SOLUTION BRIEF
ADVANCED AUTHENTICATION

How do I increase trust and security with my online customers in a convenient and cost effective manner?

ca technologies

CA Advanced Authentication provides transparent, risk-based evaluation and a flexible set of easy-to-use, multi-factor credentials to improve security and trust by identifying and preventing potential online identity fraud.

Executive Summary

Challenge

The application economy has changed the way businesses interact with their customers. Users demand anytime, anywhere access to online services and expect the same user experience across multiple devices and access channels. Great opportunities and efficiencies exist for organizations that can effectively leverage the Internet to deliver their services. However, the app economy also presents challenges. Passwords are the most common way for users to authenticate to Internet portals and mobile applications, but they are also a critical, weak link in an online security system. The enterprise needs to provide a more secure way to protect user identities and ensure data privacy without undue burden for the customer.

Opportunity

CA Advanced Authentication provides a secure, user-convenient and cost-effective way to protect consumer portals and mobile applications. CA Risk Authentication allows the enterprise to silently and transparently collect data and assess risk based on device identification, location and user behavior, among other factors. CA Strong Authentication provides a wide variety of software-based, two-factor authentication credentials and technology to make passwords more secure. Together they enable an intelligent, layered security approach to protect user identities and organizational data.

Benefits

A centralized approach to authentication across both traditional and new channels of customer interaction helps provide a consistent and positive user experience. CA Advanced Authentication provides additional security for all the applications and confidential data that can be accessed through a browser or mobile device and thus helps reduce the risk of online identity fraud and other data breaches. Enabling this protection in a familiar, user-friendly manner allows organizations to improve security and reduce fraudulent activity without impacting the customer experience.

Section 1:

Customers know you through software.

Your customers are far more likely to experience your brand and interact with your enterprise through software than a live person. To thrive in this new reality, every industry, from retail to government, entertainment to banking, manufacturing to healthcare, needs to have a mobile strategy and presence—specifically a mobile app that allows consumers to connect to the enterprise. For organizations who can execute these strategies and leverage mobile apps effectively, the payoffs are significant.

In 2014, CA Technologies commissioned a global survey of 1,425 senior business executives on how global enterprises are responding to these challenges, the business results they are achieving and how to remain competitive in this new reality. The survey uncovered “leaders” in the application economy who are significantly out performing “laggards” and demonstrated an application divide between the two.

The application economy leaders (compared to the laggards) experienced:

- More than double the revenue growth
- 68 % higher profit growth
- 50 % more business coming from new products and services[1]

Although consumers are increasingly turning to mobile apps as their preferred access channel, they are a fickle bunch. Many enterprises struggle with mobile app adoption. A complicated or poorly designed interface or bug ridden app will not be tolerated by today’s mobile app savvy users; superior user experience is the ultimate priority. And this challenge is further compounded when the enterprise considers security. Among the companies surveyed, security was identified as the top obstacle for mobile applications.

Standard passwords with complex composition rules are not user-friendly and four or six digit PINs can be easily guessed. Passwords can be stored within the app, but then the account can be easily compromised if the device is lost or stolen. Incorporating intelligent risk analysis in combination with a user-friendly credential significantly increases the security of the mobile app without impacting the user’s experience. In addition, embedding a multifactor credential into the app provides a powerful layered security approach that can address regulatory compliance requirements.

The Battleground: Consumer Portals

The proliferation of Internet websites has presented greater opportunities for corporations and government entities to deepen relationships with consumers and citizens. But opening the enterprise via the Web is not without its challenges. With the growth in users and applications came the inevitable increase in the amount and types of sensitive data that users can access online—from personally identifiable information to financial data to healthcare and patient data—all of which needs to be protected from inappropriate access, a battle that enterprises are losing. New breaches are reported daily in the news. Why does this keep happening? One reason is that identity theft and fraud is a big business. Another reason is that many websites continue to use simple passwords for authentication.

