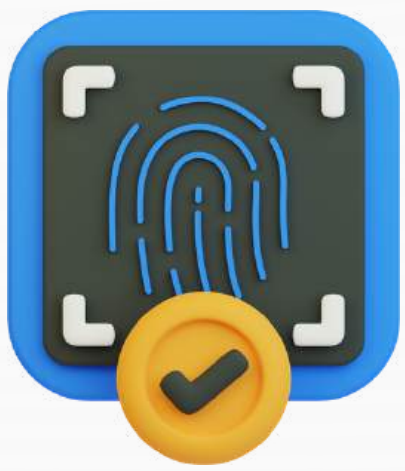
SECUREB4
We Strengthen Your Security

7 Types of Passwordless Authentication



Secureb4.global

SECUREB4
We Strengthen Your Security

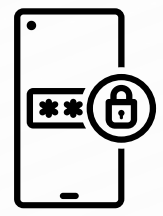
Biometric Authentication

Biometric authentication utilizes an individual's unique physical traits, such as fingerprints, facial recognition, voice recognition, or iris scanning, to verify identity. It provides a high-security level because these characteristics are inherently difficult to replicate.

However, biometric data is sensitive and requires robust protection measures to prevent unauthorized access or misuse. It's essential in environments where security is paramount, and the speed of access is also critical.

SECUREB4
We Strengthen Your Security

One-Time Passwords (OTPs)



OTPs are unique, time-sensitive codes generated by an authentication server and sent to the user's device, typically through an SMS or authentication app. They offer a more secure alternative to static passwords and are commonly used in two-factor authentication systems.

However, OTPs can be vulnerable to interception, particularly if transmitted over unsecured channels, thus necessitating encrypted communication protocols to safeguard them.

SECUREB4
We Strengthen Your Security

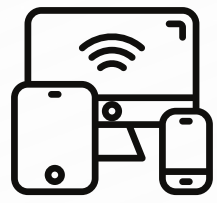
Security Tokens

Security tokens, such as smart cards or USB tokens, store cryptographic keys or digital certificates and are used in conjunction with PIN or biometric data for authentication. The physical nature of tokens adds a layer of security, as possession is required to access the protected resource.

However, the downside is the potential for loss or theft, which could result in unauthorized access if additional safeguards are not in place.

SECUREB4
We Strengthen Your Security

Mobile Device Authentication



This method leverages the user's mobile device for authentication, employing device-based biometrics or unique device identifiers. It's an effective form of security, often used as a component of multi-factor authentication strategies, providing convenience without significantly compromising security.

Mobile devices can implement security measures such as device encryption and remote wipe capabilities to further enhance their role in secure authentication.

SECUREB4
We Strengthen Your Security

Push Notifications

Push notification authentication sends a prompt to a registered mobile device when an attempt is made to access a protected resource.

The user must approve the attempt, adding a layer of user verification to the process. This method is user-friendly and increases security awareness among users by involving them directly in the authentication process for each access attempt.

SECUREB4
We Strengthen Your Security

QR Code Authentication

QR code authentication requires a user to scan a code which then verifies their identity through a secure mobile application. It's a quick and user-friendly method, ideal for scenarios where conventional authentication methods might be less practical.

However, the security of QR code authentication hinges on the secure generation and display of the QR codes. The QR codes should not store sensitive information and must be designed to be single-use to ensure they cannot be reused by an attacker.

SECUREB4
We Strengthen Your Security

Magic Links

Magic links involve sending a unique, one-time-use URL to the user's registered email address. When the user clicks on the link, they are verified and granted access to the resource. This method eliminates the need for users to remember passwords, streamlining the login process.

However, the security of magic links depends on the security of the user's email account; a compromised email can lead to unauthorized access. It's crucial to implement additional security checks, like verifying the user's device or using time constraints on the link's validity, to enhance security.

Our Solutions

SECUREB4
We Strengthen Your Security

- Vulnerabilities Management and Compliance (VM)
- Vulnerabilities Discloser Program (VDP)
- Passwordless Authentication
- Privacy and Consent Management
- Privileged Access Manager (PAM)
- Patch Management
- Open-Source Software Protection
- Integrated Digital Risk Protection (IDRP)
- Identity and Access Management (IDAM)
- Cloud Security Posture Management (CSPM)
- Behaviors based Multifactor authentications
- Age Assurance and Online Safety (AAAOS)
- Continuous Threat Exposure Management (CTEM)
- Cyber Risk and Compliance (Secure Operator)
- Attack Surface Management (ASM)
- Breach and Attack Simulation (BAS)
- Bug Bounty Program (BBP)
- Cloud Security and Compliance
- Continuous Automated Red teaming (CART)
- Data Foresight and VM Foresight
- External Threat Landscape Management (ETLM)
- End-to-End Encryption and Data Protection
- Extend Security Posture Management (XSPM)
- Application Security Posture Management (ASPM)
- Data Security Posture Management (DSPM)

www.secureb4.global
info@secureb4.global

Get in Touch with us.

SECUREB4
We Strengthen Your Security

Have Questions?
We’re Just a Message Away!

Our Phone:

+971 565612349

Our Website:

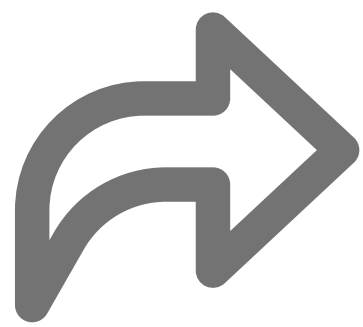
www.secureb4.global

Our Email:

info@secureb4.global

SECUREB4
We Strengthen Your Security

Like 

Share 

Save 

Follow us!