# 7 TRENDS

## THAT WILL SHAPE THE FUTURE OF IDENTITY

*By Ping Identity's CISO Advisory Council, comprised of CISOs from 12 enterprise organizations, including: Frank Aiello, CISO for American Red Cross; Diane Ball, CISO for BCBS Tennessee; Steve Martino, CISO for Cisco; Stanton Meyer, CSO for CoBank; Ben Mayrides, CISO for Cvent;  Sam Masiello, CISO for Gates Corporation; Larry Whiteside, CISO for Greenway Health; Michael Strong, CISO for GCI; Chris Gullett, VP of Information Security for Allegiant Air; and Adrian Mayers, CISO for Vertafore.*

The identity and access management (IAM) space is constantly evolving, and the pace of transformation is only accelerating as new security threats arise, expectations increase for streamlined and transparent experiences, and IT environments grow more complex to support business initiatives like cloud adoption.

Over the course of this evolution, identity has become a key business driver across the organization. Businesses are using IAM to help them accomplish a number of goals, including:

- Managing identities, profiles and attributes
- Authenticating people, systems and things
- Enabling access to resources
- Managing runtime access to applications and application programming interfaces (APIs)

With the rapid pace of change and increasing scope of identity, it's hard to stay on the cutting edge of trends in the IAM space. Ping Identity recently invited the Chief Information Security Officers (CISOs) from leading enterprises to share the seven trends they believe will shape the future of identity.

#1

**NEW METHODS OF IDENTITY PROOFING** For centuries, identity proofing has required people to show up at a physical location and have their identity documents inspected. This method isn't going to scale in the age of the internet. New methods of remote proofing and social proofing are currently being developed that will change the way people trust each other online.

#2

**PASSWORDLESS AUTHENTICATION** When individuals interact online, they frequently do things that attackers would never do, like pay bills, order small items to be shipped to their homes or send a note to say hi to mom. Authentication will eventually be smart enough to recognize these as contexts that are low risk and don't require a password. There are also many contextual pieces of information that could indicate people's true identities, like the devices they use and how they interact. Authentication of the future—for both individuals and enterprises—will be adaptive and contextual so a password is required only when necessary.

#3

**BEHAVIORAL ANALYTICS AND MACHINE LEARNING** It used to be that you could grab a latte in the morning and hop into a cab with no one knowing who you were. Starbucks and Uber have changed that forever. People increasingly interact with the world in an authenticated context, which means that the companies with which they interact have a lot of information about their behavior. Machine learning gives businesses an even bigger opportunity to apply the data in different ways. They will be able to remove frustrations and friction from their customers' daily lives by remembering who they are, what they like, when they're likely to access services and exactly how much whipped cream their kids like on their hot chocolate.

#4

**CONSENT AND PRIVACY** Customers are getting more savvy about understanding how and when their data is stored—especially as more of them have been victims of data breaches. New regulations require that companies gather consent to store personally identifiable information and then only use that information for agreed-upon purposes. The days of 100-page terms of service are gone. Expect to see short, clear requests for information as it's needed during a transaction.

#5

**BLOCKCHAIN AND OTHER DISTRIBUTED LEDGER TECHNOLOGIES** How new distributed ledgers will shape identity management is a question still to be answered, but many companies are eagerly playing with the technology and trying new things. There's a lot of excitement about the new tools that this technology could enable, particularly in spaces where global coordination is needed. However, since everything that's put on a blockchain is immutable, it's important that they remember the privacy and security implications of these tools as they build new things.

#6

**INTERNET OF THINGS (IoT)** As identity becomes the new perimeter for both security and privacy, it's increasingly critical that the industry gets device identity right. The number of devices individuals carry and install in their homes is growing dramatically, and the enterprise use cases are exploding—from production line monitors to water sensors to medical devices. We're going to need new norms and policies to differentiate between trusted users, threats and different members of a household.

#7

**BIOMETRICS** Biometrics are emerging as a quick and easy way for users to authenticate, but they're not perfect. As usage grows, the technology to fool biometric sensors will get more advanced and easier to produce. Right now, unlocking local devices using a locally stored biometric has a low likelihood of compromise, but using biometrics at scale over the web carries more serious security implications that the industry will have to wrestle with over the next few years.

**About Ping's CISO Advisory Council:** Made up of CISOs from leading global enterprises, this group provides insight to Ping Identity on security, privacy and compliance challenges within the global enterprises we serve. It helps inform Ping's strategic vision, product roadmap and go-to-market strategies. Interested in getting involved? Please reach out to your account executive to learn more.

To learn more about how identity can help you secure your business, improve productivity and provide personalized customer experiences, visit pingidentity.com.

Ping Identity

**About Ping Identity:** Ping Identity leads a new era of digital enterprise freedom, ensuring seamless, secure access for every user to all applications across the hyper-connected, open digital enterprise. Protecting over one billion identities worldwide, more than half of the Fortune 100, including Boeing, Cisco, Disney, GE, Kraft Foods, TIAA-CREF and Walgreens, trust Ping Identity to solve modern enterprise security challenges created by their use of cloud, mobile, APIs and IoT. Visit pingidentity.com.