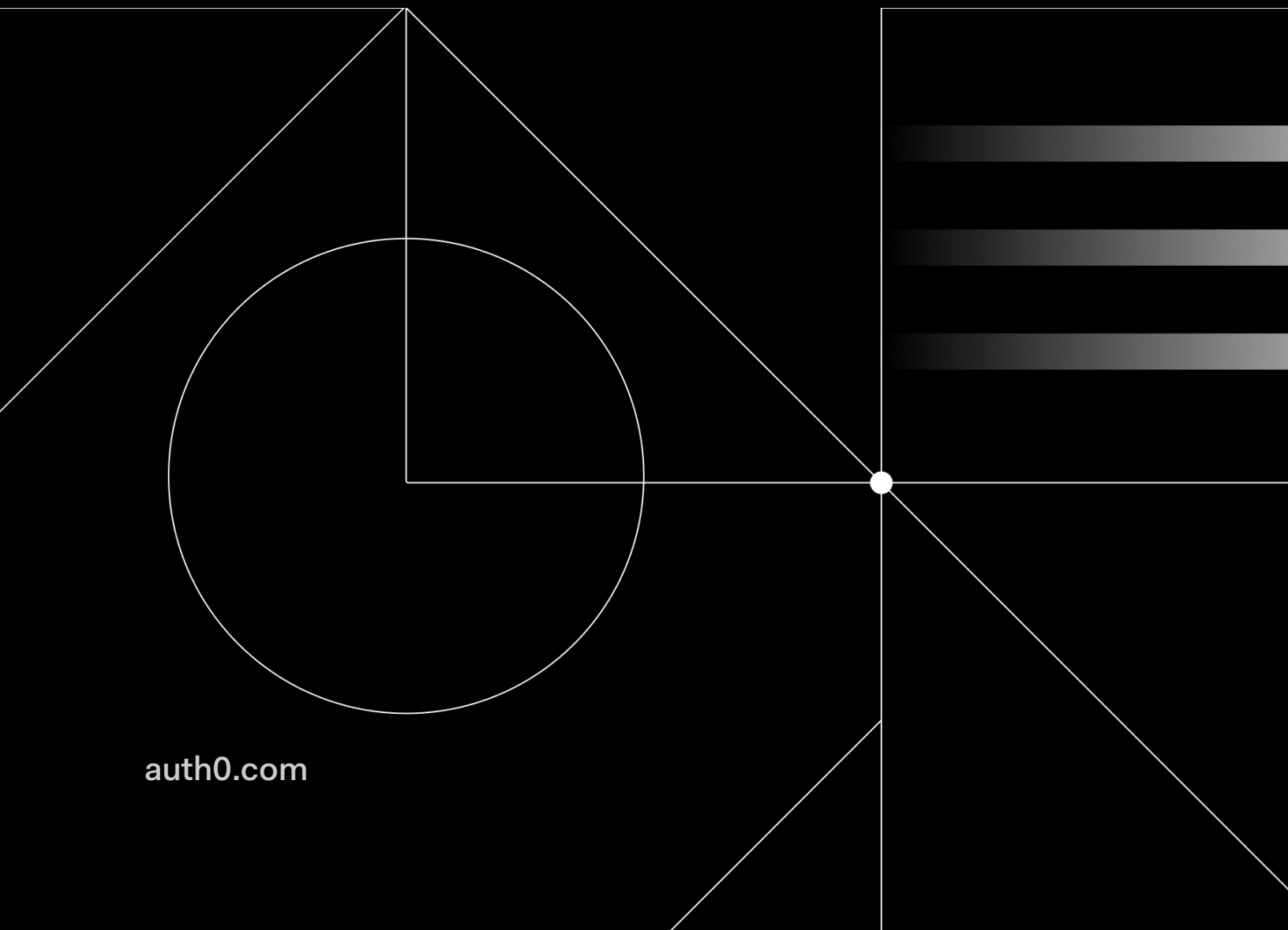
Auth0

# Checklist: Is Your Identity Secure?

## Preventing Broken Authentication



auth0.com

Authentication is a mission-critical component of most applications, making it a high-value target for attackers. According to the Open Web Application Security Project (OWASP), broken authentication, or the improper and insecure implementation of authentication, is the second-most critical web application security risk.

## Use this checklist to determine if your identity is vulnerable.

- **Does your product support MFA?** Multi-factor authentication (MFA) is one of the most effective ways to combat attacks, including credential stuffing and phishing.
- **Are passwords encrypted?** Passwords are critical information and should be encrypted at rest and in transit. Storing passwords in plain text is a major security risk.
- **Are users forced to use strong passwords?** Simple and weak passwords are vulnerable to brute force and dictionary attacks. Enforce password length, complexity, and rotation based on NIST recommendations or other evidence-based policies.
- **Are passwords checked against breached password lists?** Credential stuffing attacks, which rely on users reusing previously breached passwords, are increasing in frequency and sophistication. By automatically checking passwords against lists of breached passwords, you can significantly limit the effectiveness of credential stuffing.
- **Does your product ship with default credentials?** When a product comes with default credentials, especially administrator credentials, many users never change the password. This leaves them vulnerable to attacks.
- **Are all failed login messages the same?** Many threats rely on user enumeration attacks to generate a list of valid usernames. These attacks are made possible when there are different failed login messages for valid and invalid usernames.
- **Is your session management secure?** Use a server-side, secure session manager that generates a new session ID after login. In addition, do not put session IDs in the URL and ensure they are securely stored and invalidated after logout.
- **Is there a limit to failed logins?** Bot-driven attacks, such as credential stuffing, generate thousands of failed logins for every successful one. Locking accounts and blocking IP addresses and devices after a high number of failed login attempts is an effective way to combat these attacks.

