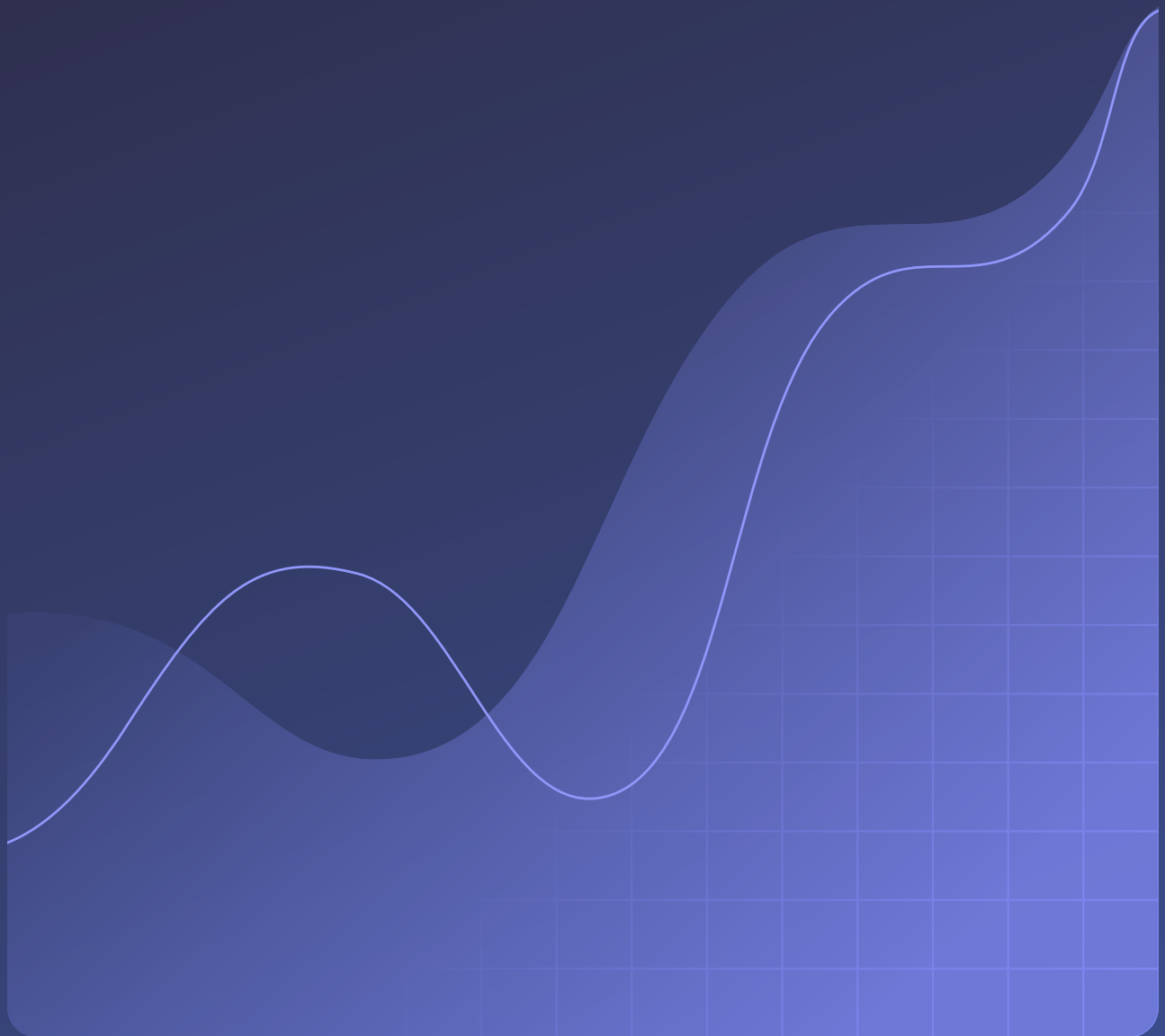




CASE STUDY

How a Washington, D.C. Think Tank Went from Cyber Vulnerable to Vigilant





Company description

Headquartered in Washington, D.C., [New America](#) is a think tank dedicated to honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

Industry

Nonprofit

Company size

150-180 employees

The challenge: Protecting classified data and providing user-friendly credential management

New America is a new kind of think tank in an era marked by rapid technological advancement and shifting social landscapes. Headquartered in Washington D.C., New America represents a fusion of diverse organizations—a research institute, a technology lab, a solutions network, a media hub, and a public forum.

The organization's hybrid workforce spans the United States and beyond. They navigate a fluctuating employee count ranging between 150–180 individuals, made up of full-time staff and seasonal interns.

To perform their critical work, New America handles highly sensitive, politically charged data, including information from the State Department, which they must safeguard. Adding to the pressure, other institutions in the industry have suffered cyberattacks, and a decade ago, New America endured a state-sponsored attack.

When Abhilash Rajan, the Senior Director of Technology, Systems, and Facility Operations, joined New America, he discovered that the organization lacked a robust password management system. The members of the leadership team used Google Sheets to store passwords and shared the spreadsheets with administrative assistants.

