

Leading U.S. Retailer Solves Giant Data Management Maze

The second largest U.S. retailer sought to deliver exceptional guest experiences to more than 98 million registered users across multiple engagement channels.

THE OBJECTIVE

As its number of customer touch points increased and service offerings became more sophisticated, the retailer wanted to provide a seamless experience in its omni-channel environment. The brand also wanted to consistently apply centralized data privacy and security policies across all channels while allowing guests to self manage privacy and preferences.

THE CHALLENGE

- Data from different sources with varying controls created disjointed customer experiences.
- Existing identity and access management (IAM) system didn't support SSO or privacy and preference management.
- Lack of governance tools negatively impacted the ability to implement security best practices.
- Scale limitations resulted in performance issues.
- Brand needed to leverage data from its Master Data Management system into customer engagement initiatives.

THE SOLUTION

The Ping Identity Platform: Transitioned from a Websphere Commerce Server to a customer identity and engagement management solution by implementing the new identity and preference management platform.

SOLUTION AT-A-GLANCE

1. More than **98 million** identities managed.
2. Data management unified across **7 data sources**.
3. Enabled **single sign-on (SSO)** and **multi-factor authentication (MFA)** across 7 apps with more apps and channels being added.

THE RESULTS

- Web scale performance supporting 98 million identities and growing
- Unified view of each customer across omni-channel touch points enabling personalized interactions that increase conversion rates
- Flexibility to support the deployment of new apps in cloud and virtualized environments while reducing time to market
- Improved customer experience with seamless SSO, modern MFA, permission-based services and high-performing apps
- Rapid adoption of security best practices and ability to satisfy governance, security and audit requirements

