BEYOND IDENTITY

Device Trust: A Key Element of Zero Trust Authentication

The ongoing presence of remote work means more endpoints are accessing resources on enterprise networks. Employee and contractor laptops, tablets, mobile phones, and IoT devices all represent significant risk vectors for credential-based attacks.

Despite many organizations being far along in their digital transformations, applying secure user authentication to cloud applications is still a top security challenge. Given the growing complexity of cloud environments, the old perimeter-based security model is no longer applicable. As organizations continue to undergo digital transformation, more and more users require access to systems and data. The reality that most employees have multiple identities, connect to the network with multiple devices, and collaborate with outside vendors significantly increases cyber risk. Add in remote work and cloud adoption, and you have a surge of identities, making traditional multi-factor authentication (MFA) methods ineffective.

Zero Trust Authentication is the answer

With so many managed and unmanaged devices handling your organization's data, it's critical to eliminate cloud-security blind spots by verifying that a device is known, secure, and authorized to access a given resource. Zero Trust Authentication helps you continuously ensure that only authorized users can connect to your network—and only access the resources needed to perform a given task.

SEVEN PILLARS OF ZERO TRUST AUTHENTICATION

- **Passwordless:** Shared secrets can easily be obtained or captured
- **Phishing resistant:** No opportunity for phishing, adversary-in-the-middle, or other phishing-related attacks
- **Validated user device:** Requesting devices are bound to a user and authorized to access data
- **Device security posture:** Determine if devices comply with security policies
- **Risk signals:** Collect and analyze data from endpoints and security and IT management tools so policy engine can assess risk
- **Continuous assessment:** Evaluate risk throughout session
- **Integrate with security infrastructure:** Improve risk detection and accelerate responses to suspicious behavior

Effective Zero Trust Authentication is built on device trust. This means verifying user identity and the security posture of a device prior to granting access—and then on an ongoing basis. That way, you can respond accordingly if at any point the device poses a new security risk.

How to achieve device trust

With the right tools and policies, you can preempt credential-based attacks and avoid costly mitigation and damage to your brand's reputation. It's critical to leverage an authentication platform that provides high-confidence user authentication with minimal impact on your workflows.

To establish device trust with high confidence, user authentication should be:

1. Risk-based

It's not enough to classify a device as managed or unmanaged. The question should be, is this device trustworthy enough right now to access this resource? Making an informed, risk-based decision around user permissions requires comprehensive signals around the cyber health of the device. For instance, is the firewall enabled? Is the required security software running on the device? Is it encrypted?

Beyond Identity allows security teams to access risk signals from both managed and unmanaged devices through our out-of-the-box risk attributes. You can configure our flexible policy engine to allow or deny each user authentication request based on the risk profile of the device and your security and compliance policies.

2. Biometric-enabled

To verify user identity and establish device trust with high confidence, the secret used for authentication needs to be resistant to attack vectors. Unfortunately, commonly used secrets (i.e., passwords and 2FA codes) are vulnerable to credential theft through social engineering and compromised apps. Using a secret that cannot be stolen or tampered with is the best way to avoid credential-based attacks.

Beyond Identity leverages asymmetric cryptography to bind user identity to the device, eliminating all phishable factors. At enrollment, a secure key is created and stored within the device's secure enclave or trusted platform module (TPM). It is then assigned to any of the user's subsequent devices. This private key, which cannot be tampered with, is paired with an encrypted public key to authenticate the user at login, eliminating the need for passwords and one-time passcodes.

3. Continuous

While an initial login can recognize a trusted device, it can't account for what a compromised, negligent or malicious insider may do after logging in. This makes it very difficult to detect security breaches in real time, highlighting the importance of continuous risk-posture monitoring.

With Beyond Identity's frictionless solution, you can continuously monitor the security posture of devices across your fleet after the initial authentication. Every ten minutes, we check the device's security controls and poll the device to detect abnormal behavior without requiring input from the user.

REQUIREMENT	HOW BEYOND IDENTITY HELPS
Device risk signals that are relevant to your business	Platform authenticator delivers device-security context for every authorization request
Ability to allow, deny, or step up authentication based on risk	Fully configurable policy engine to meet your security and compliance requirements
Tamper-proof authentication keys	Device-bound private keys cannot be cloned, altered, or moved
Continuous user authentication and security monitoring	Checks device compliance and user behavior every 10 minutes

Take control of your organization's security today. Download the book Zero Trust Authentication: Securing User and Device Access for a Distributed, Multi-Cloud World and learn how Beyond Identity's passwordless, risk-based authentication can help you eliminate blind spots and prevent credential-based attacks.

Download the book