Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

Keep the Door Open for Users and Closed to Hackers

ca technologies

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

A Shift in Criminal Activity

Your Web site serves as the front door to your enterprise for many customers, but it has also become a back door for fraudsters.

According to recent reports, cybercriminals have expanded their reach beyond traditional targets of consumer banking and credit cards. They are now looking to harvest valuable data that is accessible online or via mobile devices.

The top five sectors Breached:[1]

Healthcare	Retail	Education	Gov. & Public	Financial
37%	**11%**	**10%**	**8%**	**6%**

This year, organized crime became the most frequently seen threat actor for Web app attacks.[2]

[1] *Symantec Internet Threat Report 2015*
[2] *Verizon Data Breach Report 2015*

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

Password Vulnerabilities

Left to their own devices, users often choose simple passwords—ones that they can remember without much trouble. This means they use a word, phrase or number that has special meaning to them. But an intruder who knows something about the user may be able to crack the password with little difficulty.

However, even when strong passwords are used, users are not safe. Recent attacks such as phishing, Man-In-The-Middle (MITM), brute force, Spyware and social engineering show how easily strong passwords can be compromised.

95%

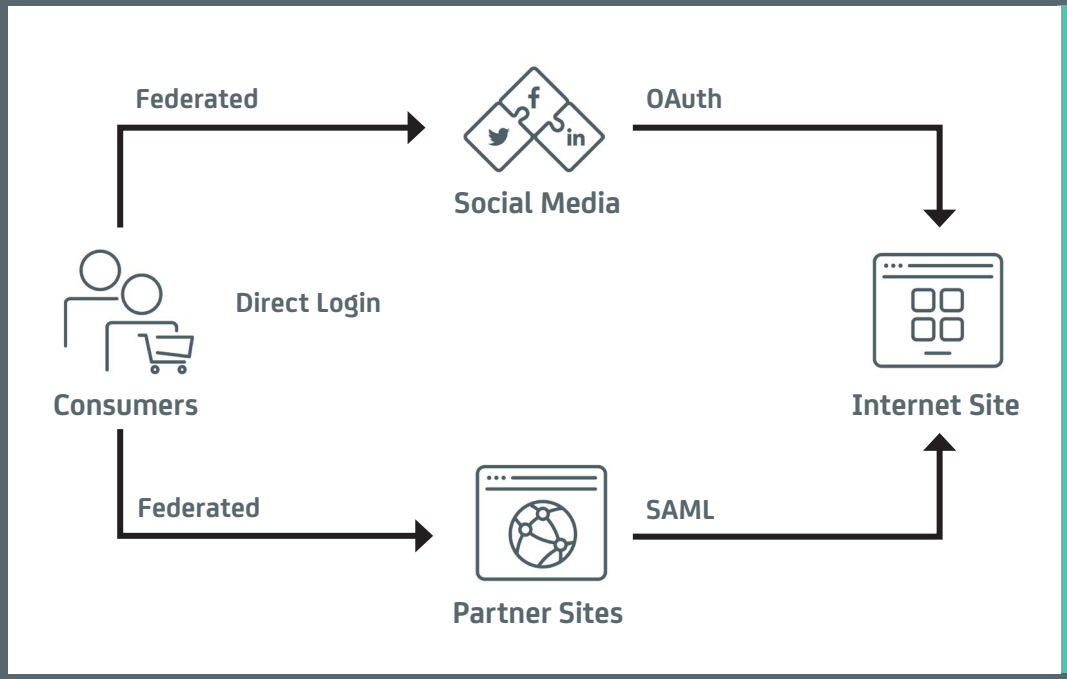
Of [Web app] incidents involve harvesting credentials stolen from customer devices and using them to log into Web Apps.[3]

[3] *Verizon Data Breach Report 2015*

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

Routes to Your Internet Site

Not only do users favor simple passwords, but they want to simplify the sign-in process by...



53%

of survey respondents use social login in order to avoid filling in registration forms.[4]

...logging in with social networks like Twitter, Facebook, LinkedIn, Instagram, etc. and federating in from partner sites which puts data at an even greater risk.

[4] *Statista, Reasons for users in the United States to Use Social Login as of July 2014.*

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

And the danger does not stop with login.

Since the beginning of Web application delivery, there has been an opportunity for fraudsters to get into the middle of a transaction and impersonate the legitimate user. Since the credentials used for this fraud are valid and "expected to be under the control of the real user," this type of impersonation has been difficult, if not impossible, to detect and stop.

This requires that organizations implement authentication strategies based on the type of data or application being accessed. Security measures should not just take place during initial authentication but continuously throughout the user's session in order to prevent cookie replay attacks.

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

What if a user's account is compromised?

What types of data could a hacker access?

How would you know there was a breach?

What types of actions could be performed?

What would be the impact to the end user?