The Shift in Criminal Activity

The financial institutions were the first to experience online attacks and in response, governments and industry bodies enacted laws and issued guidelines to improve security. The consensus view was that simple username and password authentication were not sufficient to protect personal identity information and that continued identity fraud would erode customer confidence in online banking. As a result, stronger authentication mechanisms were recommended for sensitive transactions, including initial login and funds transfers.

Meanwhile criminals have expanded their reach beyond traditional targets of consumer banking and credit cards. They are now seeking to harvest valuable information from government organizations and sensitive enterprise data that has been exposed via Internet portals.

Any enterprise that is exposing sensitive data via their Internet portal is a potential target to criminals.

The Top 5 Sectors breached:

Healthcare	37%
Retail	11%
Education	10%
Gov & Public	8%
Financial	6%[2]

Passwords—The Weak Link

It is not news that passwords are not secure. Passwords can be easily cracked or stolen, which presents a problem. When used as the only form of authentication, they can be a weak link in security which leads to identity theft and fraud.

> “95 percent of [Web app] Incidents involve harvesting credentials stolen from customer devices, then logging into Web applications with them.”[3]

As a result, many organizations have implemented rules on password composition. But while these rules make passwords harder to guess (strong passwords), they also make them harder to remember, which has led to increased password reset calls to service desks and frustrated customers, not to mention the reuse of passwords across multiple sites. In addition, composition rules do not make “strong passwords” any more secure. Recent attacks such as phishing, man-in-the-middle (MITM), brute force, spyware and social engineering show how easily strong passwords can be compromised.

Another point of attack for a security breach is the stored repository of passwords—that is, the password hash file. Common practice is to protect passwords using hash algorithms. But the directories and databases where these files are stored are a common target for hackers. In fact, many brute-force attacks exist today that can decode these files to reveal and compromise passwords in realistic timeframes. The continued storage of hashed passwords makes these attacks possible.

The stronger authentication mechanisms initially recommended for online banking are rapidly becoming a necessity for all Internet-facing applications. Simply adding a transparent contextual risk evaluation to your existing password authentication provides greater assurance that the user is who they claim to be. And because user sessions can also be easily stolen and replayed, risk can be actively assessed throughout the session, especially when the user is about to conduct a sensitive transaction.

> "If you have a web presence (e-commerce or otherwise), you should be tracking user behavior and using some form of fraud detection to get an early warning of suspicious behavior...To combat Web app attacks head-on, we recommend strengthening authentication. The use of two-factor authentication for Web applications—even by customers—will go a long way toward keeping your organization from being used and abused."[4]

The combination of a two-factor credential with risk-based authentication can provide a powerful layered security approach that can significantly reduce the risk of inappropriate access and address regulatory compliance and auditing requirements. This approach makes it much more difficult for an attacker to gain access to customer data and can be used to eliminate stored password files.

Section 2:

CA Technologies Multi-Layered Authentication

Our identity-centric approach to security delivers both the risk protection companies need and the flexibility and ease-of-use users expect. CA Advanced Authentication provides an intelligent approach to authentication security to help combat the increasingly sophisticated cybercriminal especially as enterprises expand their applications beyond the perimeter.

