Secure Work

Beyond Identity's Unphishable MFA

BEYOND IDENTITY

Challenges today:

In today's cloud-centric and remote work world, people are accessing software-as-a-service (SaaS) applications from more and more devices, faster than companies can identify or secure them. This creates a security blind spot. Attackers are increasingly stealing credentials and gaining unauthorized access to critical business data stored in cloud services from unknown and insecure devices. To combat these threats, multi-factor authentication (MFA) must deliver on three fronts: identify the user, identify the device, and stop the authentication if it's risky.

Scale remote access, especially in this SaaS world

Solve persistent bring your own device (BYOD) problem across entire workforce (employees, contractors, partners, etc)

Improve user experience (UX) to increase compliance and reduce support costs

Step 1:
FIDO-like, unphishable authentication factors

Step 2:
Eliminate passwords in authentication, recovery, and directory

Step 3:
Invisible, extensible security checks and a frictionless UX

Step 4:
Control user authentication on devices

Unphishable authentication factors

Utilize high-assurance, scalable public key cryptography to verify the identity of every user and every device:

1. Device biometrics and PINs
2. Cryptographic security keys stored in the Trusted Platform Module (TPM) of the device
3. Security checks of the user, device, and transaction at the time of login

With advancements in TPMs, key pairs can be generated and stored in the secure hardware chips of computers, tablets, and phones. The private key can't be cloned, moved, or modified on the device and is protected by the device's biometric or pin. This ensures that authorized users can easily register their device(s). IT security teams can then identify registered devices and block access from unknown devices.

Eliminate passwords from authentication, recovery, and directory

Passwords can never be used during the authentication process. Even if malicious actors steal or purchase passwords on the dark web, they're denied access because passwords aren't accepted at the login window. They also cannot be used to recover access because there's no password reset button. There are no passwords in the directory, only a list of registered devices. By eliminating weak knowledge factors like passwords, IT security teams can greatly reduce the risk of credential-based attacks, ransomware, and lateral movement.

Invisible, extensible security checks and frictionless user experience

Beyond Identity turns each authenticating device (computer, tablet, and phone) into an authenticator. Users simply unlock their device using their biometric or pin and then request to login—all key and security checks occur behind the scenes, invisible to the user. This provides a frictionless user experience, which increases adoption and compliance across the organization and reduces help desk support costs. This creates internal buy-in to enable MFA across more apps to protect company data from unauthorized access.

android | iOS | LINUX | macOS | Web | Windows 10

Control user authentication on devices

Each authenticating device is bound to an identity, so unregistered and insecure devices are stopped from authenticating. Furthermore, IT security teams can create extensive device security policies to stop risky authentications. This includes checks if a device is jailbroken, firewall is enabled, if it's managed, has a pin enabled, has an EDR running, and more. For example:

Critical Apps

Finance, HR, engineering apps

Allow managed and compliant Windows and Mac devices only—and non-managed, compliant iOS and Android devices with posture checks.

If...

Windows and macOS

- Managed by Intune or JAMF
- Crowdstrike Running
- Firewall On
- OS Version # or higher

Linux, iOS, and Android

- Not jailbroken or rooted
- PIN or password set
- Then approve authentication.

Upgrade your MFA or add an additional secure device trust factor today.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.