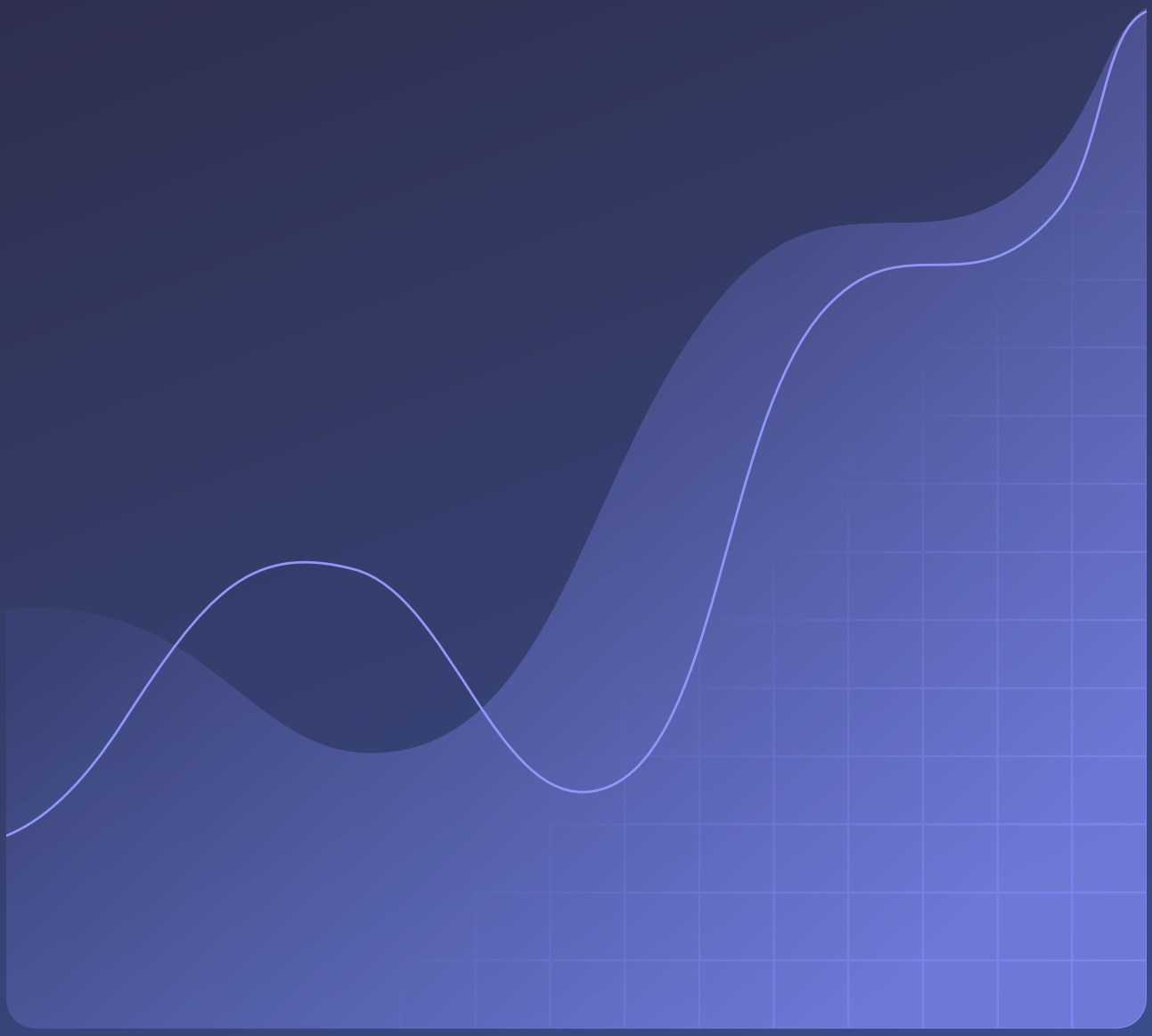
DASHLANE

CASE STUDY

How a Large Convention Center Took Control of Password Security Across 500 Employees



rai AMSTERDAM

Company description

RAI Amsterdam is a large international convention and exhibition center in Amsterdam that hosts trade shows, conferences, and large-scale events across a physical campus and hybrid IT environment.

Industry

Events and hospitality

Company size

500 employees

The challenge: Regaining control over fragmented credential practices in a complex hybrid environment

As RAI Amsterdam's digital footprint grew, so did the complexity of managing credentials across employees, systems, and devices. With only a handful of internal IT decision-makers supporting about 500 employees, the team needed a scalable way to bring consistency and control to password practices without slowing down day-to-day operations.

