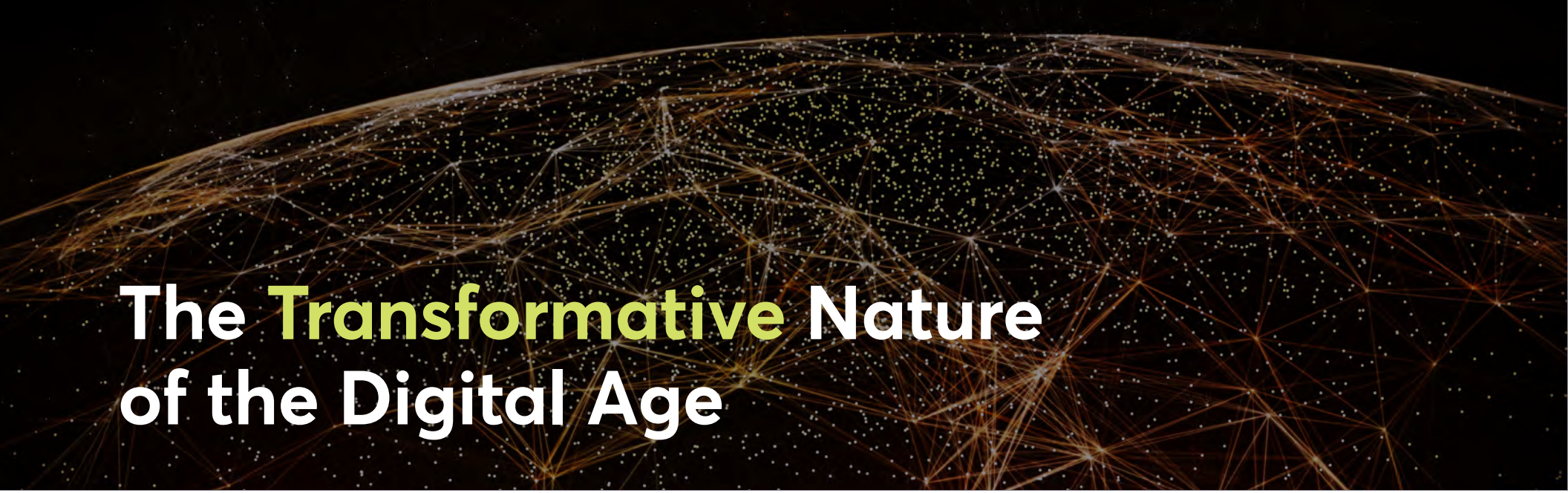
# Modern Identity and Access Management

## Building Trust Without Sacrificing Security

ca technologies



# The Transformative Nature of the Digital Age

The world is now in the early stages of the Fourth Industrial Revolution—the Application Economy. In its scale, scope and complexity, the digital revolution is unlike anything we have previously experienced. It is altering the way we live, work and interact with one another; it is changing who we are.

The world of the Fourth Industrial Revolution is global, responsive, customer-focused and technology-driven—with software at the center of it all. Companies are rapidly transforming themselves and the ways they provide services to customers, employees and partners, resulting in what's known as the Modern Software Factory.

### Transformation brings risk

Business has always been built on trust, but this trust can be quickly broken and unwoven due to a security breach. No matter how services are accessed, or how many users or devices access them, a fundamental concern remains:

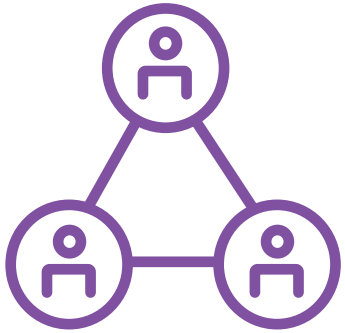
Organizations need to protect larger volumes of sensitive data while still allowing users to easily conduct business. A modern identity and access management (IAM) solution can address these challenges.

# Balancing User Experience and Security in a Zero-Trust World

With the creation of the application economy, users have been given more choices for services than ever before, and they are overwhelmingly choosing experience as the differentiator.

For most, the primary challenge in embracing the app economy revolves around developing agile approaches to software delivery to meet customers' expectations. However, rushing applications to market to stay competitive often comes at the expense of quality and security, and these defects can have a devastating impact to the business.

**Can security improve without impacting user experience?**



*"If people like you, they will listen to you, but if they trust you, they'll do business with you."*
*— Zig Ziglar*

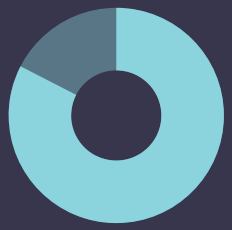
# The answer is yes.

