# Beyond Identity and Cybereason Integration

## Enable Zero Trust Authentication for secure identity and device access

## Benefits

**Secure Access:** Provide phishing-resistant, passwordless, and policy-based authentication

**Device Trust:** Ensure expected endpoint security controls are in place and enforced at the point of authentication

**Continuous Authentication:** Continuously assess device security controls throughout the user session

**Automated Response:** Automatically quarantine any device that falls out of compliance

## Market Challenge

The rise of remote work in a cloud-centric world has completely dissolved the traditional castle-and-moat security perimeter. In this new era, users are accessing critical applications and resources with weak credentials from anywhere in the world on devices that are not authorized or lack adequate security controls. Despite ongoing training efforts, users will inevitably click on phishing links, leading to potential credential compromise. As a result, threat actors are compromising identities by the use of valid credentials and exploiting inadequately secured devices in order to spy, steal, and hold business for ransom.

Legacy multifactor authentication (MFA) methods fall short of solving this problem because they cannot establish strong identity validation given their reliance on shared secrets and weak, phishable factors. This explains why roughly half of all external breaches can be attributed to credential theft. The increase of signing fools attacks, where the attacker can phish a user and trick them into signing their challenge, creates further vulnerability. And even when these tools do broker access for the correct identity, they cannot decipher between a legitimate managed device and an illegitimate insecure device. To compound this challenge, what happens when an authenticated device is compromised during a session?

## Joint Solution

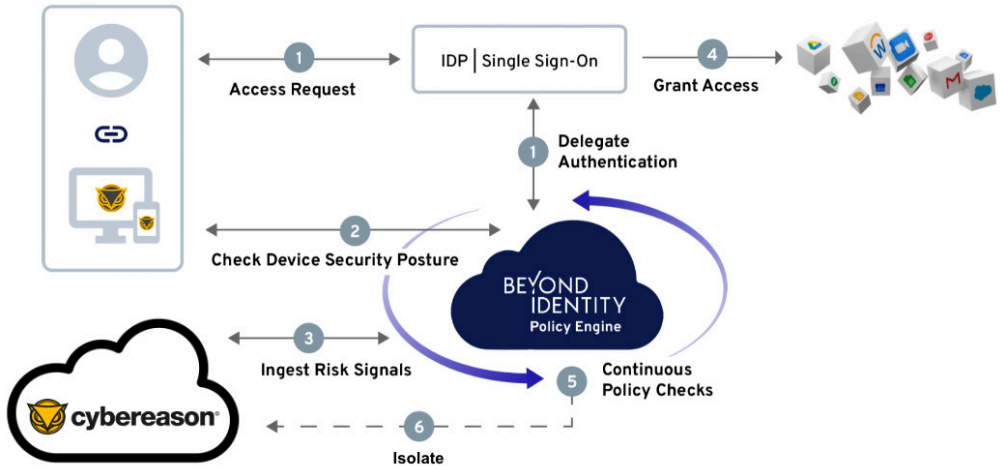
Organizations need to combine strong identity validation, device trust based on granular risk telemetry, and continuous device posture checks and policy enforcement. Beyond Identity Secure Workforce and Cybereason EDR seamlessly integrate to provide this end-to-end coverage, which is called “Zero Trust Authentication.”

Beyond Identity validates identity by eliminating all phishable

factors such as passwords and one-time passcodes, replacing them with phishing-resistant factors -asymmetric cryptography and biometrics. Security is then augmented by a policy-based device inspection that checks for the presence and configuration of the Cybereason agent, and ingests risk signals that indicate device compromise. In this way, the integration serves as a preventative security tool to stop threat actors before they get through the door. After a session is established, Beyond Identity and Cybereason continuously monitor the security posture of the device, ensuring adherence to precise authorization policies throughout a session. And if a policy is violated at any time, Beyond Identity automatically signals Cybereason to isolate the out-of-compliance device, thereby ensuring automated security coverage.

***"Combining Beyond Identity Secure Workforce and Cybereason EDR provides security-minded organizations the toolset required to apply end-to-end zero trust principles with seamless and best user experience" - Alan Idelson, CISO***

1. End user initiates access, and IdP delegates to Beyond Identity phishing-resistant MFA
2. At the point of authentication Beyond Identity ensures the user/device are authorized and device posture meets security policy, including presence of the Cybereason agent
3. By ingesting risk signals from Cybereason, Beyond Identity will authenticate only devices that meet policy
4. Phishing-resistant MFA to authorized applications
5. Continuous validation of the device, including Cybereason agent and risk signals to ensure the device continues to meet security policy
6. Automated isolate action signal when Beyond Identity's continuous authentication detects a device out of compliance




## 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 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 and stay connected with us on Twitter, LinkedIn, and YouTube.