Ping Identity

A UNIFIED APPROACH TO DELIVERING EXCEPTIONAL CUSTOMER EXPERIENCES

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

> "Many organizations are feeling and responding to the pressure to provide a better user experience and return more on the investment in their online presences and user databases. To do so, they must capture more identity data from users, with their outright consent, and then transform it into meaningful information to increase consumer satisfaction and, ultimately, improve their bottom lines."[1]

There's no denying that your competitive advantage has become a matter of delivering the best experience to your customers. They're engaging with your brand across a growing number of touch points, spanning mobile, web and IoT. And they expect a consistent, seamless experience across them all. Cohesive multi-channel experiences are no longer just a nice-to-have. They're a business imperative.

While multi-screen behaviors have become a normal part of your customers' day-to-day lives, they present anything but ordinary challenges for your enterprise. You must work with complex environments to deliver the frictionless experiences your customers demand, without compromising data security.

A unified profile begins at the authentication layer with single sign-on (SSO) to all of your applications. But unifying the authentication layer is just the tip of the iceberg. Once customers are logged in, your apps need access to a single view of their profiles to enable consistent experiences across channels. Creating this unified view requires a highly secure single source of truth at the data layer. This can be challenging if you're managing multiple identity directories that have been built up over time, supporting different applications and dealing with different sets of data about the same customers. However, it's what's required to deliver the personalized experiences your customer expect.

Read on to learn how to deliver seamless and secure experiences through a fully unified customer profile that extends to the data layer.

1 KuppingerCole Leadership Compass: CIAM Platforms, June 2017

UNIFYING THE AUTHENTICATION LAYER

We all hate managing login credentials, and your customers are no different. Having to remember dozens of login credentials across the many brands they interact with is what drives customers to engage in unsafe security practices.

> 80% of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords.[2]

When they have to manage multiple login details, your customers write passwords down, choose easy passwords to remember and reuse the same password over and over. If they can't easily authenticate, they're also more likely to abandon transactions. Bottom line: if you aren't providing a consistent login experience, you could be increasing your exposure to security threats, as well as putting yourself at risk of losing customers and revenue to your competition.

SINGLE SIGN-ON (SSO)

Single sign-on allows customers to prove their identity just once to gain access to your internal apps. It can also include features like social login that allow your customers to leverage their credentials from sites like Facebook and Google.

Eliminating the need for repeated user sign-ons is one of the top reasons to implement a customer identity and access management (IAM) platform. When your customer IAM solution supports federated SSO built on open standards, you're able to take SSO—and your customer's experience—to the next level.

The challenge is there are many disparate applications that your customers interact with. Some may be hosted on premises, while others are in private clouds. They may have varying support standards and protocols. Providing SSO in these scenarios requires a well-established set of standards, like OAuth, OpenID Connect, WS-Fed and WS-Trust. A true federated identity solution can easily extend single sign-on beyond your internal applications to external and third-party applications (as shown in Figure 1), regardless of inconsistencies in the standards and protocols they support.

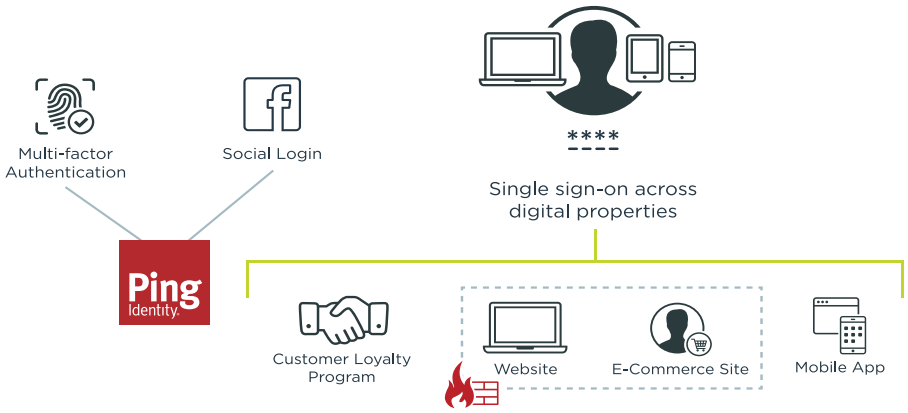

Figure 1: How the Ping Identity Platform supports SSO to both internal and external applications.

