

# Beyond Identity Secure Workforce

Protect your organization with passwordless,  
phishing-resistant authentication

Trusted By Customers Like:



Cornell University



## KEY BENEFITS:

- ✓ Reduce the risk of password breaches
- ✓ Shrink attack surface
- ✓ Enable Zero Trust Authentication
- ✓ Delight users

Prevent credential-based breaches with phishing-resistant MFA to power your extended workforce.

Workforces are demanding access to critical resources from anywhere in the world, at any time, and across devices. They're working beyond the confines of the traditional network perimeter. Security vulnerabilities like insecure passwords and weak, legacy multi-factor authentication (MFA) authentication no longer protect your organization.

Beyond Identity eliminates passwords, phishable factors, and their inherent vulnerabilities. We ensure organizations can verify the identity of every user and device using strong cryptography; force adherence to your organization's security policies so all devices, including unmanaged ones, meet your security posture requirements; and continuously evaluate fresh contextual data, including key risk telemetry, to evaluate trustworthiness and reduce risk.

# Use cases

## Passwordless authentication

Prevent credential based breaches by eliminating passwords for applications and desktop logins.

[Learn more](#)

## Phishing-resistant MFA

Phishing-resistance MFA eliminates “phishable” second factors in authentication, such as SMS codes, magic links and OTP. These factors are highly targeted in recent attacks against traditional MFA solutions. Phishing-resistant MFA increases your organization’s authentication security AND its usability.

[Learn more](#)

## Validate device security settings

Shrink the attack surface by stopping risky devices from accessing applications and infrastructure. Combine identity-bound devices with real-time device-health checks for secure access.

[Learn more](#)

## Enable zero trust authentication

Meet all seven Zero Trust Authentication requirements that increase authentication security and delight users with effortless access.

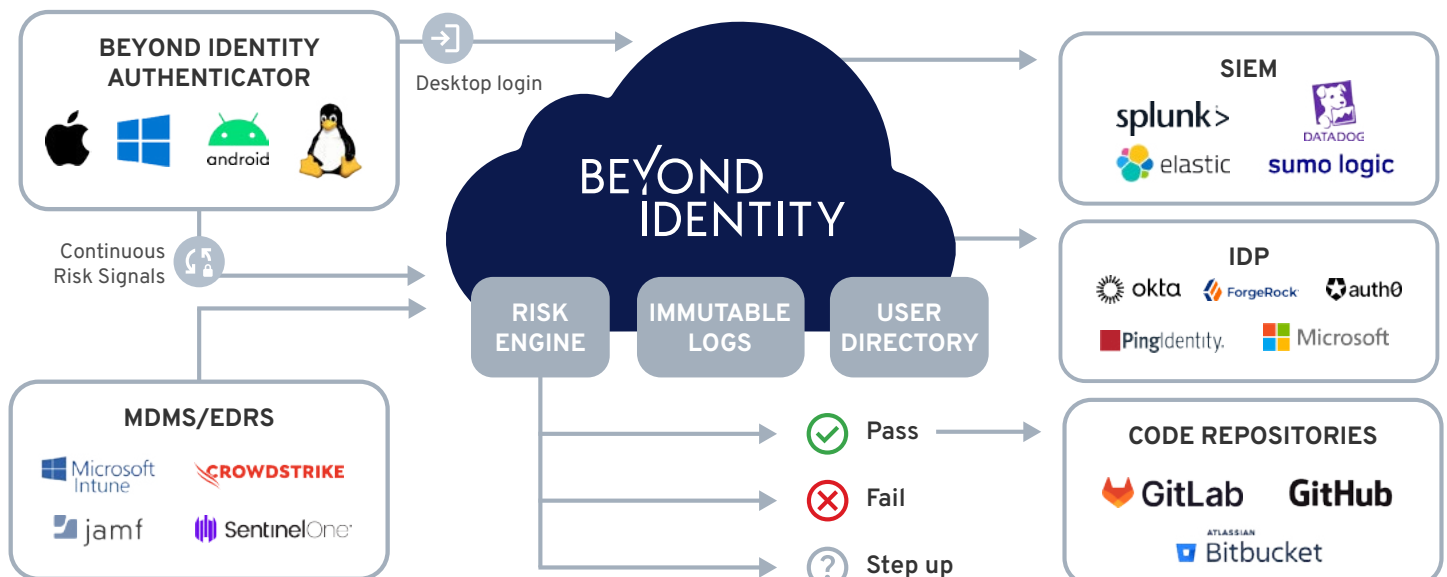
[Learn more](#)

