials remain a key factor in keeping many of these systems secure.

As the organization moved to more cloud-based tools, the number of credentials to manage increased. Without a unified approach, it was harder to monitor password health, enforce best practices, and reduce risks from weak, reused, or compromised credentials.

Adopting a credential manager became a major step toward safeguarding both staff and operations while keeping workflows smooth.

The solution: Centralized, easy-to-use credential security

When reviewing credential management solutions, the aquarium's IT team had clear requirements:

- **Zero-knowledge architecture,** ensuring that only the user, not the credential manager or any third party, can decrypt a user's vault
- **Easy-to-use browser extension,** reducing friction and increasing adoption
- **Secure password sharing,** enabling teams to safely share access when budgets limit the number of licenses
- **Automated risk alerts,** informing employees of weak or reused passwords and guiding them to self-remediate

Dashlane checked every box, so the IT team rolled it out to all South Carolina Aquarium employees. Then, when Dashlane launched the Omnix™ proactive credential management platform in 2025, the team upgraded to Omnix to secure every employee credential, whether or not it's stored in a vault.

With Omnix, admins get visibility across all employees to prioritize mitigation and keep risks from turning into threats. Credential Risk Alerts encourage employees to immediately secure at-risk credentials and close security gaps. And AI Phishing Alerts keep employees safe as they browse with phishing-resistant autofill and in-context employee alerts the moment they visit a suspicious site.

Omnix integrated seamlessly with the aquarium's existing SSO setup using Microsoft Entra ID, making adoption simple and fast for employees.

"It's super easy," Jamie shares. "Employees just logged in automatically because they're in the Edge browser, which is connected to their business account."

The results: Stronger security and smoother operations without added friction

Since choosing Dashlane, South Carolina Aquarium has significantly strengthened its credential security posture while making day-to-day work easier for both employees and IT. Jamie says the organization has zero compromised passwords detected, a major improvement over its previous unmonitored state.

“Having a proper solution in place for password health makes a huge difference,” Jamie says. “Security is in a much better place overall.”

Work credentials are no longer scattered across personal Gmail accounts and browser storage. Instead, employees securely store and access work accounts through Dashlane, giving IT clear visibility and confidence that passwords are protected.

Many employees also appreciated their complimentary Friends & Family plan, which enables them and up to nine loved ones to secure and easily access their personal credentials.

In addition, secure password sharing has enabled teams to collaborate safely when individual licenses aren’t available, removing a long-standing operational workaround without introducing new risk.

From an IT perspective, centralized password management and automated logins have reduced time spent on resets, access issues, and troubleshooting. Admins can monitor security behavior, and employees are guided by Credential Risk Alerts to fix weak or reused passwords on their own, eliminating the need for IT to enforce password hygiene manually.

> “Credential Risk Alerts are great. They’re quite important so employees can understand that they've got all these passwords that are exactly the same and be told to change them.”
>
> **Jamie Ratcliffe**, IT Manager, SC Aquarium

Jamie also credits Dashlane’s password generator with changing employee behavior for the better.

“The generator’s a very good feature,” he said. “We don’t make passwords up anymore. We just create them with the generator.”

Dashlane has transformed credential security at the aquarium from a fragmented, ad hoc process into a centralized, reliable system, giving IT and employees peace of mind in an environment where reliability truly matters.

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