SECUREAUTH

White Paper

Advanced Authentication and Access Control:

A Guide to Selecting the Best Solution for Your Enterprise

October 2015

TechTarget Custom Media
A TECHTARGET WHITE PAPER

Authentication and Access Control: The Critical Criteria

When you evaluate advanced authentication and access control solutions, it is easy to get lost in the details. But before you create a long feature checklist, it pays to identify the high-level issues that will have the most impact on your organization.

This short guide outlines four categories of critical selection criteria for authentication and access control solutions. Products that meet these criteria are most likely to provide you with the optimal combination of better security, ready user acceptance, and low cost of ownership.

Table of Centents

Criterion #1: Comprehensive Security in One Solution

1a. Integrated Access Control Solutions

You may have noticed an industry trend to converge authentication, access control and single sign-on (SSO) products into an integrated product line, or even into a single solution.

The logic driving this trend is compelling. End users are much more likely to accept a unified user experience, rather than multiple products with different user interfaces and authentication processes. Administrators spend less time installing and managing a single solution. Policies can be configured in one place and enforced consistently. In addition, you don't have to worry about integrating separate products with each other and with your infrastructure.

You should look for solutions that combine

1. Two-factor (or multiple-factor) authentication
2. Adaptive authentication
3. Federated SSO
4. Password reset
5. Certificate management

1b. Coverage of Multiple Environments

End users now expect to have a consistent experience and use one set of credentials across all types of applications and environments. Administrators want to avoid managing multiple products in parallel technology silos.

Look for comprehensive solutions that provide consistent authentication and access control across:

- On-premises applications
- Applications in the cloud
- Mobile applications
- Applications accessed over VPN connections

Integrated in Name Only?

Some solutions that claim to be integrated really aren't. Clues of nominal "check the box" integration include:

- Products or modules sold separately
- Modules acquired from different companies or maintained by separate development groups
- Very few customers using the entire solution (which you can test by asking a vendor for customer references)

Criterion #2: Satisfying End-User Experiences

2a. Convenient Two-Factor Authentication

User acceptance is critical to the success of any access control technology. No matter how great the security justification of a project, it will fail if users have to work too hard. Older forms of two-factor authentication involving smart cards and key fobs gained reputations for being inconvenient, particularly because it was so easy to forget or lose the small item.

You can still use smart cards and key fobs, but look for advanced two-factor authentication solutions that support innovative alternatives such as:

- One time passwords (OTPs) sent to mobile phones in texts, SMS messages or automated voice calls.
- OTPs sent in email messages to laptops, tablets or smartphones.
- Sign-ins from social network applications such as Facebook, Google and LinkedIn.

- Making the mobile device or laptop itself the second factor through a "fingerprint" (its unique profile based on data such as chip type, operating system, browser level, and time zone setting).

2b. Adaptive Authentication: Minimum Appropriate Friction

Adaptive authentication techniques make authentication "frictionless" whenever possible, low-friction when appropriate, and demanding when necessary. A suitable authentication method is determined in real time based on risk factors related to an access request.

For example, a user inside a physically secured facility could be authenticated transparently, without requiring even a password. A user on a known device in a known location might need only a password. A user connecting from a new location might be asked to answer a personal question or use two-factor authentication. But a request coming from an unknown device at a suspicious IP address, requesting access to a resource not normally touched by that user, could be presented with multiple authentication tasks or simply denied access to the requested resource or to the entire network.

You should consider adaptive authentication an essential criterion for any authentication and access control solution, because it balances convenient end-user experiences with rigorous security. It also substantially reduces the ability of attackers to abuse stolen end-user credentials, a major element of the most damaging advanced targeted attacks.

2c. Support for Established Access Processes

In most enterprises, users have deeply rooted expectations about the access control process for each application. These processes may differ widely from one application to the next, and even between different users of the same application.

The ability to replicate these access processes helps enterprises achieve user buy-in (or at least user indifference) during the initial implementation of an authentication and access control solution. It also allows them to evolve toward additional sophistication and consistency across applications over time.

Look for solutions that support a wide range of authentication methods and tools. Verify that each solution allows you to replicate your existing authentication workflows. You should be able to replicate sequences of authentication tasks, and also exception logic that changes the sequences for specific users such as system administrators and top executives.

