Beyond Identity for Technology Leaders

BEYOND IDENTITY

Serving cloud, SaaS, and telecommunications companies with zero trust authentication that enables agility

Overview

Technology and software-as-a-service (SaaS) companies have disrupted traditional business models and became the dominant force in business. As businesses that ship code at scale, security must provide coverage of all cloud-applications that enable employee productivity, be deeply ingrained in the development process to protect infrastructure-as-code and ensure product integrity, and enable visibility and control over all devices requesting access to company resources, including non-managed devices. Not to mention, technology companies must compete to win business with end-users who place a premium on frictionless authentication experiences and account security.

Tech leaders must be equipped with an innovative authentication solution that disrupts the old-school password and perimeter-based security approaches.

Beyond Identity allows companies to take the burden of security off of users while shifting security left to prevent attacks instead of responding to them. As the only solution that delivers phishing-resistant MFA with zero user friction, Beyond Identity enables SaaS and tech companies to secure critical company data, code repositories, and applications confidently and without frustrating users. Moreover, the Beyond Identity Zero Trust Risk Engine enables continuous authentication using risk-based policies that process real-time user and device risk signals in real-time, captured from the endpoint or ingested via detection and response tools.

Unique Benefits

- ✓ **Zero friction passwordless user experience** to enhance productivity and accelerate onboarding with NO second device, codes, or push notifications needed
- ✓ **Phishing-resistant, invisible MFA** with two strong factors by default to eliminate password-based breaches
- ✓ **Cloud-native, API-first platform** to minimize deployment effort, enable flexible customizations, and provides support for industry standards to ensure extensibility
- ✓ **Zero Trust Authentication** with dynamic risk-based policies that incorporate risk signals produced by leading security tools like EDR, XDR, ZTNA and SIEMs.

Trusted By Technology Leaders

snowflake yotpo. ROBLOX Bolt unqork

The challenge: enabling agility while increasing access security

Against the context of a competitive cloud-native world, the shift to remote work and hybrid work environments, and increasingly effective attacks bypassing first-generation MFA, technology companies must contend with the proliferation of attack surfaces and trajectories without decreasing productivity.

However, providing secure access in a cloud-first, hybrid environment cannot be solved with a patchwork of tools from SSOs, first-generation MFA, VPNs, or MDMs. While these technologies are important components of enterprise security architectures, they leave glaring blindspots around:

- Authentication factors vulnerable to phishing attacks
- Patching, configuration, and security posture of bring-your-own-devices (BYOD)
- Real-time security posture of all devices and zero trust risk policy enforcement
- Cryptographic assurance of user identity behind access requests and code commits

When anyone with any device can access any cloud application with a password—including HR systems, code repositories, data platforms, and CRM tools—breach prevention is critical to protect corporate data, code, and intellectual property.

Exacerbating the problem, all companies using first-generation MFA are facing a security emergency.

Attackers are increasingly adept at bypassing MFA and publicly available phishing kits have rendered phishable MFA wholly ineffective. In fact, the US government, CISA, and NYDFS issued statements calling for the "discontinued support of authentication methods that fail to resist phishing such as phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications." Given that CISA identifies information technology as a critical infrastructure sector, the criticality of securing access has never been more consequential.

The key is securing access without burdening users. Requiring employees, partners, contractors, and customers to jump through MFA loops lowers productivity, slows down onboarding, and increases IT overhead.

The solution: MFA built for agility in a zero trust world

As the front door to all data, resources, and services, authentication security is critically important. In order to meet the demands of the business and extended workforce, authentication must be frictionless, phishing-resistant, and future-proofed for a zero trust architecture.

- **Frictionless:** Authentication should be simple, easy, and fast to enable productivity and accelerate onboarding. This means there should be no extra steps, including one-time codes, push notifications, or picking up a second device at all.
- **Phishing-resistant:** There should be no dependency on any phishable factor for authentication to ensure account security and protect sensitive data. Phishable factors include passwords, push

notification, and one-time codes.

- **Zero trust compliant:** Increasing adoption of zero trust strategies means authentication must comply with the "never trust, always verify" primitive of a zero trust approach. Authentication should immutably verify user identity and the integrity of devices used.
- **Strong device trust:** Acquire relevant and granular risk posture about every device including BYOD to ensure device security prior to granting access and continuously during authenticated sessions without relying on VPNs, VDIs, or MDMs.
- **Ease of deployment:** Leverage API-first, cloud-native platform that supports highly available deployments to meet workforce, devops, and customer access security use cases with elastic scalability and flexible customization.

Employees & Extended Workforce	IT Admins	Developers	Customers
Secure access to resources and cloud apps from anywhere with any device Improved productivity from lowered authentication friction Lowered help desk costs associated with password resets Respect privacy on personal devices while ensuring security without heavyweight MDMs	Lower IT operational cost from password resets and MFA issues Control tooling proliferation with a solution that consolidates risk signals and integrates with tools across all security categories Simple policy configuration within visual interface	Cryptographic identity assertion for every commit to ensure code integrity Ensure only authorized developers using machines with appropriately configured security controls can deliver software to the SDLC pipeline Supports integration with all major repos	Accelerated onboarding and login with zero-friction authentication Maintain high brand trust by fully safeguarding customers from credential-based attacks Consistent, universal experience across mobile and web apps on any device

How Beyond Identity can help

Modern workforces cannot rely exclusively on controls that only target employees and corporate-owned devices. Modern customers do not want to deal with the hassle of complicated password requirements and MFA steps.

Beyond Identity provides identity security that can be extended to contractors, partners, and other BYOD users without resorting to heavyweight, onerous and intrusive solutions based on MDMs, VPNs, or VDI. In alignment with a zero trust approach, we deliver phishing-resistant MFA, real-time device posture across managed and unmanaged devices, and enable enforcement of risk-based policy assessments to inform allow, deny, or step-up decisions at the moment a user attempts to login and

access critical applications.

For customers, there is zero authentication friction and they can be fully protected from account takeover fraud. Plus, your developers can focus on building your product instead of secure authentication from scratch.

Zero Trust Authentication Requirement	*Beyond Identity*	*Differentiation*
Frictionless: Easy for users to adopt and accelerates speed to resources.	✓	Beyond Identity lowers MFA friction to zero by completely removing the need for second devices.
Phishing-resistant: No reliance on phishable factors including one-time codes, push notifications, and magic links.	✓	Beyond Identity delivers unphishable MFA with: • Something you have - possession of private key within device secure enclave • Something you are - local device biometric
Passwordless: Eliminate threat of password-based attacks and save on help desk costs for password resets and lockouts.	✓	Given our architecture, passwords can be fully eliminated from the user experience and database at your pace. What doesn't exist cannot be breached.
Zero trust compliance: Never trust and always verify every user and device, in real-time and continuously, that is requesting access.	✓	Given our architecture, each device is cryptographically bound to a specific user identity to ensure that the right person, with a secure device, is accessing the right data. Every authentication is also evaluated continuously for real-time device risk gathered from the endpoint directly or ingested from detection and response tools continuously.
Ease of deployment: API-first, cloud-native platform that supports highly available deployments for workforce, devops, and customer use cases	✓	Beyond Identity is highly available, elastically scalable, and integrates with all major IDPs/ IDaaS solutions while providing support for hybrid IT environments.

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.