Why Strong Authentication Is a Must for All Users
Authentication Snapshot

The trends impacting business today—cloud adoption, increased mobility, rise of social media and the increased amount of online data sharing—make the need for strong authentication more important than ever.

The IT department can no longer firmly establish a network perimeter and rely on simple username and password credentials for security. There are more users, more information and more points of entry to safeguard.

With critical data and applications online, strong authentication for every user is essential to protect and enable business.
Evolving Trends, Evolving Threats

Ensuring risk appropriate security across the enterprise means that organizations must understand the importance of strong authentication in the context of major technological trends including:

- **The Explosion in the Number and Type of Users**
  In most organizations the end user base has been extended to include employees, contractors, partners and customers—and IT must carefully consider the full range of use cases, access scenarios and numerous privileges.

- **Social Media**
  Utilizing social identities to facilitate the registration or sign-on process is a popular strategy to increase engagement and simplify the user experience but user-friendly strong authentication methods can be used to compliment this strategy and to protect more sensitive data and transactions.

- **Mobility**
  Laptops, tablets and smartphones allow users to access data anytime from anywhere.

- **The Cloud**
  Increasing reliance on cloud and web services is rendering the notion of a “network perimeter” obsolete.

- **Increasing Threats**
  Fraud, identity theft and targeted attacks on an array of industries are becoming more frequent and sophisticated.

“Most companies (nearly 70%) allow some form of BYOD for smartphones. That figure will continue to grow to more than 80% by 2020.”

A Changing of the Guard

Organizations struggle with an array of security challenges, including:

- Controlling access to Web applications
- Providing security for mobile devices
- Keeping up with the pace of sophisticated data breaches
- Compliance with industry regulations
- Deploying a scalable security solution while controlling costs

Is the era of the password over?

“Even if your password is exposed only in an obscured, ‘hashed’ form, it’s vulnerable to hackers converting it to plain text. This is especially true for weak passwords, although we’ve seen that even relatively strong passwords can be cracked. If a password you use across many sites is exposed in this way, you could see hackers take access of your e-mail, financial accounts, and social networking profiles.”

– Jon Brodkin
The secret to online safety: Lies, random characters, and a password manager
Ars Technica, June 3, 2013
Finding the Weakest Link

You just have to watch the news to see that attacks to online data happen all the time. One problem is that the username/password combination is emerging as the weakest link in the enterprise security chain, as industry experts are seeing:

- A rise in the frequency and sophistication of phishing attacks
- The continued theft and publication of passwords (more than 100 million passwords have been published online as plain or cipher text)
- An increase of password re-use by users

According to an APWG industry advisory, the average uptime of phishing attacks increased approximately 70 percent during the first half of 2013—a strong indicator that hackers continue to target usernames and passwords as vulnerable gaps.

While speed and convenience mean that companies may still find valid uses for the username/password combination, a growing number of organizations will look to emerging authentication methods to strengthen their defenses.

What is “collateral damage?”

In the era of skyrocketing connectivity, limiting the damage caused by stolen usernames and passwords is critical. The average web user maintains 25 accounts with just 6.5 passwords to protect them. And without the proper security protocols, these stolen passwords can be used to compromise dozens of other accounts, as well.

In May 2013, Germany surpassed the United States as the top country hosting phishing-based Trojans and downloaders. This is the first time that Germany has been ranked at the top. The United States returned to the top spot in June 2013.

Read more >>

---

1 Global Phishing Survey: Trends and Domain Name Use in 1H2013, APWG, September 16, 2013
3 Ars Technica, Why passwords have never been weaker—and crackers have never been stronger, August 20, 2012
“Inside the network” and “outside the network” are increasingly irrelevant designations because the network is now everywhere. Today, guarding the weakest link means emphasizing *identity* as the focal point of enterprise security—an approach that has several advantages:

1. The level of authentication is determined and required upfront, even if it’s different than what the application itself requires.
2. IT professionals can authorize which applications each user can use and audit their activity across the range of applications.
3. Identifying which authentication credentials are needed based on risk level helps to block suspicious activity.
4. Detecting and blocking fraudulent activity before it occurs without affecting legitimate users and negatively impacting operational costs is of major importance.
Five Keys to Strong Authentication Success

In addition to a focus on identity, strong authentication should be pervasive, transparent and risk-based. To meet these criteria, organizations are seeking efficient, cost-effective authentication methods that provide users with a frictionless experience.

