SECUREAUTH

SecureAuth IdP

Adaptive Access Control

Authentication – Single Sign-On – Self-Service

Determine Your Identities with Confidence

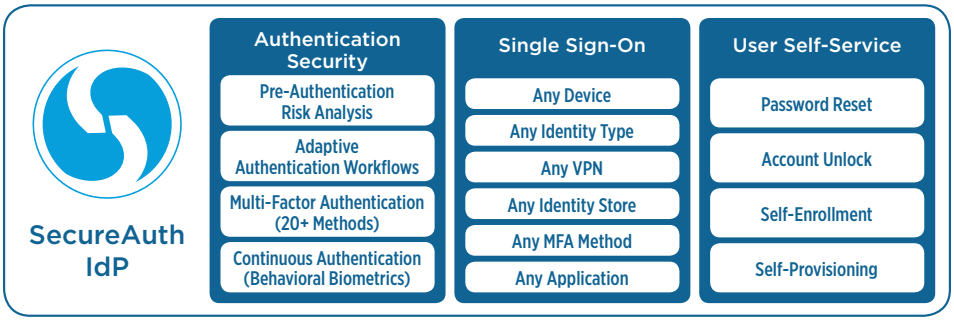
The proliferation of user access devices (home & work PCs, tablets, smartphones) and cloud and mobile applications has created more access points — and corresponding security vulnerabilities — than ever before. You may have spent millions on endpoint and network security, yet breaches continue. Why? The fact is, the most common attack method now is compromised valid user credentials. Therefore, securing identities has become today's security perimeter. In this new reality, authentication systems limited to ID and password or even two factors are no longer sufficient for protecting your applications and data while delivering a frictionless user experience.

Benefits

+ Pre-authentication risk analysis increases security without impacting users.
+ The authentication process can easily be tailored to different types of users (admins versus sales reps; employees versus partners).
+ Continuous behavioral biometric verification extends protection beyond the authentication process.
+ Adaptive and multi-factor authentication protects legacy resources.
+ Enterprise-wide SSO can include any device, ID type, ID store, VPN, and application.
+ Standards-based architecture & connectors complement existing security investments.
+ Self-service password reset and account unlock maintain productivity and reduce help desk calls.
+ Activity and utilization logs simplify compliance.

A Single Solution for the New Security Frontier

SecureAuth IdP is just what the name implies: an identity provider and a unique approach to securing user access. With control of the device, application, and even the infrastructure moving out of the datacenter, an IdP is the perfect solution for maintaining secure control of user access to your resources and data, whether on-premises, in the cloud, via mobile applications, or through VPN. SecureAuth IdP provides authentication security (multi-factor and adaptive authentication), single sign-on (SSO), and user self-service tools, unified in a single product that is unmatched by other vendors. In short, SecureAuth IdP enables strong identity security with minimal user interruption.



"We're able to eliminate smartcards and, over a year and a half period, we were able to eliminate soft FOB and hard FOB usage."

— Chris Joerg, Director, Global Information Security, Unisys

Visit www.secureauth.com/unisys to hear Unysis describe their use of SecureAuth IdP

Authentication Security

Increase Security without Impacting Users

Pre-Authentication Risk Analysis

Streamline legitimate logons while blocking attackers. Pre-authentication risk analysis (adaptive authentication) looks at multiple risk factors to determine the legitimacy of each user identity. If — and only if — sufficient risks are present, IdP requires multi-factor authentication.

SecureAuth offers more risk factors than any other vendor:

+ SecureAuth Threat Service
+ Device recognition
+ Geo-location
+ Geo-velocity
+ Directory lookup
+ Behavioral biometrics

Adaptive Authentication Workflows

Tailor the authentication workflow to the associated risk. For example, SecureAuth IdP can apply more scrutiny to the authentication of users with access to sensitive applications and data, such as administrators and finance staff, than to marketing people.

Multi-Factor Authentication

Passwords alone are no longer enough to protect your critical resources and data. With multi-factor authentication, you can combine something a user knows (username and password) with something the user has (phone, email, token, etc.) to ensure that access is granted securely and appropriately. SecureAuth IdP supports 20+ authentication methods — SMS, telephony, email one-time passwords (OTPs), push-to-accept, USB keys, and more — so users don't need a new gadget; they can use things they already carry every day.

Continuous Authentication

Most authentication solutions consider their job done once authentication happens. SecureAuth IdP uses behavior biometrics to continually monitor users and devices for inconsistencies, delivering a far deeper level of protection. It builds a unique profile of each user's unique rhythm of keystroke dynamics and mouse movements on each device they use, and analyzes this profile each time the user logs in and every time the device is used throughout the day. If someone other than the owner of a given device tries to use it, they will be prompted for multi-factor authentication. This critical additional security is not offered by any other vendor as of the writing of this document.

Single Sign-On

The number of passwords users have to manage grows daily, putting security at risk. SecureAuth IdP enables you to give each user a single set of credentials to remember and manage, streamlining secure access to on-premises, mobile, cloud, VPN, and legacy resources while eliminating stored, passed or synced credentials. If the identity is compromised, continuous authentication helps ensure the attacker will be challenged with multi-factor authentication and stopped.

Self Service

You can't afford to tie up your help desk with a never-ending stream of requests to reset password or unlock account, or to idle valuable employees while they wait for access to the resources they need to do their jobs. With SecureAuth IdP, you can enable your users to securely reset their own passwords and unlock their own accounts at any time without assistance from the help desk. The process takes less than a minute, ensuring high productivity while slashing overhead costs. Users can even self-enroll for multi-factor authentication.

The SecurePath to Strong Access Control