How Beyond Identity Works

Beyond Identity is just like FIDO and more

Beyond Identity uses similar standard FIDO protocols for public key cryptography to provide stronger authentication and protect user privacy. As such, private keys and biometric information never leave the user's device.

Beyond Identity is a SaaS platform that goes above and beyond FIDO standards. Our passwordless, invisible MFA validates the user, verifies the device is authorized for access, checks the security of the device, and executes an authentication decision based on the company's risk policies.

We support broader authentication use cases, turn all devices including computers, tablets, and phones into authenticators, and check the security of all devices at the time of authentication.

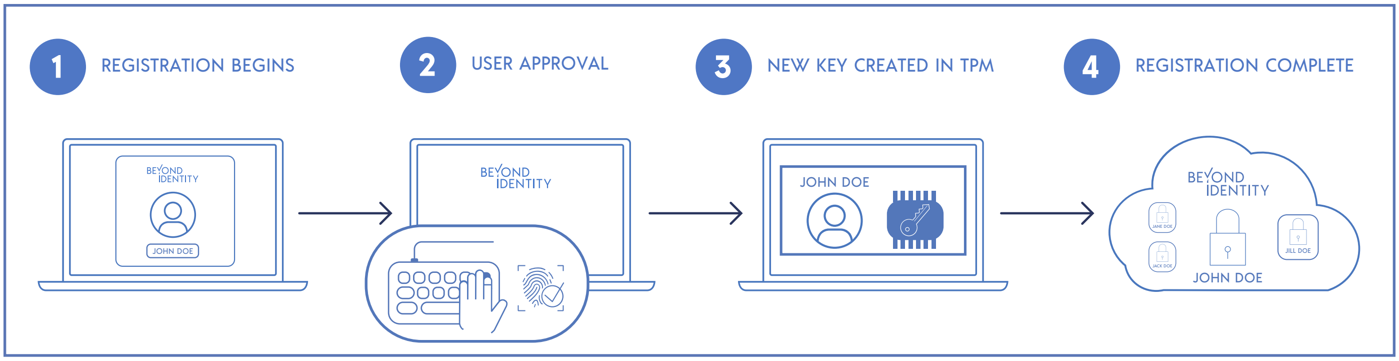
At the core of Beyond Identity's architecture is our patented technology which creates new key pairs on all client computers, tablets, and phones authenticating to our cloud to secure users across all of the devices they login from.

Registration

During registration with Beyond Identity, the user's client device creates a new key pair in the TPM or secure enclave. No one has access to the private key in the TPM and it cannot be moved from the device. The device TPM retains the private key and registers the public key with Beyond Identity. This binds the user's identity to the device.

All client devices authenticating are bound to a user and registered with the Beyond Identity Cloud. Users can enroll as many devices as the company allows. Each new device creates a key pair branch that's bound to the user and bound to the hardware of the device.

Computers, tablets, and phones have the same core Trusted Platform Module (TPM) technology to perform the creation and storage of key pairs. Beyond Identity supports all device operating systems to create and store key pairs. Other FIDO-based solutions limit the creation of key pairs to mobile devices or Universal Second Factors (U2Fs) which reduces the number of use cases and security checks companies can support.



Registration of devices:

- User unlocks their computer, tablet, or phone using a local biometric or PIN
- User authenticates to their existing IAM provider - or clicks a time-limited one-time code sent via email, SMS, or QR code
- User's device creates a new public/private key pair unique for the local device and that user's account in the TPM
- Public key is sent to Beyond Identity and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device.

Control registration of devices:

- Users can enroll devices that meet the company's requirements.