2d. User Self-Service Tools

User self-service tools such as password reset, user enrollment and account lock are critical for minimizing end-user frustration, as well as for controlling help desk costs.

Look for user self-service capabilities that are fully integrated with authentication and SSO features, and that can leverage two-factor and adaptive authentication. This integration ensures that resets can be handled smoothly in ways that dramatically improve user productivity and satisfaction while maintaining very strong security.

Criterion #3: Integration With Your Existing Infrastructure

3a. Out-of-the-Box Integration With Infrastructure and Management Tools

An authentication and access control solution that works with the infrastructure products and management tools in your environment will save you time and money. Not only will it eliminate the need for time-consuming and costly integration work, it will reduce the chances for inconsistencies and errors that could lead to security vulnerabilities.

Look for Out-of-the-Box Integration With...

- Enterprise directories and databases
- Multiple two-factor authentication solutions
- Internal web servers
- VPN and WAN acceleration products
- Legacy SSO solutions
- Federation services such as SAML
- SaaS applications such as Office 365 and Google Apps
- Mobile applications and platforms

3b. Support for Standards

Standards ensure that authentication and access control solutions will work with more tools and applications today and in the future. Verify that solutions support standards such as SAML, WS-Fed/WS-Trust, OpenID, OpenID Connect, OAuth and Forms Based Authentication (FBA).

Criterion #4: Easy Implementation and Management

4a. Rapid Customization of Workflows and Processes

Every enterprise has unique business requirements that dictate how authentication should be managed and how access to specific applications should be provided. When adaptive authentication is employed, it is also necessary to create workflows that "branch" so they can appropriately handle low, medium and high-risk logon events.

Look for solutions that let you customize workflows to match your unique business requirements. For example, it should be easy to have varying authentication steps based on both the user requesting access and the application being accessed. The tool should be able to handle a multitude of different workflows out of the box.

You should also focus on the ability to improve back-end processes, such as password resets, self-service enrollment, profile updates, and automated help desk functions for lost passwords and for second factor capabilities. This ability will help you automate time-consuming tasks typically performed manually by the help desk and support staff.

There are very substantial differences between authentication and access control solutions in ease of implementation. Some products feature an architecture and tools that allow the solution to be onboarded in days or weeks without disrupting existing operations. Others can require months of intensive work to achieve the same goal.

4b. Rapid Integration With Non-Federated Applications

SSO modules typically work out of the box with applications that support SAML and other authentication and authorization standards. However, there are plenty of commercial and home-grown applications that don't. Look for solutions that have tools for integrating with these applications

"I'm confident with the high level of security, control and scalability with SecureAuth IdP. I am also pleased with the best-in-class service and support we've received from the SecureAuth team."

Todd Holloway, Senior Manager of Information Security, Marvell Semicondcutor

Bonus Criterion: Top-Notch Customer Support

Customer support by vendors is a subjective selection, but it can be critical. Excellent customer support and efficient professional services increase the likelihood of a short, smooth implementation and a high ROI over time.

Request customer references from vendors. Ask the contacts about the vendor's support team in areas like professional experience, project management, and dedication to customer success.

SecureAuth IdP

When you are evaluating alternatives for advanced authentication and access control, be sure to take a look at SecureAuth IdP, a solution that:

- Provides multi-factor authentication, SSO, user self-service and certificate management in a single solution.
- Helps protect on-premises applications, applications in the cloud, mobile applications, and critical VPN connections.
- Supports over 20 authentication methods, including convenient two-factor authentication methods and advanced adaptive authentication techniques.
- Makes it easy to support unique access workflows.
- Delivers out-of-the-box integration with a wide variety of applications and infrastructure products.
- Supports all of the major IAM and federated identity standards.
- Features an architecture and tools that allow it to be integrated with some of the world's most complex production environments in weeks, not months.
- Offers some of the industry's best customer support and professional services (ask our customers).

Take a Look at SecureAuth IdP

Learn more about SecureAuth IdP, an advanced authentication and access control solution, by visiting http://www.secureauth.com and requesting a demo with one of our solution engineers.

SECUREAUTH

8965 Research Drive | Irvine, CA 92618

p: 1-949-777-6959 | f: 1-949-743-5833 | **secureauth.com**