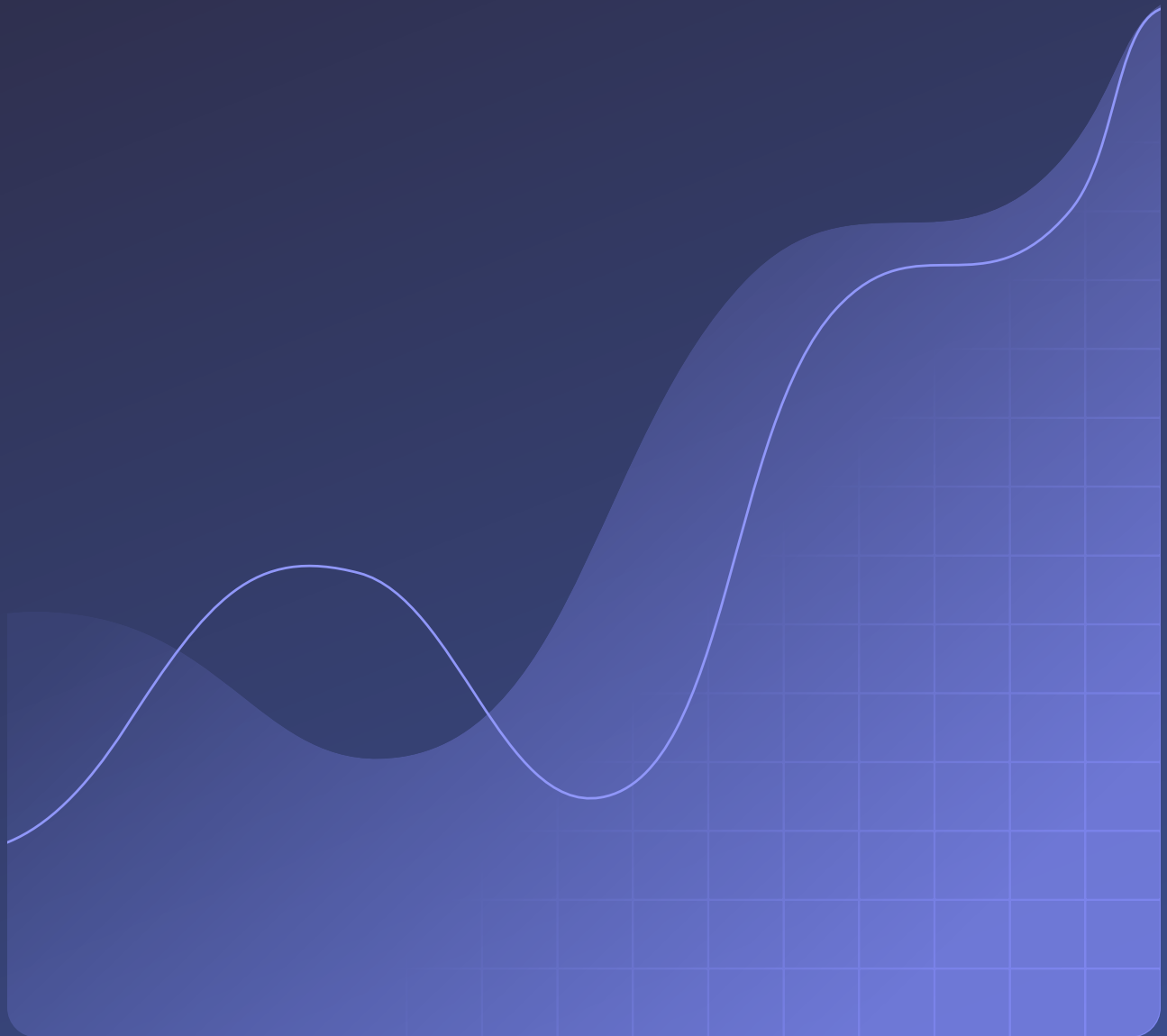




CASE STUDY

How a Leading SaaS Company Accelerates Growth Without Compromising Data Privacy





Company description

HelloCSE is a market leader in software technology that helps French employers manage mandatory employee benefits.