2 Verizon 2017 Data Breach Investigations Report

MULTI-FACTOR AUTHENTICATION (MFA)

Modern multi-factor authentication (MFA) enables policies that evaluate the context of users and their devices. Adaptive MFA allows you to step authentication requirements up or down, depending upon the risk associated with the request. You can allow users to conduct low-value transactions from trusted locations and devices without interruption, while prompting multi-factor authentication during high-value transactions on untrusted networks and devices.

It's also important to provide your customers with MFA technology that is both secure and convenient. Your customers typically aren't willing to download a third-party mobile application for MFA, and mediums like SMS have been deemed vulnerable by multiple groups, including the National Institute for Standards and Technology (NIST).

A better approach for customers is to turn your own mobile application into a secure second factor. This allows you to maintain a branded experience during authentication and transaction approvals. It's also far more secure than using SMS or email as a second factor.

When using MFA in this way, you want customers to be able to self-manage their devices. They need to be able to use their preferred device as a second factor, but they shouldn't have to engage your support department each time their preferred device changes. That would be inconvenient for the customer and costly for you.

A modern MFA solution will allow you to expose device management capabilities, so customers can add, remove or block devices themselves. You'll still want to enable your support department with delegated device management capabilities if, for example, a customer loses their device or forgets their password. But by offering self-management of devices, you'll ease the burden on your support team, while delivering the type of experience your customers prefer.

Providing secure, standards-based SSO and contextual MFA are key components to unifying customer profiles at the authentication layer. When done correctly, you can provide a consistent log-in experience across channels that your customers will love. However, unifying the authentication layer is just the tip of the iceberg. The real key to delivering the consistent, multi-channel experiences today's consumers expect goes beyond authentication and into the data layer.

UNIFYING THE DATA LAYER

Once your customers have authenticated, their expectations are far from met. They now want seamless self-service profile management. They want to update their personal information on their account just once and have it instantly recognized no matter where they interact with your brand. They expect to be able to manage their preferences in a single location and have those preferences apply across channels.

Imagine a banking customer's frustration if they update their address on a banking website, then when they order checks from the bank's mobile app they have to update it again. Or worse, they're shipped to the wrong place. What if a consumer opts out of all emails from their local supermarket, but still receives emails from the store's pharmacy?

To avoid these types of poor customer experiences, you must unify customer identity and profile data at the data layer. This enables you to maintain a single source of truth about your customers' identities, attributes and preferences that is accessible to all applications.

But creating this single source of truth in a centralized directory is anything but a slam dunk when you have multiple identity repositories supporting various production applications. If your enterprise is like most, you've added new apps and channels over time, and additional data silos to support them. Bringing these disparate silos together can be challenging.

There are three questions you need answer when creating a unified profile:

1. Where will I store my customer data?
2. How do I unify profiles in that location?
3. How do I connect my live apps?

STORING CUSTOMER DATA

You first need to determine where you'll store your customers' data. You may be tempted to use your legacy workforce directory for this purpose. In short, this isn't a viable option. Multi-purpose databases and legacy LDAP fail to provide the flexibility, security or performance you need for customer identity management. Their limitations can expose your organization to breaches, performance lags and outages that can damage your brand and lead to lost revenue for your enterprise. Many legacy repositories also have a bloated hardware footprint and high TCO.

Instead, you need a high-performance directory that's purpose-built for the demands of managing customer identities. These requirements include:

SECURING CUSTOMER DATA

It's imperative that customer data is encrypted in every state–at rest, in motion and in use. You also want to employ best practices, like active and passive alerts, and tamper-evident logging. These are not only a crucial part of securing customer identities, but can also play a role in meeting regulatory requirements such as PCI DSS, HIPAA and others.

SUPPORTING SCALABILITY AND GROWTH

As your customer base grows, your customer IAM solution's ability to scale becomes vital. The solution should be able to manage tens or even hundreds of millions of customer identities and billions of attributes. It must be able to handle large deployments even during peak usage scenarios.

