

A CHANNEL-FIRST COMPANY

Beyond Identity Secure Access is a security-first Access Management Platform engineered to eliminate identity-based threats.



## Top Use Cases We Solve



### Eliminate Identity Threats

Eliminate, not just reduce the largest attack vector, including: phishing, brute force, MFA bypass, adversary-in-the-middle attacks, or any other credential-based threat.



### Secure your entire device fleet

Easily enforce device security controls for managed and unmanaged devices, contractors, and partners, supporting all operating systems, including BYOD.



### Meet and exceed audit and compliance requirements

Simplify audit and compliance with MFA that surpasses PCI DSS, GDPR, SOC 2, NIST, CISA, NYDFS, CMMC, and more.



### Complete your customer's Zero Trust program

Instantly achieve Zero Trust program maturity for both Identity and Device in accordance with CISA guidelines.

### Additional Value Adds:

- ✓ Reducing password friction and costs
- ✓ Accelerating incident response and triage
- ✓ M&As and new employee onboarding or de-provisioning
- ✓ Defend against AI Impersonation attacks

## What Sets Us Apart:

We engineered our access management platform with a security-first approach. Continuously evaluating the security of both users and their devices to provide and maintain secure, trusted access. We do this in a way that is entirely seamless to the users while providing a delightful single-device, passwordless user experience.

By leveraging hardware-bound passkeys and assessing real-time device posture telemetry, we ensure that only compliant devices and trusted users can access systems and applications without ever relying on phishable, shared secrets.

Our proprietary platform authenticator (PA), integrated with the customer's security tool stack, continuously monitors device compliance and transforms risk signals into actionable access decisions (e.g., deny, block, quarantine, reauthenticate, etc.). We apply this across managed and unmanaged devices and support all major operating systems. Using our easy-to-configure, fine-grained policy engine, we ensure customers can enforce access decisions that precisely fit their unique business and compliance requirements.

### Always phishing-resistant on any device

Only uses device-bound, passwordless, asymmetric credentials. Supports all common OSs and never falls back to phishable factors.

### Device security compliance

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

### Continuous risk-based authentication

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

### Enforce precise access controls

Easily configure customizable, adaptive risk-based policies tailored to your exact security and compliance requirements. Leverage signals natively collected by Beyond Identity and other security tools in your stack.



## Ideal buyer

## NOT a good fit

### Director or above within:

- Security Teams
- IAM Teams
- IT Teams
- SecOps Teams

### In companies who:

- Security is a core part of their business strategy
- Cloud-first, innovation-driven organizations
- Mid to large enterprises with 5-10K employees. Our customers have up to 60K Licenses
- Have unmanaged devices accessing resources

- Customers who don't care about security and have not made investments in security tools
- Strictly on-premise infrastructure and applications
- Apps that don't support modern authentication protocols (e.g., SAML 2.0, OIDC)
- Customers with MSFT stack who love using E5 and will are not open to switch.
- Physical Key / Smart Cards reliant for Authentication

## Product Offerings

### Zero Trust Identity & Device

- Phishing-resistant MFA
- Single-device, passwordless UX
- Support for Windows, Mac, Linux, iOS, Android, ChromeOS
- Desktop login
- Fine-grained risk policy engine
- Continuous authentication
- Robust 3rd party integrations
- Access to add-ons

### Secure Access Complete

All Zero Trust Identity & Device features, PLUS:

- Secure SSO
- Customizable app launcher
- Per-application risk-based policies
- Least privilege access management
- Fast SSO migration tool

## INTEGRATIONS

### We support a range of common tools:

Endpoint security, Device Management, Network Security, Threat Analysis, Privileged Access, 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.**