BEYOND IDENTITY

PASSWORDLESS IDENTITY PLATFORM FOR WORKFORCE

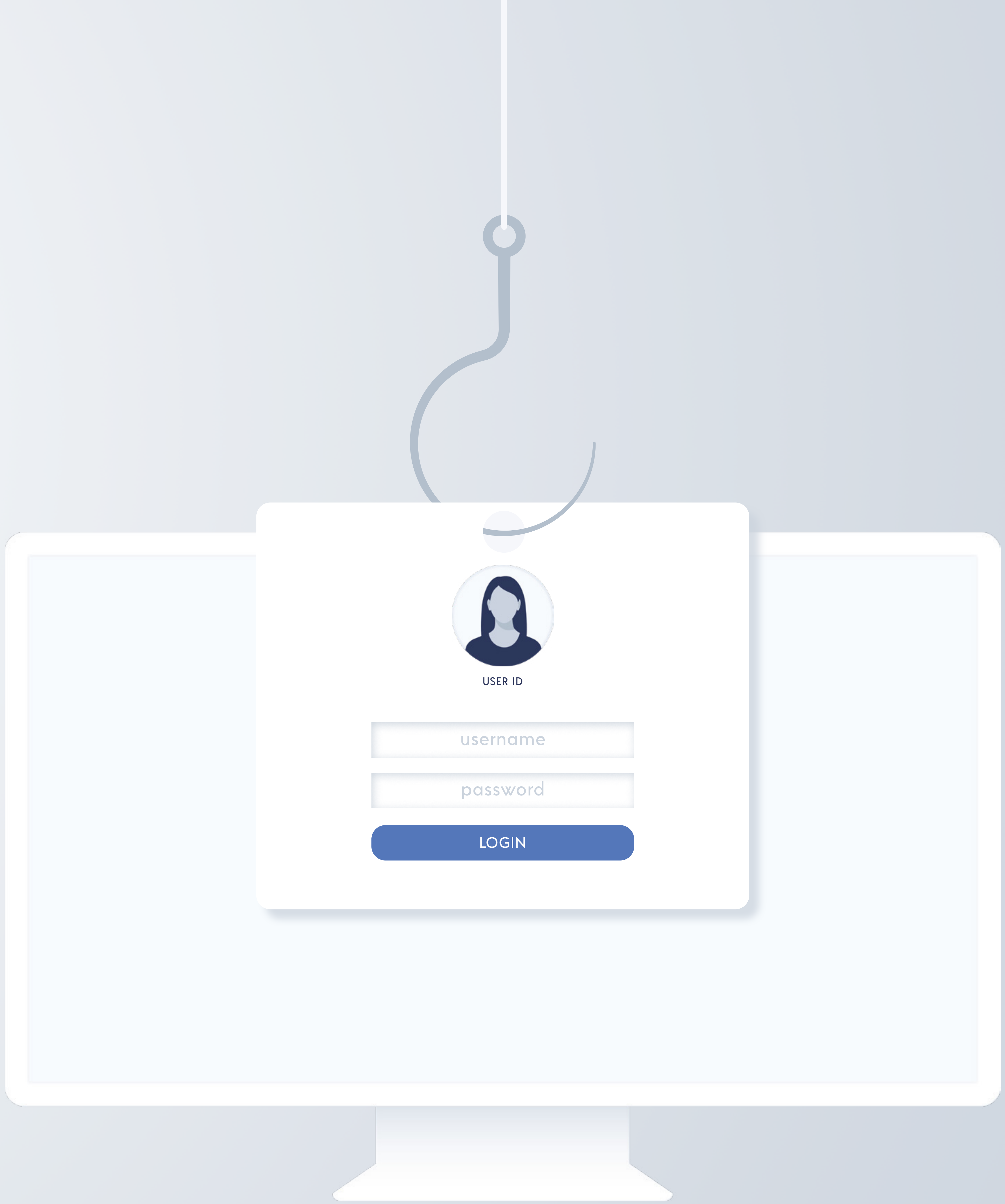
SOLUTION BRIEF | BEYOND IDENTITY FOR WORKFORCE

ATTACKERS SIMPLY NEED TO LOG IN

Today's enterprise is dealing with the added complexity of more resources in the cloud, the workforce working remotely, off the network, and on all types of devices, including personal devices. It's easy for attackers to get access to company accounts: they simply need to log in. Passwords are the default in most systems, however, they can be easily stolen/reused, leading to account takeovers and data loss.