If your Internet site has **1,000,000** users, **0.7 percent** of your users will have their passwords compromised annually,[5] which is approximately **7,000** breached accounts per year and estimated data breach costs of **$1.5 million** annually.[6]

[5] *Verizon Data Breach Report 2015*
[6] *2015 Cost of Data Breach Study by Ponemon Institute*

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

Strong Authentication—Striking the Right Balance

Future enterprise authentication initiatives will be guided by three considerations:

Appropriate Security

User Convenience

Total Cost of Ownerhip

The right combination of the above will help organizations lock down sensitive data but also offer users a frictionless experience regardless if they interact with the enterprise online or from a mobile device.

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

A Layered Security Approach

In strong authentication, factors are commonly categorized as:

Something you know

(examples: password, PIN, Q&A)

Something you have

(examples: certificate, device)

Something you are

(examples: fingerprint, retina scan)

There are a number of emerging methods of authentication as well, such as:

Where you are

(examples: IP, geo-location)

Is device trustworthy

(examples: known or unknown)

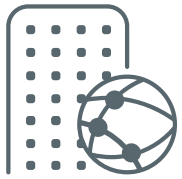
What is behavior

(examples: normal or abnormal)

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

Risk-Based Authentication

Risk-based authentication—also known as "contextual authentication"—is a server-side initiative that offers users a simpler experience while simultaneously bolstering security.



Where is the user?

- Have they been there before?
- Where were they recently?
- Is connection type consistent?

Which system or device is being used?

- What kind of device is it?
- Has this device been used before?
- Has the device changed since it was last used?

What is the user trying to do?

- Is this a typical action for the user?
- Is the action inherently risky?
- Have they taken similar actions before?

Is the user's behavior consistent?

- Is this a normal time of day?
- Is the frequency of login abnormal?
- Is current behavior consistent with prior behavior?

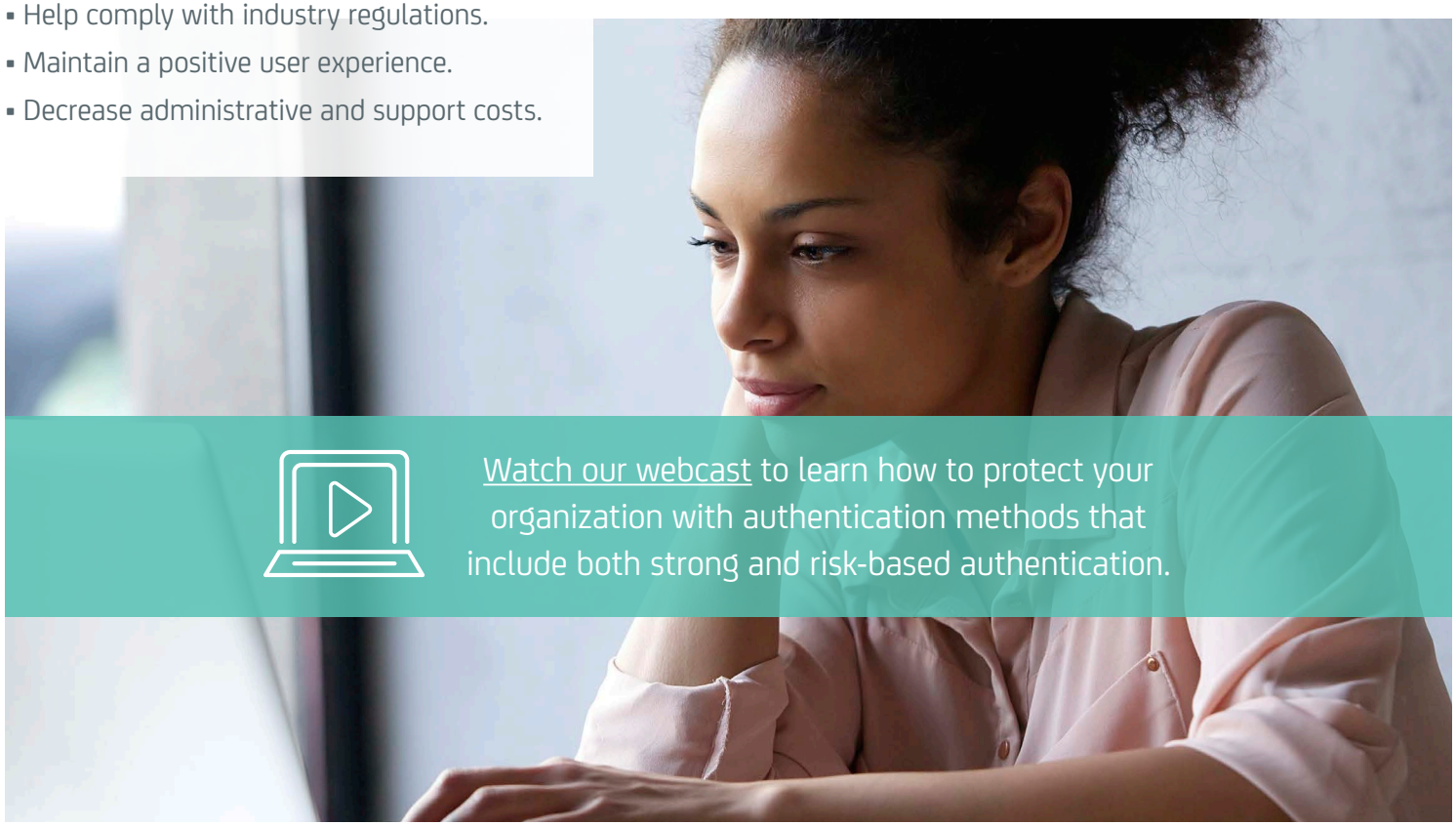
Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

Intelligent authentication includes both strong and risk-based authentication.

