# RISK-BASED AUTHENTICATION

AUTHTAKE

www.authtake.com

# Introduction

When a system access request is made, the basic authentication information requested from the user in traditional methods consists of a username and password. However, rapidly increasing cyber attacks result in user identity information being easily compromised. Research also reveals that 81% of data breaches occur due to weak or stolen identity information.

So, what is being done to eliminate this risk?

The most commonly preferred security measures are to force applications to connect through the organization's internal network or to increase security measures with IP restrictions. However, with the Covid-19 pandemic and the adaptation to remote work models, this is no longer feasible.

IT managers and experts are working to eliminate or minimize access risks by proving the accuracy of user identities with additional authentication factors. This sometimes results in requiring one or more methods such as SMS, push notifications, emails, calls, or PINs from the end-user. Although traditional and frequently used methods such as SMS, email, and OTP continue to be preferred, they are no longer reliable due to their susceptibility to manipulation. The FIDO WebAuthn method, considered the most reliable method in recent years, is in the process of becoming widespread, thanks to the notification approval process carried out using the built-in biometric authentication on mobile devices. However, the lack of support for this method in some mobile devices still in use is an obstacle to its widespread adoption.

▸ How will we distinguish an unauthorized user who obtains user information and additional verification methods?

▸ Will we continue to subject the authorized user to consecutive verification processes in every access request?

# What is Risk-Based Authentication?

Risk-Based Authentication (RBA) determines real-time threat signals by analyzing the behavior of a user who wants to access a resource or system, and generates a risk score for each access request. If the access request is deemed risky, it can request additional identity information or deny the access request.

The widespread adoption of hybrid work and the consequent rise of phishing attacks are forcing organizations to adopt a Zero Trust strategy. Risk-Based Authentication eliminates unnecessary friction by distinguishing between attacker and trusted users for users.

In summary, RBA analyzes user behavior to determine the risk associated with a given access request and uses that analysis to decide whether to allow or deny access or to request additional authentication factors. This helps organizations to protect against cyber threats while minimizing the inconvenience for authorized users.

## Customize Risk Set

Determine which risk factors will be used for each resource or system access in your organization, and what the weights of these factors will be.

## Eliminate Frictions

When a reliable device, IP address, time, OS, or other risk factors are detected for an access request and the risk score is low, users are exempted from rigorous identity verification processes.

## Increase Security Level

Detect threat signals and request additional identity verification factors in case of potential risk.

# Why Risk-Based Authentication?

Risk-Based Authentication (RBA) determines real-time threat signals by analyzing the behavioral patterns of a user who wants to access a resource or system, and creates a risk score for each access request. If the access request is deemed risky, it may request additional identity information or deny the access request.

The widespread adoption of hybrid work and the consequent increase in phishing attacks require organizations to adopt Zero Trust strategies. Risk-Based Authentication eliminates unnecessary frictions by distinguishing between attacker and trustworthy users.

# What Are The Risk Factors?

Risk-based authentication uses the real-time AuthTake Risk Engine to obtain a holistic view of the context in each access request.

The Risk Engine analyzes the following factors in the background, taking into account previous successful/unsuccessful access requests, without causing any noticeable delay for the end-user:

- IP Addres
- Device Type
- Country
- ISP/VPN/TO
- Applicaiton
- Time
- Login Successful
- Operation System
- Region
- IS Attack IP
- City
- Login Metot
- Browser
- Login Velocity
- Display resolution
- Impossible Location

## Impossible Location

Taking into account all these factors, it analyzes the new access request by considering the Geo Location information of the last successful login and verifies the presence of impossible location information.

To describe it through a scenario; when a user who last accessed from city X in country A makes a new access request 30 minutes after that access, the country and city of the new request are checked.

If there is a difference in the new locations, it analyzes whether there was a possibility to travel between these two locations during the elapsed time (in this example, 30 minutes) and decides based on the result of this analysis.

# Risk Levels

When an access request is received, a Risk Score between 0-100 is generated by analyzing risk factors. Based on this risk score, it is determined which standard risk level it belongs to, and the action/actions that need to be taken are triggered accordingly. Risk Score intervals can be customized according to the levels.

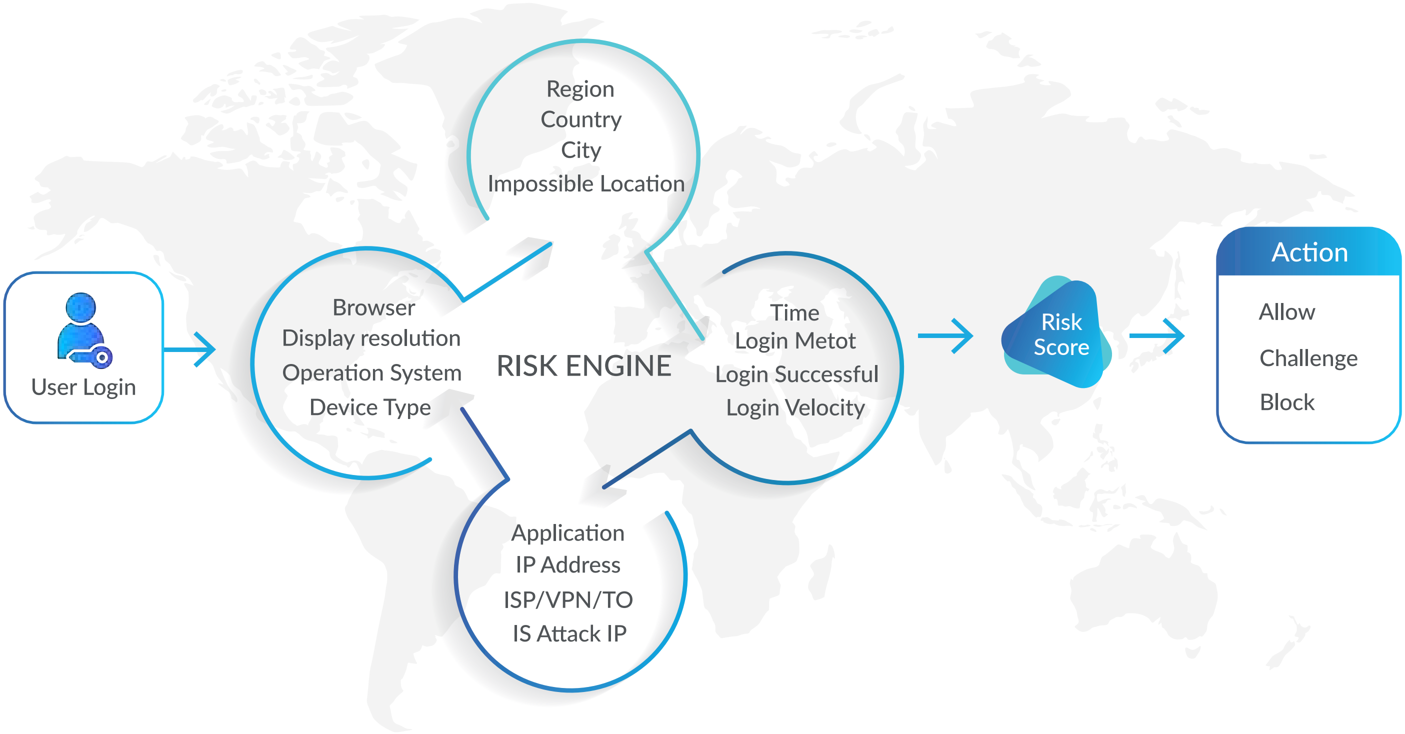
Standard Risk Levels and actions (Customizable):

Low Level: Allow access
Medium Level: Request additional verification
High Level: Request multiple additional verifications or deny access.

# How Does It Work?

When a user attempts to access a system, a risk score is generated through the AuthTake Risk Engine based on predetermined risk factors. The weights of these risk factors vary for each user. Actions are taken based on the resulting risk level determined by the calculated risk score.

Thanks to this approach, security is maximized while minimizing friction for trusted users.



# Why AuthTake?

AuthTake guarantees a highly secure and user-friendly authentication process with FIDO WebAuthn Passwordless Authentication and Risk-Based Authentication.

Unlike competitor solutions, it not only uses basic factors such as IP, Time, OS, and Browser but also hosts the healthiest risk analysis engine by using over 15 risk factors. This allows for overcoming the difficulties encountered in traditional RBA solutions and maintaining user privacy.

In addition, AuthTake allows IT administrators to determine application-based risk factors and assign different risk and security levels for each application.

With Adaptive Authentication, AuthTake enables the ability to define User, Group, Schedule, and other policies, providing users with increased security levels without any noticeable changes.

With its provided SSO solution, it offers the possibility to quickly replace password-based login processes in the majority of your systems with passwordless MFA that is resistant to identity theft, and also speeds up your transition to risk-based authentication.

AUTHTAKE

**Phone:** +90 850 303 7005
**Web:** www.authtake.com
**E-Mail:** info@authake.com
**Address:** Kızılırmak Mh.1443. Cd.
No:25/B - 117 Çankaya/Ankara