## Prevent Broken Authentication with Auth0

Auth0 takes the frustration out of preventing broken authentication. Our identity experts have developed a robust security program designed to ensure our platform is secure and simple to use. Auth0 provides secure login flows, session management, and credential management. You can also use the Auth0 platform with your own identity provider if you want to maintain control over your user credentials.

Here are a few Auth0 capabilities that help secure your valuable data.

### Bot Detection

Bot detection is designed to combat credential stuffing and other forms of bot-driven attacks. It works by correlating a variety of internal and external data sources to identify and mitigate bot-driven attacks before login. When an IP address is deemed suspicious, it is presented with a CAPTCHA on login, which prevents most bot attacks from successfully authenticating.

### Breached Password Detection

A Credential stuffing attacks are a major threat to any web application. These attacks rely on users reusing a password that was previously compromised in another breach. Auth0 keeps a continually updated database of known breached credentials. When a user is detected using breached credentials, admins can choose to warn them but allow the login, deny the login and force a password reset, or trigger MFA.

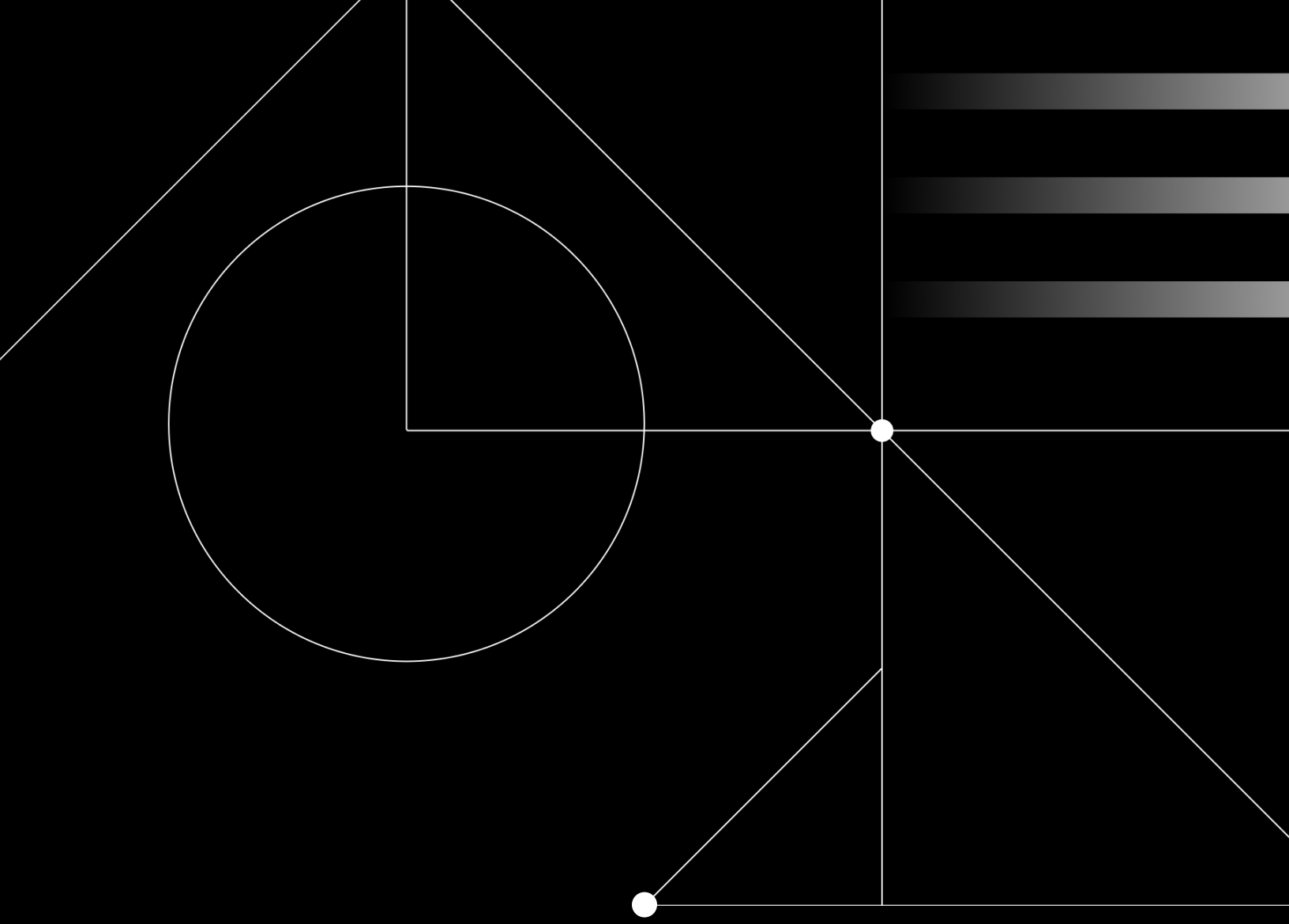
### Guardian MFA

MFA is one of the most effective defenses against an attack. Auth0 Guardian MFA supports a variety of factors, including SMS and push notifications. In addition, Guardian SDKs allow you to embed MFA capabilities into an existing app or whitelabel your own dedicated MFA app. Contextual MFA allows you to trigger MFA only when an IP address is deemed suspicious, ensuring legitimate users rarely have to use MFA to access their accounts.

## Learn More

Broken authentication is one of the most critical and widespread web application security risks. User credentials are considered among the most valuable data an organization has, and poorly implemented authentication places it all at risk.

To learn more about protecting yourself from the risks of broken authentication, reach out to our team.



Auth0

**About Auth0**

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and development teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit www.auth0.com or follow @auth0 on Twitter.