Leading organizations understand that breaches have become the norm in today's connected world. With information everywhere and personalized experience driving the digital transformation, identity is critical. Identity is the foundation for trust.

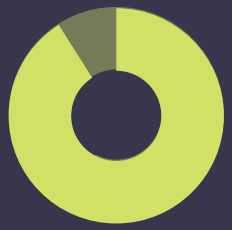
But how do we establish this trust without burdening users? There are five critical questions that need to be addressed by any modern IAM solution:

- How do I identify a legitimate user from a fraudulent one?
- What confidence do I have that you are who you claim to be?
- How do I make security frictionless while decreasing my exposure?
- How do I efficiently manage identities and access entitlements?
- How do I reign in privileged users and protect against insider threat?

**2/3** of large businesses have suffered a data breach in the past year[1]



**83%** of U.S. consumers say having a positive customer experience with a brand is more important than the product itself — Harris Poll of U.S. consumers



**92%** of CEOs have a digital transformation focused on redefining customer experience – Forbes

1 Dr. Rebecca Klahr, et al, U.K Government, "Cyber Security Breaches Survey 2016," May 2016, www.gov.uk/government/publications/

# How to Identify Your Users?

George Bernard Shaw said, **"The single biggest problem in communication is the illusion that it has taken place."** This is because people talk, but they don't always listen. However, in the digital world, this isn't the case. Dialogue happens or nothing happens. This means that the single biggest problem in digital communication is not that it has taken place, but rather that it has taken place with the right person.

Consider the most common interaction—authentication. Users request access and then are challenged to identify themselves. This digital dialogue occurs millions of times every second around the globe, and it is built on one very simple principle: trust. The application is trusting that the legitimate owner is submitting these credentials. But this trust is easily compromised, as passwords—the most common login credential—can be easily stolen, guessed or given away.

## Exploring new identification techniques

Therefore, organizations are exploring alternative methods to identify their users, including: biometrics, out-of-band one-time-passcodes, push notification and other forms of multifactor authentication credentials. Each of these methods can increase your confidence that the user is who they claim to be, but each also has their disadvantages, the principal being impact to user experience. The critical question is how to apply one or more of these credentials in an intelligent manner; that is, only when necessary.

**73%** of data breaches were financially motivated[1]

**81%** of hacking-related breaches used either stolen or weak passwords[2]

**~$6.5B** in annual financial losses due to account takeover[3]

1 Verizon, "2017 Data Breach Investigations Report," April 2017, www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2 Ibid.
3 Forrester, "The Forrester Wave™: Risk-Based Authentication, Q3 2017," Andras Cser, July 2017

# How to Increase Confidence in the User's Identity?

The key to balancing security against user convenience is risk. At the most fundamental level, a user's identity does not change—my identity is always me. But as a user, my environment and context change frequently, and this impacts my risk profile. This is known as adaptive identity risk.


### Actions and methods of access

What the user is attempting to do must also be considered. Some activities are riskier than others. In addition, you also need to consider how the user is accessing applications. The emerging wave of mobile and Internet of Things (IoT) must be factored into the modern IAM solution. Devices have identities and their relationship to users must be established and monitored. For this reason, many organizations are leveraging contextual authentication to complement their user login process.

Real-time risk evaluation can detect and protect against inappropriate access by analyzing a wide set of factors, including:

- User behavior
- Device characteristics
- Geolocation
- Velocity data

And all of this needs to be done without requiring any direct input from the end user. When the risk exceeds a specified threshold, the user can automatically be prompted to submit additional credentials or information to further prove their identity. This makes it a secure, user-convenient and cost-effective way to protect sensitive applications and data.

# How to Improve Consistency?

The application economy is altering the way we live, work and interact with one another. This is being driven by the speed and scope of the digital revolution.

In October 2015, EMV chips were introduced in the United States to counter against criminals using stolen credit cards at stores.  Within a few months, card-not-present (CNP) fraud began increasing at a rate of three to one versus card-present fraud as criminals sought channels where the EMV chips were not used. As security was increased on one channel, criminals switched to another.

Therefore, the critical question is: How can the business provide the same user experience and consistent level of security across every access channel, including Web, mobile, IoT and Web services?

