SecureAuth IdP
Adaptive Access Control

Authentication | Single Sign-On | Self-Service
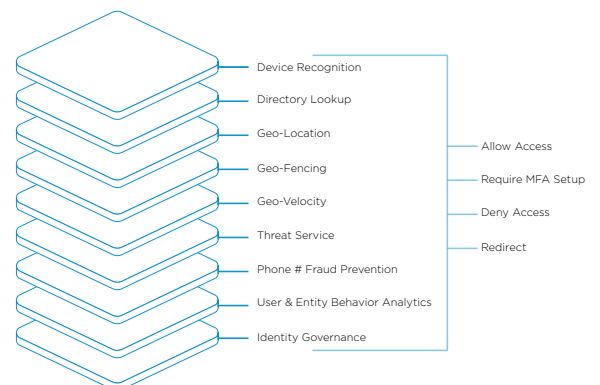
SECUREAUTH + CORE SECURITY

Benefits

+ **Increase security without impacting users** with pre-authentication risk analysis.

+ **Easily tailor authentication process** to different user types with flexible workflows.

+ **Maintain productivity and reduce help desk calls** with user self-service password reset and account unlock.

+ **Improve user convenience** and protect against password fatigue with single sign-on.

+ **Progress secure access** with flexibility and choice among 25+ multi-factor authentication methods.

+ **Optimize, rather than replace,** existing security investments. With our standards-based architecture, we just fit it.

+ **Empower user to go *Passwordless*** with high identity confidence.

+ **Easily deploy enterprise-wide** and eliminate the cost and complexity of multiple disparate security solutions.

+ **Correlate identity threats and data** with SIEMs and other security systems for more holistic and orchestrated protection.

Prevent the Misuse of Stolen Credentials

Worldwide security spends increased in 2016 7.5% to ~$73 billion, yet breaches increased 40% over the same time period. On average, organizations protect a little over half their resources with multi-factor authentication (MFA), meaning a little less than half are protected with password at best. According to the 2016 Verizon Data Breach Investigations Report, 63% of reported breaches involved the use of weak or stolen credentials. Attackers are simply walking in the front door. Identity has fast become the security vulnerability at most organizations, yet you only spend ~7% of the security budget on it. MFA is not the end all be all answer either, with cyber attackers getting innovative and able to defeat many MFA methods. With breaches costing the average US organization $4 million per, it's time to protect your identities and better secure the access control gap.

Adaptive Authentication
Invisible Security - Pre-Authentication Risk Analysis

SecureAuth + Core Security provides multiple silent risk checks without users even knowing and evaluates the credentials and innovative ways to defeat MFA methods. "riskiness" of every access request. This adaptive authentication enables you to allow access for low risk requests without a MFA step, require MFA for medium risk and deny or redirect for high risk — delivering the most user-friendly authentication experience while stopping attackers cold, even if they have stolen credentials and innovative ways to defeat some MFA methods.

Device Recognition
Directory Lookup
Geo-Location
Geo-Fencing
Geo-Velocity
Threat Service
Phone # Fraud Prevention
User & Entity Behavior Analytics
Identity Governance

Allow Access
Require MFA Setup
Deny Access
Redirect

"The end users love the new system. When they're on premise, they don't even have to be prompted for their credentials, however if they take that same device off network, they're automatically prompted for credentials. It's really a nice solution and a lot of time people don't even realize they are using it"
- Matt Johnson, Manager, Server Engineering, Houston Methodist Hospital

Customize Authentication Workflows

We don't believe in a one size fits all approach and delivery infinite number of different workflows. Different workflows can be in-house developed for a particular user, group of users, or specific applications. 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 and sales people.

Eliminate Passwords from Authentication

A user name, fingerprint print scan and a phone click and users are authorized. Passwordless authentication using fingerprints, layered risk checks, and convenient Push-to-Accept MFA method, provides stronger authentication and greater confidence than passwords. Users will love that they no longer have to remember, change, and enter passwords. Imagine the helpdesk call reduction.
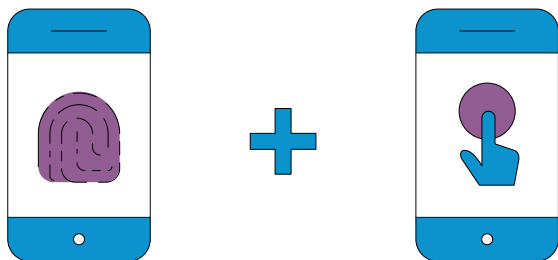
Multi-Factor Authentication

With 25+ authentication methods ranging from SMS to telephony to email to push notification and more, SecureAuth adapts to your preferences and provides maximum choice. We have multiple methods that utilize things users already carry around or use daily. What's more, our multi-factor authentication deploys right into your infrastructure, tying to your enterprise directories, web servers, VPNs, on-premises, cloud, and even your homegrown applications.

Data Sharing for More Holistic Protection

Focusing on security alerts that matter saves time and resources. It's even better to correlate data from multiple sources to get a clearer picture of real threats vs false alarms. We not only display key data in a clean dashboard, we have pre-built integrations with major SIEMs so anomalies can be correlated among identity, network, and endpoint threat data.

Enhanced Convenience with Single Sign-On

The number of passwords users have to manage grows daily, putting security at risk. SecureAuth 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, adaptive authentication helps ensure the attacker will be challenged with multi-factor authentication and/or denied access. Time savings with Single Sign-On and Passwordless Authentication can be significant.
Calculate your savings with our online calculator - www2.secureauth.com/SSO_Calculator

Reduce IT Workload with User Self Service

You can't afford to tie up your help desk with a never-ending stream of requests to reset passwords and unlock accounts, or to idle valuable employees while they wait for access to the resources they need to do their jobs. With SecureAuth, 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. Users can even self-enroll for initial multi-factor authentication. The process takes less than a minute, ensuring high productivity while slashing overhead costs.

Step 1. Calculate Number of Help Desk Calls

Total Number of Employees:

5,000
(Editable Field)

Average Number of Help Desk Calls Per Employee, Per Year:

12
(Editable Field: META Group estimates 1.75 calls/month or 21/year per user)

Average Number of Help Desk Calls Per Year:
60,000

Step 2. Calculate Number of Password Reset Calls

Percentage of Help Desk Password Reset Calls:

30 %
(Editable Field: Gartner estimates 20-50% of all calls are for password resets)

Total Number of Password Reset Calls Per Year:
18,000

Step 3. Estimated Cost Per Password Reset Call

$ 35.00
(Editable Field: Cost estimates typically fall between $15-$70 per call)

Annual Password Reset Call Cost Savings: $630,000

Calculate your savings with our online calculator - www2.secureauth.com/Password_Calculator