Authentication That Is Convenient, Secure and Cost-effective

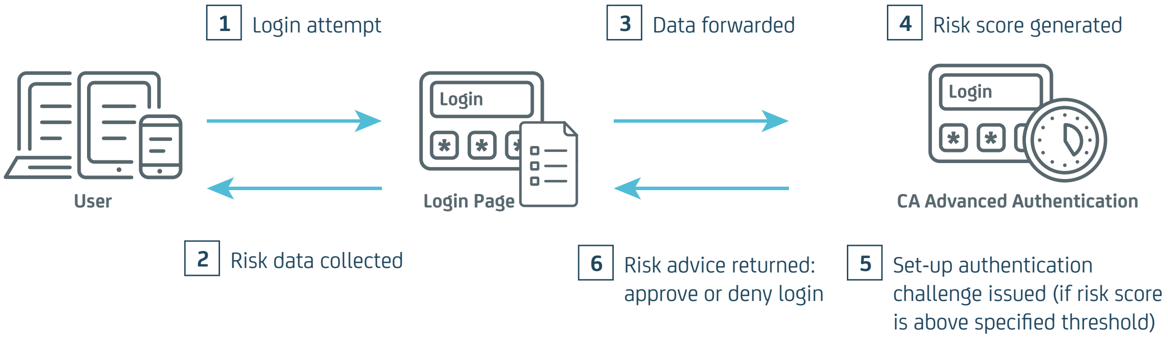
CA Advanced Authentication combines risk-based analysis, user behavioral profiling and a variety of credentials to more accurately authenticate genuine users without interrupting their activity. This makes it easy for your customers to access their accounts and gives you greater assurance that the access is by a legitimate user.

The risk-based component, CA Risk Authentication, can detect and protect against higher-risk access attempts and transactions by analyzing a wide set of factors without requiring any direct input from the end user. The risk evaluation produces a risk score that is combined with your business policies to determine if any action is required. This allows legitimate users, the majority of the login attempts, to continue uninterrupted because their risk score is low. In the case of an unacceptable risk score where the user's behavior is outside the norm, the user can automatically be required to do step-up authentication to further prove their identity. This could include answering knowledge-based questions or entering an OTP that has been sent (out-of-band via SMS, email or voice) to their mobile phone. High-risk access attempts can be denied and/or cause an alert that triggers security or service desk intervention if necessary. The organization has the ability to use preset rules and/or add custom rules to control and adjust the risk scoring process to fit their environment.

Risk analysis can detect and stop inappropriate access on its own to catch fraudulent activity even if credentials have been compromised.

Figure 1.

CA Advanced Authentication risk assessment workflow


1 Login attempt
3 Data forwarded
4 Risk score generated
Login
Login
User
Login Page
CA Advanced Authentication
2 Risk data collected
6 Risk advice returned: approve or deny login
5 Set-up authentication challenge issued (if risk score is above specified threshold)

CA Risk Authentication provides the following:

- **Better User Experience:** CA Risk Authentication Can authenticate your customers without complicated user credentials. Enterprises can use risk-based authentication with simple passwords and only require step up authentication if the login seems risky. This provides a frictionless login experience for most users, improving satisfaction and customer retention while reducing calls to service desk for halted or blocked transactions.
- **Greater Accuracy:** Using an enterprise-specific model that understands legitimate and fraudulent behavior, we can determine the validity of a user in context of what is normal for that individual. In real time during authentication, CA Risk Authentication takes a multidimensional view of the login by using elements such as the device characteristics, geolocation, login velocity and historical user behavior.
- **Faster Speed of Change:** CA Risk Authentication allows enterprises to make changes to rules and business policies on the fly. With access to case information for all logins, an administrator can update authentication policies based on action that triggered step-up authentication or denied login. Policies can be updated or added dynamically as required by the business needs. There is no dependency on the vendor to make changes.