**2.8B** smartphone users by 2020

**38B** connected devices by 2020

**>1.8B** users of intelligent digital assistants by 2021[1]

1 Steffen Sorrell, Juniper Research, "The Internet of Things: Consumer, Industrial & Public Services 2016-2021," December 14, 2016, www.juniperresearch.com/researchstore/iot-m2m/internet-of-things/consumer-industrial-public-services

# How to Provide Seamless User Experience?

The use of traditional Web single sign-on was, at one time, critical to controlling access to online resources while providing a frictionless and secure experience for online users. It enabled them to readily move from one Web-based transaction to another, smoothly interacting with other applications or external sites along the way. But as organizations move beyond web-based operations to support mobile devices, IoT and cloud-based services, they need to extend single sign-on to secure these new services and methods of access. To the end user, the location and delivery methods of an application should be invisible and the transition across multiple applications should be seamless.

Federated single sign-on can enable user credentials to be trusted across multiple IT systems or applications, leveraging industry standards—such as OAuth, Open ID Connect and SAML. However, there are also emerging use cases that would further expand the notion of federated single sign-on to cross-device and cross-mobile app SSO. These cases may include allowing a user to generate a shopping cart with their app, and then transfer that cart to a kiosk in a store for purchase; signing into an ATM machine from a mobile banking app; or paying for a mobile purchase from a mobile wallet.

# How to Streamline the Management of Identities?

Providing seamless access is not the only issue. The IT environment is becoming increasingly distributed, complex and heterogeneous. When it comes to deciding who has access to what and reliably enforcing those policies, it becomes a multifaceted challenge that requires both a shift-left and a shift-right approach.

Managing identities is a critical need for both internal and external user communities. For this reason, identity lifecycle management and governance needs to be driven by a DevOps-oriented approach that leverages APIs so that access requests and self-service can be embedded into applications. Similarly, IAM solutions have traditionally been highly technical and complex, but shrinking IT budgets and an increased focus on empowering users have required modern IAM solutions to be business-friendly and easy to use. The enterprise needs a solution that is easy to deploy, easy to use and can manage its hybrid environment.

**64%** of organizations have no IAM monitoring tools[1]

**72%** don't do access review or certification[2]

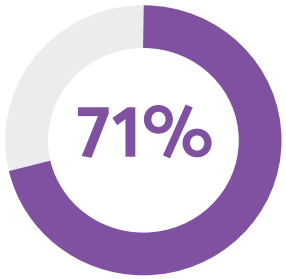
**62%** have no access request process in place[3]

1 Ponemon Institute, "Privileged User Abuse & The Insider Threat," May 2014, www.raytheon.com/capabilities/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf
2 Ibid.
3 Ibid.

# How to Address the Privileged User Dilemma?

In today's data breach epidemic, some of the most embarrassing fraud cases are related to excessive access. Unfortunately, the attack pattern is common and repeatable—a user's credentials are compromised and then the hacker gains access, elevates privileges and steals data. What makes this so compelling is that these cases are easy to solve with a modern access management solution.

In addition, organizations are increasingly being required to certify privileged access on a regular basis to either comply with internal security policies or external regulations. This means that this is not just a technology problem; it is also a governance problem. Therefore, tight integration between the identity governance and privileged access management solutions is critical. This not only reduces the overall attack surface but also addresses a plethora of compliance mandates.




