BEYOND IDENTITY CROWDSTRIKE

Beyond Identity & CrowdStrike Integration

Combine Beyond Identity and CrowdStrike Falcon to enable zero trust with continuous, risk-based access

Challenges

In a cloud-centric world, users can access applications and resources from anywhere, at any time, and with any device. This reality completely dissolves the framework of a corporate network security perimeter. Exacerbating the problem, the rise of remote work, bring-your-own-devices (BYOD), and proliferation of SaaS applications means that the implicit trust of perimeter-based security models creates opportunities for lateral movements and significant security vulnerabilities.

Passwords and legacy multi-factor authentication (MFA) methods fall short of establishing strong identity validation given its reliance on shared secrets and weak, phishable factors. Devices themselves can have malware, missing security patches, or misconfigured security settings. Furthermore, what happens when an authenticated device is compromised during a session?

Solution

Responding to these vulnerabilities gave rise to the idea of zero trust. Zero trust is a security framework based on the notion of "never trust, always verify" which eliminates the implicit trust that defines the "castle and moat" perimeter-based approach to security. Given the need for strong identity assurance, passwords and MFA that rely on phishable factors are fundamentally incompatible with a zero trust strategy.

CrowdStrike stops breaches in real-time and Beyond Identity prevents credential-based breaches by eliminating the single largest source of attacks – passwords. The Beyond Identity and CrowdStrike integration enables companies to achieve their zero trust strategies consistent with NIST Guidelines with unphishable MFA, establish strong device trust using real-time risk signals at time of authentication, and continuously monitor and enforce risk-based access policies using granular user and device signals.

Key Benefits

- Establish fundamental building block of Zero Trust with unphishable, frictionless MFA
- Replace passwords entirely with X.509 certificates, and cryptographically bind identity to device
- Validate the security posture of the authenticating device in order to establish trust, leveraging the CrowdStrike Falcon agent presence and CrowdStrike's ZTA score
- Continuously enforce granular, risk-based access policies, establishing trust in the user and the device with the ability to quarantine devices based on real-time security signals

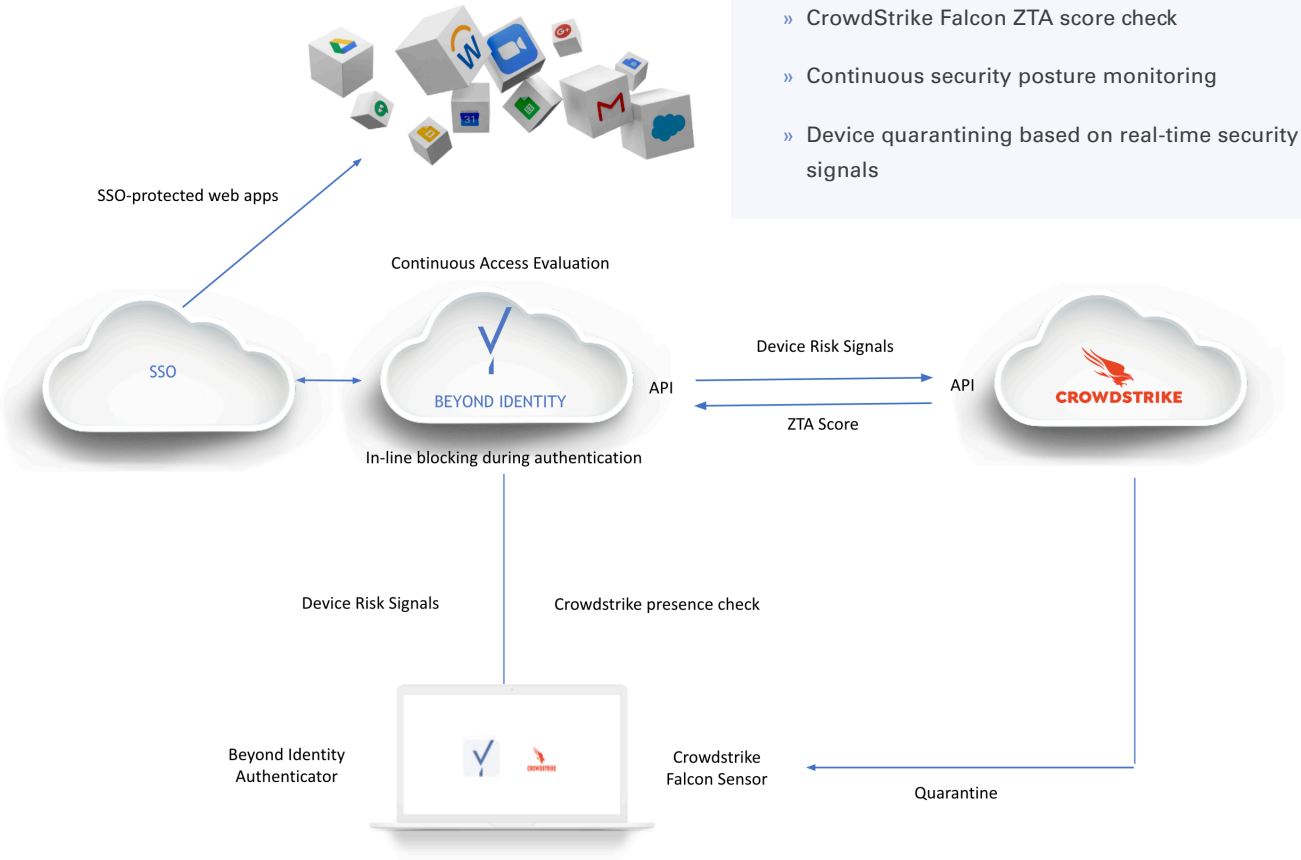
Business Value

Use Case	Solution	Benefits
Replace passwords with unphishable multi-factor authentication (MFA) that provides cryptographic proof of user identity	"Never trust, always verify" is the basis of zero trust. However, as long as passwords are being used, no company can genuinely claim it is compliant with that principle. Beyond Identity's platform replaces the password with unphishable, secure credentials based on X.509 certificates and public-private key pairs. In this way, Beyond Identity cryptographically binds the user's identity to their device. These keys can never leave the device, and every log in is frictionless and completely secure.	Remove the most insecure authentication method and bind identity to device
Establish device trust with every endpoint at point of authentication with CrowdStrike Falcon Agent Validation & Presence Check	Beyond Identity's customizable device posture and device trust policies include the ability to validate software and configurations. At time of authentication, Beyond Identity is able to validate the presence of the CrowdStrike Falcon agent on the endpoint as well as properties of the installation such as the verison, confirm running state, etc.	Establish trust with all endpoints by ensuring that they have the CrowdStrike agent installed, running, and up to date at the time of authentication to all or selected applications
Establish device trust with every endpoint at point of authentication with CrowdStrike Falcon ZTA score integration	At the time of authentication, Beyond Identity leverages the Falcon ZTA API, which allows IT admins to write more fine-grained authentication policies based upon the ZTA Overall Score. This capability allows Beyond Identity and CrowdStrike customers to not only ensure the installation and state of the agent on the machine at time of authentication, but adds additional context that leverages Falcon ZTA's monitoring of 120+ different unique endpoint settings- including sensor health, applied CrowdStrike policies, and native operating system (OS) security settings.	Greatly augment device trust by leveraging the additional risk signals captured by the CrowdStrike Falcon ZTA score
Continuously assess and manage risk	While most MFA solutions will only authenticate upon login, Beyond Identity and CrowdStrike continuously monitor and enforce granular, risk-based access policies, establishing trust in the user and the device during every identity transaction. Beyond Identity continuously validates: » Is this an authorized user requesting access to a given resource? » Is the device they are using to log in to the resource authorized to do so? » Does the device meet the security and compliance requirements? (i.e. Is the CrowdStrike Falcon agent running on the device? Is the device's ZTA score within the acceptable limits?)	More closely adhere to Zero Trust principles by continuously monitoring the security posture of both internal and external assets that have access to the organization's network.
Continuously monitor user and device security posture with the ability to quarantine non-compliant endpoints during authenticated sessions	User and device attributes are dynamic. Go beyond simply monitoring user and device security posture to taking action with the ability to quarantine endpoints that fall out of compliance with your security policies during authenticated sessions	Achieve continuous verification to ensure that all access requests are vetted in an ongoing manner and deny access to any endpoint that does not meet security policies
Give you users a better a experience	These granular security checks are invisible to the user as they are running in the background. Additionally because the authenticator exists on the authenticating device, there is no need for users to find a second device. The joint solution is a rare case of having your cake and eating it too…and seamlessly inspecting the cake to make sure it isn't poisoned.	Increase MFA adoption. No passwords for your users to remember or reset and no need to pick up a second device to type in a one-time code or respond to a push notification

Technical Solution

Key Solution Capabilities

- Passwordless MFA
- CrowdStrike Falcon presence check
- CrowdStrike Falcon ZTA score check
- Continuous security posture monitoring
- Device quarantining based on real-time security signals



Description

- Upon an authentication request, the Beyond Identity Authenticator signs a challenge from the Beyond Identity Cloud with the private key stored on the TPM of the device
- As part of that ritual, the device security posture is natively assessed across 70+ Device Risk Signals
- With the CrowdStrike integration, an additional check is made for the presence and current state of the CrowdStrike Falcon Sensor
- A second security posture check is made through an API call to the CrowdStrike Cloud to retrieve the authenticating device's Falcon ZTA Overall Score
- If either the CrowdStrike presence check fails or the Falcon ZTA score is not above the policy threshold, access is blocked
- The Beyond Identity Authenticator sends this device information on a continuous basis with the ability to quarantine devices during authenticated sessions

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

About Beyond Identity

Beyond Identity is fundamentally changing how the world logs in with a groundbreaking invisible, un-phishable MFA platform that provides the most secure and frictionless authentication on the planet. We stop ransomware and account takeover attacks in their tracks and dramatically improve the user experience. Beyond Identity's state-of-the-art platform eliminates passwords and other phishable factors, enabling organizations to confidently validate users' identities. The solution ensures users log in from authorized devices, and that the device meets the security policy requirements during login and continuously after that. Our revolutionary approach empowers zero trust by cryptographically binding the user's identity to their device and analyzing hundreds of risk signals on an ongoing basis. The company's advanced risk policy engine enables organizations to implement foundationally secure authentication and utilize risk signals for protection, rather than just for detection and response. For more information on why Intuit, Snowflake, and Roblox use Beyond Identity, please visit www.beyondidentity.com.