The Rise of Zero Trust Authentication

BEYOND IDENTITY

How phishing resistant, passwordless authentication advances zero trust security

Why Zero Trust Is Top-of-Mind

The way enterprises work has changed profoundly in the past few years. "Zero trust" is the cybersecurity community's leading response to the challenges of our new world.

Until recently, the default work scenario for most enterprises was employees in offices, using devices managed by the IT group, connecting to applications in corporate data centers from the wired corporate network. In this scenario, access controls and monitoring at the perimeter of the enterprise's network ensured adequate security for most data. The small number of workers outside the perimeter could be forced to accept inconveniences like complex VPN dial-in procedures.

Today, the default scenario is WFH and BYOD with SaaS, PaaS, and IaaS.[1] A large proportion of employees and computing resources are outside the protection of the network perimeter. The "enterprise workforce" has expanded to include a diverse population of contractors, independent agents, partners, and suppliers. Both internal users and customers at large no longer tolerate intrusive and cumbersome security methods.

Finally, there is widespread recognition that our primary methods for authenticating users – passwords, augmented with some flavor of weak multi-factor authentication (MFA) – are wholly inadequate. Passwords and weak MFA are fundamentally insecure, for reasons we discuss in this document. They are also expensive to support, error-prone, and burdensome to employees and customers.

Experts and industry leaders have responded to these developments by rethinking cybersecurity. The concept of the secure perimeter has been supplanted by a new framework known as "zero trust."[2]

[1]Work from Home, bring your own device, software as a service, platform as a service, infrastructure as a service.

[2]The term "zero trust" was originally popularized by the industry analyst firm Forrester. The original framework has been amplified and extended by other industry analysts (notably Gartner, who contributed ideas such as CAT – continuous adaptive trust), government and standards bodies such as NIST and OWASP, leading-edge enterprises, and cybersecurity solutions vendors.

Key Principles of Zero Trust

The term "zero trust" could easily be "earned trust." The core concept is that no entity (person, device, or software module) is trusted by default, the way computers on the corporate LAN were in the past. Instead, any request to access computing assets must provide enough information to earn trust. When that trust is granted, it extends only to the specific assets required to perform a task, and for a limited timeframe.

This core concept has a number of corollaries. One of the most important is that the process of providing information to earn trust must be secure, reliable, and easy for the requestor. Experience shows that any approach to zero trust that can't meet these conditions is not practical in the real world.

For the purposes of this document, we can summarize the key principles of zero trust and its major corollaries as:

- No entity is granted trust by default (sometimes rendered as "never trust, always verify")
- Access must be limited based on the level of trust established
- Access must be limited to the specific assets needed to perform a task (i.e., apply the principle of least privilege)
- Risk-based access decisions should leverage as much contextual information as possible
- The level of trust should be revisited continually as new information becomes available; it is not a "once and done" proposition
- The process of providing information to earn trust must be completely secure and reliable
- The process of providing information to earn trust must not place unacceptable burdens on people requesting access.

The Role of Authentication

Most zero trust frameworks focus on two topics:

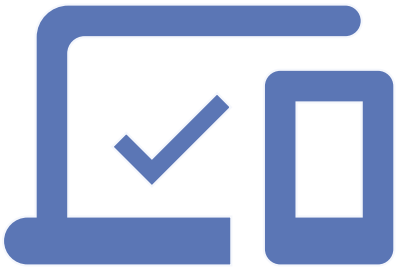
- Authentication (gathering and using information to establish a level of trust)
- Access control (segmenting networks and controlling access to resources based on identity and the level of trust)

For example, 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." (emphasis in original)

Why is excellence in authentication so important to zero trust?

From a theoretical perspective, authentication is the process by which entities prove their ownership of a trusted identity. Without accurate, data-rich, continuous, risk-based authentication, there is no basis for granting (and limiting) access.