By combining both strong and risk-based authentication, you have an authentication solution that can:

- Give users the appropriate credential for a specific time and place.
- Reduce the potential for data breaches.
- Help comply with industry regulations.
- Maintain a positive user experience.
- Decrease administrative and support costs.

In an environment where identity theft, data breaches and fraud are increasing, as anywhere, anytime access for employees, partners and customers is also increasing, a comprehensive solution of strong and risk-based authentication is important to every organization's security strategy.



Watch our webcast to learn how to protect your organization with authentication methods that include both strong and risk-based authentication.

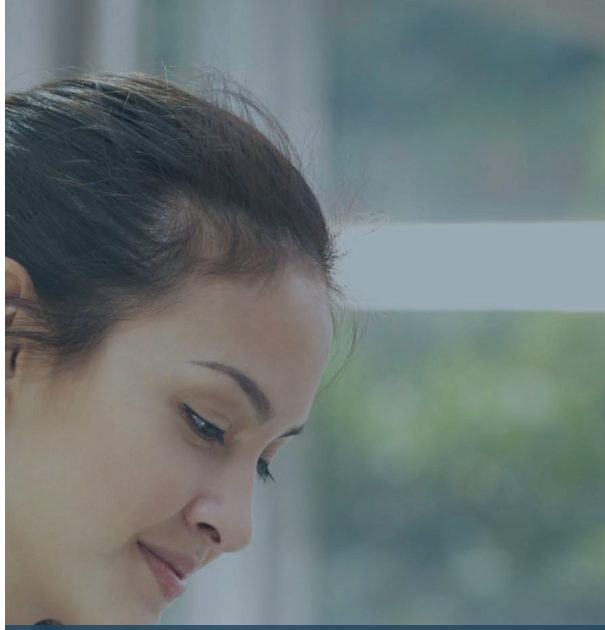
Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

Strategies for Preventing Session Hijacking

With so many access points to protect, and no guarantee that users or app and web developers are prepared to do their part, session security can seem like an uphill battle. But just as cyber-crooks have adopted new techniques over the years, you have new technologies and strategies you can put in place to protect user sessions as well.

The two most successful methods for enhancing session security are continuous device verification and risk-based authorization. Continuous device verification repeatedly reconfirms that the user who initiated the session is still in control. And risk-based authorization ups the security ante as the user attempts to access more sensitive data, requiring new and more robust authentication before opening the next door.

Both methods can be extremely helpful in securing user sessions on their own. And when used together, they can help you establish a virtually impenetrable shield between your users and the bad guys looking to hijack their sessions.



Session Security Tip

Having a secured centralized session is a much better approach to application security than having to manage session security separately for each individual application.

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

Solutions to Prevent Security Breaches From CA Technologies

CA has solutions that can provide your organization with the security it needs to protect your Internet sites from inappropriate access, data breaches and online fraud. They include:

CA Advanced Authentication can implement a transparent, intelligent risk evaluation to an existing password to provide greater assurance that the user is who they claim to be. It evaluates risk based on device identification, geo-location, user behavior and velocity, and when risk score exceeds a defined threshold, it automatically triggers a step-up authentication process. CA Advanced Authentication can also provide two unique software-based two-factor authentication credentials, which can be used to address regulatory compliance and auditing requirements.

CA Single Sign-On (CA SSO) provides a centralized security management foundation that enables Web single sign-on across on-premises, hosted or partner-based applications for your customers and business partners. It supports social login and registration and identity federation. It also embeds the CA Advanced Authentication risk analysis engine to provide enhanced session assurance with DeviceDNA™. This capability helps prevent unauthorized users from hijacking legitimate sessions with stolen cookies.

To learn more, contact your CA Technologies sales representative or visit our website: www.ca.com/securecenter.

Criminal Activity
Password Vulnerabilities
Routes to Your Site
Danger Doesn't Stop
Compromised Account
Strong Authentication
Layered Approach
Risk-based Authentication
Intelligent Authentication
Preventing Session Hijacking
CA Solutions
About CA

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**.

The annual savings shown above are estimations derived from analyses of CA Technologies customer contracts. These values are not a guarantee of achievable results and will vary depending upon your current infrastructure, people and processes, as well as the appropriate, effective implementation, adoption, and use of the CA Technologies solution. Some information in this publication is based upon CA or customer experiences with the referenced software product in a variety of development and customer environments. Past performance of the software product in such development and customer environments is not indicative of the future performance of such software product in identical, similar or different environments. CA does not warrant that the software product will operate as specifically set forth in this publication. CA will support the referenced product only in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product. CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein.

CS200-168327