Phishing-Resistant, Low Friction MFA Advances Zero Trust Security

BEYOND IDENTITY

What is zero trust and why does it matter?

You've likely seen the term "zero trust" a lot lately. It's quickly becoming an industry buzzword, with every company claiming to offer zero trust solutions. The truth is, zero trust security is a complex, multi-faceted framework that requires your entire system of resources to work together in a way that provides optimal protection. While all of those companies (including Beyond Identity) can offer resources and elements that help you institute a zero trust framework, no one company offers every element of zero trust security.

The core concept of zero trust (you might also think of it as earned trust) is that no person, device, or software module is inherently trust-worthy. When you implement zero trust security any request to access your resources must provide enough information to earn trust. Not only that, the trust earned extends only to the specific assets that user or device needs to perform a specific task.

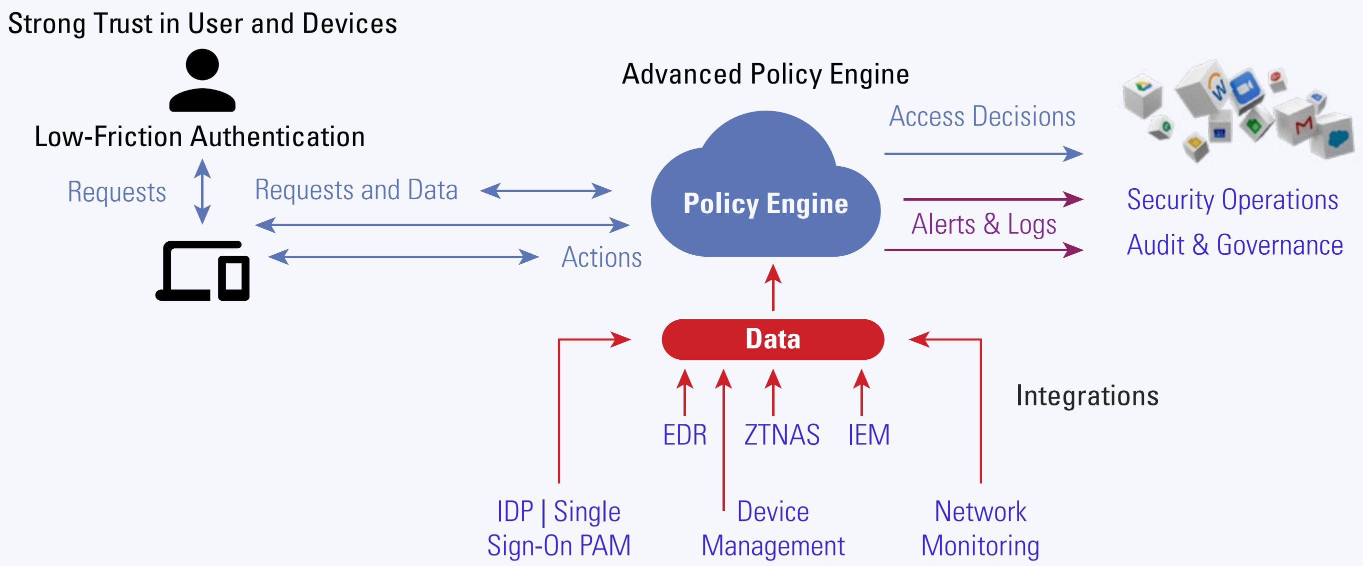
The key principles of zero trust are:

- No user or device is inherently trust-worthy ("never trust, always verify")
- You need to limit access based on the level of trust established
- User and device access is limited to the assets needed to perform a task
- Risk-based access decisions leverage as much information as possible
- Continually revisit the level of trust as new information becomes available
- The process of providing information to earn trust must be secure and reliable
- The process of providing information to earn trust must not burden the user

How authentication plays a role in zero trust

Most zero trust frameworks focus on authentication and access control. NIST Special Publication 800-207, "Zero Trust Architecture," states "the crux of the issue [zero trust] … is the goal to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible."

Authentication is a vital aspect of zero trust security for a very good reason. Authentication is the process by which users and devices earn trust. Without accurate, continuous risk-based authentication, you have no parameters for granting access.



Requirements for effective authentication

Based on the zero trust principles and the recent experience of zero trust initiatives, we can identify seven requirements for effective authentication in a zero trust environment.

Strong user validation: passwordless and phishing-resistant

The foundation for any zero trust initiative must be strong user validation. Without near-absolute certainty that the user requesting access is who they say they are, the rest of the controls provided by zero trust environments are of limited value.

The key requirement for strong validation of users is a multi-factor authentication method that is both phishing-resistant and passwordless.

Traditional MFA has, up to this point, been the primary answer to password vulnerability. That is no longer the case. The ever-increasing number of breaches clearly shows the weaknesses caused by the use of phishable factors.

Strong device validation

Strong device validation is also critical for a zero trust environment. Many conventional MFA solutions use devices as secondary authentication factors. Attackers are then able to compromise those devices. Compromised endpoints are frequently used as the initial attack vector for unauthorized access.

Verifying that the device requesting access is bound to the user and is currently in that person's possession removes the risk that a device has been stolen. It also confirms the user isn't accessing resources from a compromised device. If compromised, attackers might capture user credentials or access target resources by hijacking a session created by the user.

Device security posture

When considering device security posture, Zero Trust Authentication makes two key assumptions:

1. Just because a device is managed doesn't mean it can be trusted
2. Just because a device has antivirus software installed doesn't mean it is free of threats

Validating device compliance, verifying the identity and integrity of the device before granting access—without respect to location, and confirming the device meets set organization security policies ensures the device meets security posture standards. Traditional MFA and perimeter-based security frameworks don't include this critical check and trust the device is up to the standards of the organization if it falls within the corporate perimeter.

Risk Signals

Collecting and analyzing risk signals is central to zero trust security. Authentication is not just checking one or two factors and making a yes or no access decision. Your policies should ensure that decisions are made based on risk assessments that incorporate both data and contextual information.

If the policy engine detects suspicious behavior or incorrect location data, it can alert your system to lock down the device in real-time. This increases your security posture by accounting for incidents that occur in between security checks in a traditional approach.

Continuous Risk Assessment

Assessing risk during the initial authorization isn't enough. For zero trust security, you must continuously verify user identity, device identity and security posture, and risk signals. Instead of a simple authentication system that trusts that user identity is enough, a risk-based policy considers the user's entire behavior and risk profile. This allows you to block access if the system detects risky or abnormal behavior during the session or you can ask for additional authentication for high-risk situations.

Integrations with IT management and security tools

Integrations are vital to zero trust security, and they are an integral part of authentication. Risk-based access decisions, which should leverage as much contextual information as possible, and the continuous assessing of user and device level of trust often involve the integration of multiple tools. The data collected by those tools is then sent to a policy engine, which makes access decisions based on the information.

Beyond Identity: phishing-resistant, frictionless MFA

Setting up your zero trust security plan doesn't have to be overwhelming. Beyond Identity offers a phishing-resistant, low-friction zero trust MFA solution that is completely passwordless and is frictionless for your users and your security team.

Beyond Identity adheres to zero trust principles, can be deployed quickly, and complements investments in other zero trust technologies such as zero trust network access (ZTNA) and network segmentation.

Want to know more about how you can make your zero trust security implementation a success? Read our white paper on 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.