From a practical perspective, effortless authentication is the key to acceptance by users. If authentication is too burdensome, employees, contractors, and others will find shortcuts around it and subvert security. If the user experience is too difficult, users will bombard the help desk with support requests. Some users, for example C-suite executives, will demand less obtrusive alternatives that result in security degradations such as setting long session timers to reduce the frequency of authentication prompts, or even turning off MFA altogether.



A good starting place

Enterprises starting their zero trust journey should consider addressing authentication very early in the process. Zero trust authentication can provide immediate wins for a zero trust initiative by:

- Immediately improving security, especially by eliminating passwords and replacing weak MFA with inherently secure strong authentication methods.
- Streamlining, personalizing, and transforming user experiences
- Reducing costs and administrative challenges related to managing passwords and multiple device or token-based MFA tools
- Protecting against the latest threats featuring MFA prompt bombing and other increasingly popular MFA bypass attacks

In addition, zero trust authentication is relatively easy to deploy.

The rest of this document will provide an overview of the requirements for zero trust authentication and approaches to meeting them.

Authentication Requirements for Zero Trust Environments

Based on the zero trust principles outlined earlier and our recent experience with zero trust initiatives, we can identify several requirements for effective authentication in a zero trust environment. Several of these are shown in Figure 1 (below), and the rest in Figure 2 (on page 10).

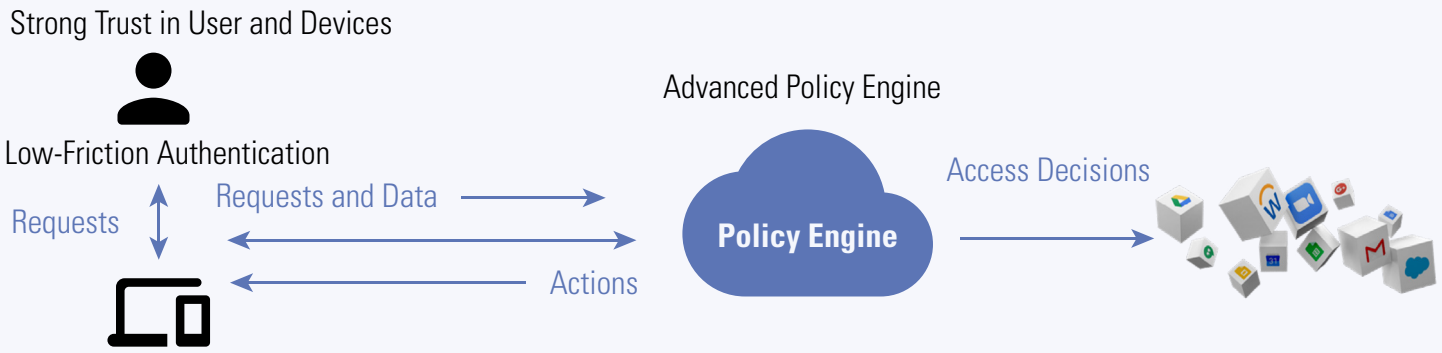


Figure 1: Requirements for effective zero trust authentication (part 1)

1 Strong trust in user identities

The starting point for any zero trust initiative must be establishing strong trust in user identities. Unless we can furnish near-absolute certainty that the people requesting access to assets are, in fact, the authorized users (and not threat actors impersonating those users), the rest of the controls provided by zero trust environments are of limited value.

The key requirement for establishing strong trust in users is a multifactor authentication method that is both **phishing resistant** and **passwordless**.[3]

Authentication methods that rely on passwords and shared secrets are fundamentally insecure. Threat actors commonly obtain passwords through phishing and social engineering, discover them using brute force attacks, or simply buy them on the dark web, where prices for credentials vary from a fraction of a cent to a few dollars.

People frequently reuse passwords across business and personal accounts and social media platforms. Many of those passwords have been compromised by data breaches and put up for sale on the web, enabling attackers to reuse them when targeting corporate data.

Technical solutions to these problems, such as password managers, do not remove the password from the authentication equation. They are also cumbersome and usually fail the test for low-friction authentication (discussed below). Lastly, most of these technical solutions rely on master passphrases that can be captured, exposing all of the user's passwords. In short, technologies like password managers attempt to mitigate a fundamentally flawed approach to authentication without eliminating the root cause of the problem.

