How Beyond Identity Secures Its Workforce with Our New CrowdStrike Integration

BEYOND IDENTITY

CROWDSTRIKE

Like most of our customers, Beyond Identity is on a zero trust journey. We leverage our own zero trust authentication to establish high trust in the user identity and the endpoint device.

During each authentication transaction, and continuously thereafter, the solution evaluates device security and incorporates additional risk signals to ensure that only endpoints that meet our risk policies are granted and maintain access to resources.

After taking the step of eliminating passwords and implementing strong, phishing-resistant authentication, Beyond Identity sought to further leverage the power of other tools in our security stack, including CrowdStrike. CrowdStrike protects and monitors our endpoints, and a recently released integration between CrowdStrike and Beyond Identity enables our policy engine to incorporate the CrowdStrike Falcon Zero Trust Assessment (ZTA) score in our risk-based authentication decision. With the integration we can deny access to any endpoint with a ZTA score below our policy threshold—an important added layer of protection at the point of authentication. Then, on a continuous basis, devices with ZTA scores that fall below this threshold, or devices that fail other risk-policy checks, can be quarantined using the CrowdStrike's Network Contain capability.

Beyond Identity faces the same security challenges many of our customers face

- We have a largely dispersed workforce.
- Our employees work both on company-managed hardware as well as personal devices.
- Employees need access to different resources and software applications depending on their responsibilities.
- We need to ensure endpoints are secure and meet security requirements.

Ease of use

Beyond Identity's authentication is designed to be frictionless to our workforce—both employees and a few contractors. Our team wanted to make authentication both secure and an easy user experience to ensure adoption and maintain productivity levels.

For administrators, the process of integrating CrowdStrike and Beyond Identity is a three-step process. The first two steps—setting up the API key and adding the key on the Beyond Identity admin console—took less than ten minutes. The third step was integrating CrowdStrike into our risk-based policy engine and we did that in two stages.

Stage one: Monitoring. It was important to analyze how CrowdStrike worked in our environment by monitoring the potential effect of the policy. The rule was set to a Monitor state. This allowed us to collect login data on the range of reported ZTA scores and make an informed decision, in line with our security policies, where to set the ZTA threshold, as we didn't want to inadvertently lock out a user. We use monitor mode rules to ensure the intended effect for other policy changes.

Stage two: Enforcement. The next step involves using the data we glean from Beyond Identity metrics and logs to determine when we want to set our enforcement policies. Once those policies are set, the system can react immediately to potential threats by denying access or instructing CrowdStrike to quarantine the device.

Benefits of the Beyond Identity and CrowdStrike integration

Zero trust programs are a team sport achieved through integrations and security ecosystem data sharing to strengthen defenses. The risk protection achieved with the Beyond Identity platform is enhanced by the CrowdStrike integration. Here are the benefits we've achieved.

We **set policies** that determine device security using CrowdStrike Falcon and the device's ZTA score in partnership with our policy engine to deny access if security measures have been circumvented on the device.

New employees are **prevented from accessing critical resources** if the device is not managed by CrowdStrike. New employees can use a personal device they want to enroll with Beyond Identity, but they are denied access to anything other than email and their calendar until they receive the company-provided gear with CrowdStrike installed.

We **leverage CrowdStrike when enforcement action is needed.** If a device's security posture falls outside of specific policies Beyond Identity instructs CrowdStrike to quarantine the device.

The results speak for themselves. The combination of Beyond Identity and CrowdStrike create a solid foundation for our zero trust program. We believe it and utilize the integration.

Beyond Identity

Beyond Identity is revolutionizing secure digital access for workforces, contractors, customers and developers. Our Universal Passkey Architecture provides the industry's most secure and frictionless multifactor authentication that prevents credential-based breaches, ensures device trust, and delivers secure and frictionless digital access, eliminating passwords entirely. Industry leaders like Snowflake, Unqork and Roblox rely on Beyond Identity to solve their access security challenges for their customers, employees, contractors and developers and to advance their journey toward Zero Trust Security. To learn more about Beyond Identity's solutions and innovations, visit www.beyondidentity.com and stay connected with us on Twitter, LinkedIn, and YouTube.