“We were especially worried about the vulnerabilities this strategy created when traveling, which our members of the leadership team frequently do,” Abhilash explains. “Passwords were visible and the solution could be breached.”

The members of the leadership team weren't the only employees who faced credential challenges: Some staff were managing almost 200 credentials, which is impossible for anyone to remember without help. The IT team realized that addressing these vulnerabilities demanded more than good intentions—it required the right technology.

“Good password hygiene isn’t just going to happen. You need the tools to support it.”

Abhilash Rajan, Senior Director of Technology, Systems, and Facility Operations, New America

Relying on grants and donations for funding, New America often needs to provide information about their cybersecurity, including whether they have a password manager in place. They wanted to be able to confidently answer those questions.

“To protect our organization and our classified information, we have to be on top of our InfoSec strategy,” says Abhilash. New America knew it was time to find a credential management solution to fortify their cybersecurity framework and ensure seamless operational efficiency.

New America's ideal solution would provide:

- Streamlined access for employees
- Clear oversight for credential management
- Licensing that scales to match staff fluctuations
- A secure way to store and share credentials
- A VPN employees could use on the go

The solution: A credential management solution that secures data and streamlines access from anywhere

When Abhilash evaluated the market, Dashlane stood out as a comprehensive credential management solution that offered a VPN.

“Dashlane’s VPN is extremely beneficial when our employees travel because it keeps our traffic encrypted,” Abhilash shares. While finalizing his decision, Abhilash had the opportunity to speak with Dashlane’s CEO, which helped him see how much his feedback was valued, solidifying his choice.

“Dashlane checks all the boxes.”

Abhilash Rajan, Senior Director of Technology, Systems, and Facility Operations, New America

With Dashlane, New America benefits from:

- A VPN that ensures a secure Wi-Fi connection and enables employees to browse privately anywhere
- 2-factor authentication (2FA) that adds a layer of security to passwords by requiring two steps when logging in
- A digital wallet that supports the unlimited storage of payment types
- Secure Notes that give employees a space to securely store and share information and documents
- Secure sharing that lets employees securely share encrypted passwords with individuals or groups
- A mobile app that syncs employee data and credentials across all devices
- Dark Web Monitoring that alerts employees when their passwords have been compromised and provides recommended next steps to secure those passwords

The results: Stronger oversight, faster access, and a competitive differentiator

New America started with 100 Dashlane licenses and made the solution part of their onboarding process. Now, the IT team sends new employees a Dashlane invitation on their first day, making onboarding straightforward and ensuring everyone has the appropriate level of access. As an organization with many remote employees, the IT team also appreciates that it's fast and secure to offboard.

"We're engaging in best practices and have leading technology with Dashlane," shares Abhilash. "Dashlane gives me a sense of satisfaction in our cybersecurity. Now we know who has access."

Dashlane Dark Web Monitoring is always on, scanning billions of breach records to help ensure no threat goes undetected. If credentials were to be compromised, Dashlane would automatically send an alert.

"If anything happens, Dashlane will notify me and I can evaluate the situation."

Abhilash Rajan, Senior Director of Technology, Systems, and Facility Operations, New America

The solution's user-friendliness has stood out to Abhilash.

"I haven't had a reason to contact support," he says. "That speaks volumes about Dashlane. And we can access passwords anywhere and on any device without worrying about getting breached. Dashlane works everywhere."

Whether working in the office, from home, or on the go, employees can autofill logins, saving them time and the hassle of trying to remember their credentials.

“With Dashlane, logging in is simple, secure, and takes a matter of seconds,” Abhilash adds.

New America has found numerous use cases for Dashlane.

As Abhilash explains, “Dashlane is more than a password manager.”

Secure Notes are critical at New America, enabling employees to store recovery codes, driver’s license details, TSA information, and more. The solution has even helped employees in a pinch because managing this much information would be challenging without Dashlane.

“There have been a few instances where Dashlane has really saved me,” Abhilash recounts. “Like when I was booking a flight and didn’t have my passport or wallet.”

“Any chance I get, I recommend Dashlane. The ease of use and secure access are unbeatable.”

Abhilash Rajan, Senior Director of Technology, Systems, and Facility Operations, New America

When talking to their investors or auditors, it’s now easier for New America to answer questions about their cybersecurity, and they’re confident in their responses. Beyond having a trustworthy credential management solution in place with Dashlane, they also have 2FA and a secure IT framework, which helps distinguish New America in a competitive industry.

“Dashlane helps us differentiate ourselves,
which makes it easier for us to get funding.”

Abhilash Rajan, Senior Director of Technology, Systems, and Facility
Operations, New America

Audits are also simpler with Dashlane, freeing Abhilash to focus on other initiatives, like incorporating AI into New America’s IT strategy.

In the ever-evolving cybersecurity landscape, New America feels they can navigate confidently because Dashlane is by their side.

Looking back over their time using Dashlane, Abhilash reflects, “We’re so grateful we picked Dashlane.”

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