MFA was once seen as the answer to the password vulnerability. It was thought that the inconvenience to users of grabbing their phone, inputting a one time password (OTP), or replying to a push notification was more than offset by the fact that threat actors could not steal that second factor.

[3] For an example of how security leaders are now mandating authentication that is both phishing resistant and passwordless, see the text box below with excerpts from the U.S. Office of Management and Budget memorandum "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." The same push is coming from regulators in industries such as finance: see the New York State Department of Financial Services memo "Guidance on Multi-Factor Authentication."

Unfortunately, that last assumption has proven to be unfounded. Threat actors have developed techniques to capture second (and third) factors such as using:

- Phishing emails to drive users to a spoofed landing page that requests the OTP or confirmation code.
- SIM swapping to have codes and notification methods sent to the threat actor instead of the user's smartphone.
- Man-in-the-middle and man-in-the browser attacks to intercept codes and steal session keys[4]
- MFA prompt bombing[5]

The crux of the problem with weak MFA solutions is that the authentication process is that any password or code is vulnerable. Information in a user's head can be phished. Passwords in a database can be hacked. Codes traversing a network (which are really just passwords with a special name to make them sound secure) can be intercepted. Using a second, special password to make a first password more secure will not stop intelligent attackers.

We will discuss an approach to phishing resistant, passwordless MFA in the "Meeting the Requirements" section later in this document.

A memorandum from the U.S. Office of Management and Budget published in January 2022 sets forth a zero trust architecture strategy for federal agencies and establishes requirements in a number of areas related to zero trust. Titled Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, it contains unequivocal statements that secure authentication must eliminate reliance on passwords and use "phishing resistant MFA":

> ***"Strong authentication is a necessary component of a zero trust architecture, and MFA will be a critical part of the Federal Government's security baseline...Agencies must integrate and enforce MFA across applications involving authenticated access to Federal systems by agency staff, contractors, and partners."***

> ***"However, many approaches to muti-factor authentication will not protect against sophisticated phishing attacks…For agency staff, contractors, and partners, phishing resistant MFA is required."***

> ***"Agencies must require their users to use a phishing resistant method to access agency-hosted accounts. For routine self-service access by agency staff, contractors, and partners, agency systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications."***

Note: the memorandum defines phishing resistant authentication as:

> ***"authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system."***

[4] For more details on how MFA solutions can be phished and hacked, see the Beyond Identity blog post How Your MFA Can Be Hacked (With Examples).

[5] In MFA prompt bombing (sometimes called an "MFA fatigue attack"), a threat actor attempts to log into an application with a user's stolen credentials. The authentication solution protecting the application pushes a verification request to the user (e.g.: "Did you just attempt to sign in? [Yes] [No, that's not me]"). If the user rejects the request, the threat actor tries again, and again, and again until the user gives in and approves the request. Boom! The attacker completes the login and gains access to the application. For more background, see Wired, A Sinister Way to Beat Multifactor Authentication.

2 *Strong trust in devices*

Establishing strong trust in devices is also critical in a zero trust environment. Threat actors have found many ways to subvert weak MFA by compromising or stealing user devices, or by exploiting situations where users log in from insecure devices. Reliable zero trust authentication is only possible when those types of attacks can be prevented.

Three elements can be used to establish strong trust in devices:

1. Verifying that the device making the request is in the possession of an authorized user.
2. Verifying that the device itself is registered with the authentication solution and authorized to access resources
3. Determining if the device's security posture complies with policy; that is, that it has the expected configuration and that security controls are installed and enabled as defined by the organization's security policies

Verifying that the device being used is in the user's possession and is authorized to access resources removes the risk that the device has been stolen, or that it never belonged to the user at all. It also prevents the user from logging in from a personal or home computer or a device especially vulnerable to compromise, such as a computer or kiosk in a library, an internet cafe, or a hotel lobby.

