CASE STUDY

Northland Communications

Overview

Northland Communications delivers telecommunications and internet services to customers who rely on them around the clock. As a phone provider, ISP, and hosted systems operator, the company faces elevated exposure to identity based attacks.

Following a NIST based security audit that exposed a need to move beyond shared spreadsheets and ad-hoc password resets, Northland adopted LastPass. More than a decade later, LastPass remains central to Northland's secure access strategy. With the adoption of LastPass Business Max, the company extended its mature password management program with SaaS Monitoring, giving IT clear visibility into how employees use browser based business tools as SaaS and AI driven apps continue to expand.

The **Challenge**

Before LastPass, employees stored passwords in Word documents, spreadsheets, or shared them informally—practices that introduced unnecessary risk for a 24/7 organization supporting mission critical services.

The IT team faced several challenges:

- **Fragmented credential management and unmanaged password sharing**
- **Heavy reliance on shared passwords without sufficient controls or oversight**
- **Limited visibility into which browser based SaaS apps employees were using**

As SaaS adoption accelerated and new tools like AI-powered services became easier for employees to access, IT lacked a practical way to understand real usage patterns across the organization. Northland needed visibility to confirm whether users were operating within approved applications or introducing unvetted tools into daily workflows.

Rollout & Implementation

After selecting LastPass, Northland completed a companywide rollout using the Active Directory Connector to automatically provision accounts and activate users, eliminating manual setup and ensuring full coverage across the org.

To support fast adoption, LastPass training videos were embedded into Northland's internal learning management system. All employees completed short modules during rollout, and new hires continue to receive the same training during onboarding.

What made the rollout stick:

- **Shared folders for consistent access and easier collaboration**
- **Policy controls and password strength scores that improve hygiene across teams**
- **Early integrations (e.g., Royal TS) that securely autofill credentials stored in the LastPass vault directly into remote connections, boosting day to day productivity for technical teams**
- **Families as a Benefit to reinforce secure habits beyond the workplace**

LastPass

Impact

Greater Security and Consistency

Northland reduced exposure by replacing spreadsheets and passwords in documents with a centralized vault. Shared folders ensure consistent access across teams, while admin oversight surfaces weak or reused credentials.

SaaS Visibility Without Added Friction

As more work shifted into the browser, Northland began using SaaS Monitoring, included with Business Max, to understand which apps employees actually use daily.

Rather than blocking tools outright, Randy highlights that SaaS Monitoring can be a visibility and conversation tool—helping IT understand behavior before it becomes risky.

> **"There are so many apps based off the browser now. SaaS Monitoring shows me where people are going and whether they're using tools they shouldn't be…Most users stick to the apps we give them, and I can warm them–or just talk to them–if something looks off."**

This visibility helps Northland:

- **Confirm use of sanctioned tools**
- **Spot early signs of shadow IT, including emerging AI sites**
- **Have conversations with users rather than enforcing strict blocking**

Productivity Improvements

Beyond security gains, LastPass drives meaningful productivity improvements—especially for IT and engineering teams that require rapid system access.

> **"I easily save 30 minutes to an hour per day thanks to LastPass integrations — and our engineers probably save double that time. Not typing passwords all day adds up fast."**

For a 24/7 telecommunications provider, these reclaimed hours translate into faster response times and greater operational efficiency.

Conclusion

Northland Communications relies on LastPass to secure credentials, streamline access, and stay ahead of evolving SaaS and browser based risks.

With Business Max, Northland didn't just secure credentials; they gained visibility into how access happens across the browser, without slowing employees down.