Securing Consumer Portals:

Consumer Access Management as Business Driver and Protector

ca technologies

A Growing Need for Simple, Secure Consumer Access

Managing user access has been a top-of-mind concern for IT and security experts for years, but the realities of today's application economy have recently made it a more urgent and challenging topic to address. This is especially true for customer- and partner-accessed applications, because the proliferation of mobile devices, apps and social media have conditioned users to expect a simple, seamless way to authenticate and interact with their favorite brands.

While these endpoints represent new opportunities to enhance the customer experience, they're also attractive points of exposure for hackers and other cyber criminals to attack. This has CIOs asking the question, "How do we make it easy for customers to interact with us, while still protecting their identities and sensitive data from harm?" And how they answer that question can mean the difference between success and failure—for themselves and the business.

63% of mobile users will access online content through mobile devices by 2017.[1]

68% of shoppers abandoned online shopping carts worth an estimated $4.9 trillion in 2015.[2]

95% of web application breach incidents involve using stolen customer credentials to log in.[3]

1 Statista, "Statistics and facts on mobile internet usage."
2 Bolton, Hazel, "Shopping Cart Abandonment Rate Statistics," Formisimo, February 20, 2015.
3 Verizon, "2015 Data Breach Investigations Report," 2015.

The Flaws of Password-Driven Security

Most CIOs understand that a rich, dynamic and easy-to-navigate digital presence—whether a mobile app, Web portal or both—is critical for building and sustaining effective relationships with their customers and partners. They'll spend incredible resources refining the user interface and increasing performance and speed in the hopes of exceeding customers' ever-increasing expectations.

Why is it, then, that many fail to put the same energy and thought into managing and securing their customers' identities?

Oftentimes, they're content with a standard user name and password approach, with complex composition rules or PIN numbers for security. However, there are two significant problems with this approach:

1. **Complex passwords are difficult to remember** and make it frustrating for customers and partners to manage their identities.

2. No matter how "strong" a password is, it **can still be compromised** by such attacks as phishing, man-in-the-middle (MITM), brute force and spyware.

Frustrating users is the quickest way to drive them into competitors' arms. And of course, once an organization is compromised by an attack, it faces significant damage to both its reputation and bottom line.

From Stopgap Solution to Comprehensive Access Management Strategy

The fact is, complex passwords were a stopgap solution for a problem that has become business-critical: accurately identifying legitimate users from fraudulent ones. And in an increasingly competitive market, businesses like yours simply can't risk driving customers or partners away due to a frustrating or risky user experience.

What's needed is a more comprehensive strategy—one that not only simplifies the identity management experience for customers and partners, but also ensures privacy and protection of sensitive data. Gartner refers to such a strategy as Consumer Identity Access Management (CIAM).

According to Gartner:
"Organizations should plan on the scope of digital business expanding to encompass the use of smart devices, such as increasingly intelligent vending machines, ATMs, cars (that can interact with a consumer's phone) and even cardiac pacemakers. Because more of the devices that we rely on for our health and safety now include a software component, properly controlling consumer access and engagement with systems has moved from an issue of convenience to an issue of financial risk management and physical safety."

In other words, a CIAM strategy is no longer a "nice to have," but rather a **critical success factor in the application economy**.

4 Gartner Research, "Consumer Identity and Access Management Is a Digital Relationship Imperative," G00293444, December 30, 2015.

Unique Requirements for Consumer Access Management

On its surface, CIAM is all about managing customer or partner identities with a similar level of care and attention as employee-facing identity and access management (IAM). That said, there are some unique capabilities that make consumer access management (CAM) stand apart—and enable you to provide a secure, unified and compelling customer experience across multiple channels.

1. Social Registration

When users can leverage their existing social media identities (e.g., Facebook, Twitter, Google+, etc.) to log into your site or portal, it streamlines the login process and gives them one less password they have to remember. Yet while social logins reduce friction, they can be insecure themselves, so it's important to have step-up authentication processes in place when more sensitive transactions are being attempted.

