SaaS Company Prevents Password Monkey Business

Name: MailChimp
Industry: Software as a Service
Location: Atlanta, GA
Employees: 360

Challenge
Encrypt company passwords to meet penetration testing recommendations and improve overall security posture

Solution
- LastPass Enterprise on desktop, Chrome browser
- LastPass Enterprise mobile app on smartphones

Results
- Gained centralized, cost-effective password management
- Significantly strengthened security and password-related processes with strong passwords and folders for shared access to credentials
- Reduced time spent provisioning new employees from several days to minutes
- Increased employee convenience with linked personal and work accounts

Challenge

Founded in 2001, MailChimp is a leading provider of online email marketing solutions that allow individuals and businesses to manage contacts, send emails with impact, and track results. Security is a priority at MailChimp, and regular penetration testing is part of the company's ongoing commitment to protecting its assets. MailChimp also needed a secure way to share sensitive information that was convenient enough to prevent people from using email or other means.

At the same time, it was becoming harder to maintain secure passwords that needed to be shared with a team. For example, encrypted files were kept on a locked-down server. As the engineering team grew, it quickly became too difficult to maintain strong protection while enabling everyone to have easy access to the latest credentials.

MailChimp looked for a password protection solution, one that supported all in-house operating systems as well as providing a way to manage work and personal credentials seamlessly. These needs led MailChimp to implement LastPass Enterprise—a comprehensive password manager that saves users' passwords and logs in on behalf of the user on password-protected websites, with secure access from every computer and mobile device.

Solution

LastPass Enterprise solves the password problem for teams, providing centralized, cost-effective password management and Single Sign-On. MailChimp originally deployed LastPass Enterprise for its Mandrill team; the solution was so well-received that it quickly became the standard for the company.

> *"LastPass has helped us significantly improve password management. And better password security certainly contributes to our overall corporate security posture. LastPass Enterprise just makes it so much easier to have—and maintain—secure practices."*
>
> **Homer Bartlett,**
> Director of Internal Resources at MailChimp

Using LastPass Enterprise's Policies, MailChimp's corporate security team established a company-wide policy requiring a certain level of password length and complexity. They also implemented multifactor authentication with the YubiKey, a token that generates secure one-time passwords for a second layer of protection. New employees receive YubiKeys that authenticate them and provide appropriate access to assigned resources. Teams also use the LastPass Enterprise mobile app, giving them safe access to the logins and passwords they need, even if they're away from their desks.

Share Folders, Not Data

Public notes, database files, Excel spreadsheets, Word documents, or Sticky Notes containing password information are a thing of the past. Logins and notes can be easily and securely shared across functional teams as well as between individuals with LastPass Enterprise.

"One of the best features of LastPass for me is the enterprise folder capability," said Homer Bartlett, Director of Internal Resources at MailChimp. "It makes it easy for me to manage team-level credentials and pass logins or notes securely."

The Mandrill, operations, and company teams use shared folders extensively. Folders contain different sets of information for team members, and each folder contains passwords that are shared by the designated team. LastPass automatically syncs changes across all users who have access to that folder.

Team members share logins to websites, notes about projects, procedural passwords, and process instructions. For example, the IT team has their Apple login in a shared folder so team members can place orders for new equipment when needed. The Quality Assurance team shares access information to several testing accounts that

they use when testing updates to the MailChimp service. The Support team shares Hotmail, AOL, Yahoo, Gmail, and other account logins so that any team member can test how a particular email renders in those clients.

So Easy, Even a... Monkey Can Do It

LastPass makes it easy to provision new employees and manage access. It used to take several days to coordinate passwords and access—today it takes just a few minutes. Designated admins easily add and remove employees to LastPass Enterprise, and assign them to the tools and logins they need to hit the ground running. They can also customize permissions to hide passwords on a folder-by-folder or employee-by-employee basis.

Strong Passwords, Without the Hassle

LastPass also provides feedback about password strength with the Security Challenge. Administrators can see at a glance if employees are using weak and duplicate passwords. LastPass alerts them to vulnerabilities so they can take steps to remedy password issues.

"I used to reuse passwords a lot, especially if the site wasn't storing credit card information," said Bartlett. "Now I just let LastPass generate something crazy long and random, and I don't even think about it. It's just much easier to maintain good password habits with LastPass."

Personal and Work Passwords, Together But Separate

Many MailChimp employees also have personal LastPass accounts. These are securely linked to their work account, allowing them to access what they need from both accounts when logged in at work. The personal account remains private, so that the company can't see or access those personal passwords, and company policies don't apply to the personal account. Employees have convenient access to both, but the company only has control over the company account. The employee doesn't have to worry that their data will be lost if they leave the company, while company data remains locked down.

Better Security. SOC Audits Say So.

Thanks to LastPass, recent penetration tests have had a much more difficult time breaking in through weak or compromised passwords. Each year MailChimp also undergoes a Service Organization Controls (SOC) audit. Although LastPass is not called out specifically, it clearly plays a role in several categories, including logical and physical access controls, risk management and control implementation, and communications.

"LastPass has helped us significantly improve password management," said Bartlett. "And better password security certainly contributes to our overall corporate security posture. LastPass Enterprise just makes it so much easier to have—and maintain—secure practices."

Try LastPass Enterprise free today at LastPass.com/enterprise