CrowdStrike Store Partner

BEYOND IDENTITY

CROWDSTRIKE

Data Sheet

CrowdStrike and Beyond Identity: Continuous, risk-based authentication

Enable Zero Trust authentication for secure identity and device access

Challenges

In a cloud-centric world, users access applications and resources from anywhere, at any time 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.

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 CrowdStrike 2023 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?

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.

Key Benefits

- Validate the security posture of the authenticating device to ensure only compliant, low-risk devices with the CrowdStrike Falcon® agent gain access
- Continuously evaluate identity and device trust, and quarantine non-compliant devices
- Prevent stolen credentials and simplify users' experiences by going passwordless
- Establish a fundamental building block of Zero Trust with phishing-resistant, effortless MFA

CrowdStrike Store Partner

CrowdStrike and Beyond Identity

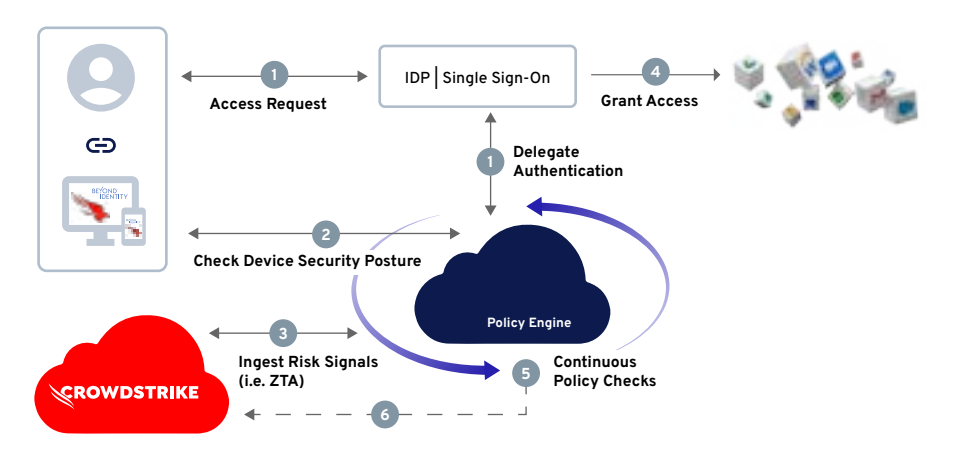
Beyond Identity helps organizations achieve their Zero Trust strategy starting with password elimination, replacing shared secrets with a public-private key pair that cryptographically validates user identity for every authentication. Beyond Identity then continuously inspects the authenticating device's 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



1. End user initiates access, and identity provider (IDP) delegates to Beyond Identity phishing-resistant MFA
2. At the point of authentication, Beyond Identity ensures the user/device are authorized and the device posture meets security policy, including presence of the CrowdStrike Falcon agent
3. By ingesting risk signals from CrowdStrike, Beyond Identity will authenticate only devices that meet policy, such as being within a specified ZTA score
4. Phishing-resistant MFA secures access to authorized applications
5. Continuous validation of the device, including monitoring risk signals and ensuring the presence of the CrowdStrike Falcon agent, ensures the device continues to meet security policy
6. Automated quarantine action is taken when Beyond Identity's continuous authentication detects a device out of compliance

CrowdStrike Store Partner

CrowdStrike and Beyond Identity

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.

About 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. The company's 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, Unqork, and Roblox 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 FIDO2 certified multi-factor authentication (MFA) solutions, visit beyondidentity.com and stay connected with us on Twitter, LinkedIn, and YouTube.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

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

Follow us:

Try the app in the CrowdStrike Store