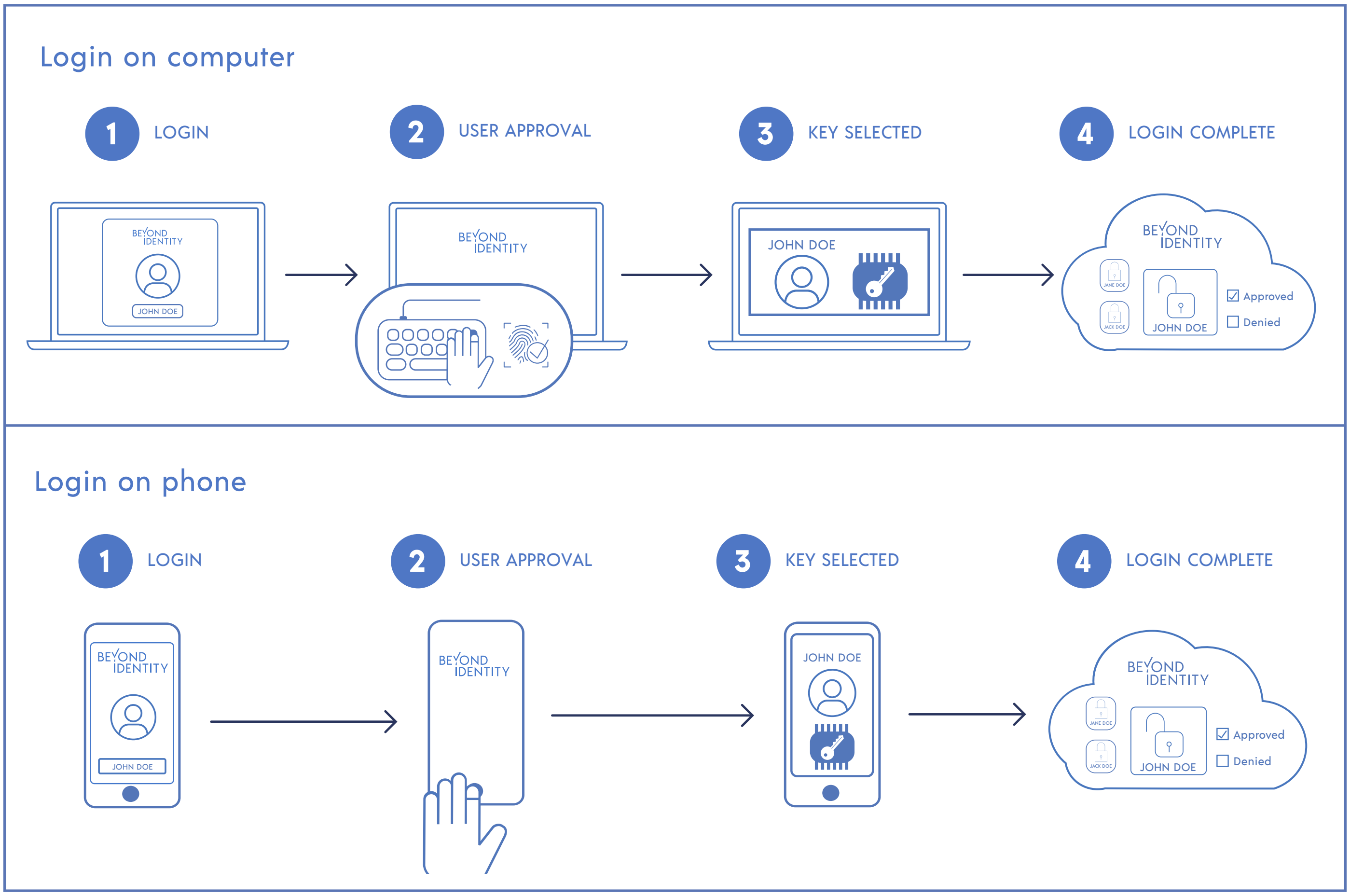
Support registration of all devices and major operating systems:

iOS	Mac	Android
Windows 10	Linux	Web

Sample Business Requirements	Example device registration policies
Workforce - BYOD and Unmanaged Devices	• If managed device, allow registration • If unmanaged computer (mac, windows, linux), deny registration • If unmanaged phone (iOS or android), allow registration
Customer Identity and Access Management - Crypto wallet vendor	• If device is not Jailbroken, allow registration
Customer Identity and Access Management - Media, Publishing, Entertainment	• If user has X number of devices already registered, deny registration

Login

When the user requests to login, the client device that is authenticating proves possession of the private key in the TPM to the Beyond Identity Cloud by signing a challenge. The client's private keys can only be used after the device is unlocked with a local biometric or PIN.



