Authentication Strategy: Balancing Security and Convenience
Today’s Identity and Access Security Strategies Are Being Driven by Two Critical Imperatives:

**Enable business growth** by:
- Quickly deploying new online services
- Leveraging new advances in cloud computing and virtualization
- Accommodating the needs of a variety of demanding, tech-savvy users
- Driving greater employee productivity and increasing business intelligence

**Protect the business** by:
- Mitigating the risk of fraud, breaches, insider threats and improper access – from both internal and external sources
- Safeguarding critical systems, applications and data

Ultimately, these goals serve a specific purpose: securely enable online business.

With online applications and services driving the market – and providing a key competitive differentiator – organizations are under mounting pressure to remain agile and accelerate the delivery of web-enabled capabilities. But at the same time, they must ensure that new online offerings are supported by security measures capable of effectively protecting personal information – plus critical business data – without impeding the user experience.
Mobility Presents Additional Considerations

The rapid proliferation of mobile devices has created additional security requirements for any organization attempting to increase its presence in the online market. And because smartphones and tablets afford end users a variety of new ways to interact with the enterprise, IT needs to evolve the security measures designed to protect online applications and services accordingly.

These challenges will only increase as the mobility trend gains even more momentum.

“Business spending on mobile projects will GROW 100% by 2015.”

“In 2016, 350 million employees will use SMARTPHONES — 200 million will bring their own.”

New Trends Are Reshaping the Security Landscape

Before the rise of online applications and services, not to mention the ubiquity of smartphones and tablets, security was a relatively simple process:

Enterprise applications were contained within a network firewall, access was limited to internal employees and it was easy to manage identities and understand the context of a user’s actions.

But as online interactions expand to include customers, mobile users and business partners – as well as on-premise and cloud-based applications – the traditional network perimeter has become less and less effective.

Essentially, the concept of the firewall – and the idea that most interactions occur inside the network – is no longer valid. As a result, IT’s long-held ideas about how to manage security must change.

But how? If IT security teams can no longer rely on the network perimeter as an adequate means of securing the enterprise, where can they turn?

The answer lies in intensifying the focus on users and confirming their identities before access is granted.
As identity becomes the driving force behind new security paradigms, IT must respond by placing a stronger emphasis than ever before on authentication – the process of ensuring that users truly are who they say they are.

To this end, businesses should account for three crucial factors when planning their authentication strategies:

**Security**

More applications, users and devices mean no one-size-fits-all approach will be sufficient, so developing a secure, centralized way to provide layered, risk-appropriate authentication is imperative.

**User Experience**

A simple, yet secure, authentication process is essential to preserving the user experience – and can be a key differentiator for driving adoption of customer-facing, web-based applications.

**Cost Control**

A flexible, efficient and centralized authentication solution can help reduce IT costs – from initial deployment through ongoing maintenance and support.

Additionally, a key point IT should consider is the fact that today’s complex and evolving online environment emphasizes the need to review both current and future authentication needs and develop strategies that can cover a broad spectrum of predictable user groups and use cases.
Authentication Methods Must Reflect Today’s Security and Access Requirements

In the past, most IT departments employed authentication approaches that asked the majority of individuals to provide nothing more than a valid user ID and password – and only a small set of executives were required to offer additional, “stronger” credentials when they needed to access highly sensitive resources.

But given the recent trend of hackers and other malicious entities targeting common users and their basic passwords as an entry point for advanced persistent attacks, organizations must strengthen their authentication methods for all employee, partner and customer profiles – leveraging strategies that go well beyond the weak user ID-password approach.

As organizations look to expand the use of strong authentication methodologies, it is especially important for them to:

- Enable access to online applications from a variety of devices
- Accommodate unique user groups with different access requirements and privileges
- Provide the appropriate level of security based on the risk of a given activity
- Protect an individual’s identity – and the sensitive data in applications – without placing an undue burden on end users
- Extend authentication capabilities to both cloud-based and on-premise applications
- Safeguard transactions against new threats, such as man-in-the-middle attacks
Advanced Authentication Methods That Scale and Provide a Unique Combination of Security and User Convenience

The complexity of today’s authentication requirements and the evolving threat landscape may leave IT feeling as if there is no way to effectively secure the enterprise.

