HOW BEYOND IDENTITY REINFORCES YOUR ZERO TRUST STRATEGY

BEYOND IDENTITY

BEYOND IDENTITY

CONTENTS

EXECUTIVE SUMMARY

In a cloud-centric world, applications and users are no longer confined to corporate locations. Users access applications in the public or private cloud, at any time and from anywhere. When your customers and workforce frequently access apps and resources in the cloud from non-enterprise locations, the idea of enterprise-centric trust boundary loses any relevance.

Consequently, access control solutions like firewalls and virtual private networks (VPNs) designed for perimeter security fail to keep up with new attack vectors of a "perimeter-less" world. While many organizations turned to password-based multi-factor authentication (MFA) as a solution, the prevalence of weak authentication factors like passwords, SMS text messages, one-time codes, and magic links in these solutions remain ineffective against modern threats and are easily compromised and hacked. MFA must provide strong identity validations in today's threat landscape with fluid trust boundaries.

In a perimeter-less ecosystem, when your enterprise data, users, and applications are everywhere, your security policies and enforcement points must be everywhere too. That's the new shift in security thinking that zero trust promotes.

Zero trust is not any single product or solution. It is a security framework that eliminates implicit, transitive trust that underpins the perimeter-centric approach – it is a refutation of the idea that everything inside the corporate perimeter is trustworthy. In a "perimeter-less" world, zero trust never takes trust for granted. It advocates never trust, always verify. Thus, zero trust begins with strong identity validation. It verifies a user's identity and the security of transactions every time without relying on implicit trust. An ideal zero trust architecture goes a step further by establishing trust in every device and user accessing enterprise resources, not once but continuously.

This whitepaper examines the critical role of strong identity and device trust in any zero trust strategy and how Beyond Identity helps you implement the foundational requirements of a zero trust strategy as laid out by the National Institute of Standards and Technology (NIST) and General Services Administration (GSA).

ZERO TRUST: WHERE IS THE NEW TRUST BOUNDARY?

With zero trust, there is no universal perimeter—every single action and application has its own perimeter. Traditional security architectures relied on the corporate trust boundary, also known as the network perimeter. Perimeter security implies everything within the network perimeter is trusted implicitly. That's probably acceptable when applications, data, and devices are on-premises, and only company-issued devices could access enterprise resources over VPNs or later solutions like a cloud access security broker (CASB). However, the growing adoption of SaaS apps, remote and hybrid work, and bring-your-own-device (BYOD) policies have blurred this network perimeter.

For example, when employees remotely access SaaS apps from an airport or hotel lobby, the enterprise network and firewalls are entirely bypassed. Recognizing this blurring trust boundary, in 2009 Forrester alum John Kindervag first defined zero trust as a security framework that trusts nothing—regardless of whether the thing is inside or outside the perimeter. Zero trust back then was mostly confined to a theory. The years that followed saw a sharp rise in SaaS apps and remote work. Mobile workers and BYOD policies became ubiquitous. The workforce routinely accessed apps and resources from both managed and unmanaged devices.

In cloud-first organizations, where users constantly access company data from anywhere, using any device, "implicit trust" itself becomes a vulnerability.

The rise of remote work and BYOD further weakened the security posture of organizations relying on perimeter-based implicit trust.[1] Identity-related threats rapidly rose as a top attack vector. However, it was not until the massive shift to remote work following the pandemic that these factors reached "critical mass" proportions, making zero trust an imperative.[2]

66% of employers around the world are redesigning their workplaces to accommodate hybrid work arrangements.[3]

– Microsoft Work Trend Index

Distributed workforce requires organizations to move toward an architecture where trust is not implicitly granted, and access to enterprise resources such as servers, applications, networks, and data is granted primarily using the principle of least privilege every time.

KEY FACTS ABOUT ZERO TRUST

WHAT? Zero trust is not a product. It's a security strategy.

WHY? Prevent unauthorized access by always verifying users and devices anywhere.

HOW? First, verify, then continuously analyze and evaluate risks to users and devices.

ZERO TRUST BEGINS WITH STRONG IDENTITY AND DEVICE TRUST

In SaaS-dominant enterprises, user and endpoint identity is the new perimeter.

Zero trust allows for maximum freedom in how and from where your employees work and what device they use while maintaining a high level of trust. Zero trust proactively prevents unauthorized access by collecting and analyzing user data at the point of authentication to stop attackers from getting in the first place. To positively validate that users are who they claim to be, authentication using weak factors like passwords doesn't help. Passwords do not prove someone who they are, which attackers exploit to gain unauthorized access. Although MFA uses multiple factors, password-based MFA remains vulnerable to password exploits and fails to provide the strong authentication zero trust requires.