For success, organizations need to:

1. **Know the full range of users** (employees, contractors, partners, customers) and understand the requirements and access levels of each group

2. **Provide the appropriate level of authentication security** based on the risk of the situation or activity

3. **Protect identity and the sensitive data in related applications** without placing an undue burden on users

4. **Keep in mind** that you may need to protect both cloud-based and on-premise applications

5. **Explore ways to protect transactions** against new threats, such as “man-in-the-middle” attacks

It’s also important for IT to know that:

- **There is no one-size-fits-all approach**: IT needs to carefully assess authentication needs and develop protocols appropriate to the user or situation.

- **More isn’t always better**: A multi-step authentication process may create tighter security but may frustrate the user, resulting in a lost client, for example.
Risk-based Authentication: Striking the Right Balance

Enterprise authentication initiatives are typically guided by three considerations:

- Risk-appropriate Security
- Simple User Experience
- Reduced Costs Admin/Support

The right combination of the above will help organizations lock down sensitive data and also offer users a frictionless experience that will help them interact with information and applications wherever they are.
Risk-based Authentication: Security + Transparency

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

Risk-based authentication can evaluate an array of contextual information by checking a wide range of factors, including:

- Device identification
- Geo-location
- IP address
- Device-based rules

In many ways, risk-based authentication has been evolving in tandem with the IT landscape. It’s more available, more flexible and more powerful. It is also more cost-effective than other strong authentication methods because it bolsters security while being less expensive to deploy.
Risk-based Authentication: A Closer Look

Risk-based authentication is fundamentally different than other credential-based forms of strong authentication. Instead of the user providing information to verify identity, risk-based authentication examines a wide variety of contextual information to verify identity:

Where is the user?
Access location is a vital factor in assessing identity. Risk-based methods use IP addresses to judge whether the user is accessing data from a suspicious location or if the log-in device is inconsistent with the connection being used to gain access.

Which system or device is being used?
Risk-based authentication also recognizes device type and use. If the user is attempting to gain access with an unrecognizable device or one that has not been previously used, the system will elevate the risk score.

What is the user trying to do?
Risk-based authentication also gauges each particular user request. IT can set rules around various user actions (for example, accessing a specific database) to better protect sensitive data from attack. If a user’s request is unusual or triggers a particular rule, the system can deny access and flag the interaction for investigation.

Is the behavior consistent?
User behavior is also a factor. A high frequency of log-ins, attempts to access large amounts of data or other inconsistent user behavior will affect how the authentication system handles the request for access.
Risk-based Authentication: Advantages at a Glance

Risk-based authentication solutions often strike the right balance for security, user experience and cost.

**User Friendly**
Risk-based authentication works in the background, and users won’t need to go through additional steps to verify identity.

**Simple to Deploy**
Because they live on the server-side system, risk-based authentication solutions are easy to deploy and don’t require a client on a mobile phone, tablet or computer.

**Flexible**
These solutions can be adapted to meet the current needs and risk tolerances of the organization. They can also be easily adjusted to address evolving cyber threats.

**Multichannel Support**
Risk-based authentication methods can be customized for a variety of interaction channels, such as mobile or web.

**Rules and Behavior Modeling**
With risk-based authentication, IT can implement rules to address different user profiles and user behavior.

**Device Agnostic**
These solutions protect access and transactions from a wide variety of devices and operating systems, including tablets, mobile phones, and PCs.

**Cost-effective**
Risk-based authentication methods are often less expensive than traditional hardware token-based methods.

Out-of-band, two-factor authentication

When step-up authentication is required because of elevated risk (such as a user trying to login from an unrecognized laptop), a one-time password can be sent out-of-band to their phone (by SMS, email or voice) to help verify identity and reduce the risk of fraud.
Risk-based Authentication: Assessing Risk

Implementing the right level of strong authentication calls for a careful assessment of risk across the entire spectrum of users and user activity. Organizations must consider:

- What is the user population?
- What is the user’s location when accessing information/applications?
- What devices will the user be using?
- What type of data is included?
- What types of activities/transactions are possible?
Strong Authentication Solutions from CA Technologies

CA Advanced Authentication is a flexible and scalable solution that incorporates both risk-based authentication methods like device identification, geo-location and user activity, and a wide variety of multi-factor, strong authentication credentials.

The CA Advanced Authentication solution, which includes CA Strong Authentication and CA Risk Authentication, allows organizations 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 popular mobile devices. CA Advanced Authentication helps organizations to cost effectively enforce the appropriate method of strong authentication across environments without burdening end users.
For more information on strong authentication solutions from CA Technologies, visit ca.com/securecenter.