LAYERING SECURITY ON TOP OF PASSWORDS CAUSES FRICTION

As a response to this, we've put a lot of barriers in place to protect company resources, often at the expense of the workforce. It's difficult to put security controls in place to protect user accounts without adding a lot of friction for the workforce to log in.



HOW OUR SOLUTION CAN HELP YOU

We set out to radically change the way the world logs in. Our Passwordless Identity Platform verifies workforce identities using a new type of authenticator (powered by proven, industry standard X.509 certificates, without any certificate management required). It continuously evaluates risk signals of every user and every device requesting access at the exact time of login, enabling you to enforce continuous risk-based authentication. Unlike other multi-factor authentication solutions, Beyond Identity eliminates passwords, and provides users with a frictionless way to authenticate without one-time codes or having to pick up a second device.

BENEFITS

PROTECT ACCOUNTS FROM UNAUTHORIZED ACCESS

Reduce a major source of risk by eliminating account takeovers from compromised credentials.

REDUCE FRICTION FOR YOUR WORKFORCE

Access applications from every device, without passwords, one-time codes, or using a second device.

CONTROL ACCESS BASED ON CONTINUOUS RISK SIGNALS

Enforce dynamic access decisions using 12+ risk signals from the user and their device's security posture.

SAVE IT/HELP DESK COSTS WITH SELF-SERVE OPTIONS

Enable users to self-serve, register, and recover their own passwordless credentials to reduce lockouts and help desk calls.

SIMPLIFY AUDIT AND COMPLIANCE PROCESSES

Export an immutable record of each login transaction for streamlined reporting.

ENHANCE ACCESS CONTROL WITH MDM AND EDR CHECKS

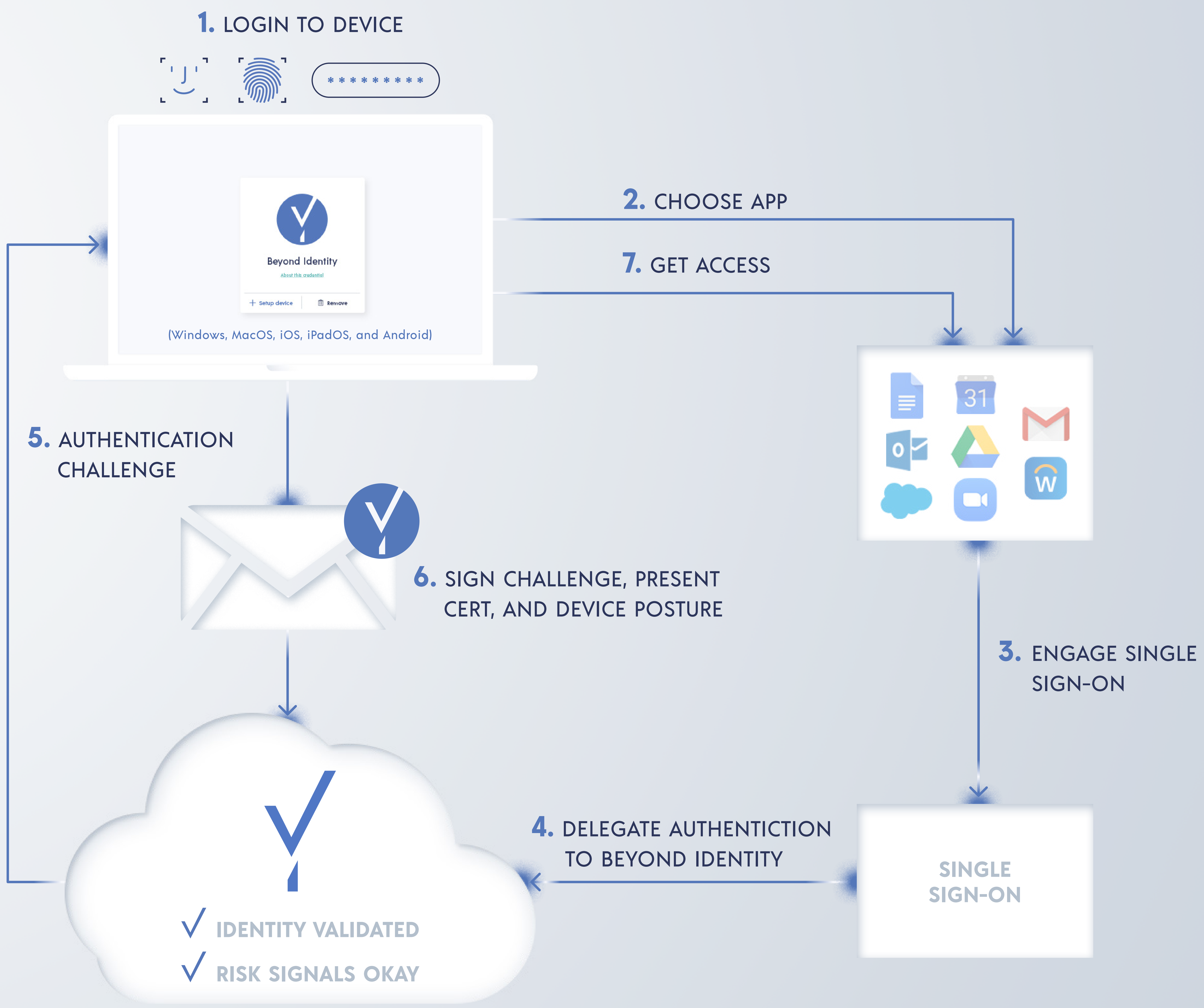
Check devices for mobile device management (MDM) and endpoint detection and response (EDR) software.