Strong authentication can only be achieved with stronger and more secure factors like biometrics built into modern devices, PIN codes, smart cards, hardware keys, credentials stored in

[1] https://heimdalsecurity.com/blog/common-network-vulnerabilities/

[2] https://www.forbes.com/sites/forbestechcouncil/2021/07/01/work-from-anywhere-get-hacked-from-anywhere-why-zero-trust-security-is-vital-for-remote-work/?sh=42f62e1c1a8f

[3] https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work

trusted platform modules (TPM), etc. These strong factors are the building blocks of unphishable, passwordless MFA.

But that's only half of the equation. In addition to positively authenticating users, zero trust insists that you can not trust the device on which the user is authenticating. Phishing campaigns are increasingly successful in making users download malware on the devices they use. The situation gets riskier when employees access enterprise applications and download company data while using unmanaged or BYOD devices. It becomes imperative to establish a high level of trust in devices. A malware-infected device can easily hoodwink your firewalls and identity and access infrastructure. You need a high assurance way to authenticate the user and the device. That's the only way to control who and what devices have access to your resources irrespective of where they are with respect to the trust boundary.

"Strong authentication and device trust are the starting point of zero trust."

If you can't provide high levels of identity assurance and device trust during every request, you have not addressed the foundational tenets of zero trust. In the zero trust framework, it is not enough to validate users and devices only once. Zero trust needs to assess user and device risk continuously. This eliminates transitive trust by ensuring strong identity claims.

Your identity solution must authenticate users and devices continuously while accessing company data and applications.

WHY PASSWORD-BASED SOLUTIONS FAIL AT ZERO TRUST

Before granting access to apps and company data, user identity must be validated with a high degree of assurance. That's where password-based MFA solutions fall short. Regardless of how long or complicated a password is, there's no dearth of reported breaches where hackers break into password databases and millions of credentials are compromised.[4] Phishing sites and credential theft malware do not care whether a password is four or four hundred characters. Passwords rely on trust without any proof that the device is safe and the user is who they say they are, there's no assurance provided by passwords. Along with passwords, these legacy MFA solutions rely on other authentication factors, like one-time codes or magic links, that are hacked easily (and often).

With passwords, you will never have zero trust.

Traditional, password-based solutions rely on transitive trust and lack granular access control. This is an impediment in implementing least privilege access control for users—which is a foundational tenet of zero trust. Another problem with password-based MFA solutions is meeting the basic requirement of zero trust: "never trust; always verify." This requires validating users and device identity at every access checkpoint. Moreover, usability challenges with password-based MFA often force security teams to limit MFA to only a few select apps or increase session timeouts for apps with MFA to as high as several days, weeks, or even months. Leaving sessions unauthenticated for such long periods contradicts zero trust.

[4] https://www.securelink.com/blog/81-hacking-related-breaches-leverage-compromised-credentials/

PSST! HEY, YOUR USERS HATE PASSWORDS AND MFA

From Salesforce to Bank of America, many business and consumer-oriented platforms use password-based MFA. Yet, the inconvenience and insecurity of passwords, along with the friction caused by numerous steps and devices, persists today.

- Only an estimated 11% of enterprise cloud users have adopted password-based MFA, even though MFA was the top security technology chosen due to global shifts to work from home in response to Covid-19[5]
- Of those who have not adopted, 43% have blamed the clunky user experience as the reason[6]
- Of those who have not adopted, 41% cited complexity as the reason[7]

KEY CONSIDERATIONS FOR ZERO TRUST STRATEGY

Implementing a zero trust strategy rests on three major pillars:

1. **Positively authenticate each user**

Eliminate passwords entirely from the authentication flow and directory. Cryptographically binding identities to devices provides immutable proof of identity and possession of the device to positively verify user identity claims.

2. **Positively identify each device**

Authenticate the device and ensure compliance by cryptographically binding identity to the device. Zero trust offers the flexibility of using any devices, whether company-issued, BYOD, or unmanaged. But before granting access, it's essential to positively validate the device is trustworthy.

3. **Continuously enforce security and compliance policies**

Device configuration may change during access rendering it less secure. It is important to continuously check device risk levels against predefined settings like firewall, disk encryption, or biometric authentication.

For implementing zero trust, you need to consider the key tenets from NIST SP 800-207.

[5] https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication/

[6] https://www.yubico.com/blog/75-of-enterprise-security-managers-plan-to-increase-mfa-spending-according-to-new-study-by-yubico-and-451-research/

[7] https://www.yubico.com/blog/75-of-enterprise-security-managers-plan-to-increase-mfa-spending-according-to-new-study-by-yubico-and-451-research/

NIST DEFINES THE SEVEN TENETS FOR ZERO TRUST

1. Every data source and computing service is a resource. This can include personally owned devices if they have access to internal resources.
2. Network location doesn't matter. All communication is secured, no matter its origin.
3. Access to a resource is only granted for that session. The network must re-authorize subsequent access.
4. Access to a resource is not a static concept. Missing security patches, a login that seems suspicious, and other factors may still block access even if the requesting client is authorized to view a particular resource.
5. An organization must continuously monitor the security posture of both internal and external assets that have access to the organization's network.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. Organizations should use the information collected from initial zero trust deployments to ease the transition and improve their security posture.