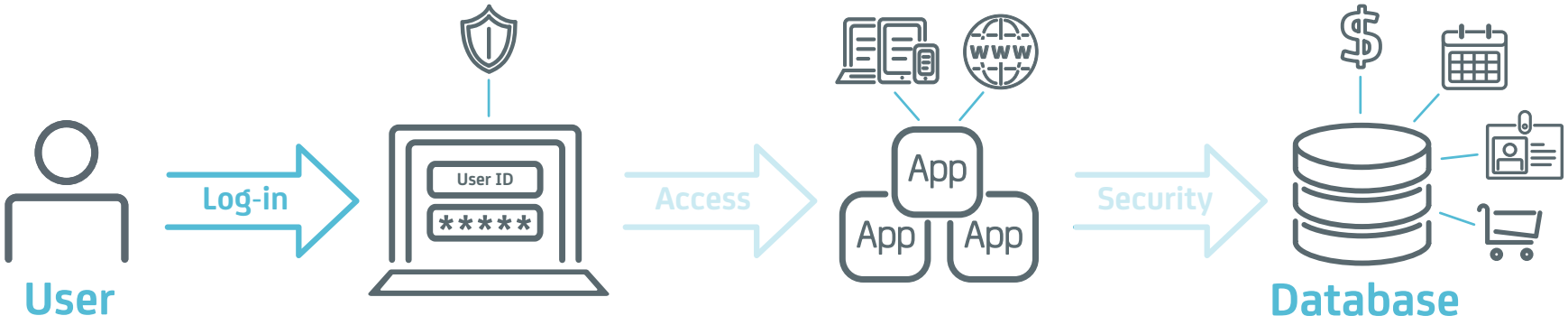
2. SSO and Federation

If you can provide seamless access for customers and partners to all of your web applications, portals and security domains via a single sign-on, it makes it easier for them to consume more of what you offer, which helps strengthen your relationships and open up new—or bolster existing—revenue streams.

3. Context-Sensitive Security

Whether users authenticate with social media credentials or log in directly with a password, both are inherently insecure, as they can be easily stolen. As a result, it's critical to be able to apply risk analysis and user behavior profiling to the authentication process, so you can more accurately identify legitimate users from fraudulent ones. And, when the context of the access appears too risky, you can issue an out-of-band challenge to their registered mobile device.

Exploring CAM in Action



1

The **user logs into the portal with social credentials**, eliminating an opportunity for a new password to be targeted with a brute-force attack. Additionally, the CAM solution initiates a step-up authentication process if/when the user attempts to access a high-risk area of the site.

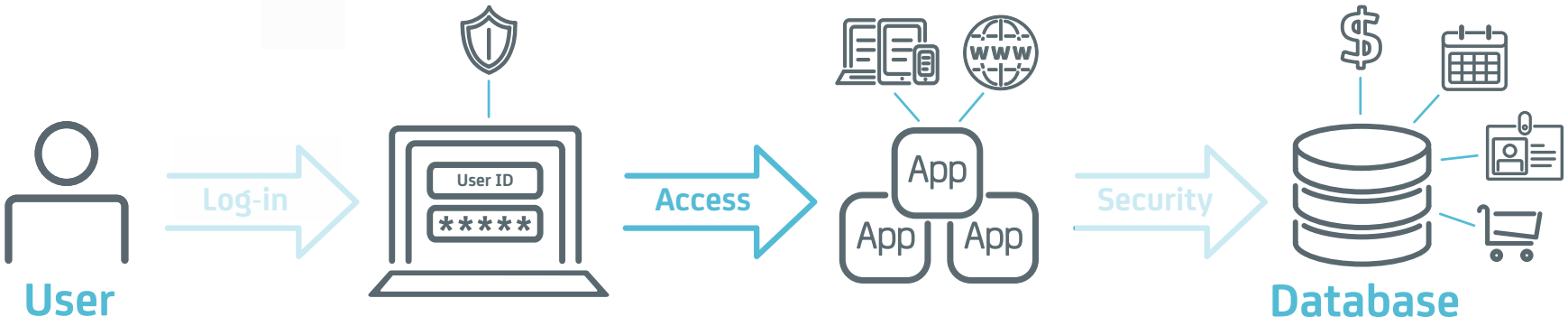
2

Prevent ACCESS Breach

3

Prevent SECURITY Breach

Exploring CAM in Action



1

Prevent LOG-IN Breach

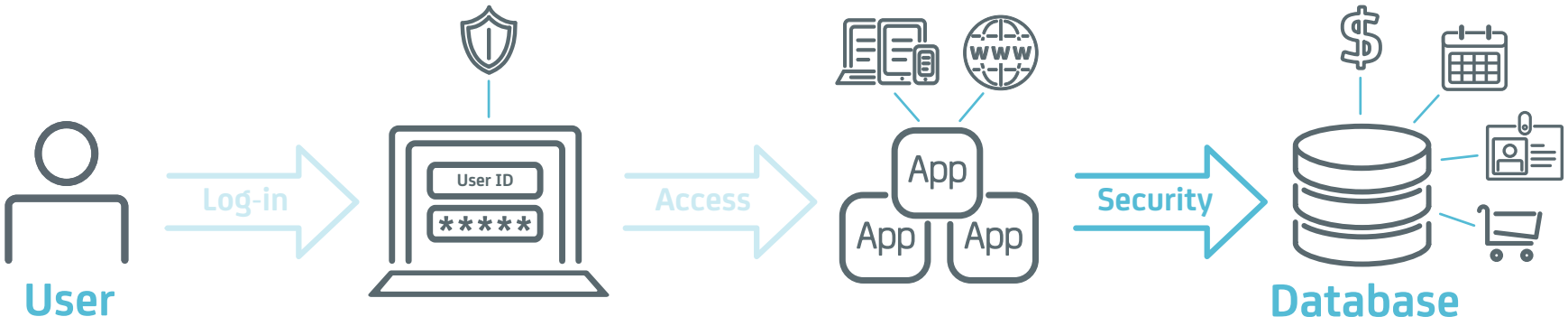
2

The CAM solution recognizes and **authenticates the device** the user is logging in from, enabling access to approved apps and web services and preventing any session hijacking attempts.