HOW IT WORKS

Our platform supports passwordless logins to desktops and single sign-on applications. Our authenticator can be used on every device, and because of our unique architecture, we can provide 12+ granular security signals from every device requesting access to make risk-based access control decisions. We also integrate with third-party tools such as mobile device management (MDM) and endpoint detection and response (EDR) solutions to enhance this data set of risk signals for risk-based policies.

OVERVIEW OF A PASSWORLDESS LOGIN TO A SINGLE SIGN-ON:

1. User securely logs in to the device using a biometric
2. User selects the app
3. User inputs their username, clicks next
4. App delegates access to single sign-on
5. Single sign-on delegates to Beyond Identity
6. Beyond Identity Cloud issues an authentication challenge to that device's Beyond Identity Authenticator
7. Beyond Identity Authenticator signs the challenge leveraging the private keys in the TPM, gathers device security posture, and puts all this info into a signed JSON Web Token (JWT)
8. Beyond Identity validates the challenge, evaluates device security posture info in JWT, and makes a risk-based auth decision in Beyond Identity's policy engine
9. Beyond Identity cloud service provides the identity to the single sign-on
10. Single sign-on completes login by providing identity to the application



PARTNERS AND INTEGRATIONS:

okta

Ping Identity

ForgeRock

Microsoft
Active Directory
Federation Services

SAMPLING OF CUSTOMERS:

NEA

taulia

snowflake

KOCH

KEY DIFFERENTIATORS

— No passwords, no second devices, no one-time codes

— Support passwordless authentication to web-based and native apps, both on desktops and mobile devices

— Acts on risk signals from the user and their device's security posture data at the exact time of login

Risk signals include:

- Biometric enabled
- Hard drive encrypted
- Firewall enabled
- Gatekeeper enabled
- UEM, MDM, EDR check, and more

— Leverage proven, existing X.509 certificates, with no certificate management

— Reduce costs with user self-service and recovery,99% uptime availability with full support

ABOUT BEYOND IDENTITY

Beyond Identity's mission is to eliminate passwords and radically change the way the world logs in.

Our authenticator runs on Windows, MacOS, iOS, iPadOS, and Android.

Authenticates users on mobile and desktop devices, to web-based and native applications.

Supported industry standards: OIDC, OAuth, SAML, and SCIM.

Visit beyondidentity.com for more information.