SECUREAUTH

RELEASE FOCUS —

SECUREAUTH IDP 9.3

Machine Learning & High-Risk Account Analysis to Improve Access Control & Making Administration More Efficient

Key Enhancements At-a-Glance

+ Advanced adaptive authentication powered by machine learning
+ High-risk account analysis
+ New cloud-based architecture
+ Reusable directory integration objects
+ Application on-boarding & template library

Key Enhancements Details

Behavioral analysis powered by machine learning

Breaches rose again 44% last year[1] despite a global spend nearing 100B[2]. We know passwords are no longer enough, but now we're seeing serious evidence that attackers are bypassing multi-factor authentication[3]. Advanced adaptive authentication powered by machine learning can supplement your access control strategy by monitoring user behavior for suspicious activity. Baselining normal user behavior over time and analyzing for deviations can unmask attackers masquerading as legitimate users and uncover hard to detect insider threats.

Machine learning examples

SecureAuth IdP 9.3 analyzes the following authentication behaviors. Changes in these behaviors can provide fine grained signals that risk is present.

+ **Unusual Time of Day**
+ **Unusual Day of Week**
+ **New or Rarely Used IP Address**
+ **New or Rarely Visited Country**
+ **Change in login success frequency**
+ **Change in login failure frequency**
+ **Increase in application login activity**
+ **Decrease in application login activity**

John always logs in between 7-9am and logs out between 4-6pm every day.

Why has he recently been regularly accessing systems outside those times?

For others, this might not be a big deal, but for John, compared to previous months/years, it causes some concern. Forcing an MFA step or password reset could help verify if John is really John.

Tom rarely fails authentication attempts, and boasts a 98% success rate.

Why recently has he failed more authentication attempts than he's passed?

For users that are more forgetful this could be explained. Tom rarely fails an authentication attempt. Based on his typical behavior, it is reasonable to assume an attacker has gotten ahold of Tom credentials and is attempting to brute force access. In this case, we might deny Tom's access until further investigation, or force a secure password reset.

High-risk account analysis

To improve identity-related breach protection, we have unveiled high-risk account analysis, which enables higher than normal authentication requirements for sensitive and privileged access and identifies and responds to segregation of duty violations. Attackers seek out accounts with the access needed to reach their objective, often assuming or creating the identities of those with elevated access. SecureAuth gives you the ability to identify these accounts, as well as violations of segregation of duties rules, and require owners to pass more risk checks and authentication steps than normal users. This is a great example of merging identity and security data to improve authentication and prevent identity-related breaches.

[1] https://www.idtheftcenter.org/2017-data-breaches/

[2] Gartner - https://www.gartner.com/newsroom/id/3836563

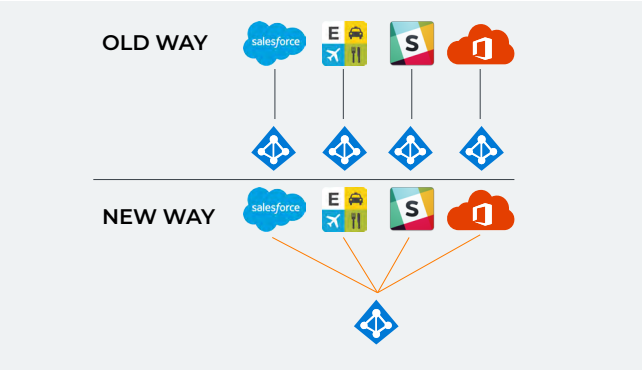
[3] Identity 101: Why two-factor authentication is not enough - https://www.ibtimes.co.uk/identity-101-why-two-factor-authentication-not-enough-1665422

New cloud-based architecture

With the move to a cloud-based architecture, your administrators can get the most up-to-date settings, features, and enhancements without undergoing time-consuming upgrades. **Save your organization: Time and labor costs**

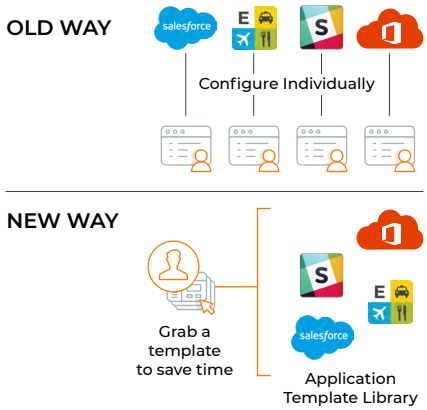
Reusable directory integration objects

Instead of going through the time-consuming process of integrating to your directory every time a new application or system is deployed, administrators can now build much fewer directory integrations and reuse them without having to build new for each system. When changes need to be made, they are made once and propagated through your environment automatically. **Save your organization: Time while increasing process efficiency.**



Application on-boarding and template library

The application on-boarding experience has been streamlined and shortened with the creation of a library of application templates. Instead of building integrations to enable 2FA, Adaptive Authentication, or SSO for each application individually, your administrators can now simply pick the applicable template from the library. For templates not yet built, we can accelerate the process by auto-populating fields. **Save your organization: Time while increasing productivity.**



Additional IdP 9.3 Noteworthy Enhancements

Support for Proof Key for Code Exchange (PKCE) standard – The PKCE standard helps prevent man-in-the-middle attacks, or interception of authentication information, between users and systems, via an improved communication protocol. **Save your organization: Budget, time, and hassle, associated with the catastrophic disruption or breach.**

Inline initialization enhancement – Users can now be redirected to a self-service page to update their profile and continue the authentication process. This helps to preserve a good user experience while minimizing administrator and helpdesk involvement. **Save your organization: Time and labor while increasing process efficiency.**

Customizable PIN length – To increase security, administrators can now configure the length of PINs making them longer and more difficult for attackers to guess. Instead of the default 4-digit PIN, administrators can choose a 4, 6, 8, or 10-digit PIN. The longer the pin, the less likely it will be compromised. **Save your organization: Budget, time, and hassle, associated with the catastrophic disruption or breach.**

Inverted user risk score – We can consume 3rd party risk scores for use in evaluating authentication risk, but varying solutions value risk differently. With this release, IdP is able to change the risk score scale to accept scores on varying scales. **Save your organization: Time in converting data, Improve risk evaluation.**

More Information

IdP 9.3 Release notes/Documentation - https://docs.secureauth.com/display/SI
Contact Support to request your IdP 9.3 Virtual Appliance - support@secureauth.com *or* +1.866.859.1526

Visit our **Intersection Community** (customer community) -
Login: https://secureauth.force.com/intersections | Request access: here

Contact Sales or Customer Success departments - https://www.secureauth.com/contact