3

Prevent SECURITY Breach

Exploring CAM in Action



1

Prevent LOG-IN Breach

2

Prevent ACCESS Breach

3

The CAM solution **grants access to various apps and data** based on risk, asking for additional, stronger authentication from the user (e.g., a one-time password sent via SMS) when the risk level crosses a certain threshold.

What Can CAM Do for You?

What if you could ...

With **CA Single Sign-On** and **CA Advanced Authentication** as your CAM solution, you can:

... authenticate customers and partners connecting from multiple devices and interfaces supporting a wide range of identity credentials?

Efficiently deploy and provide secure access control to applications and capture new growth and innovation opportunities with customers and partners.

... provide access to multiple applications and services from the same authentication transaction?

Enable users to sign on once for a secure and unified online experience, reducing frustration and increasing engagement.

... analyze risk based on behavior, device and location and initiate step-up authentication when risk is high?

Deliver consistent, centralized security management that supports multiple access methods and heterogeneous applications, so you can protect your business from fraud, hackers and other threats.

With CA Single Sign-On and CA Advanced Authentication as your CAM solution, you can **give customers and partners secure access to essential information and applications**—whether on-premises, in the cloud, from a mobile device or at a partner's site.

About the Solution from CA Technologies

Key capabilities include:

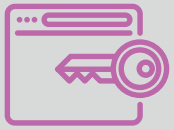
Federation and Open Standards

- Flexibility to support traditional access management (i.e., "tightly coupled") and federation (i.e., "loosely coupled")
- Support for SAML 2.0 profiles for accessing SaaS apps, OAuth 2.0 for social media identities and STS translation to WS-Federation for Office 365®
- Documented integration with SaaS applications

Authorization and Access Management

- Ability to restrict access by user, role, groups, dynamic groups or exclusions
- Fine-grained authorization at the file, page or object level
- Access decisions or redirection of users based on type or context of authentication or authorization request
- Centralized administration and auditing

Session Management and Security



- Enhanced Session Assurance with DeviceDNA™, a patent-pending device identification technology native to CA Single Sign-On
- Strong defense from session hijacking with Session Linker, which extends protection to applications (e.g., SAP, WebSphere, etc.) that use their own session cookies

Why CA for CAM?

As part of the larger suite of CA Security solutions, CA Single Sign-On has contributed to notable benefits for customers.

71%
OF BUSINESSES ARE BETTER ABLE TO ENGAGE WITH THEIR CUSTOMERS.

EVERENCE FINANCIAL WAS ABLE TO:

Bring **new apps** to market more than **20% faster**

Increase revenue through faster delivery of new services

Improve employee **productivity** by **up to 10%**

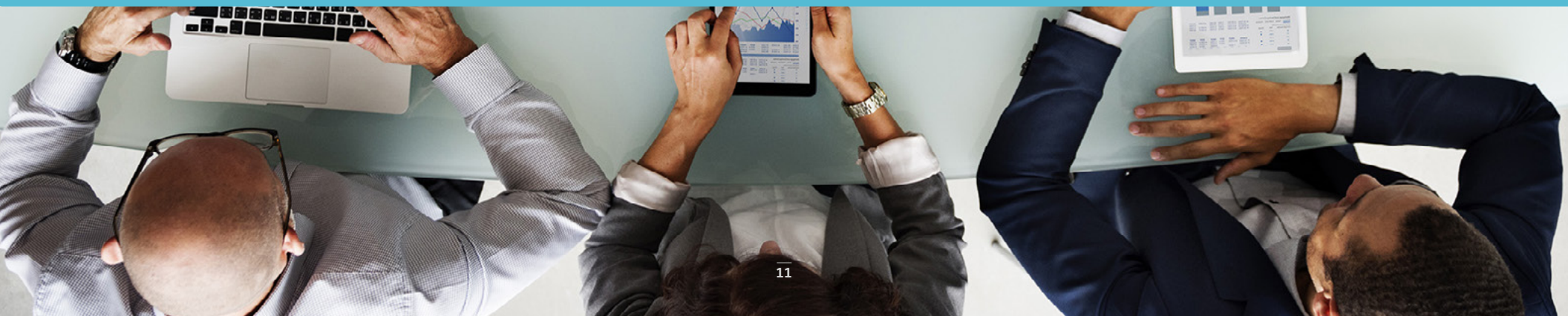
CA Single Sign-On increases confidence in protecting against security breaches "by creating a consistent and secure front door."

— Donald Murphy, IT Manager, First Niagara Financial Group, Inc.

"CA Single Sign-On (formerly CA Siteminder®) has significantly simplified securing our environment."

— Rob Blucker, IT Director, Everence Financial

The above customer data comes from TechValidate research commissioned by CA Technologies.



How Secure Are Your Consumer and Partner Portals?

Simplifying sign-on, authentication and the overall user experience is key to keeping your customers and partners coming back for more—but not at the expense of protecting your business-critical applications and data. With CA Single Sign-On and CA Advanced Authentication, you can protect and propel your business in the fast-moving and ever-evolving application economy.

For more information, visit ca.com/single-sign-on

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.

200-202562

ca technologies