of users say they have access to data they shouldn't

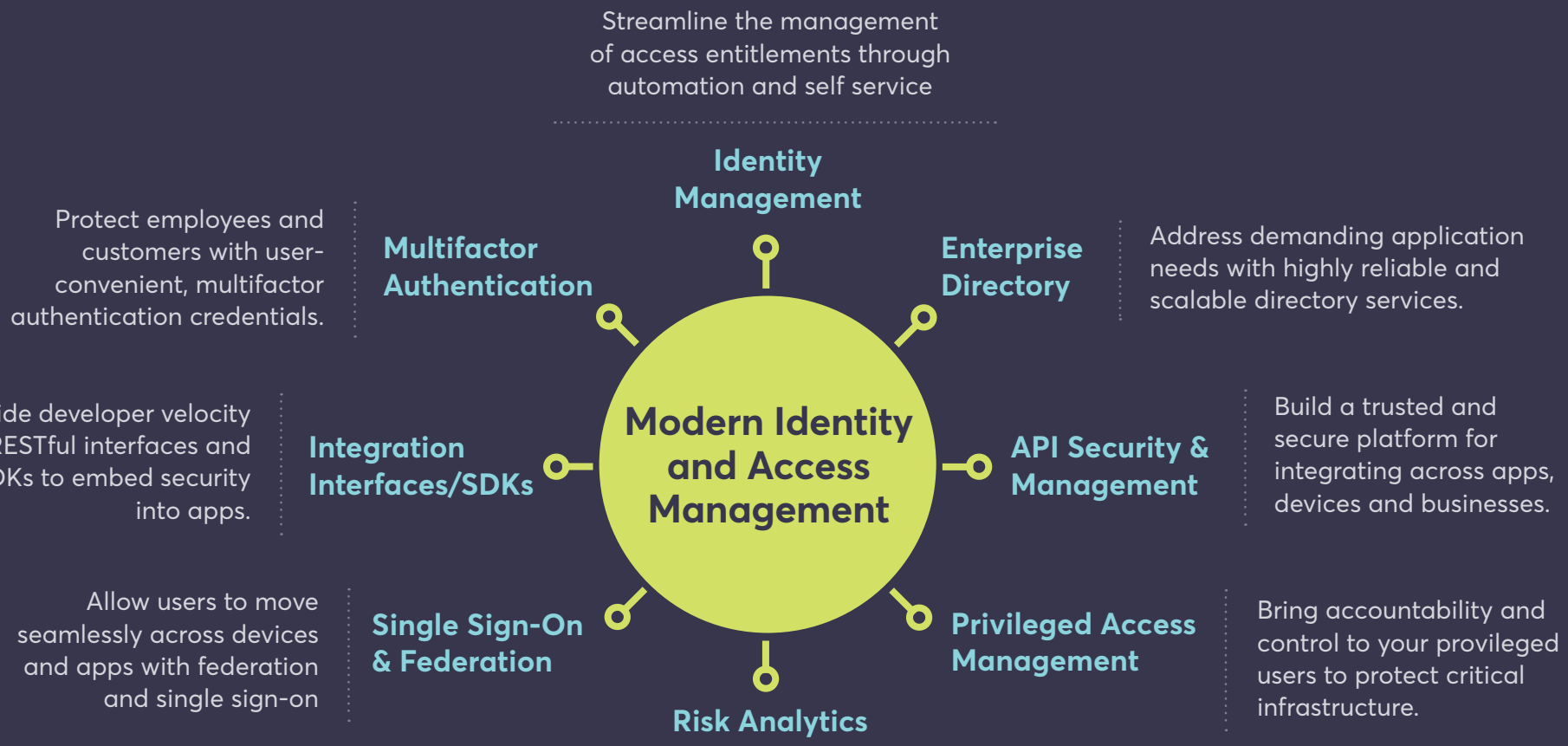

of IT professionals say their company does not enforce least privilege


of companies don't have an automated way to provision privileged access


don't have a way to certify privileged access on a regular basis[1]

1 Ponemon Privileged User and the Cyber Threat - http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

# Introducing a Modern Identity and Access Management Solution



# The CA Difference

In today's world where breaches are the norm, information is everywhere and personalized experiences drive digital transformation, identity is the key. Identity is the foundation of trust in a zero-trust online world. At CA Technologies, we understand how important it is to strike the right balance between enterprise data security and convenient user access. To this end, we have adopted three strategic initiatives to differentiate our IAM solutions:


## Hybrid cloud

Just as your application environment is moving to a hybrid model, we believe the modern IAM solution should do so as well. Your IAM infrastructure is mission critical, but it is also highly customizable. This can make it difficult to add new functionality quickly. We deliver a hybrid model that leverages the benefits of SaaS but also provides an on-premises component to enable the right level of control, governance and usage insight you need for your enterprise.

## Behavioral analytics

Gaining visibility into what users and their accounts are doing is key for two reasons. First, you can detect anomalous activity either for a malicious insider or to identify an account that has been taken over. Second, you can simplify the user experience and reduce friction by positively identifying legitimate users from fraudulent ones. Our strategy is to apply advanced analytics into our security products to make IAM processes more effective.

## Developer velocity

For IAM to be integrated into your enterprise, it needs to be API-enabled. We believe that a simple and easy developer experience is critical to getting broad adoption. Your teams understand the value of implementing security, but they need to move fast. We deliver APIs and mobile SDKs that enable security to be quickly implemented so the development teams can spend more time focusing on app functionality, not IAM.

# CA Security Solutions

We've developed solutions that address the requirements for IAM for the modern software factory.

### Access Management

Secure and frictionless access for employees, customers and partners

### Identity Management

Increase user productivity and business flexibility with user provisioning and identity governance

### Privileged Access Management

Who is accessing your privileged accounts, friend or foe?

For more information, please visit ca.com/security.

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.



CS200-329858

ca technologies