It seemed like a good idea at the time

Here is a scenario that, unfortunately, is not uncommon:

The chief financial officer on a business trip, in a hotel lobby, gets a (legitimate) text to transfer money from the organization's bank account to a vendor. Rather than going to get the laptop currently in a room on the 24th floor, the CFO uses a computer in the hotel's business center to make the transfer, confident that the organization's (weak) MFA solution makes access to the accounting system secure. However, a threat actor who has previously compromised that shared computer is able to capture the CFO's PIN, access the accounting system, and transfer funds to an offshore account.

The authors of the U.S. Office of Management and Budget memorandum cited earlier include a mandate for device trust as part of zero trust authentication:

"Agency authorization systems should work to incorporate at least one device-level signal alongside identity information about the authenticated user when regulating access to enterprise resources."

In that same vein, NIST 800-207, while discussing determining access to resources by dynamic policy, states;

*"Access to resources is determined by dynamic policy—**including the observable state of … the requesting asset… An organization protects resources by defining what resources it has**, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need."*

Establishing strong trust in devices is key to fulfilling those conditions.

As for the third point, to establish strong trust in a device, it is necessary to ensure that (a) the device is correctly configured, and that (b) all the security controls required by the organization's policies are installed and enabled. Unless both of these conditions are met fully, there is an unacceptable risk that the device may have been compromised and could be under the control of an attacker.

There may be situations where an organization decides that devices can be trusted for some activities without testing for all of the conditions we have discussed here; that is a policy decision. However, a zero trust authentication solution must be able to establish all of these elements if that is what the organization's policies require.

3 *Low-friction authentication for users (and administrators)*

Avoiding employee and customer resistance

The French philosopher Michel de Montaigne once wrote: "The smallest annoyances disturb us the most."

Unfortunately, small annoyances, like forgetting where we left the darn phone and which password goes with this or that account, disturb a lot of people to the point where they undermine security. Many employees use the same password for multiple business, personal, and social media accounts. C-level executives and other users with clout (lawyers, top sales people, doctors in healthcare settings, etc.) demand exceptional treatment, such as limiting or turning off MFA challenges. IT and security staff exclude themselves from burdensome authentication procedures.

Oops

A few years ago, the desktop admin team at a Fortune 50 company deployed a sticky-keys root shell to over 250,000 computers. This saved the team hours of work on trouble tickets every week.

Unfortunately, it also allowed anyone to take administrator-level control of any desktop computer by hitting the shift key five times.

As a result, many organizations face so much resistance to MFA that they only implement it for selected applications with inescapable compliance requirements, to specifically audited environments and accounts, or to employee groups where the use of MFA is a condition for cyber insurance coverage. A recent Microsoft study found that only 20% of users with Active Directory accounts were using MFA. And they often set session timers to days, or even weeks or months, giving an attacker an extended window of opportunity.

This market evidence makes it clear that a zero trust authentication solution must not only establish strong trust in users and devices, it cannot unduly annoy employees and customers.

Reducing work for administrators and support staff

Password-based authentication and weak MFA both create a huge volume of work for administrators and support staff. This includes managing processes and infrastructure for creating, storing, and resetting credentials, for managing OTPs, push notifications, and verification apps, and for shipping, replacing, and resetting hardware tokens and dongles. It also involves creating, deploying, and maintaining the security policies that govern password complexity, access, step-up authentication, and other elements of these processes. Finally, a significant amount of overhead is required to educate users and provide hand-holding when they get stuck or have issues.

These activities drive up costs and absorb staffing when most organizations face a shortage of qualified personnel. In fact, expanding the use of advanced authentication is only sustainable if the burden on administrators and support staff can be reduced.

4 *Integrations with IT management and security tools*

Integrations to acquire data

Two of the key principles of zero trust listed earlier are that risk-based access decisions should leverage as much contextual information as possible and that the level of trust must be revisited continually as new information becomes available. To achieve these goals, a zero trust authentication solution must collect a wide range of data about users, devices, and transactions on a recurring basis so a policy engine can make access decisions based on the latest information.

