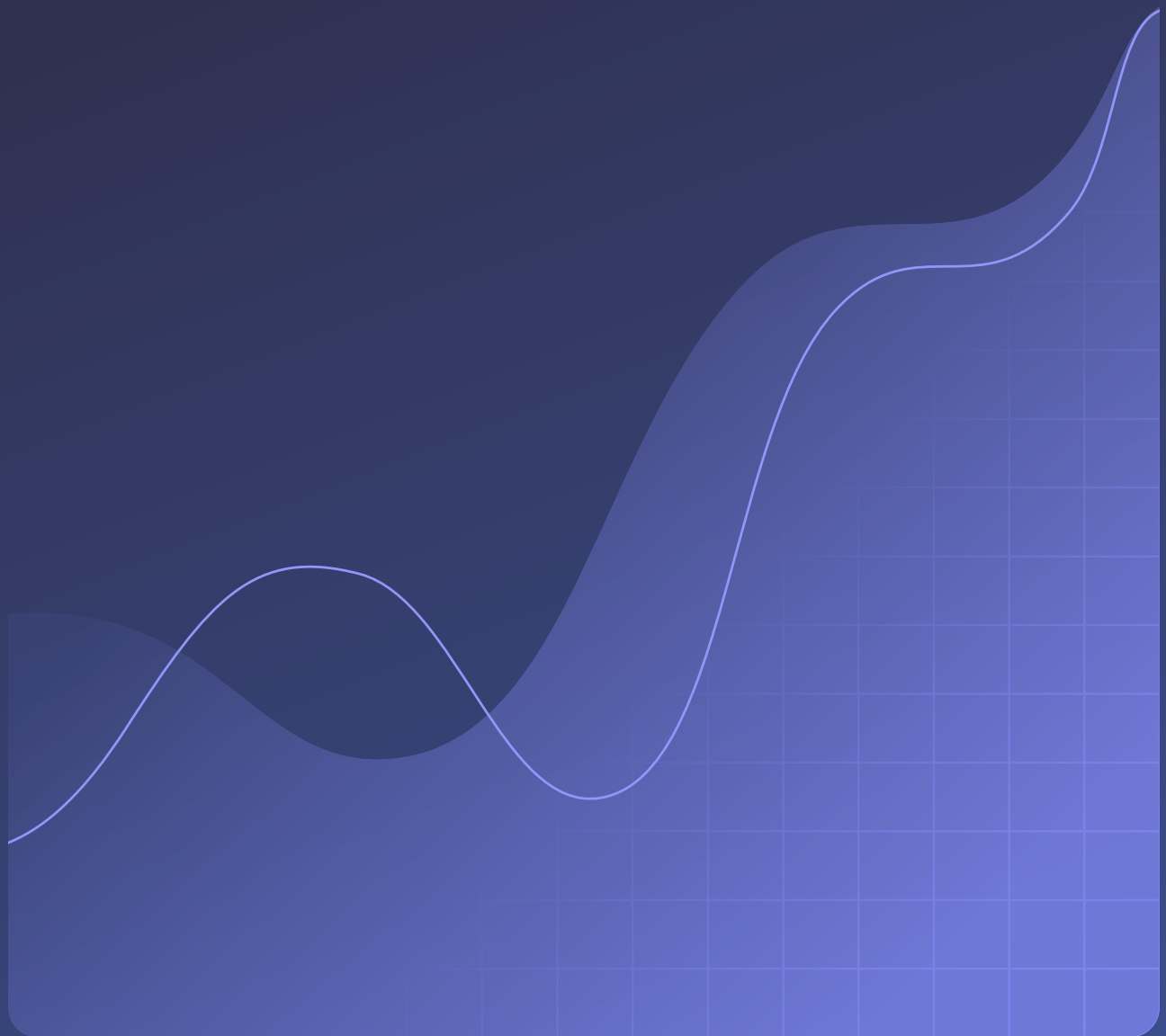




CASE STUDY

How a Financial Services Organization Guards Financial Fortunes and Aces Audits





Anonymous

Industry

Financial Services

Company size

100-500 employees

The challenge: Navigating remote work and compliance complexity

Founded in the mid-2000s, this financial services organization has become synonymous with innovation, diligence, and exceptional service in the financial sector. While the company boasts a stellar reputation, they grapple with unique challenges when it comes to safeguarding their information: They must ensure their data remains within Canada's borders.

This requirement poses additional complexities, especially when employees travel internationally or contractors live in other countries. Regular audits conducted by one of Canada's financial services further heighten the pressure to uphold strict compliance standards.

Nevertheless, this financial services organization remains unwavering in their commitment to cybersecurity and fostering a remote work environment.

This financial services organization recognized the need for a robust credential manager to enhance security, simplify compliance, and support their remote workforce. They required a trustworthy solution, which meant they were looking for top-notch technology.

“We needed advanced encryption methods to provide a high level of protection for our sensitive data.”

CIO at the financial services organization

However, the financial services organization knew that this technology would only be effective if employees were using it, so they sought an intuitive solution that their employees would want to use. Across the organization, employees must access the same accounts, which makes sharing credentials complicated because most people work remotely.

The financial services organization required a way to onboard new employees and securely manage and share credentials.

"Emailing passwords or writing them on sticky notes is a hard habit to break," explains the IT Manager.

The financial services organization's ideal solution would provide:

- Transparency for audits
- Fast onboarding
- Secure ways to share passwords
- Clear oversight
- A virtual private network (VPN)
- An intuitive user experience (UX)

The solution: A UX-friendly credential manager that builds a security culture

The organization's CIO had experience using Dashlane for their personal accounts. Using Dashlane made such a positive impression on them that they recommended it for the organization as a whole. While the organization evaluated various competitors, Dashlane stood out.

