Zero Trust Authentication:

Laying the Foundation for Zero Trust Security

BEYOND IDENTITY

Businesses have long relied on traditional password-based authentication and more recently first generation MFA methods for user access, but these can be challenging to manage and are vulnerable to cyberattacks. Fortunately, there's a solution: Zero Trust Authentication.

Let's look at the problems of password-based and current MFA authentication, the advantages of Zero Trust Authentication, how it works, and key benefits your organization can expect when you implement a zero trust architecture built on a foundation of Zero Trust Authentication powered by Beyond Identity. Strong authentication is the first steps toward Zero Trust security strategy

Disadvantages of traditional authentication methods

Passwords are incredibly vulnerable and challenging to manage. Traditional multi-factor authentication (MFA) solutions utilize weak second factors—one-time passwords (OTPs), SMS push notifications, or phishable magic links.

Current authentication systems also fail to consider important contextual information, such as who is making the request, what device settings are being used, when and where the authentication request is happening, or any identity beyond username and password. Security for full-time employees is often prioritized over contractors, agents, employee personal devices, and third parties that may need access to company resources. And those devices are often at a higher risk of compromise.

This means authentication decisions are made with limited information. Some include location or time as an added layer of security, but still don't consider device settings. Integration between MFA solutions and other security measures is minimal, resulting in a siloed system focused only on authentication.

Zero Trust Authentication: An alternative to traditional MFA

A Zero Trust Authentication solution must focus on seven requirements that ensure your organization is well-equipped for modern threats and risks.

1. **Passwordless:** Passwords and shared secrets are fundamentally insecure as seen in the cyberattacks happening every day.
2. **Phishing-resistant:** Phishing-resistant MFA uses factors like cryptographic keys and biometrics, which do not rely on trust because the key is tied to the device.
3. **Cryptographically validating user device:** You need to verify device possession and that the device is authorized to access resources. Validation should also prevent access by devices vulnerable to compromise.
4. **Ability to evaluate device security posture:** Ensure devices are compliant and meet security standards.
5. **Incorporate many types of risk signals:** Utilizing risk signals and a robust policy engine allows you to either block access if risky or abnormal behavior is detected or require step-up authentication for high-risk situations.
6. **Continuous authentication:** Risk-based access at login isn't enough. To achieve Zero Trust Authentication, the solution must continuously verify the user's identity and their authorization to access sensitive resources.
7. **Integration with existing security infrastructure:** Leverage the entire security ecosystem to institute robust authentication decisions to secure resources. This requires the sharing of data between tools in the security ecosystem to improve risk detection.

Zero Trust Authentication functionality

Traditional authentication methods result in a wide variety of security issues, forcing organizations to make compromises. This leads to an increased risk of phishing, breaches and potential negative financial impact. To help protect data and resources, Beyond Identity offers a high level of assurance that verifies the user's identity and the device accessing your sensitive resources.

- Beyond Identity eliminates the need for passwords with its phishing-resistant multi-factor authentication. You'll always know who's remotely accessing your resources and environment. It also cryptographically binds user identities and devices together to guarantee that only approved devices gain access.
- You can set specific security device posture thresholds for internal users, contractors, and third-party vendors at the point of authentication.
- The Beyond Identity policy engine can analyze multiple risk signals, allowing for intelligent authentication decisions to be made quickly.
- Continuous authentication helps maintain a secure environment by ensuring all

devices remain compliant and sanitized. If an endpoint is compromised, or security settings are tampered with, Beyond Identity can send a signal to your endpoint security platform to end the privileged session immediately

- Detailed, immutable authentication logs are integrated into your system, making it easier to detect risks quickly, respond faster to suspicious behaviors, and boost audit and compliance reporting capabilities.

All of this occurs frictionlessly so you can increase your security posture and enhance the user experience.

Beyond Identity and Zero Trust Authentication

- **Minimize breaches:** By utilizing passwordless authentication, you can protect your organization from malicious actors.
- **MFA protection:** The use of cryptographic passkeys and biometrics provides a higher level of protection than traditional MFA.
- **Validate user and device:** Unique identification of the user and device combination helps reduce the attack surface by confirming all devices accessing sensitive resources meet your required security standards.
- **Intelligent authentication decisions:** By analyzing multiple risk signals with existing authentication factors, your security team can make intelligent decisions about granting access to keep applications and data safe from malicious actors.
- **Continuous validation and risk monitoring:** For an extra layer of protection, continuous validation against device security settings keeps users safe from human error or malicious intent. Detailed logs make it easier to detect suspicious behaviors quickly and accurately.

Want more information? Read our white paper on Zero Trust Authentication. For a more in-depth discussion, download the Zero Trust Authentication: Securing User And Device Access For A Distributed, Multi-Cloud World ebook.

Ready to implement a Zero Trust Authentication solution? Book a demo today.

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.