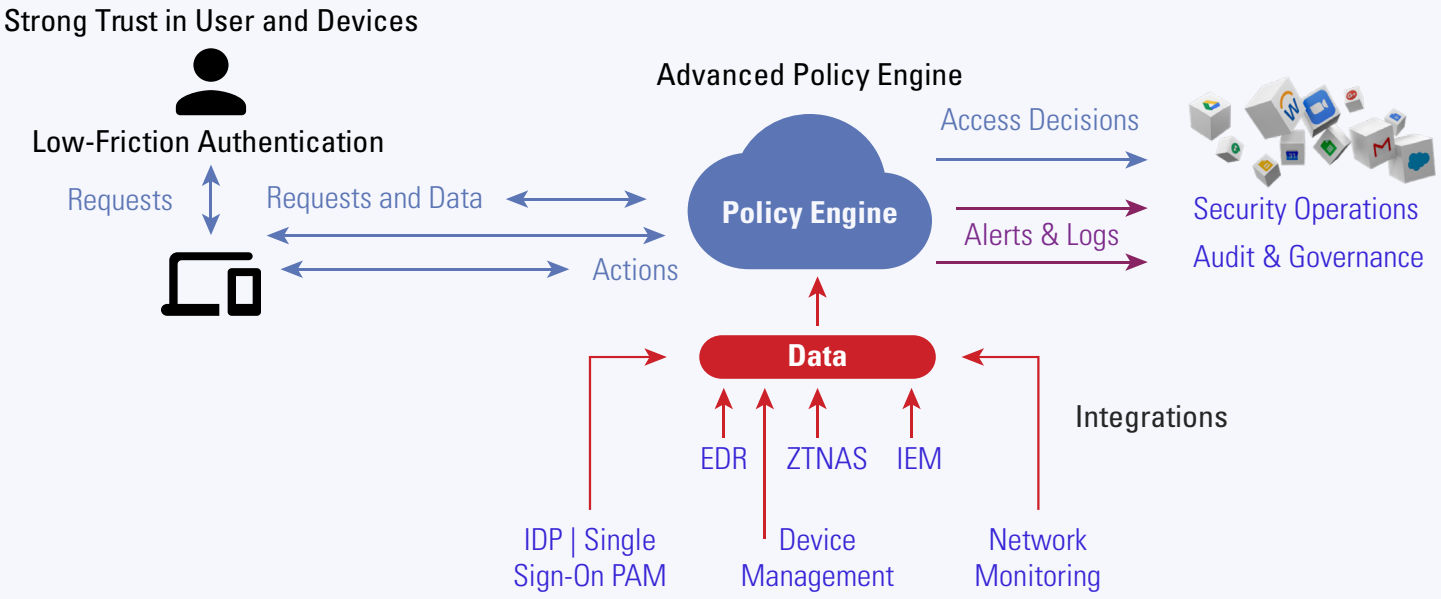
The contextual data needed for risk-based access decisions comes from a number of IT management and security tools. Examples of the types of data and their sources are listed in Table 1.

Why is the continuous assessment of risk based on large amounts of contextual information so important? Ant Allan, an analyst at Gartner, has articulated the reasons in a description of what he calls "continuous adaptive trust," or CAT.

Allan makes the point that accurate risk assessments cannot be made simply by counting authentication factors or evaluating a few pieces of data related to the user and the device. Instead, zero trust authentication decisions should be made on the basis of credentials (not including passwords) plus a large amount of contextual data related to the device, the network, and geolocation. Further, the data must be reevaluated continuously and trust levels revised based on new information.

	Data	Sources
User	Identity Permissions Role	Single sign-on tool Identity management platform Privileged access management (PAM) tool
Device	Security posture Software levels Security features enabled TPM (aka, Secure Enclave) enabled Custom Attributes	Authentication solution Endpoint detection and response (EDR) tool Device management/Mobile device management (MDM) system
Transaction	Login activity Transaction requests Geolocation	Authentication solution Network/cloud monitoring system
Analytics	Risk score	Risk management system

These integrations, as well as the ones discussed below, are illustrated in Figure 2.



