Channel Partner

Beyond Identity Overview

BEYOND IDENTITY

Who is Beyond Identity

Security first Access Management platform engineered to prevent identity threats. Every other AM platform was built to drive productivity, making security an afterthought and providing a highway for bad actors to exploit.
Beyond Identity is the only AM platform foundationally built to ensure only trusted users and secure devices can gain and maintain access.

What We Do

At the core of our solution sits our platform authenticator (PA) that authenticates users with hardware-bound passkeys and collects real-time device posture. Using our policy engine, you can use those posture signals together with risk data from other security tools to continuously monitor device compliance and make appropriate access decisions (e.g. block. reauthenticate, etc.). This applies to all OS, and both managed and unmanaged devices.

How we are Different

Always phishing-resistant. on any device

Only uses device-bound, passwordless, asymmetric credentials. Never falls back to phishable factors.

Device security compliance

Ensure access is only granted to a trusted device, whether managed or unmanaged, with the appropriate security posture as defined by your policy.

Continuous risk-based authentication

Adapt access control to the changing state of users and devices. Continuously monitor risk signals collected by Beyond Identity and other security tools from your stack to make real-time authentication decisions.

Enforce precise access controls

Easily configure customizable per-OS, per-app, and per-group policies. Leverage risk signals collected by Beyond Identity and other security tools in your stack.

Best Fit and Sales Triggers:

We focus on cloud-first and security-invested mid to large enterprises with business-critical assets to secure.

- ✓ **Security is a core part of the businesses strategy** Low risk tolerance, builds/purchases tools with baked-in security.
- ✓ **Have a Zero Trust Program** and looking for a user authentication piece that leverages existing EDR, ZTNA, or MDM tools.
- ✓ **Personal BYOD devices** accessing email or SaaS apps for day-to-day operations, if via partner, contractor, or personal unmanaged BYOD devices.
- ✓ **1K-10K employee mid to large enterprises** with in-house security or IAM team are the sweet spot. Note: our clients range to over 60K licenses.

Making the conversation happen

How to position Beyond Identity to customers

- Are phishing and identity-based attacks something you are concerned with? Are you using passwordless phishing-resistant MFA across the board?
- Does your org. allow access through BYOD devices? (Ipads, Mobile, Personal Computers) How do you ensure they are compliant?
- How important is device trust/posture to you? do you care about authentication policies?
- Do you feel you are sufficiently leveraging your security stack for authentication decisions?

*>> "**One of our partners** - Beyond Identity, with their passwordless phish-resistant MFA, can eliminate identity-based attacks and ensure only trusted users and secure devices can gain and maintain access."*

Solution Overview

BEYOND IDENTITY

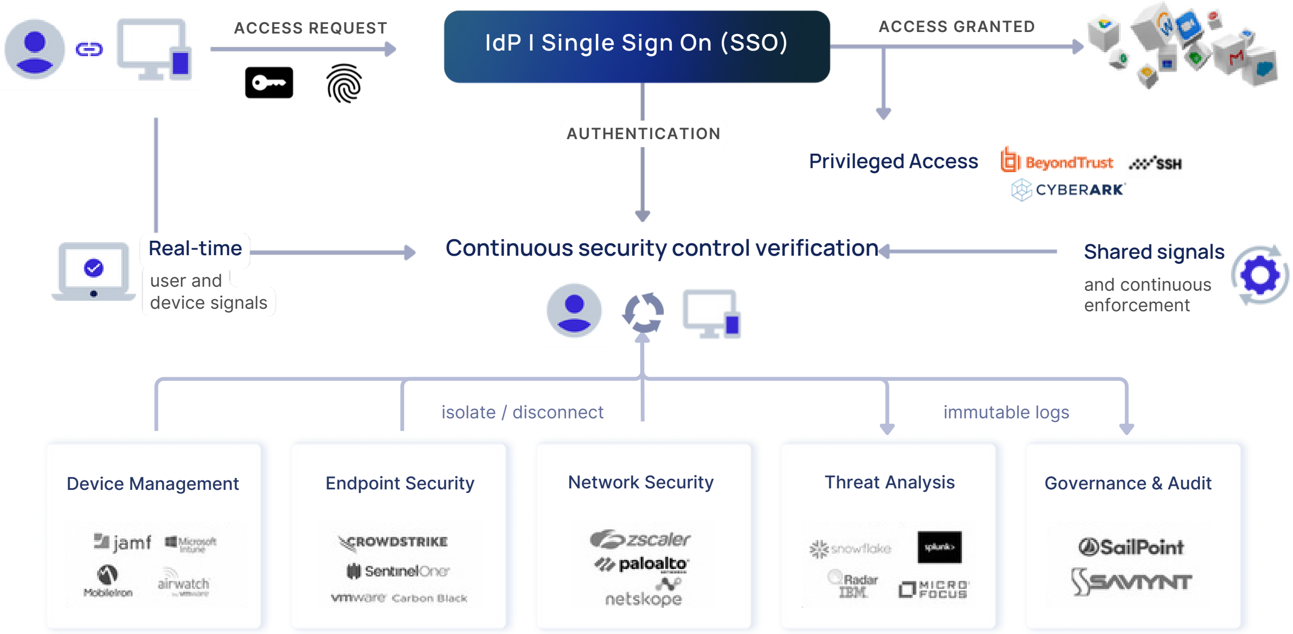
Architecture & Integrations

At the core of our solution sits our platform authenticator (PA) that authenticates users with hardware-bound passkeys and collects real-time device posture. Using our policy engine, you can use those posture signals together with risk data from your trusted security tools to continuously monitor device compliance and make appropriate access decisions (e.g. block. reauthenticate, etc.). This applies to all OSs, and both managed and unmanaged devices.

We support a range of common tools:
Endpoint security, Device Management, Network Security, Threat Analysis, Governance and Audit. Can augment with an existing IdP or become the Identity Provider.

Our integrations optimize existing investments in MDMs, EDR/XDR, and ZTNA/SASE tools. **Turning real-time risk signals into access decisions**

NO integrations needed to be functional and valuable.



ACCESS REQUEST

IdP I Single Sign On (SSO)

ACCESS GRANTED

AUTHENTICATION

Privileged Access

Real-time

user and device signals

Continuous security control verification

Shared signals

and continuous enforcement

isolate / disconnect

immutable logs

Device Management

Endpoint Security

Network Security

Threat Analysis

Governance & Audit

Secure Access Platform

Security-first access management platform

Phishing-resistant MFA

Single-device passwordless, phishing-resistant MFA backed by an adaptive engine to control access based on real-time user and device risk.

Secure SSO

Secure-by-default configuration and authentication, flexible directory, and per-application policy to provide complete access protection.

Device Trust

Fine-grained, customizable device query to provide visibility and control for device compliance across managed and unmanaged devices.

RealityCheck

Secure video conferencing integration validating AAL3 user authentication and device security to prevent AI deepfake threats.