Before Dashlane, password management was largely fragmented. Employees relied on convenience-based tools such as browser-saved passwords and native device password storage. While these tools were easily accessible, they created significant challenges for IT in terms of visibility, governance, and standardization. Plus, it made securely offboarding employees difficult.

According to IT Project Manager Bas Vasterman, who's worked for RAI Amsterdam for 25 years, "People were using the password managers from Chrome, Microsoft, whatever was handy for them...and yeah, we didn't have control of that."

This lack of centralization created a number of operational risks. Password reuse and duplication were common, employees often stored multiple credentials for the same service, and IT had limited insight into how sensitive access was being managed across the organization.

At the same time, RAI Amsterdam operates in a highly hybrid environment. Employees work across Windows, Linux, and Apple devices while also interacting with systems tied to physical access control, commercial Wi-Fi services, and event infrastructure. This mix made it even more important to have a unified approach to credential security.

To sum up his password manager requirements, Bas says, "What we needed was something that was multi-device compatible, had data storage inside the EU, and had an admin backend to see adoption and how people were really using it."

The solution: Centralizing password management and strengthening governance

To identify the best credential management solution, RAI Amsterdam worked with Pro CISO, a Netherlands-based firm that acts as an outsourced security expert, helping clients protect their systems and meet security compliance requirements without hiring an in-house security executive. Bas has worked with his Pro CISO cybersecurity consultant, Mario, for four years now.

“We look at security risks daily,” explains Bas. “If there’s something big happening in the world with a hack or I need backup, I ask Mario, ‘Can you look at this?’ And then we combine our answers to get a good solution for the company. It’s great working with Mario.”

For RAI Amsterdam to standardize credential management, Mario recommended Dashlane. After about 8 years of using Dashlane in his personal life and for his own business, Bas was familiar with the credential security solution and agreed that it met his requirements, including having EU-based data residency.

Omnix™ is the only platform to secure all employee credentials, whether or not they’re stored in a vault. It enhances visibility into credential risk, helping security teams identify weak, reused, or potentially compromised passwords at scale. It also introduces proactive protections against phishing and credential-based attacks while giving IT teams a clearer understanding of how credentials are being used.

Omnix also supports RAI Amsterdam’s broader identity strategy by integrating with SSO. This helps reduce reliance on standalone passwords for internal apps while maintaining secure authentication flows. Such alignment is particularly important in an environment where SSO is heavily used for business-critical systems.

> “It was a combination of everything that made the team decide to go for Dashlane.”
>
> **Bas Vasterman**, IT Project Manager, RAI Amsterdam

RAI Amsterdam deployed Dashlane Omnix to all employees, interns, and temporary staff, ensuring that credential security practices are consistent across every user type.

From a deployment perspective, the IT team was able to integrate Dashlane into their existing endpoint management workflows using Microsoft Intune and browser extension distribution. This allowed them to scale the rollout efficiently without requiring complex manual onboarding processes for end users.

The results: Improved visibility, control, and standardization

Since deploying Dashlane to all employees, RAI Amsterdam has significantly improved the consistency and governance of its credential management.

Password practices that were previously scattered across browser tools and personal devices have now been consolidated into a single, centrally managed platform. Employees can automatically create strong, unique passwords for each account while autofill capabilities reduce friction in daily workflows.

Now, IT has far greater visibility into password hygiene across the organization, making it easier to identify weak practices, reinforce security policies, and guide users toward safer behavior.

“Dashlane has helped us secure more than we used to,” Bas says. “Overall, I’m quite happy.”

Bas also appreciates the in-browser security alerts that detect employees’ at-risk passwords and prompt them to change those passwords with clear, simple guidance—no IT effort required.

Importantly, Dashlane has also helped RAI Amsterdam better align its security practices with its SSO strategy. With many apps already centralized through SSO, Dashlane fills the gaps for remaining systems that still rely on passwords, helping reduce risk across the broader environment.

While employee adoption required training and support—as is typical in large operational organizations—the IT team has been able to establish a stronger baseline for credential security across all user groups, including contractors and temporary staff.

Today, RAI Amsterdam continues to refine its security posture, balancing usability for employees with stronger governance and visibility for IT. Dashlane plays a central role in that strategy, helping the organization manage credentials more consistently across a complex and highly dynamic environment.

> "It's hard to keep up with the hacks and everything that's happening in the world. We have to be one step in front of the rest. Dashlane does that; we do it together."
>
> **Bas Vasterman**, IT Project Manager, RAI Amsterdam

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