Integrations to alert, log, and improve operations

As we will discuss in a moment, a zero trust policy engine will use this data and policy rules to make risk-based decisions about actions. Additional integrations are needed so those actions can be carried out. That includes, of course, communicating decisions to permit or block access to policy enforcement points such as identity providers (IDPs), EDRs, zero trust network access (ZTNA) products. It also includes:

- Sending alerts and notifications to security operations centers (SOCs) so they can react more quickly and accurately to threats
- Sending log data to aggregation points such as a SIEM or an enterprise data lake for further analysis, analysis that can yield actionable insights into attacks and help security teams analyze and improve their policies and operations.
- Providing trustworthy data to auditing systems and governance applications, especially accurate data about access requests, approvals, and denials.

5 *Advanced policy engine*

The final requirement for effective zero trust authentication is a policy engine that can apply the enterprise's security policies to control access to information assets. NIST calls this element the "Policy Decision Point/Policy Enforcement Point" or "PDP/PEP," and it's where all the elements of zero trust authentication come together.

Let's touch on some of the key functions of the policy engine.

Defining security policies

A good policy engine starts with a clean user interface that makes it easy for a security team to define authentication policies for their user communities. This includes policies on how to assess risk levels and rules on what actions to take based on the user's identity and permissions, the request being made, contextual information, and risk scores generated by the authentication solution or external analytics and risk management systems.

To meet the needs of zero trust authentication, the policy engine needs to be flexible enough to handle a wide variety of use cases. As we mentioned in our discussion of low friction authentication, it must also be easy to create, deploy, and maintain policies, so these activities don't overwhelm security teams. It must be able to perform these duties across a range of user types, including employees, contractors, agents, and customers.

Associating context with users and devices

The policy engine must be able to associate context data with users and devices. To scale to tens of thousands of devices, the collection process should be automated and operate without perceptible impact on the devices or the network.

Ideally, a zero trust authentication solution should allow data to be captured by management and security tools, or by the authentication solution itself, or by some combination. For example, a zero trust authentication solution should be able to leverage an MDM or EDR agent on devices where those are installed, yet also collect data directly from the device when they are not. This last capability is especially important when devices belong to contractors and to employees in a BYOD setting, because the IT group cannot deploy MDM or EDR agents on those devices to perform data collection.

Collecting data from IT management and security tools

As we discussed in the integrations section, above, a zero trust policy engine needs access to data from a wide range of IT management and security controls in order to make accurate assessments of risk. In some situations it is desirable to leverage risk scores from analytics and risk management systems rather than raw data.

Evaluating data and initiating actions based on policy

The core function of a policy engine is to evaluate data in the light of the enterprise's security policies and determine what action(s) to take. Actions might include:

- Approving a request for access to an asset or for a transaction
- "Stepping up" authentication by asking the

user for additional factors or actions

- Blocking access or the transaction
- Displaying custom user notifications to enable self service actions
- Quarantining a suspicious device or removing network access
- Sending alerts and notifications
- Updating logs of requests and actions

The zero trust authentication solution then communicates the actions to the policy enforcement points and IT management and security tools.

Managing continuous risk assessment

The policy engine must also be able to manage continuous risk assessment. Users sometimes disable security controls on devices, for example disabling the firewall, turning off the device pin/ biometric, locking screen controls, or turning off security software. These actions degrade the security posture of the devices and significantly increase the risk that they could be compromised by malware.

A zero trust authentication solution should be able to schedule periodic checks of the security posture of devices. That includes both collecting endpoint data by itself and acquiring data or risk scores from EDR and MDM solutions installed on devices. That way, the risk state of the device can be accessed without waiting for the user to log off and log on again and the policy engine can initiate actions such as denying access or quarantining the device. In addition, current data about the device and potential issues can be provided back to the ecosystem of security tools for analysis and continuous improvement.

