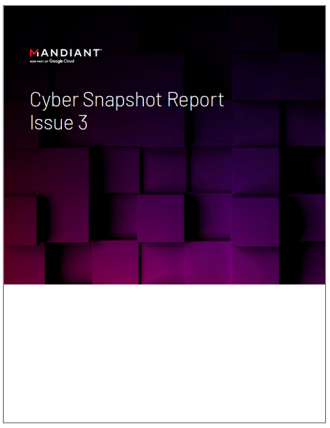
MANDIANT
NOW PART OF Google Cloud

THREAT INTELLIGENCE
WHITE PAPER

The Journey to Passwordless Authentication

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 3.



Historically, challenge-response authentication using a singular password has been one of the primary mechanisms leveraged by organizations to positively verify an identity for authorization. However, following this model of a singular transaction for authentication, without additional identity verification requirements, could create substantial risk to an organization.

As attackers adopted more sophisticated tactics for compromising identities, new controls and methodologies were introduced to help mitigate risk. The most common control that many organizations have adopted is the requirement for multi-factor authentication (MFA), a concept that combines two or more independent methods to positively verify an identity.

Throughout numerous incident response investigations, Mandiant has observed that while organizations increased their adoption of traditional MFA methods, attackers continued to advanced threat tactics to compromise identities using techniques such as:

- **bypassing enforced MFA**
- **abusing weaker MFA methods (e.g., SMS, push notifications, phone calls)**
- **enrolling attacker-controlled devices for MFA verification and authentication**

This elevated threat shifted the focus of aligning MFA adoption to newer tools with stronger MFA methods, such as number matching, contextual telemetry notifications, and inputting time-based one-time passwords (TOTPs). Additionally, vendors and organizations are further enhancing MFA methods by leveraging either Fast Identity Online 2 (FIDO2) keys / tokens, software / hardware Open Authentication (OATH) tokens, or certificate-based authentication.

Authenticators

To further enhance authentication security, the concept of "authenticators" has started to become integrated as part of identity and access management practices for organizations. Authenticators move away from the singular context of a password, and require multiple components to positively verify an identity. Example authenticators can include a multi-context of a username/password combined with strong MFA methods, certificates, device state context, identity risk calculation, or passwordless methods.

When aligning under the concept of "authenticators," the overall risk of a compromised password is greatly reduced as the singular nature of the password is no longer the first and last line of defense for authentication.

What is Passwordless?

Building off strong MFA methods, passwordless authentication is starting to become part of the "authenticator" equation for many organizations. Passwordless is essentially a method of verifying an identity without the requirement for a knowledge-based secret. Instead, the identity authenticates by using something they have (device) or something they are (biometric). Under the premise of passwordless, the requirement for either possession and/or inherence-based factors increases security by removing the requirement for a "something you know" (password) factor being part of the authentication equation.

Practical and scalable methods of leveraging passwordless authentication can include:

- **Mobile Authenticator Applications** – which can either generate a one-time passcode (OTP) (based upon a synchronized algorithm) or can be used to approve or match a number sequence that is displayed to a user.
- **FIDO2 Hardware Tokens and Keys** – which can interface with a device using either a physical connection, Bluetooth, or near field communication (NFC). With the FIDO2 WebAuthn method specifically, the device-bound hardware token can be used to authenticate to the destination application using a unique cryptographic keypair (stored on the roaming authenticator device) and exchanged using public-key cryptography. FIDO2 Webauthn is an effective method of leveraging passwordless authentication to combat phishing, spoofing, and adversary-in-the-middle (AitM) attacks.
- **Passkeys** – which operate like a FIDO2 token, where a cryptographic keypair is generated and stored locally on a mobile device, and exchanged using public key cryptography with an application that is the target for authentication (which holds the public key). To access a configured passkey, a mobile device will require either biometric identification or a PIN / swipe pattern common with popular mobile devices.
- **Digital Certificates** – which can be used to generate a valid digital "identity" signature in response to an authentication request by using public and private keypairs. On modern devices, the trusted platform module (TPM) can be used as the internal authenticator to store the private cryptographic key, which is used to sign a certificate that will be validated for "passwordless" authentication using a corresponding public key.
- **Biometrics** – which can leverage the unique physical features of a human to validate an identity. Most commonly, biometric authentication will include fingerprint (Touch ID and Fingerprint Unlock as an example) and facial recognition methods (Face ID and Face Unlock as an example), which are inherent to many smartphones, mobile devices, and modern laptops.

Planning for Passwordless as an Authenticator

Legacy applications and infrastructure that do not readily support enhanced authentication methods can present a speed bump for organizations attempting to align under the concept of authenticators. Rather than focusing on integrating the authenticator equation for each individual application, it is now common for organizations to leverage a third-party single sign-on (SSO) solution as the front door for authentication, which will then broker authenticated access to backend applications.

Planning for passwordless as part of the authenticator equation can take time. A high-level overview of considerations include:

Identify:

- Current-state technologies and platforms that function as authoritative identity stores and platforms (IdP).
- Existing identity stores natively support passwordless authentication methods – or will require third-party integration and brokers.
- Identities that exist within an organization, including identity types that could test and verify the passwordless experience.
- Compensating controls and enhanced detections for identity types that don't support passwordless or strong authentication methods (e.g., programmatic / service accounts).
- The impact to guest / third-party users that may not support passwordless integration.
- Devices that users currently leverage for authentication and access — and verifying if these devices support passwordless methods.
- Applications that can be integrated directly for passwordless, or applications that support SSO integration with a third-party platform that supports passwordless methods.

Developing a plan for:

- Procuring and securely delivering and onboarding devices that will support passwordless authentication.
- Training curriculum to educate users about the passwordless experience.
- Identity store and device configuration modifications to onboard the passwordless integration.
- Testing and validating the passwordless integration with pilot users and scoped applications.
- Initial roll out and onboarding as well as expanding the scope of passwordless throughout the organization.

Another important consideration for passwordless is aligning recovery steps when a device or key is lost or stolen, as these are now core components to the authentication process for an identity. Planning for secure recovery steps must include weighing not only organizational risk, but the pros / cons to the overall user enrollment and self-service experience.

While internal authenticators (e.g., devices with an integrated TPM) can provide the ability to export (store) or sync private keys between devices, this can also introduce a risk if the keys are not secured and stored properly. When using third-party identity providers, recovery keys and phrases can also be considered as a method for recovering a passwordless identity for reconstitution on a new device. When roaming authenticators are used for passwordless authentication, options for identity recovery can include validating messages sent to a mobile device or email address.

Migrating from the concept of singular passwords to passwordless as an authenticator is a journey. Many organizations adopting the concept of authenticators have found that strong MFA is a foundational building block in support of a passwordless roadmap. While the journey requires proper planning, execution, and validation, the security benefits and risk reduction are invaluable, especially as identity is the new security boundary in today's hybrid operational model.

Read more articles from **The Defender's Advantage Cyber Snapshot**.

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud