Continuous Authentication and Crowdstrike

Defending a static perimeter around a physical network is no longer an effective method of protecting your organization. Protecting dispersed workforces, cloud-based software solutions, and other resources located outside of an organization's physical location requires an increased emphasis on cyber security.

Attacks on your resources are no longer a "what if" situation. It's a matter of when it is going to happen. Each month, an increasing number of attacks and breaches fill news feeds. So how do you prevent a bad actor from breaching your security perimeter? By constantly evaluating risk signals and establishing a zero trust architecture to properly protect your data and control access to your resources.

Continuous authentication, establishing a policy of never trusting any user or device, even after initial authentication, is vital to effectively protecting your resources.

The risks of perimeter-based systems

Continuous authentication, when user and device risk are assessed in real time both at time of authentication and on an ongoing basis during authenticated sessions, has become essential to a zero trust approach to cybersecurity. This is because traditional, perimeter-based systems that use first-generation multi-factor authentication (MFA) instead of continuous authentication can only assert that a user knows a password and has access to a known device one time prior to giving access. This means if a device is compromised after the user is already logged in, the entire system is vulnerable to being breached.

"Castle and moat" security may have been secure enough in the past, but the move toward cloud-based software makes such systems look less like castles and more like open venues with people and devices, both managed and unmanaged, streaming through.

Users are accessing applications and resources at any time, from any location, and with any device. This has created numerous new risks. Older systems operating with implicit trust—where people are logging in and automatically gaining access to all parts of the network—can be more easily abused by bad actors looking to steal data.

It is unsurprising, then, that numerous large corporations have recently experienced cyberattacks due to security holes in their cloud-based systems. The monetary price of this can be enormous: according to an IBM report, failing to use zero trust solutions leads to an average cost of $5.4 million per breach. On top of the monetary hit, organizations then have to deal with lost trust and a damaged reputation.

The Beyond Identity and CrowdStrike integration —never trust, always verify

The urgent need for continuous authentication is why Beyond Identity partnered with Crowdstrike to provide an integration that enables companies to:

- Continuously monitor and enforce risk-based access policies with the ability to quarantine devices based on real-time security signals.
- Establish fundamental building blocks of zero trust that are in accordance with NIST guidelines with phishing-resistant, frictionless MFA.
- Establish strong device trust using real-time risk signals prior to and during authentication.

With the integration between Beyond Identity and Crowdstrike Falcon, Beyond Identity can make an API call to Crowdstrike and quarantine any device that does not meet policy requirements during the initial authentication, or at any point during the user's session by continuously validating user and device security posture.

Making sure all access requests are continually vetted in this manner, and denying access to any endpoint that falls out of compliance, guarantees the most up-to-date, secure authentication possible.

- Beyond Identity continuously requires verification that:
- The user requesting access to a given resource is authorized to do so.
- The device they are using to log in to the resource holds the proper credentials.
- The device meets the necessary security and compliance requirements, such as ensuring the CrowdStrike Falcon agent is running on the device.

The Beyond Identity and Crowdstrike integration allows your admins to customize the security and compliance requirements you need to secure your resources in the cloud with visibility and fine-grained control. For example, you can specify that devices without Crowdstrike Falcon installed and/or with a zero trust assessment (ZTA) score of less than 50 should be denied access.

Or you can specify that devices with Crowdstrike Falcon running , but whose ZTA scores are still less than ideal—between 50 and 75, perhaps—should be prompted for additional biometric verification. And if at any time a device falls out of compliance, for example a firewall is disabled or Crowdstrike Falcon is uninstalled, its access will be immediately removed.

Beyond Identity and Crowdstrike protect your resources

Are you ready to move to a simple to implement zero-trust, continuous authentication system powered by Beyond Identity? Beyond Identity verifies each of your users by cryptographically binding identities to their devices, which enables passwordless authentication and phishing-resistant multi-factor authentication with a zero-friction user experience.

Book a demo today and see how Beyond Identity's continuous authentication capabilities can help you ensure your cloud-based resources are secure.

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.