- Beyond Identity Cloud challenges the user to login with a previously registered device that matches the company's acceptance policy
- User unlocks the device using a local biometric or PIN
- Device uses the user's account identifier provided by the company to select the correct key in the TPM and sign the company's challenge
- Client device sends the signed challenge back to the company, which verifies it with the stored public key and logs in the user

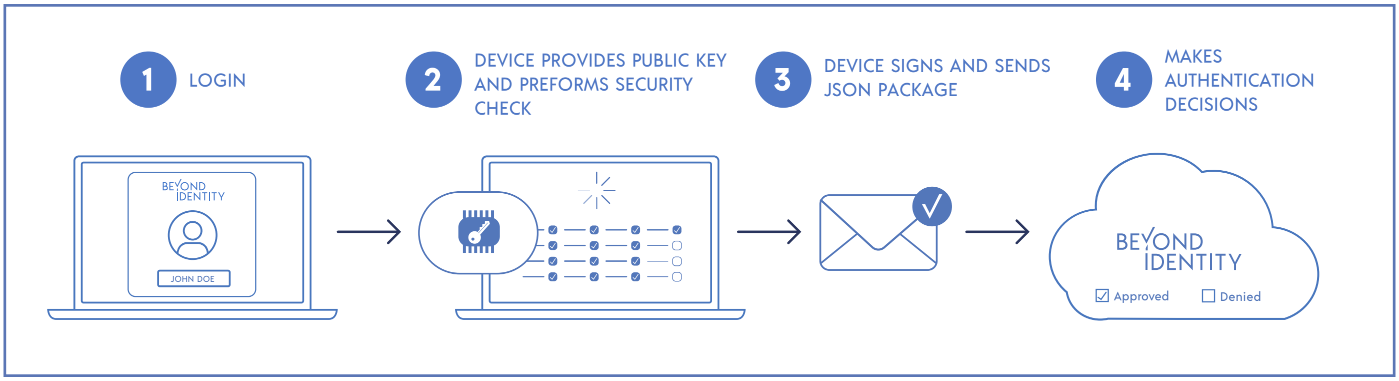
Supports login to apps and services:

Web apps	Mobile apps	Native desktop apps
Desktops	WiFi	

Device security checks at login

Every user client device is registered with Beyond Identity. The client device turns into a self-signed OpenID provider that issues checks for security programs, files, apps, and settings running on the device at the time of login.

During the authentication request, Beyond Identity challenges the client device, and the client device signs the token certificate and sends a JSON package with the results of the device posture check. Security checks run on OSQuery for extensibility and customizability by the company. This checks the device to ensure it meets policy requirements before allowing access.


1 LOGIN
2 DEVICE PROVIDES PUBLIC KEY AND PREFORMS SECURITY CHECK
3 DEVICE SIGNS AND SENDS JSON PACKAGE
4 MAKES AUTHENTICATION DECISIONS
BEYOND IDENTITY
JOHN DOE
BEYOND IDENTITY
☑ Approved
☐ Denied

Security Attributes	Example Values (not limited to)	Supported Platforms
Standard		
Number of Devices Registered	• Number • Equals ___ • Great than > ___ • Less than < ___	Windows, macOS, iOS, Android, Linux
Platform	• Android • iOS • macOS • Windows • Linux	Windows, macOS, iOS, Android, Linux
OS Major / Minor Version	• Equals ___ • Great than > ___ • Less than < ___	Windows, macOS
Disk Encryption	• Enabled • Disabled	Windows, macOS, Linux
Firewall	• On • Off	Windows, macOS
Device Rooted / Jailbroken	• Detected • Not detected	iOS, Android
Screen Locked Enabled (Biometric, PIN)	• Screen lock enabled • Biometric enabled • Pin enabled	iOS, Android
User FileVault is...	• On • Off	macOS