Industry

Software

Company size

120 employees

The challenge: Rapid growth without a consistent, secure method for managing passwords

HelloCSE provides a platform for France’s social and economic committees (CSEs)—mandatory employee-representative bodies—to manage employee benefits. The company has been recognized by a French government initiative called French Tech 120 as one of the country’s most successful startups poised to become world-class leaders.

A major CSE provider, HelloCSE serves a diverse range of customers. They include massive global enterprises, law enforcement agencies, and other types of organizations that handle highly sensitive data.

To serve their user base on the CSE platform—currently around 1 million employees—HelloCSE uses multiple accounts shared across teams. The shared accounts have access to private user information, and preventing unauthorized access to these accounts is critical.

In the early days, HelloCSE struggled with securely onboarding and offboarding employees to the shared accounts. Passwords were being shared unsecurely, typically by email. Many of the passwords were reused across different websites. And there was no consistent system for tracking onboarding and offboarding processes.

As the company grew rapidly, managing the expanding number of credentials manually consumed valuable time and resources.

“When employees have to ask the right person for a password to an account, maybe it’s fine if you’re a team of five. But if you have more employees, you lose time. It’s not efficient.”

Marin Godart, DevOps Engineer, HelloCSE

Their credential risk also expanded with the number of employees and clients. With limited visibility into password health and employee security practices across the company, the IT team couldn't manage the risk effectively.

While seeking new opportunities to scale, HelloCSE recognized that enhancing their security approach could drive business growth.

“We're a fast-growing company without external funding,” Marin shares. “We wanted to work with bigger companies, and bigger companies means bigger security requirements, like password management and encryption.”

“Security is a top priority for us—that's one of the main reasons we chose Dashlane.”

Marin Godart, DevOps Engineer, HelloCSE

The solution: A credential management platform that helps manage risks proactively

A longtime Dashlane user, Marin felt confident the tool would be a great fit for HelloCSE. Together with the company's financial director—another regular Dashlane user—he made the case to their board about investing in Dashlane to manage their password risks and protect data privacy.

“The key point was to be safer and make sure we don't have data leaks,” Marin says. “Dashlane was one of the first security products we invested in early on.”

Adoption of a new security tool across the entire organization can be challenging. Employees may be concerned about the impact on their workflows and productivity, and buy-in is especially difficult when they don't understand why the new tool is essential. Dashlane's onboarding resources helped eliminate that friction for HelloCSE.

“Onboarding was easy, and it was really nice to have the onboarding resources from the Dashlane team. It made the process easier and removed the resistance to change.”

Marin Godart, DevOps Engineer, HelloCSE

Since implementing Dashlane, the IT team has gained confidence in their ability to safeguard their clients' and users' sensitive data. Dashlane's group sharing feature allows the company to easily share passwords with new employees and among teams.

Teams can also securely store and share sensitive internal data with Secure Notes. The DevOps team, for instance, uses Secure Notes for key information for their staging environment and API secrets.

After the launch of Dashlane Omnix™—a proactive credential security platform— HelloCSE immediately recognized the opportunity to strengthen their security further.

With Omnix, HelloCSE gets complete credential protection, including:

- **Credential Risk Detection:** Gain total visibility across the entire organization to proactively uncover risks and enable fast mitigation, preventing risks from becoming reality.
- **Credential Risk Alerts & Notifications:** Automate risk response with in-browser alerts and Slack notifications that encourage employees to immediately close security gaps.
- **AI Phishing Alerts:** Real-time, in-context alerts empower employees to outsmart phishing attacks, serving as a critical last line of defense.

“The listing of [Dashlane Omnix on the AWS Marketplace](#) has made the purchasing process much easier and has also helped strengthen our relationship with AWS. Upgrading to Omnix was a logical choice for us, and it gave us more features.”

