Zero Trust and Continuous Authentication

BEYOND IDENTITY

In the United States alone, 58% of employees across a range of sectors now have the option to work remotely at least one day a week. This tectonic shift to remote and hybrid work, combined with the existing growth in cloud and mobile device usage, has created a myriad of potential new security vulnerabilities. And while companies have invested in the technology to support remote work, many are underprepared for the corresponding change in their threat landscape.

Although the old castle-and-moat approach to cybersecurity may have worked in the past, simply defending a static perimeter around a physical network is no longer enough. In the face of a growing attack surface, zero trust is the key to enabling a high level of security while allowing your employees freedom in how and where they work.

True zero trust requires authenticating users more frequently, so how do you strengthen security without harming user experience? We'll show you.

Why do you need a zero trust security architecture?

- The average number of cyberattacks per company increased by 31% between 2020 and 2021
- Insider threat incidents have increased by 44% over the past two years
- Cybercriminals can breach the local network perimeter of 93% of companies
- The average cost of a data breach reached $4.35 million in 2022
- 66% of people use the same password across multiple accounts
- Almost 50% of data breaches stem from stolen credentials

Zero trust requires a mindset shift

No single technology or solution can help you achieve zero trust; it's a framework on which to build a security program. Adopting a "never trust, always verify" approach means no source is trusted by default, whether it's located inside or outside the traditional network perimeter. Every user, packet, interface, or device that attempts to access your corporate network must be authorized, authenticated, and encrypted—wherever it originates.

Further, microsegmenting the network and only granting users the minimum level of access necessary makes it far more difficult for malicious actors to compromise network security. If they succeed, they're unable to move laterally within the network, ensuring damage is contained.

A user or device passing your initial authentication checks is not the end. Compromised, negligent, and malicious insiders are a significant and growing risk, and with limited insight into what users are doing post-login, a security breach is almost impossible to detect in real time. Creating a true zero-trust framework requires continuous authentication.

Validate – then continuously authenticate

Only by constantly evaluating risk signals can you set a strong foundation for a zero-trust architecture that properly protects your data and controls access to applications and other resources, whether on-premises or in the cloud. Continuous authentication, therefore, requires that you never trust any user or device, even once they are authenticated.

How do you make continuous authentication actually continuous?

To successfully incorporate continuous authentication into your zero-trust architecture and ensure that it is, indeed, continuous, your security team should address the following key points:

- **Eliminate transitive trust:** Every user or device must be authenticated and authorized to access data or applications and then continuously authenticated to keep that access. Single sign-on combined with passwordless MFA can reduce friction for the user, while an architecture that cryptographically ensures only authorized devices gain access lets you establish a high level of trust in a device.
- **Enforce your endpoint security policy:** Consider your organizational security policy for endpoint devices and ensure that it's met each time a device connects to your network. For example, you may want to specify that a device is not jailbroken or rooted, has a firewall activated, is protected by the corporate approved EDR/XDR solution, and has biometrics enabled.
- **Continuously analyze risk signals:** An essential component of continuous authentication is checking risk signals at short time intervals to detect any changes in device state or user behavior. This near real-time visibility gives you the opportunity to take appropriate action to contain any perceived threats.

Your authentication process must be seamless and completed in the background to avoid disrupting employee productivity and harming user experience. You may, however, want to request additional authentication factors (such as biometrics) if you can't establish a satisfactory confidence level in a user or device or in specific cases, such as requests for sensitive data or privileged actions.

How to seamlessly implement continuous authentication

With Beyond Identity, you can implement and support a zero trust framework in your organization without making your users jump through hoops. Our frictionless solution enables security teams to

securely authenticate users, validate the initial device security state, then continuously monitor their behavior and device security posture for a multitude of risk signals.

To ensure strong and continuous authentication, we:

- **Use robust phishing-resistant MFA:** Rather than using weak factors like one-time codes, SMS messages, and magic links that malicious actors can intercept, we establish trust in the user's identity with our passwordless MFA platform. This process takes place on the same device, further reducing friction.
- **Enable device trust:** Our architecture lets you cryptographically ensure that only authorized devices can access your resources. You have full control over your risk policies and can define what meets your "authorized" criteria. For example, you can decide whether to allow or deny access to BYOD, contractors' devices, mobile phones, or tablets. This is the first step in establishing an appropriate level of trust in the device.
- **Confirm the device's security posture:** You have the ability to ensure the endpoint device complies with your organization's security model before allowing it to access resources. To enforce this, we check dozens of device security posture settings during every authentication transaction.
- **Monitor continuously:** It's a disturbing fact that things do change post-login, but we can help you catch incidents. Every 10 minutes, we poll the device to see if there are any changes in user behavior factors, and we monitor the device's security posture settings. For example, we can check if the user's geolocation has unexpectedly changed, whether they're downloading an unusual type of data, or if the firewall has been disabled after login. We do this invisibly, behind the scenes, with no input needed from the user, making it 100% frictionless.
- **Offer an integration with CrowdStrike:** If a device fails to meet your policy requirements during or after initial authentication, you can automatically quarantine it using CrowdStrike. For example, if the firewall is turned off on a device post-login, you can revoke access immediately and potentially disrupt an attack in progress.

Adding continuous authentication to your zero trust program strengthens your security to dynamically handle the changes in your organization's threat landscape. To find out how Beyond Identity can help you seamlessly implement zero trust without damaging your user experience, book a demo today.

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.