EXPOSING DATA THROUGH REST APIS

Exposing identity and profile data through developer-friendly REST APIs makes that data easily accessible by applications without compromising security. By relying on standard-based protocols commonly used by application development teams, you're able to rapidly build and deliver new applications.

STORING UNSTRUCTURED DATA

In addition to structured data, there are other types of data your apps can store in your user directory. Often, this data holds a goldmine of information about your customers, so you want to be able to store and mine it. The ability to store unstructured data gives apps the flexibility to store any type of data in the unified profile and add the user attributes they need, without affecting the schema for all other apps.

UNIFYING PROFILE DATA

Consolidating identity data can be a major obstacle on the road to customer engagement. If you're like most enterprises, one of the main hurdles you'll face is consolidating the slew of disjointed data stores you've built over time. These might be relational databases, legacy IAM directories, MDM systems or others.

These data stores may have been built by different teams within your organization, or they may be the result of mergers and acquisitions. In either case, the resulting silos can be difficult to consolidate. When you're evaluating directory solutions, you'll want to prioritize those that can help unify your profile with advanced real-time synchronization tools.

Many IDaaS solutions require you to export and bulk upload your contacts into a could directory, but this isn't always feasible. In contrast, a purpose-built customer IAM solution, like the Ping Identity Platform, is tailor-made for this challenge. It can bring together data from disparate directories, no matter where they sit, through real-time bi-directional synchronization and zero-downtime migrations.

CONNECTING LIVE APPS

For customers, migrating live apps can be a scary thought. Some apps may have complexities that prevent them from being immediately migrated to leverage all the benefits of your new directory. If you are ready to migrate a live customer-facing application, outages are unacceptable. Downtime can be costly and damage your brand, not to mention your department's reputation. In either of those situations, you need a way to connect every customer identity into a unified profile. Being able to choose whether to migrate or synchronize an identity silo to your unified profile is a key benefit of modern customer directory solutions.

BI-DIRECTIONAL SYNC

With real-time, bi-directional synchronization, you can still connect live applications to a unified profile, even if you're not ready to migrate the apps from their original repositories.

Your unified customer profile can then be maintained in a secure, scalable directory that will become the single central location where all new and migrated applications can access all of your customer data. For apps that aren't ready to migrate, a real-time or scheduled bi-directional sync between the new and legacy repositories keeps all identity data current.

ZERO-DOWNTIME MIGRATION

Data synchronization also plays a critical role in the migration of your apps to your new modernized directory. In most cases, even with long-term bi-directional synchronizations, you'll eventually want to migrate your applications to a more secure and scalable modern directory solution. For customer applications, performing those migrations without interruptions to service is critical.

Zero-downtime migration solutions can move your customer data into a unified directory without any loss of service, outages or lags for your customers. The bi-directional sync can remain in place during the whole process to act as a safety net for your migrations. Once all the apps are migrated, and you're ready to hit the switch, you can decommission the bi-directional synchronization and the old repositories to enjoy the benefits of a unified profile and single high-performance directory.

CONCLUSION

To meet your customers' expectations for a seamless and frictionless experience with your brand, you need to provide a unified experience at the authentication layer and a unified profile at the data layer. A purpose-built customer IAM solution will enable you to do both, paving the way for loyalty-building and revenue-boosting customer experiences, and the security customers require.

Single sign-on that doesn't support a wide variety of standards, as well as both on-premise and cloud applications will fall short of providing the seamless SSO capabilities that customers require. Similarly, SaaS solutions built primarily for marketing purposes aren't able to provide the enterprise-grade scale and security necessary for protecting customer identity data. Looking to a traditional IAM system to manage the volume and variety of customer data you need to store is a guaranteed dead end.

In addition to facilitating the creation of a central, secure directory of customer data, a customer IAM solution must be highly secure and scalable. It must be able to store profile data, personal preferences, data-sharing consent and other unstructured data, and make it accessible to all applications through developer-friendly REST APIs.

The Ping Identity Platform provides the customer IAM capabilities you need. It allows your customers to seamlessly authenticate to all of your applications and manage personal data in a single location. When you can do these things, you're able to deliver the secure, exceptional user experiences across all channels that your customers expect.

To learn more about evaluating customer identity and access management solutions, read our Customer IAM Buyer's Guide.

#3299 | 10.17 | v02