Fortunately, there are two emerging authentication methods that promise to help organizations protect sensitive information and minimize the risk of breaches and other attacks – while providing a streamlined experience to users of all types: software tokens and risk-based authentication.

### Strong Authentication

**What it Does**

Protects employees and customers with user-convenient, two-factor authentication.

**Advantages**

- Helps reduce the risk of inappropriate risks and attacks
- Offers some of the strongest two-factor authentication software credentials on the market
- Secures data without burdening legitimate end users
- Scales with your organization’s needs

### Risk-based Authentication

**What it Does**

Reduces the risk of improper access and fraud without burdening valid users.

**Advantages**

- Reduces the risk of data breaches and fraud
- Requires step-up authentication for suspicious activities
- Helps meet compliance guidelines such as FFIEC, HIPAA, PCI, and SOX
A common challenge facing many IT organizations today is the process of confirming the legitimacy of the growing population of employees who need to access internal, cloud and partner sites from remote locations via a virtual private network (VPN). Because the typical user ID-password combination is insufficient, and may increase the risk of inappropriate access or fraud, organizations should complement this approach with a two-factor software token. This provides an additional layer of protection against inappropriate access – one that can be implemented in a variety of user-friendly ways.
But if user convenience is a major concern, risk-based authentication provides a transparent and effective way to further validate an employee’s identity – without any additional, inconvenient steps. This gives IT the flexibility to permit low-risk activities, require additional authentication for medium-risk scenarios and either deny access or send an alert to an administrator in the event of a high-risk attempt. In this way, risk-based authentication enables a just-in-time strategy that immediately grants access to the vast majority of users, while requiring additional authentication only when the risk level warrants it.

What’s more, risk-based authentication can be combined with two-factor software tokens to create a powerful, layered approach that maximizes security and minimizes the impact on the user experience.
Advanced Authentication in Action: Customer Access

Simplicity is the key when it comes to authenticating – and, by extension, attracting and retaining – customers. Because almost every individual owns at least one online identity – if not several more – eliminating the requirement to create yet another set of credentials is critical to driving the adoption of web-based services and applications.

Therefore, implementing authentication measures that integrate with widely recognized standards – such as OpenID or OAuth – will allow organizations to seamlessly grant immediate access to consumers who have existing, established credentials. This can dramatically simplify the process of building an initial identity for new users.
Advanced Authentication in Action: Customer Access

And when a critical activity must be executed, further identity validation, risk-based authentication and/or software tokens can be leveraged to provide the added, just-in-time assurance about the individual’s identity – without inconveniencing the end user. Moreover, risk evaluations can be performed multiple times per user session and independent rules and thresholds can be set up for specific activities, providing IT with an ongoing assurance about the validity of consumer transactions.
Where Do You Stand?

The first step in adopting a security strategy built on advanced authentication techniques is to evaluate the ways you’re currently managing user access. Gaining a full understanding of the types of individuals attempting to interact with the business each day – as well as the transactions they typically execute – will help you pinpoint the advanced authentication methods that are right for your organization.

Keep in mind that the evolving security landscape and growing number of user profiles and devices emphasize the importance of a robust, integrated solution capable of supporting a wide array of use cases. This type of strategy eliminates fragmented practices, enables greater control over access management, reduces costs and provides a streamlined, high-quality user experience.
CA Technologies understands the importance of effectively balancing security and the user experience. Our solutions provide the advanced authentication measures needed to secure and enable employee, customer and partner access to resources residing in on-premise and cloud environments.

**CA Advanced Authentication** is a flexible and scalable solution that incorporates both risk-based authentication methods like device identification, geolocation and user activity, as well as, a wide variety of multi-factor, strong authentication credentials. This solution can allow the organization to create the appropriate authentication process for each application or transaction. It can be delivered as on-premise software or as a cloud service and it can protect application access from a wide range of endpoints including all of the popular mobile devices. This comprehensive solution can enable your organization to cost effectively enforce the appropriate method of strong authentication across environments without burdening end users.

**CA Advanced Authentication SaaS** is a versatile authentication service that includes multifactor credentials and risk evaluation to help avoid inappropriate access and fraud. It can help you easily deploy and manage a variety of authentication methods to protect your users without the traditional implementation, infrastructure and maintenance costs.
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.