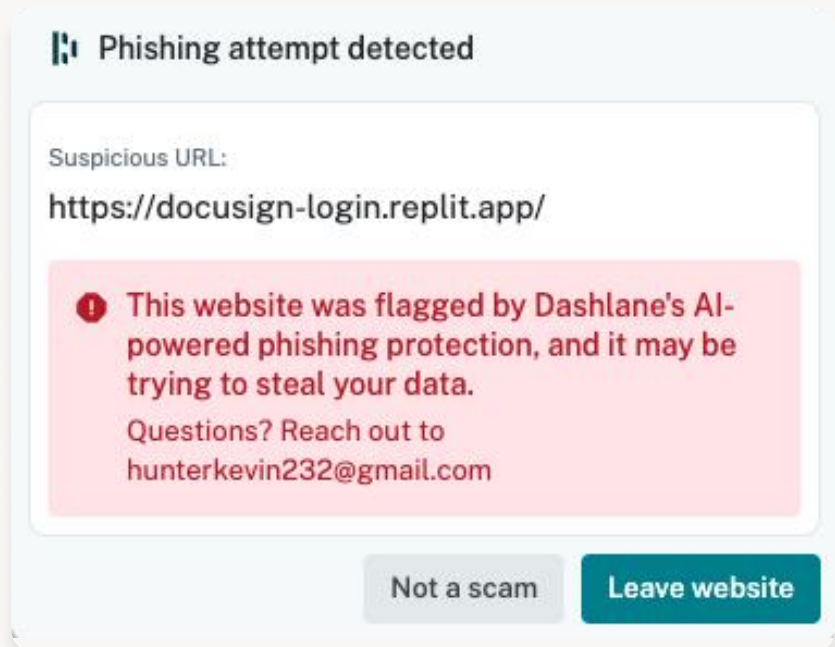
Marin Godart, DevOps Engineer, HelloCSE

The results:
A more mature approach to credential security that supports business growth

Dashlane has played an integral role in boosting HelloCSE's security posture and culture. Marin notes that many employees have dramatically increased their Password Health scores. Employees also feel more in control and aware of threats like phishing and the importance of good password hygiene.

“Having Dashlane has helped employees understand the importance of security, especially as we scaled to more than a hundred employees,” shares Marin.

“When you're growing, security is not necessarily the main focus because you have to focus on getting new clients. So we had a lot of work to do to ensure employee passwords are safe and help them understand passwords can be stolen through phishing—and Dashlane helped us achieve that.”



A recent acquisition of a competing business truly highlighted the value of the Dashlane platform for HelloCSE. The competitor had been in business for more than two decades. Many of their employees had long tenures and were accustomed to IT processes that differed significantly from HelloCSE's. This presented a big hurdle for onboarding the acquired company's team, especially for mission-critical roles such as software developers.

Dashlane made the acquisition process smooth, enabling HelloCSE to easily and securely share key operational information as they integrated the new employees.

"It was really easy to invite all the new employees to Dashlane and create a group to share all key information with them directly instead of explaining everything to them individually," Marin says.

Marin's team not only saved time but also easily standardized security across all the resources brought in from the acquired company—facilitating a smooth acquisition.

"Dashlane played a key role in the transition, helping us securely access new servers and websites and streamline onboarding for new employees."

Marin Godart, DevOps Engineer, HelloCSE

Dashlane constantly makes Marin and his team more efficient. When operational data needs changes, they simply update it in Secure Notes—and all the requisite teams instantly have access to the latest information.

As HelloCSE grows, their security matures continuously. One of their current initiatives is to obtain ISO certification, and Marin believes Dashlane will be instrumental in meeting the certification requirements.

“Dashlane will be good evidence for the ISO compliance audit,” he says. “And we also want to show prospects we do these kinds of things to make them more confident in our solution.”

See for yourself how Omnix delivers proactive credential security.
[Request a demo](#)