Executive Summary

Organizations are offering customers personalized experiences

Omnichannel access lets customers engage with your business across multiple devices and channels, while maintaining a coordinated, consistent experience throughout the customer journey. It provides customers with personalized, relevant experiences to improve customer engagement and retention.

Identity management is critical to a successful omnichannel operation.

A digital identity lets customers log in using multiple devices.

At the same time, identity management must help companies comply with privacy regulations such as the European Union’s General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA). These regulations require organizations to obtain consent to use the personal information contained in the digital identity, as well as grant customers the right to view, modify, or revoke consent at any time – all while protecting the privacy of personal customer information.

What’s the Urgency?

Support for a wide range of devices is critical

The days when customers used only a browser on their desktop PC or laptop to access a company’s online retail site or online services are long gone. Customers now employ smartphones, tablets, and other connected devices. New device categories show up frequently. Most recently, these have included wearables and windowless devices with no GUI at all, such as smart speakers with voice-controlled digital assistants. And the list of devices will only continue to grow. If companies don’t support all the popular device types and offer great user experiences across all channels, customers are more likely to stall their journeys, abandon shopping carts, and ultimately go to another vendor.

Consumer expectations have evolved, too. They expect to be able to switch devices at any stage in their journey and pick up right where they left off. For example, a customer might start browsing an online store with their mobile device, put something in a shopping cart, then go home, and complete
the purchase through a laptop or via a voice command to the digital assistant of their choice. Today, the customer, not the device, is the channel, regardless of how they choose to interact.

To deliver a seamless experience across any device a customer chooses, companies need a centrally managed digital identity and access management system. But creating and managing digital identities while maintaining regulatory compliance is complex.

Large organizations need to comply with privacy regulations for the different states or countries in which they operate. Each regulation may have different UI and procedural requirements. For example, regulations such as GDPR and CCPA both require companies to ask for consent before the customer hands over personal data. But GDPR requires the customer to opt in using a check box, while CCPA allows the company to pre-check the box. Privacy regulations also require companies to have different rules for children and adults regarding what data can be collected and what messages can be delivered.

Many smart devices have more than one user. Families might share a single tablet, smart TV, or connected car. These users may not log in to use these devices, yet the devices must identify and authenticate users, and then personalize their experience. For instance, many family members may drive the same car. You want to be able to load a specific driver’s playlist onto the car’s infotainment system or show their personal recent destinations on the navigation system.

One example of the multitude of identity management complexities can be seen in a Bluetooth-enabled smart toothbrush for children. This toothbrush connects to a mobile device, such as an iPad, through an app in which an animated character explains to the child how to brush their teeth. The app can also detect the movements of the brush, enabling it to supervise the brushing. It then sends progress reports to the child’s parents and tells them when to replace the brush head.

Because the brush is intended for kids, it must adhere to privacy rules for minors. The brush can provide the full range of collected data to parents, but it must follow privacy regulations that govern which data the toothbrush manufacturer can collect and how that data can be used. The device offers accounts for parents and children and must ensure that the child cannot access a parent’s account. If the smart toothbrush body can be used with multiple heads for different family members, the vendor must also be able to track who is using the brush so it can manage the experience for each user.
The Solution

Compliant, Device-Agnostic Access
Identity Cloud, Akamai’s solution for customer identity and access management (CIAM), is designed to handle the complexities of omnichannel customer access, so you can get identity management right.

Identity Cloud is API-centric and provides device-agnostic access. Any device that can make an API call can access identity management capabilities, whether that device is a phone, tablet, in-vehicle infotainment system, or any other type of connected device. Identity Cloud recognizes individual users across different devices, as well as groups of users, and can assist in the enforcement of data privacy regulations for each one. At the same time, it is architected to deliver excellent performance, even for use cases with hundreds of millions of users, and tight security for personal customer profile data.

Visit akamai.com/identitycloud to learn more about Akamai Identity Cloud

Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 2/20.