SDG
[technology + passion] – risk

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com

Go Passwordless to Defend Against Security Breaches

Maintaining security through password-based authentication has always been a top challenge for security leaders. In fact, according to the Verizon Breach Investigations Report, compromised credentials are responsible for more than 80% of all breaches. As a result of the COVID-19 pandemic, experts have seen an increase in attacks related to stolen and hacked passwords. Twitter and LinkedIn are some of the most recent victims of these password-centric breaches.

Today more than ever, passwords have become a liability. Ensuring secure password storage, providing technical support, and running helpdesks for password resets all require huge IT spending. Moreover, none of these expenses account for the cost of rectifying a breach after it happens. In light of the potential losses, eliminating password-based authentication systems has become increasingly compelling.

In an attempt to increase security, many organizations are adopting multi-factor authentication (MFA) processes to make static credentials more secure by utilizing OTPs, SMS or hardware tokens. However, these added layers of protection still leave organizations vulnerable to keylogging, phishing attacks, and more. In contrast, passwordless authentication enhances an organization's cybersecurity posture by significantly reducing the overall attack surface and virtually eliminating the risk of credential breaches.

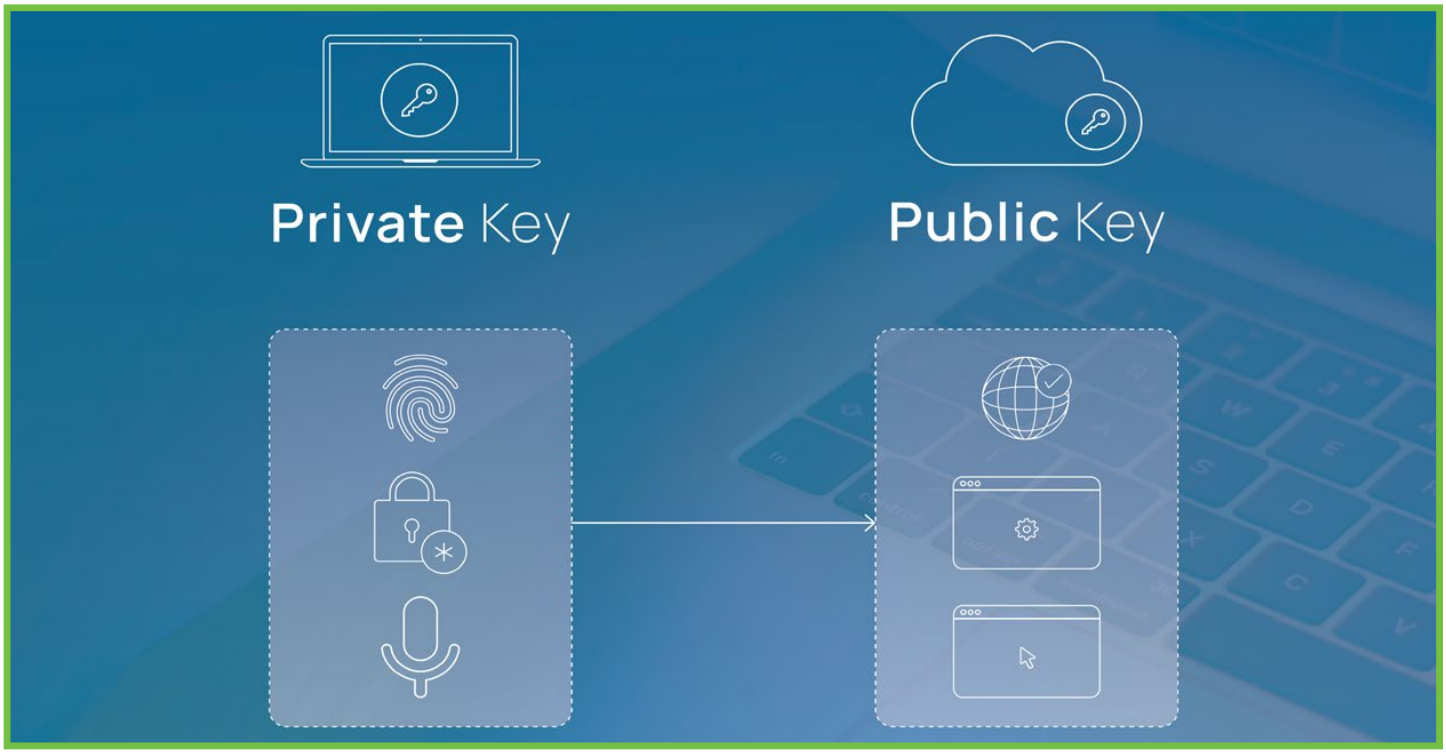
What Is Passwordless Authentication?

As its name suggests, passwordless authentication is a verification method for confirming users' identities without requiring passwords or codes. Instead, user identities are verified using one of two factors:

- **Possession Factors:** "Something a user has," such as an OTP generator, mobile device, smart card, hardware token, etc.
- **Inherence Factors:** "Something a user is," such as a fingerprint, retina, or face/voice recognition.

How Does Passwordless Authentication Work?

The process follows the same principles as digital certificates, involving a cryptographic key pair with a public and a private key. The authentication system of a website, application, or service generates the public key during the user registration process, while the private key is tied to either a possession or inherence factor and stored on the user's device. At the time of authentication, the user is prompted to enter the public identifier (username, email, mobile number, etc.) followed by one of the passwordless factors (OTP, fingerprint, etc.) as secure proof of identity. After the public-private key pair is verified, user access is granted.



By eliminating passwords from the critical authentication process, passwordless solutions can reduce the attack surface. Some of the main breaches they defend against are:

Password Spraying: A commonly used attack method that attempts to log in to several accounts with frequently used password credentials.

Brute Force Attack: An attack where malicious actors use the trial-and-error method to guess login credentials or encryption keys. All possible combinations are tried until the account is hacked.

Spear Phishing: A method of targeting organizations and individuals by executing an email-spoofing attack that tricks users into disclosing sensitive credentials for financial, espionage, or trade gains.

Social Engineering: Attackers use psychological manipulation to scam users into giving away sensitive information or granting access to critical resources.

Shoulder Surfing: A type of data theft where the intruder steals login credentials by peeking over the target's shoulder.

How to Begin Your Journey to Passwordless (Zero Login) Authentication

Benefits of Passwordless Authentication Adoption

Enhanced Security: Many security breaches are a result of phishing, spraying, brute force attacks, shoulder surfing, cracking, etc. By eliminating the use of passwords from authentication processes, organizations reduce these risks significantly.

Improved User Experience: Users no longer need to remember a password, PIN, or passcode to authenticate their identity. This makes the sign-in process easier, resulting in a seamless experience for the end user.

Reduced IT Cost: With no password management and storage required, enterprises can significantly reduce the IT spending necessary to handle password policies, password resets, compliance regulations, infrastructure, and helpdesk responsibilities.

Better Visibility: In the absence of password-based authentication, issues such as phishing, password reuse, password sharing, etc. no longer pose a threat, which means IT teams receive complete visibility over access management.

Passwords are difficult to remember and susceptible to breaches—and as more advanced technology develops, they will become increasingly burdensome. Passwordless authentication provides enhanced security by eliminating authentication vulnerabilities, improving end-user experience, and significantly reducing IT and helpdesk costs. Embark on your digital transformation journey securely by leveraging passwordless authentication to enhance your organization's cybersecurity posture.

[technology + passion] – risk

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

Contact Us: solutions@sdgc.com