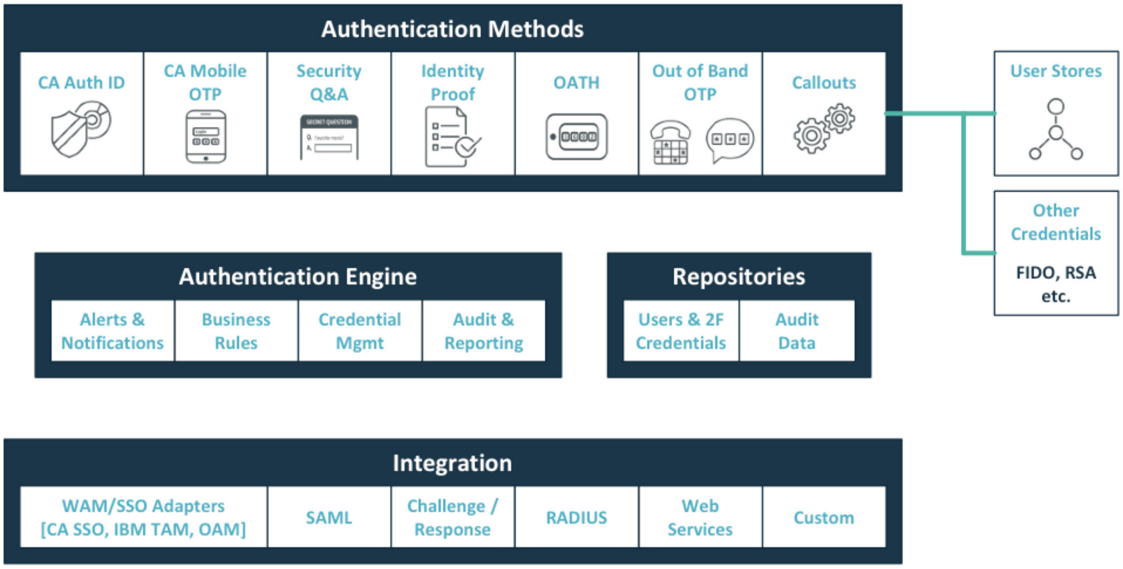
In addition CA Risk Authentication provides case management capabilities. Customer service representatives or fraud analysts can immediately access data that shows why an access was denied and provide reporting on step-up activity.

Versatile Authentication and Multiple Two-Factor Credential Options

CA Strong Authentication provides a broad set of authentication methods that can be applied as appropriate for different applications, user groups and situations, including password, knowledge-based Q&A, out-of-band, out-of-wallet Q&A, OATH-compliant tokens and the unique CA Auth ID and CA Mobile OTP.

Figure 2.

CA Advanced Authentication versatile authentication server



You can use the wide range of authentication methods and credentials available or bring your own credential as part of your centralized authentication strategy.

The CA Auth ID and CA Mobile OTP are secure software credentials that provide two-factor authentication that can be deployed on a computer, tablet or mobile phone and are protected with a patented key concealment technology called “Cryptographic Camouflage” against brute force and dictionary attacks that attempt to derive the password.

Unbreachable Passwords

The CA Auth ID is a self-contained PKI-based two-factor credential that employs a hidden challenge/response mechanism. This software-based credential is both easy to deploy and simple for users. The one-time enrollment process can be as easy as a few self-service screens, or it can be extended to include knowledge-based answers (KBA) or SMS delivery of a one-time code for extra security. After enrollment the user login experience is unchanged. The user submits their username and password as they would today and the PKI challenge/response process is completely transparent to the user. In addition, the password is used to derive the private key and is considered to be “unbreachable” because it is not stored on the server or device and is never sent over the wire; it only exists in the user’s head.

Finally, users demand anytime, anywhere access to applications. This means that they will not always login from the same device used for initial enrollment. CA Strong Authentication supports this via a concept called roaming. When using a new device, workstation or public kiosk, users can use a secondary authentication method to receive a permanent or temporary CA Auth ID, giving the user the same secure communication they would experience at their home office.

Authenticate with Mobile Device

The CA Mobile OTP credential is a secure software passcode generator that allows mobile phones, iPads and other PDAs to become a convenient authentication device. If users are familiar with an OTP approach, this is an easy way to upgrade to a software-based solution that is secure, scalable and cost-effective. It supports industry standards including OATH (HOTP, TOTP) and EMV (CAP/DPA). In situations where an out-of-band authentication method is preferred, CA Advanced Authentication can also send an OTP to the user via email, text, or voice. This mechanism can be used for primary authentication (i.e., initial login); roaming access (i.e., logging in from a new device), or as a step-up mechanism when a risk score exceeds a specific threshold.