How Beyond Identity Meets the Requirements

Beyond Identity, a cybersecurity company based in New York City, is the developer of a phishing resistant, low-friction zero trust authentication platform. It takes a unique approach to completely passwordless authentication that is simple for users, IT security teams, and identity management groups.

Beyond Identity's approach to authentication adheres to zero trust principles and meets or exceeds the requirements we have outlined above. Its authentication solution can be deployed quickly, integrated with existing single-sign-on systems. It complements investments in other zero trust technologies such as ZTNA and network segmentation.

Let's look at how Beyond Identity addresses each of the requirements we have outlined for effective zero trust authentication.

1. Strong trust in user identities

In discussing requirements for strong validation of user identities, we emphasized how zero trust stands or falls on obtaining near-absolute certainty that people requesting access to assets are authorized users. We discussed why authentication needs to be both phishing resistant and passwordless.

We also gave examples of phishing and other attacks that could defeat weak MFA solutions. These are not theoretical attacks; they are happening at scale in the wild, executed by threat actors ranging from garden-variety cyber criminals to state actors. They no longer require sophisticated knowledge or advanced skills, since they can be launched using tools and services freely available on the web.

Beyond Identity's approach to zero trust authentication is phishing resistant. Nothing that a threat actor can use to impersonate the user ever traverses the network. Beyond Identity's solution replaces passwords with asymmetric cryptography that employs public/private key pairs (often referred to as passkeys). This same technology is used in transport layer security (TLS - the lock in the browser) to encrypt billions of dollars of web transactions daily, including online banking transactions and purchases from web merchants. With Beyond Identity, a private key is stored in the secure enclave on the device, a specialized chip that is highly secure and tamper resistant and that performs cryptographic functions.

Users are securely authenticated based on one or two highly secure factors.

One factor is proof of possession of the device. This is established when the authorized user authenticates via the biometric reader on the device.

Another factor is proof that the device is "bound" to the user's identity. When an access request is made from a device, a cryptographic challenge is issued by the Beyond Identity cloud to the Beyond Identity authenticator, a lightweight app running on the device. The authenticator responds to that challenge, using the private key stored in the secure enclave to establish the cryptographic response. The Beyond Identity cloud checks

the response against the user's public key to ensure the validity of the user. The cryptographic transaction also validates the authenticity of the request from the Beyond Identity cloud to the device. This ensures there is no man-in-the-middle present and confirms that the response from the device comes from a known source. These capabilities provide "verifier impersonation resistance" as defined in the NIST 800-63B standard.

With these factors, there are no passwords or other shared secrets that can be retrieved from a device, intercepted over a network, or enticed out of a user's head.

This innovative technology completely fulfills the requirements we have been discussing for phishing resistant, passwordless, strong validation of users in a zero trust environment.

2. Strong trust in devices

In the section on requirements for establishing strong trust in devices, we reviewed three requirements.

We just described how Beyond Identity's authentication solution addresses the first two. By cryptographically binding the user's identity to a device that has been registered (details on the registration process below), it can verify that the device making the request is in the possession of an authorized user and is authorized to access resources based on the organization's policies.

Beyond Identity's platform can also determine if the device has the expected configuration and if security controls are installed and enabled. A device's security posture is assessed by the Beyond Identity authenticator running on the device. The authenticator can natively collect data such as software versions, whether security features are enabled and configured appropriately, and other security-related details (e.g., if a phone is jailbroken, or if the system is enrolled and in good standing with corporate EDR or MDM). This information is used by the policy engine to check whether the security posture of the device meets the risk-based policies defined by the organization.

Also, if the organization already collects device data using an MDM or EDR tool, the Beyond Identity solution can pull additional data from that product.

To protect against deterioration of the security posture over time, the policy engine collects and analyzes information every time the user authenticates to a network or an application. In addition, organizations can set policies to collect specific data at regular intervals so risk-based decisions can be made continuously using current information.