BEYOND IDENTITY HELPS ACHIEVE A ZERO TRUST STRATEGY BY BRIDGING AUTHENTICATION AND ENDPOINT SECURITY

Positively authenticate each user

Your organization cannot implement zero trust as long as it uses a fundamentally insecure knowledge-based authentication method: the password. Beyond Identity entirely eliminates passwords from the authentication flow. We ensure strong authentication by replacing passwords with highly secure credentials based on X.509 certificates and public-private key pairs cryptographically bound to the device's TPM. Device-binding irrefutably authenticates users and cryptographic protocols "prove" the user's identity requesting access, every time at the point of authentication.

Positively identify each device

Beyond Identity bridges strong authentication with robust device trust. Beyond Identity employs real-time security posture checks at the time of authentication that eliminates "implicit trust" while establishing device trust as close to authentication and access as possible. Restricting access dynamically in real-time based on the security state of the device and the strength of factors attesting for user identity is a key tenet of zero trust.

The zero trust framework is based on the assumption an attack is already underway. Beyond Identity's risk-based authentication of each device requesting access at the time of authentication blocks lateral movement in real-time. We empower you to change resource access requirements in real-time, and to employ step-up authentication, for example, for users identified (micro-segmented) as having a higher risk. Beyond Identity uses contextual analysis to assess the trustworthiness and risk associated with every device before granting access. If a device is not appropriately secured, it will not be allowed to access resources.

Continuously enforce security and compliance policies

Beyond Identity ensures adherence to organizational device security policies across all devices, whether company-issued or not. Access is never granted to company-issued devices by virtue of being organizationally-owned, nor to users based on their location. This satisfies the fundamental tenet of zero trust: never trust, always verify. To monitor device health continuously, Beyond Identity uses contextual factors and analyzes them in real-time to provide device posture information, creating immutable logs of authentication requests. When paired with your security information and event management (SIEM) tools, this same data collection can be leveraged to inform your overall security strategy. By continuously monitoring all devices for security policy adherence before access, Beyond Identity ensures the security of your cloud resources.

Beyond Identity supports highly granular authorization policies with precise, customizable risk policies. These policies are informed by real-time analysis of risk and trust that limits access to resources based on device security posture, location, and other factors. This enables you to implement another key tenet of zero trust—fine-grained, least privilege access that grants users access only to those resources that they need to perform their tasks.

STARTING DOWN THE PATH TO ZERO TRUST WITH BEYOND IDENTITY

Removing the concept of trust from a network goes a long way in securing it. Zero trust requires users and devices to authenticate themselves every time, regardless of their location. Zero trust also enforces granular security policies based on real-time risk and trust analysis that limit access to resources based on device security posture, location, and other factors. User access is limited to only the files and data they need for the given task. Device health is

checked continuously to establish device trust.

With Beyond Identity, your zero trust strategy complies with NIST's seven zero trust tenets. NIST's zero trust architecture considers every data source and computing service as a resource. Beyond Identity enables you to secure all resources, including cloud applications and systems, administrative functions like credentials for server access, by removing the most common attack vector — passwords — from the authentication flow and logging the activity of users requesting access. Access to systems and services in the cloud is granted to only authorized users and devices. Together, these controls are highly effective in improving an organization's security posture in today's cloud-centric world.

You can use Beyond Identity to replace your existing identity solution or, use it in tandem to integrate additional layers of security. Our platform integrates seamlessly to support your security tools like mobile device management (MDM) and endpoint detection and response (EDR). It requires no dedicated resources for continuous maintenance. We automatically enforce device security policy compliance via our on-device client and deny access based on your organization's customized rules and policies.

Beyond Identity helps you implement the critical tenets of zero trust. Our hardware-based authenticator cryptographically binds a device to a proven user identity at enrollment to ensure strong authentication and device trust and uses contextual factors to monitor device health constantly. With Beyond Identity, you can achieve zero trust to protect your organization while providing the most secure and frictionless authentication experience.

ABOUT BEYOND IDENTITY

Beyond Identity provides the most secure authentication platform in the world. Breaking down barriers between cybersecurity, identity, and device management, Beyond Identity fundamentally changes the way the world logs in–eliminating passwords and providing users with a frictionless multi-factor login experience. Beyond passwordless, the company provides the zero-trust access needed to secure hybrid work environments, where tightly controlling which users and which devices are accessing critical cloud resources has become essential. The advanced platform collects dozens of user and device risk signals during each login - enabling customers to enforce continuous, risk-based access control. The innovative architecture replaces passwords with the proven asymmetric cryptography that underpins TLS and protects trillions of dollars of transactions daily. Customers turn to Beyond Identity to stop cyberattacks, protect their most critical data, and meet compliance requirements.