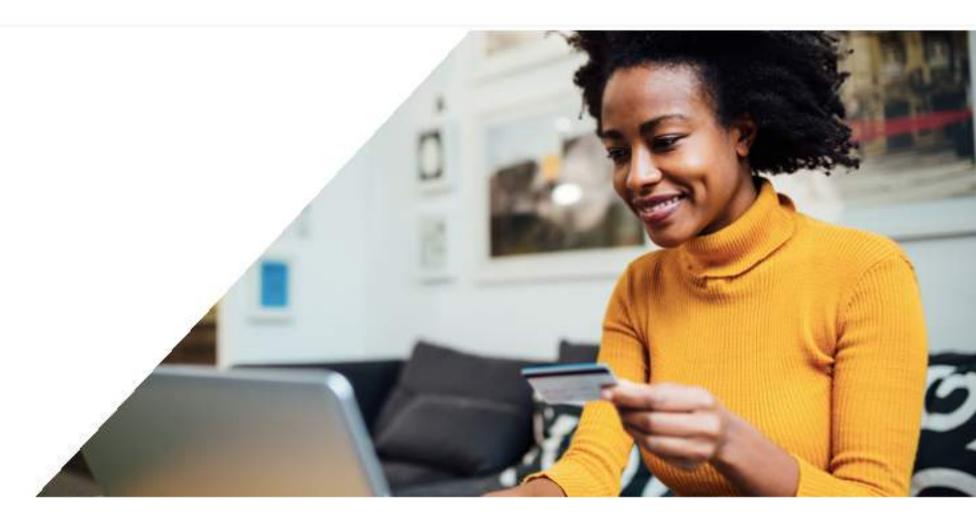WesternUnion\WU

Western Union centralizes identity for a secure future

Time to read: 4 min

Western Union is an American multinational financial services company headquartered in Denver, Colorado. A staple of the American economy for over 172 years, Western Union needed a full-scale IAM platform to scale with their business and secure access to their enterprise's applications.

INDUSTRY
Finance

COMPANY SIZE
12,000+ employees

PRODUCTS
IdentityIQ

PARTNER
Accenture

Challenge

Before SailPoint, Western Union was using four separate solutions to address their identity governance efforts, which was costly and not providing the functionality needed. Western Union decided to centralize their identity security processes and made SailPoint their single, enterprise wide IAM platform, and haven't looked back since.

Results

With SailPoint, Western Union was able to gain full visibility over all their mission-critical applications (with more on the way) for all their users, while saving both time and money. They became more efficient with managing users' access to applications, and integrated all of their 600+ applications into a single IAM solution.

> We looked at SailPoint and it seemed like an obvious win for us, especially when we could get the best of identity lifecycle management and compliance management,

Harold Black, Identity Business Solutions Architect, Western Union.

2.5 minutes

time to provision 50 new hires, reduced from 14 hours

If you transfer money across national borders, chances are you're familiar with Western Union. Western Union enables customers to send and receive money, and make payments quickly, easily, and reliably. Currently, the Western Union network includes hundreds of thousands of retail agent locations in more than 200 countries and territories.

Like any large enterprise, Western Union needs identity security to help the company more effectively manage how it onboards and manages the identity lifecycle of its employees.

The identity team went on a search for a new enterprise identity management solution. They didn't want to simply replicate the capabilities they already possessed with their previous system. They wanted to attain a new unified view of identities and access across the organization. That included an identity warehouse that would contain source data from multiple applications and combine it into a way that would create a clear, comprehensive picture of user access. "We also wanted to be able to conduct better identity reconciliations and more effective certifications," said Harold Black, Business Solutions Architect at Western Union.

The team also wanted to reduce the amount of time they had to spend managing and supporting their identity management system and reacting to regulatory changes. They wanted to shorten the time it took to provision new users.

With their older identity security solution, Western Union had separate applications that handled identity provisioning and management and identity governance. "Whenever a manager would request access remediation, they had to go through a ticketing system. Frequently, that system didn't update the identity profile properly because the systems weren't connected," Black said.

Also, their existing identity and access management system did not allow them to easily add new applications as they wanted. "It didn't have any out of the box connectors, so it required a lot of maintenance for us to provision employees," he said.

After a careful evaluation, Western Union's identity team selected SailPoint.

"We looked at SailPoint and it seemed like an obvious win for us, especially when we could get the best of identity lifecycle management and compliance management," said Black. With SailPoint, Western Union is able to see who has access to what applications, services, and files and easily determine if that access is within their security policy. And it also provides Western Union the ability to streamline provisioning, as well as user self-service and automated policy management.

Following the move to SailPoint, Western Union experienced rapid success. "We signed the contract on New Year's Eve, and we had a complete cutover from the old application to SailPoint by the following December, for about 750 applications," said Black.

First, Black and his team were able to customize their entitlement workflows effectively and improved their ability to manage their identities.

SailPoint has also helped Western Union streamline the provisioning process for departments that frequently onboard new team members. At Western Union, each new hire needed access to between seven to 10 applications and associated entitlements. Before SailPoint, that access was manually provisioned, and it took nearly 18 minutes per user to submit the access request and get the first level approval — and for these roles for these sets of applications, access was always approved. "Previously, provisioning a new class of 50 users would have taken 14 hours, and the team can do that now in 2.5 minutes," said Black.

Finally, the team built the identity warehouse that they planned. Western Union now collects all of the identity information they need from their human resource systems and then use that data as their single source for identity information regarding users and the systems they're accessing or should be accessing. "We can now easily see what access a user has, and we can compare it with what levels of access was requested, and we can fix any deltas that need to be fixed," Black said.

With SailPoint, Western Union is not only better able to certify users have access to what they need, they can also automatically trigger transfer certifications. Previously, when a staff member was assigned to a new job, the team would issue a certification request to the employee's new manager, providing a list of everything they previously could access and vet against their current access needs. Today, Western Union can increasingly automate many of these processes.

Going forward, the next big identity challenge Black and the identity team plan to tackle is service account identity management and streamlining the associated upfront identity requests. "Service accounts are a challenge for the same reason that servers are problematic: you need to have an effective upfront access request process. We currently have a larger number of service account identities and getting that effective upfront access request process for these accounts is the next big challenge ahead," said Black.