Identity Proofing

CA Advanced Authentication can be configured to callout to an external identity proofing service (e.g., Equifax, Lexis Nexis, etc.) for “out of wallet” questions. The system will use a configured number of randomized questions for the knowledge-based authentication challenge. The user must answer the expected number of challenges as defined in the policy. This mechanism can also be used for primary authentication (i.e., initial login) and roaming access (i.e., logging in from a new device, user registration, or as a step-up mechanism when a risk score exceeds a specific threshold).

Integration Approaches

The CA Advanced Authentication solution provides several integration options. First, several prebuilt adapters are available that allow the solution to be easily integrated with leading Web Access Management/SSO solutions, including CA Single Sign-On (formerly CA SiteMinder), IBM Tivoli® Access Manager and Oracle Access Manager. Similar adapters can be built for other solutions via a services engagement. If a WAM/SSO solution is not being used to protect the Internet portal/sites, then CA Advanced Authentication provides a JavaScript™ client that can be embedded into your existing login page. This client can encrypt/decrypt the two-factor credentials, sign the hidden PKI challenge, collect risk analysis data and communicate with the solution servers for authentication and risk evaluation services.

In terms of mobile devices and applications, the aforementioned integration approaches will support any browser running on a mobile device. CA Advanced Authentication also provides libraries for Android and iOS so that organizations can embed the risk data collectors and/or two-factor credentials into their mobile apps. These libraries will communicate via web services to the solution servers to request authentication and risk evaluation services.

Section 3:

Improved Online User Security Without Changing User Experience

CA Advanced Authentication delivers additional protection for your consumer web sites and mobile apps.

CA Risk Authentication enhances simple password mechanisms and can prevent unauthorized access to customer accounts and data even if login credentials are compromised. This approach is transparent to the consumer as it requires no action on their part while providing greater assurance that the user is who they claim to be. The majority of logins are performed by legitimate users and these will continue uninterrupted because their risk score is low. And for the few higher risk scenarios, CA Risk Authentication provides a simple and easy means to validate a user's identity. In addition, user behavioral profiling ensures that risk is evaluated based on what is normal for each individual user and can detect when their behavior deviates from the norm. Finally, risk can be assessed throughout the user's session, especially when the user is about to conduct a sensitive transaction. This guards against stolen cookie attacks.

CA Strong Authentication provides software and mobile credentials that make it easier to distribute, maintain and scale to a larger user communities. The simple enrollment process, familiar login formats and self-service features increase adoption and help maintain a high level of user satisfaction. The patented key concealment technology makes it more secure than other credentials. In addition, the CA Auth ID credential can be deployed such that you can eliminate high target password hash files from being stored in backend repositories.

The combination of a two-factor credential and intelligent risk evaluation can make it much more difficult for an attacker to gain access to the organization's Internet portals and sensitive data. This is a powerful combination of benefits, any one of which could be used to justify the solution, but together create a compelling business case for any organization. In addition, this type of a secure implementation can also be very helpful for dealing with compliance regulations and auditing requirements.

Section 4:

The CA Technologies Advantage

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.

Section 5:

Next Steps

Organizations should take a look at the full spectrum of data and resources that users can access via their applications and develop a risk appropriate authentication strategy. In many situations this will reveal the need for some form of strong authentication. The next challenge is to select the best combination of security, cost and user convenience to meet these needs. CA Technologies offers a wide range of advanced authentication solutions that provide additional security in a user friendly and cost effective manner.

To learn more about CA Advanced Authentication visit **ca.com/us/multifactor-authentication.**

Connect with CA Technologies at ca.com

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.

[1] All data on this slide is from "CA Application Economy Market Study," commissioned by CA, conducted by Vanson Bourne, 2014.

[2] "Symantec Internet Threat Report—2015"

[3] "Verizon Data Breach Report – 2015"

[4] "2015 Data Breach Investigations Report," published by Verizon.