

# CrowdStrike and Beyond Identity

How CrowdStrike and Beyond Identity enable Zero Trust Authentication

## Challenge

In a cloud-centric world, users access applications and resources from anywhere, at anytime and with any device. This reality dissolves the framework of a corporate network security perimeter where everything within the network is trusted implicitly. Exacerbating the problem, the rise of remote work, increase in bring-your-own-device (BYOD) and proliferation of SaaS applications have expanded the attack surface and opened visibility gaps, creating opportunities for lateral movement and significant security vulnerabilities outside of the traditional perimeter.

## Solution

By implementing a Zero Trust security framework, teams can go beyond the “implicit trust” perimeter-based approach and apply a “never trust, always verify” strategy where every action on the network is considered a potential threat, enabling a more effective response to the dynamic security challenges of today. Zero Trust is highly incompatible with passwords as an authentication method and legacy MFA methods that rely on phishable factors. Achieving Zero Trust in this area – called Zero Trust authentication – rests on three core tenets: strong identity validation, device trust based on granular risk telemetry, and continuous device posture checks and policy enforcement.

Beyond Identity helps organizations achieve their Zero Trust strategy starting with password elimination, replacing shared secrets with a public-private key pair

Passwords and legacy multifactor authentication (MFA) methods fall short of establishing strong identity validation given their reliance on shared secrets and weak, phishable factors. This helps explain why 80%+ of cyberattacks leverage identity-based techniques to compromise legitimate credentials, according to the 2023 CrowdStrike Global Threat report. And devices themselves, if left unprotected, can have malware, missing security patches or misconfigured security settings. To compound this challenge, what happens when an authenticated device is compromised during a session?

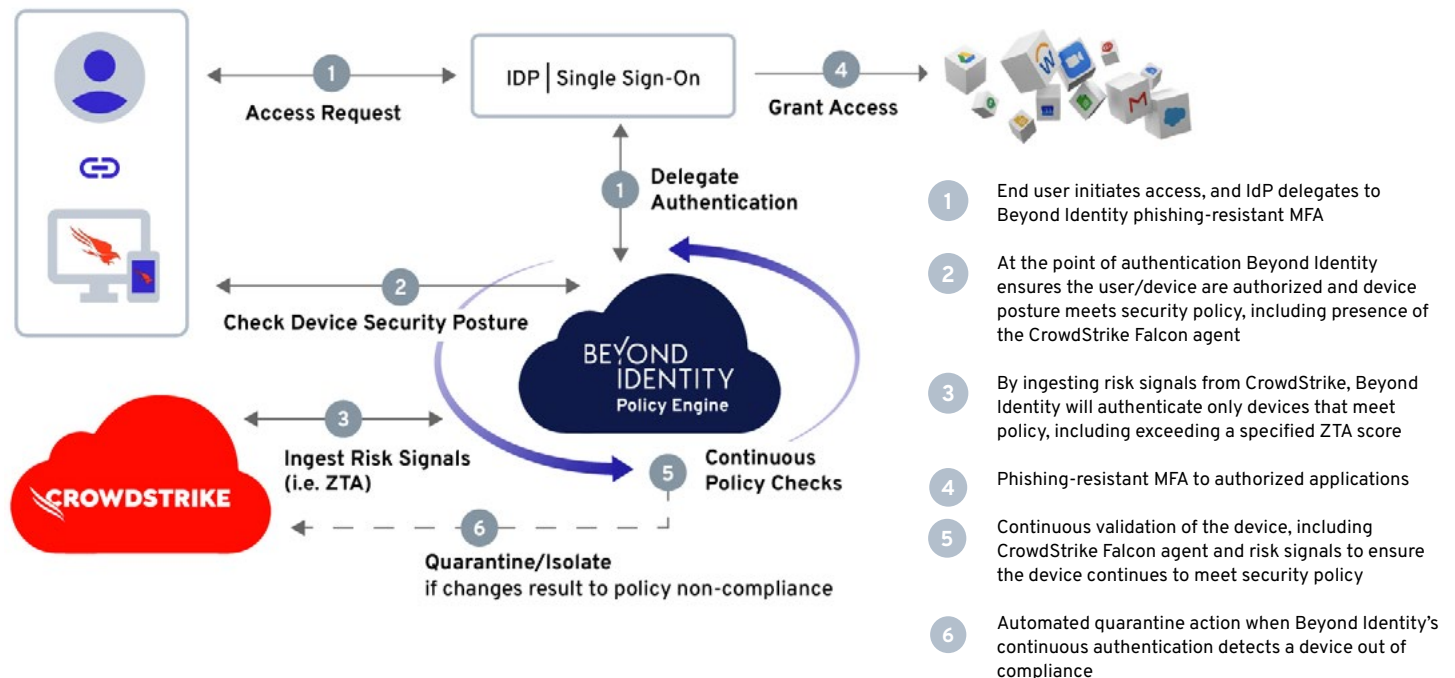
that cryptographically validates user identity for every authentication. Beyond Identity then continuously inspects the authenticating device’s security posture throughout the session, leveraging native and third-party ecosystem risk signals.

The Beyond Identity integration with the CrowdStrike Falcon® platform augments an organization’s ability to enforce device trust by validating the presence of the Falcon agent on the endpoint and ingesting CrowdStrike user and device risk signals derived from CrowdStrike Falcon Zero Trust Assessment (ZTA) scores. In this way, organizations can continuously monitor their security posture and ensure adherence to precise authorization policies throughout a session, quarantining devices that fall out of compliance.

# Business Value

Use case	Solution	Benefits
Establish device trust with every endpoint at the time of authentication.	Beyond Identity ensures the Falcon agent is installed, running and up-to-date at the time of authentication for all endpoints requesting access.	Ensure your devices are protected and enforce security hygiene for all endpoints accessing your environment.
Reinforce device trust by leveraging CrowdStrike risk signals.	At the point of authentication, Beyond Identity leverages Falcon ZTA device risk signals to inform and enhance access policies.	Increase device trust and strengthen access policies by leveraging additional risk signals from the Falcon ZTA score.
Continuously assess and manage risk, and quickly take action.	While legacy MFA solutions authenticate only at login, Beyond Identity and CrowdStrike continuously monitor and enforce granular, risk-based access policies, establishing trust in the user and the device throughout a session. If a device falls out of compliance or the Falcon ZTA score drops below a threshold, Beyond Identity can automatically call on CrowdStrike to quarantine the offending device.	Continuously verify trust in users and devices to prevent visibility gaps and high-risk actions, helping you automatically protect the organization.
Replace passwords with phishing-resistant MFA.	Beyond Identity only uses phishing-resistant factors to ensure high assurance in user identity and device security for every authentication: local biometrics or PIN, device-bound passkeys and device security posture checks.	Upgrade to phishing-resistant MFA to prevent credential theft, and safeguard your resources from the growing number of cyberattacks that leverage identity-based techniques to compromise legitimate credentials.

# Technical Solution



Beyond Identity is a trusted CrowdStrike Store Partner providing identity and device assurance for continuous, risk-based authentication, leveraging the Falcon platform's telemetry and risk signals to enable Zero Trust Authentication (ZTA).