“Dashlane was the right choice from a security perspective.”

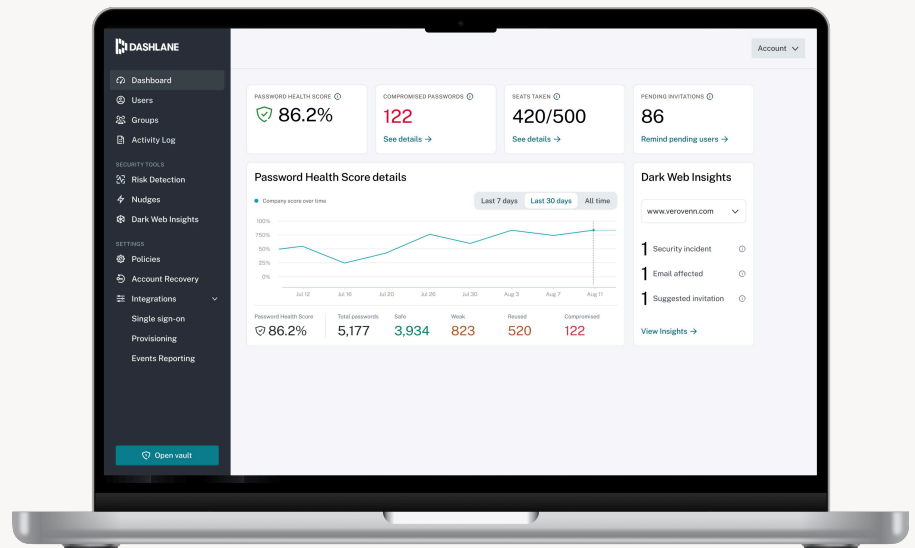
CIO at the financial services organization

“Dashlane has an intuitive interface that makes it easy for employees to understand the tool and want to use it,” the IT Manager adds.

What differentiated Dashlane from the competitors was the solution's ability to provide:

- A digital wallet that supports storing an unlimited number of payment types
- Secure Notes that give people a space to securely store and share information and documents
- A web extension that allows employees to work seamlessly and securely access their logins without repeatedly opening a separate desktop app
- Technology versatility means that employees can collaborate while using their preferred operating system
- A VPN that ensures a secure Wi-Fi connection and empowers users to browse privately anywhere
- Secure sharing that lets employees (and clients) securely share encrypted passwords with individuals or groups

- A mobile app that syncs users' data and credentials across all devices
- Cross-platform compatibility so employees can collaborate while using their preferred operating system
- An Admin Console that offers one centralized credential management system, including simple employee management and auditing when required



The results: Reducing risk while empowering employees

The organization decided to slowly roll out Dashlane, starting with a pilot user group to gauge the solution's impact and solicit feedback. Since then, the financial services organization has experienced significant improvements in cybersecurity and operational efficiency. Now, all employees are onboarded to Dashlane on their first day and use Dashlane daily.

"Dashlane is integrated into our security culture," the IT manager shares. "It's come to the point where we'll ask employees for their credentials, but they don't know them because they're in Dashlane."

Since partnering with Dashlane, the organization has remained pleased with the platform. From the beginning, they've appreciated how the cybersecurity solution safeguards their critical data. With Dashlane's zero-knowledge architecture, no one, not even Dashlane, can see users' passwords or other data.

The financial services organization is confident they found the right solution for their organization and their people. Employees were won over by Dashlane's positive impact on daily operations and how the solution made tasks simpler, including logging in.

"Dashlane's intuitive user interface and seamless integration across multiple devices have significantly improved our team's productivity by streamlining the login process and other password management tasks."

CIO at the financial services organization

Today, sharing credentials with authorized users is straightforward, and it's easy to find answers to security questions because those answers are safely stored in Dashlane's Secure Notes. The IT team has realized the benefits firsthand.

"Dashlane saves me time in two ways: With account recovery and device migrations," the IT manager explains.

If an employee gets locked out of Dashlane, it's simple for the IT team to help restore access for them. When the time comes for an employee to get a new device, migration is significantly faster with Dashlane, saving the IT team and the user the headache of reconfiguring access.

While the financial services organization appreciates that Dashlane is improving business operations, they know Dashlane does more than that: Dashlane is delivering complete credential security that harnesses the power of employees to protect the organization against breaches.

"Easier doesn't always mean safer, but with Dashlane it does," the IT manager says.

With Dashlane, the financial services organization reduces risk, and their Canadian regulatory audits have gotten simpler. Dashlane was the first major credential manager to achieve the latest version of ISO-27001 certification and to adhere to the highest standards of managing risk related to security.

Dashlane is also SOC 2 Type II Compliant and follows GDPR guidelines. Dashlane's VPN helps this organization ensure that all their data stays secure and in Canada.

Cybersecurity will always remain a top priority at this financial services organization, and they have even gamified the experience with cybersecurity initiatives that include giveaways for high Password Health scores. The financial services organization views these initiatives and Dashlane as an investment in their cyber health that pays dividends.

“Dashlane is helping our employees establish good cybersecurity habits.”

IT Manager at the financial services organization

As they continue their cybersecurity journey, the financial services organization remains committed to leveraging Dashlane's capabilities to safeguard their data and empower their workforce. The organization is currently working to bolster their end-user policies, and plans to increase their access requirements by leveraging multi-factor identification.

"Dashlane reinforces our company's overall cybersecurity posture," says the CIO.

With Dashlane at their side, this financial services organization is well-equipped to navigate the evolving cybersecurity landscape while maintaining their reputation for excellence in the financial sector.

They feel confident in the knowledge that they're doing their part to keep their clients and their data safe, with the IT manager advising, "Don't take a risk. Use Dashlane."

See for yourself how Omnix delivers complete credential security.

[Request a demo](#)