Security Attributes	Example Values (not limited to)	Supported Platforms
Customizable:		
Process Running...	*[fill in the blank]* **MDM Provider** • JAMF • VMWare Airwatch • MobileIron • Citrix Endpoint Management • Microsoft InTune • kandji **EDR/XDR Provider** • Crowdstrike • SentinelOne • Bitdefender • Cylance • Armor • Cybereason **Vulnerability Assessment** • Tenable • Netsparker • Vulcan • Alert Logic • BeyondTrust • Rapid7 • Qualys • Tripwire • F-Secure **AntiVirus Provider** • McAfee • Kaspersky • Norton • Webroot • Trend Micro • BullGuard **Client Management Tools & Backups** • Druva • Landesk • ManageEngine • SCCM • Kace • BMC Client Mgmt • Blacklist services: • uTorrent • xBox live • VNC	Windows, macOS, iOS, Android, Linux
Service Running....		Windows, macOS, iOS, Android, Linux
App installed contains...		Windows, macOS, iOS, Android, Linux
File exists...	*[fill in the blank]* • C:\Windows\System32\... • Drivers • DLL files • Configuration	Windows, macOS, iOS, Android, Linux
Registry Key / Plist value contains...	*[fill in the blank]* • Path • Key • Subkey • Number/String • Value	Windows, macOS,
Optional from integrations:		
Microsoft InTune	• Registered	Windows, macOS, iOS, Android
JAMF	• Registered	macOS, iOS
Workspace ONE	• Enrolled	Windows, macOS, iOS, Android
Crowdstrike	• Registered • Zero Trust Assessment Score	Windows, macOS

Control user authentication on devices:

- Users and devices can authenticate when it meets the company's risk policies.
- Companies can customize extensible authentication policies with unlimited, granular security attributes.

Example scenarios	Example authentication policies
Critical Apps For example: Workforce - Finance and HR apps Allow managed and compliant windows and mac devices only.	If... Windows • Managed by Intune • Crowdstrike Running • Firewall On • OS Version build 19042 or higher • User Group: Finance or HR MacOS • Managed by JAMF • Crowdstrike Running • Firewall On • OS Version 11.16 or higher • User Group: Finance or HR Then, approve authentication with device biometric or pin. If... • iOS, Android, Linux • Then, deny authentication.
Medium Risk App For example: Workforce - Chat apps Allow managed and compliant windows and mac - and non-managed, compliant linux, iOS, and Android devices with posture checks.	If... Windows • Managed by Intune • Crowdstrike Running • Firewall On • OS Version build 19042 or higher Mac OS • Managed by JAMF • Crowdstrike Running • Firewall On • OS Version 11.16 or higher Linux • Crowdstrike Running iOS • Not jailbroken • Pin or Password Set Android • Not rooted • Pin or Password Set Then, approve authentication.
Not Critical App For example - Workforce - Web conferencing apps Allow authorized users and authorized devices with posture checks.	If... Windows • Firewall on • OS Version build 19042 or higher Mac OS • Firewall On • OS Version 11.16 or higher iOS iOS • Not jailbroken • Pin or Password Set Android • Not rooted • Pin or Password Set Then, approve authentication.

User privacy

Beyond Identity is just like FIDO protocols, we built our platform with privacy in mind: biometric data never leaves the user's device. Beyond Identity shares status reports and device checks with users through the Beyond Identity App to be transparent about the device information collected. It meets GDPR, CCPA, and Strong Customer Authentication (SCA) compliance requirements so end users are comfortable setting up and using their existing devices.

About 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.

Ready to Explore Zero Trust Security?

GET A DEMO

beyondidentity.com info@beyondidentity.com

BEYOND IDENTITY