

Mitigate threats and simulate growth with CA Advanced Authentication

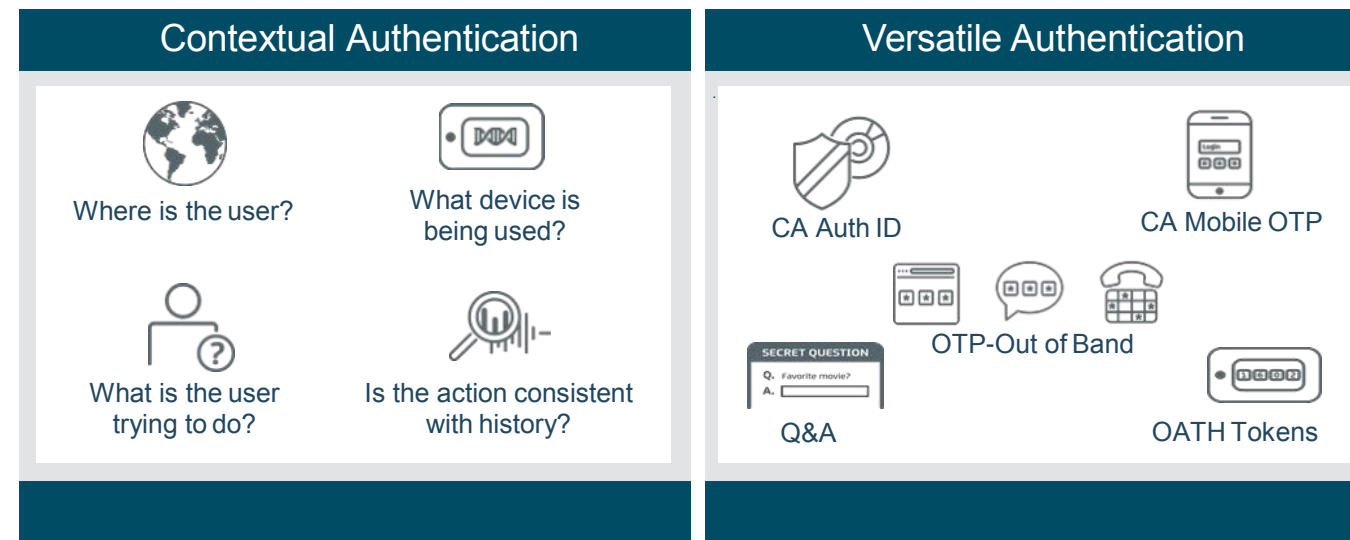
CA Advanced Authentication is a flexible and scalable solution that incorporates both risk-based authentication methods like device identification, geo-location and user behavior profiling, as well as a wide variety of multi-factor, strong authentication credentials. This solution helps organizations provide the appropriate authentication process for each application. CA Advanced Authentication is delivered as on-premise software or as a cloud service to protect end user access from a wide range of endpoints including all of the popular mobile devices.

Business Challenges

Your employees, partners and customers all need easy access to your online applications while you need to protect your sensitive data from improper access. Organizations like yours need to work with an experienced partner to:

- **Protect user identity from online attacks.** Many data breaches involve compromised user names and passwords. Convenient methods of risk-appropriate, strong authentication can protect organizations and end users from today's increasingly sophisticated attacks.
- **Provide security for mobile devices.** In BYOD environments, employees, customers and partners are using multiple devices to access and store company data along with their own. You have no choice but to secure the data they are accessing without disrupting their workflow.
- **Protect user passwords from theft or breach.** Stolen passwords are one of the most common attacks today. Any time passwords are stored on systems, even in encrypted form, the risk of damage done by a breach is significant.

CA Advanced Authentication



CA Risk Authentication™

CA Strong Authentication™

Two best-of-breed components that can be deployed individually or together

Key Features

Assess risk using DeviceDNA™ fingerprinting to identify devices accessing your applications

- Provides comprehensive user behavior modeling for improved risk analysis
- Eliminates the risk of stolen password files because passwords are never stored
- Provides default rule sets covering typical fraud patterns that make it easy to get started
- Supports wide variety of credentials – from passwords and knowledge-based authentication (KBA) methods to two-factor software and hardware tokens
- Provides out-of-band (OOB) authentication using one-time passwords (OTPs) delivered via text, voice, or e-mail
- Offers a wide variety of integration options such as SAML, API, and RADIUS
- Integrates tightly with CA Single Sign-On (formerly CA SiteMinder) and other web access management systems

Key Benefits and Results

- Reduces the risk of inappropriate access, data breaches, and attacks
- Secures data without burdening legitimate end users
- Blocks high-risk transactions and requires step-up authentication for suspicious activity
- Eliminates the risk of stolen passwords
- Scales with your organization's needs

Marquee benefits yielding \$2M per year in savings are detailed on the reverse side of this document in order to show examples of business value achievable through this CA Advanced Authentication approach

For more information, please visit ca.com/Advanced Authentication





Business Value Estimations

CA Advanced Authentication benefits can be quantified via a wide range of benefit scenarios. A selection of these is listed below to show common areas measured.



Business Value Proposition	Business Value Enabler	Specific Measurement	Solution Area	Impact Range ¹	Key Resources Affected	Average Resource Value ²	Projected Savings / yr ³
Reduction in cost of fraudulent on line identity exploits	The solution reduces the number of fraud exploits through the use of two-factor credentials, risk-based analysis, and step-up authentication	Reduction in financial losses	Advanced Authentication	55% - 75%	Total cash value in on-line customer accounts	\$1,625,000	\$1,055,250
Reduction in service desk costs	The solution provides multiple OOB methods to authenticate a forgotten user passwords, thereby reducing need for calls to the Service Desk	Reduction in labor costs for Service Desk operations	Advanced Authentication	15% - 25%	Service Desk FTEs	6	\$108,000
Reduction in cost of loyalty program exploits	The solution will reduce the number of loyalty plan financial losses through the use of two-factor credentials, risk-based analysis, and step-up authentication	Reduction in financial losses	Advanced Authentication	70-80%	Average Number of Loyalty members	700,000	\$525,000
Reduction in legacy hardware token operations costs	The solution provides software-based two-factor credential that is less expensive to deploy and maintain than a hardware-based token solution	Reduction in legacy solution support costs	Advanced Authentication	30% - 60%	Operation & maintenance costs + System Admin FTE	\$430,000	\$193,500
Enhanced revenue due to faster time to market	OOB solution can accelerate deliver of web and mobile applications by addressing the primary concern with these types of applications – security	Revenue gains	Advanced Authentication	20% - 40%	New revenue	\$400,000	\$120,000

This table shows some **key benefits** of CA Advanced Authentication. Your CA Technologies representative can also share additional and more detailed ROI business case examples for this solution by engaging the CA Business Value Analytics Team. This team works with CA's customers to develop and analyze a comprehensive set of assumptions and environment specific metrics in order to build customized projective business cases.

1. The Impact Ranges shown above are estimations derived from the analysis of benchmark data which is a composite of data derived from industry analyst published information, interviews with subject matter experts and experiential data from prior projective analyses.

2. The Average Resource column shows resource values representative of those used in business case analyses by the CA Business Value Analytics Team.

3. The Projected Savings may be representative results for organizations whose Average Resource values are similar to those in this table. Labor rates for all FTEs are assumed to be \$45/hour or \$80/hour depending on required skills. The average cash value of Loyalty points program accounts is \$100.00. Actual calculations may include additional parameters. Your CA Technologies representative can provide detailed benefit calculations for values in this column.



Please note, the values expressed in this table 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 solution.