# How It Works

Beyond Identity uses proven asymmetric cryptography to authenticate users and devices securely. Beyond Identity eliminates passwords and replaces them with Universal Passkeys with the private passkey stored in the Trusted Platform Module(TPM), binding identity to the users’ devices, and enforcing device security policy at every access attempt.

Beyond Identity acts as a delegated identity provider to your single sign-on. A policy engine that continuously verifies the user, device, application, and authentication transaction. Dozens of user, device, and third party risk signals are analyzed to enforce continuous, risk-based access control.

Beyond Identity integrates with key security ecosystem controls to enable a proactive zero trust security posture.



## Unique Benefits

### Delight users

Delight users with effortless authentication for applications and desktop login. Security teams are happy to replace passwords with phishing-resistant authentication that eliminates weak factors like passwords, SMS codes, magic links and OTP. Deploy phishing-resistant authentication that users enjoy.

### Force policy adherence

End unauthorized device access to SaaS resources—force adherence to device security policies via contextual analysis of the device and its security state at the exact time of each access request. Devices that are unidentified or unsecured have no avenue for access.

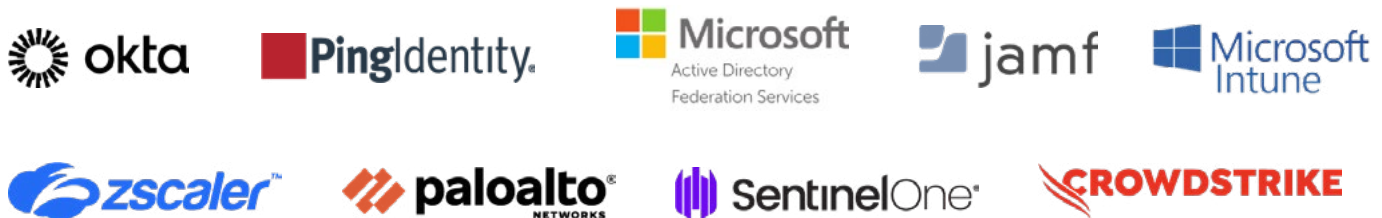
### Continuously analyze risk

Employ rule-based access via customizable policies that constantly evaluate the risk and trustworthiness of each user and device requesting access.

### Enables Zero Trust Authentication

Deliver continuous risk-based multi-factor authentication that comprehensively integrates security signals from your zero trust security ecosystem, including CrowdStrike, Palo Alto Networks, and Zscaler, to provide a phishing-resistant and passwordless user experience that prevents credential breaches.

## Integrations



[Learn more about our integrations](#)

## BEYOND IDENTITY

Beyond Identity is revolutionizing digital access for organizations looking to improve protection against cyber attacks and deliver the highest levels of security for their workforces, customers and developers. Its suite of passwordless, phishing-resistant, and zero trust authentication solutions improves security and user experience. The platform delivers continuous risk-based authentication incorporating signals from the zero trust ecosystem to ensure only valid users and secure devices gain or maintain access to critical resources. Companies like Snowflake, Unqork, and Roblox rely on Beyond Identity's highly available cloud-native platform to thwart attacks and advance their zero trust strategies. To learn more about Beyond Identity's FIDO-2 certified multi-factor authentication (MFA) solutions, visit [beyondidentity.com](https://beyondidentity.com) and stay connected with us on [Twitter](#), [LinkedIn](#), and [YouTube](#).

Get a demo

[beyondidentity.com](https://beyondidentity.com)

[info@beyondidentity.com](mailto:info@beyondidentity.com)

BEYOND  
IDENTITY