

LastPass... |



Case Study: HealtheConnections



"LastPass's quickness is what makes it so effective. It's fast and easy to use, which is why our employees love it."

Brad Sweet, Network Systems and Security Manager at HealtheConnections

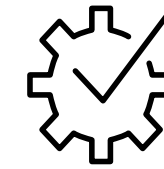


Challenge

HealtheConnections are a not-for-profit (NFP) organization that provides health information exchange services, population health improvement resources, and value-based solutions to 26 counties in New York State, and surrounding states. They support more than 11,000 physicians and the millions of patients they serve by managing cloud-based portals that retain customer health records, ensuring critical healthcare data is readily available and accessible to medical professionals, when needed.

To maintain this portal as a NFP organization, HealtheConnections had to satisfy HITRUST CSF v9.5 Certification criteria for the myConnections provider portal. Brad Sweet, Network Systems and Security Manager at HealtheConnections, realized that in order to meet HITRUST's standards, an investment in password management was essential. Christina Anastos, IT Support Specialist, at HealtheConnections, further recognised that password hygiene was becoming a prevalent challenge across their organization with employees using password protected spreadsheets, or scrawling random credentials on notepads in the office.

To meet HITRUST's requirements and introduce secure password management across HealtheConnections, Brad and Christina invested in LastPass, due to its integration capabilities, customizable policies, and user-friendly interface.



Solution

Password generation was a prevalent challenge at HealtheConnections, the team struggled to create strong credentials on a regular basis and often tracked their passwords on pieces of paper. LastPass's password generation tool produces a unique password for each account they create and can introduce parameters to ensure they are 12 characters long, and contain letters, numbers, and special characters. Christina adds: *"The password generator is one of our favourite features from LastPass, we often need to reset passwords across accounts and the generator makes it an easy process for the entire team."*

HealtheConnections sought to introduce a secure method of storing credentials across their team. LastPass stores all your passwords and other essential information in a password vault. It's a secure repository to stash everything from passwords, secure notes, and credit card information. With LastPass's zero-knowledge architecture, the vault data is protected using AES-256 encryption and 600,000 rounds of PBKDF2-SHA-256 hashing plus salting. Hashing converts your data into an unreadable output and salting takes individual outputs and makes it unique and harder to match. Brad notes: *"Our initial methods for password management opened us up to vulnerabilities, with LastPass, we can create a safe and secure space for employees to store important notes and passwords."*





Results

LastPass significantly improved HealtheConnection's cybersecurity posture and they were able to seamlessly attain HITRUST certification. It's been four years since they deployed LastPass and they are currently at 98% adoption across their organization. Brad comments on their implementation journey, *"It was just seamless and easy, we had great support from the LastPass team which really helped!"* To improve usage and adoption, the security team are on hand to provide guidance to staff and run quarterly training sessions across the business. To further strengthen the organization's cyber-resilience, HealtheConnections also integrated multi-factor authentication with Duo, which allows them to generate one-time verification codes as a secondary form of authentication for added security and reassurance.

LastPass became a key tool for staff to utilize across day-to-day operations and is an essential component of their employee onboarding program.

"The password resets have become so much easier with LastPass's Password Generation tool as it instantly creates lengthy and unique credentials for us to leverage."

Brad Sweet

Christina comments, *"Security is non-negotiable, so for us it's key that our employees are taking full advantage of LastPass's functionality to operate safely."* They further capitalized on LastPass's customizable policies to automate employee offboarding. Brad states: *"We loved being able to cherry-pick policies that worked for our business. Removing access after an employee leaves the organization was key to us, we also put some necessary parameters in place for password strength and reuse to improve our overall password hygiene."*

Learn how HealtheConnections increased their password security using LastPass.

Get in Touch