3. Low-friction authentication for users and administrators

In the section on low-friction authentication, we pointed out how resistance to the annoyances of weak MFA frequently limits the deployment of strong authentication to a narrow range of employees and a handful of consumer use cases.

Beyond Identity's process for authentication eliminates this issue. Users never need to create, remember, or reset passwords. To authenticate, they simply use a biometric scanner on their devices. They don't need to find a secondary device, retype OTPs or codes, or open additional verification applications.

Also, users can enroll their devices with a few clicks, without help from support or administrative groups. This action is controlled by the organization through the policy engine's registration rules.

We also mentioned that password-based authentication and weak MFA create a huge volume of work for administrators and support staff, and how growing zero trust initiatives might make this work unsustainable.

Beyond Identity's technology addresses these issues nicely. Eliminating passwords and weak MFA features like OTPs and push notifications can reduce at a stroke most of the infrastructure and staffing needed to educate users and support those methods. It also simplifies the tasks for creating, deploying, and maintaining security policies.

While it is sometimes tempting to focus exclusively on the security improvements provided by zero trust authentication, reducing friction for users and work for administrators and support staff can play an equally important part in streamlining the adoption of zero trust frameworks and freeing resources for other tasks.

4. Integrations with IT management and security tools

In our discussion of integrations, we looked at the value of acquiring contextual data from a wide range of IT management and security tools to better assess trust levels and realize the concept of "continuous adaptive trust." We also touched on the importance of being able to communicate authentication decisions, alerts, and log data with other policy enforcement points and additional IT tools.

Beyond Identity already offers out-of-the-box, API-based integrations with leading products in most of the areas we mentioned, and the company continues to prioritize integrations that will improve security and enhance the investments our customers have already made. For a current list of these integrations, see the integrations web page on Beyond Identity's website: https://www.beyondidentity.com/integrations.

5. Advanced, zero trust policy engine

As we mentioned just above, Beyond Identity's authentication solution makes it easy to create, deploy, and maintain security policies. It is also flexible enough to handle policies for use cases faced by most enterprises.

Beyond Identity's solution offers automated processes for collecting and utilizing an unusually extensive range of data from devices to validate users and their devices and to determine the security posture of the devices. Integrations with IT management and security tools add a wide selection of threat information and risk signals. The policy engine employs all of this data to make well-informed, risk-based authentication decisions.

The data is collected continually, so that risk-based authentication decisions can be made with current information for every authentication transaction, for initial logins and continually thereafter.

Beyond Identity's policy engine enables administrators to initiate a wide range of actions based on risk assessments. These include approving requests, stepping up authentication, blocking access, sending alerts and notifications, and making calls to third-party services to quarantine devices or kick users out of remote access systems.

These capabilities not only meet the requirements of zero trust authentication, they go farther by speeding up remediation and simplifying compliance with regulations and enterprise policies.

Summary

A zero trust approach offers an opportunity to propel cybersecurity into today's world of remote work, BYOD, and cloud computing. Improving authentication can be a huge step in that direction, laying the foundation for everything else in zero trust. Authentication solutions that rely on passwords and phishable MFA are a roadblock to the successful implementation of zero trust. They are fundamentally insecure and too costly and difficult to support.

Effective authentication for zero trust environments requires:

- Strong, phishing resistant, passwordless validation of users
- Establishing strong trust in device by verifying that registered devices are in the possession of authorized users and are secure and compliant at the time authentication and continuously thereafter, not just during initial logins
- Very low friction authentication for users and simple operation for administrators, to promote user acceptance and control the costs of implementation and support
- Integrations with a range of IT management and security tools, to provide comprehensive data for accurate risk-based decisions, and to facilitate rapid response and remediation
- A zero trust policy engine that makes it simple to define policies, collect data from devices and IT tools, evaluate data, initiate actions, and manage continuous risk assessment

Beyond Identity has developed a unique approach to phishing resistant, passwordless, authentication that is simple for both users and IT teams. It gives enterprises a powerful tool to pursue zero trust initiatives with less risk and greater user acceptance.

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.