BEYOND IDENTITY

Zero Trust Authentication Request for Information (RFI)

Sample Questions

Purpose

This document is designed to assist organizations by providing a foundational set of requirements for the successful definition and deployment of phishing-resistant multi-factor authentication with the option to expand to device trust and ultimately achieve zero trust authentication. These requirements are based on hundreds of interactions with industry analysts, industry pundits, and end-user organizations and their IT, identity, and security teams.

Section 1: Zero trust principles and architecture

Organizations can prevent credential-related breaches and minimize related risk through implementation of zero trust authentication.

1. Outline how the solution helps organizations make material progress with zero trust initiatives.
2. Describe how the solution leverages the FIDO Standards (ideally FIDO2) and which certifications have been achieved to date.
3. Explain how the solution aligns to current industry standards and/or best practices.

Section 2: Multi-factor authentication (MFA)

Multi-factor authentication is established best practice as an important security control to protect business critical resources.

1. Explain how the solution enables multi-factor authentication.
2. Describe how the solution aligns to current industry standards and/or best practices.
3. Detail the end-user experience that employees, consultants, contractors, and even third-party agents can expect and how it is different from other MFA solutions.

Section 3: Passwordless

Removing passwords from authentication, aka passwordless, removes the most breached vector. Passwordless authentication is a basic step to protect the organization.

1. Describe how the solution does or does not use passwords.
2. Explain how the solution aligns to current industry standards and/or best practices.

Section 4: Phishing-resistant MFA

As previously stated, MFA is best practice, but not all MFA is created equal. Attacks against legacy MFA solutions are increasing in volume due to use of phishable factors (e.g. OTP and SMS codes). Phishing-resistant MFA protects your organization by replacing weak, second factors with passkeys/biometrics.

1. Provide an overview of what makes the solution phishing-resistant.
2. Detail how phishable MFA techniques like push codes or push with number match, and when/where are these used.
3. Explain how the solution aligns to current industry standards and/or best practices.

Section 5: Validate user and device

Validate the user and device through unique identification of the user/device combination and cryptographically confirming this identity.

1. Detail how the solution validates the user and device.
2. Describe in detail how passkeys are used.
3. Explain how the private passkey is shared between multiple devices.
4. Provide an overview of certificate management requirements.

Section 6: Device security controls assessment

Reduce the attack surface by confirming the device security controls align with your organization's security requirements.

1. Describe how the device security controls are validated at initial authentication.
2. Detail how the policy engine supports incorporation of device security settings into the authentication flow when evaluating transaction risk. Include examples.
3. Organizations must provide access for various classes of users, including internal users (full time employees, administrators, executives), external users, and contractors. This diverse user community includes both corporate managed and unmanaged devices. Explain how secure authentication can be provided to each class of user/device combination.
4. Explain how security settings of unmanaged devices, such as for bring your own device (BYOD) and contractors devices are evaluated

Section 7: Risk signals in authentication decisions

Protect applications and the business data through intelligent authentication decisions that evaluate endpoint and cloud risk signals.

1. Outline how the solution supports risk-based decisions. In particular, how the policy engine evaluates device risk and/or state.
2. Describe the device security signals the solution captures natively.
3. Detail any additional signals used with integrations to systems such as MDM, EDR, and SASE.

Section 8: Continuous evaluation of device security settings

Minimize risk of human error and bad actor efforts by continuous validation of device security settings.

1. Provide the frequency the connecting device is re-assessed.

Section 9: Security infrastructure integration

Detailed immutable, authentication details can improve risk detection, accelerate identification of suspicious activity, and meet reporting and audit requirements.

1. Explain how authentication details are shared with security operations teams to improve risk detection and accelerate identification of threats.
2. Explain how the solution provides tamper-proof logs to support audit and reporting requirements.

Section 10: Enterprise readiness

Large organizations demand a deep set of technical and usability requirements.

1. Describe end user MFA experience for each of the in-scope operating systems; Windows, MacOS, Linux, iOS and Android.
2. Detail how IT teams can easily manage device fleets, allow only permitted devices and identify potentially suspicious devices.
3. Describe the solutions SaaS, cloud-native architecture. If not a SaaS platform, outline the product implementation/ integration, including any needed servers/databases/etc and the expected related costs.
4. List and explain each distinct administrative console required to manage the solution.
5. Document functionality surfaced via API's to facilitate automation of administrative tasks.
6. Outline how the solution architecture supports global organizations operating in different geographies.
7. Explain how the deployed architecture supports reliability, availability, and serviceability.

Wrap-up

This document detailed a foundational set of requirements for definition and deployment of phishing-resistant authentication with the option to expand to provide device trust and ultimately achieve zero trust authentication.

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. Its 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 FIDO-2 certified multi-factor authentication (MFA) solutions, visit beyondidentity.com and stay connected with us on Twitter, LinkedIn, and YouTube.