BEYOND IDENTITY

The Benefits of Integrating Zero Trust Authentication and Identity and Access Management

Zero Trust Authentication plays a pivotal role in access control for security-conscious organizations. This authentication method verifies both user and device before allowing access and then continuously authenticates both throughout the user session.

To achieve Zero Trust Authentication, you need to leverage four solutions:

- **Phishing-Resistant Multi-Factor Authentication (MFA):** MFA requires users to verify their identity with two or more factors, such as a PIN or biometric data.
- **Risk-Based Authentication (RBA):** With RBA, security enforcement dynamically adjusts to align authentication criteria to risk of target application or user and device anomalies.
- **Device trust:** Real-time device checks verify the presence of firewalls, antivirus software, biometrics, and other attributes of device security posture.
- **Continuous authentication:** Screening for changes in user, location, device posture, and behaviors during trusted sessions is critical given risk profiles change over time.

Because Zero Trust Authentication relies on secure validation of user identities, an integrated authentication and Identity and Access Management (IAM) solution provides a holistic mechanism of protection.

IAM solutions enable the management of user identities across the identity lifecycle. During the authentication process, the IAM checks the login identity against a repository of users and verifies that the person requesting access has permission for that resource.

Seven requirements for Zero Trust Authentication

1. Passwordless
2. Phishing-resistant
3. Validates user devices
4. Assesses device security posture
5. Analyzes many types of risk signals
6. Runs continuous risk assessments
7. Integrates with existing security infrastructure

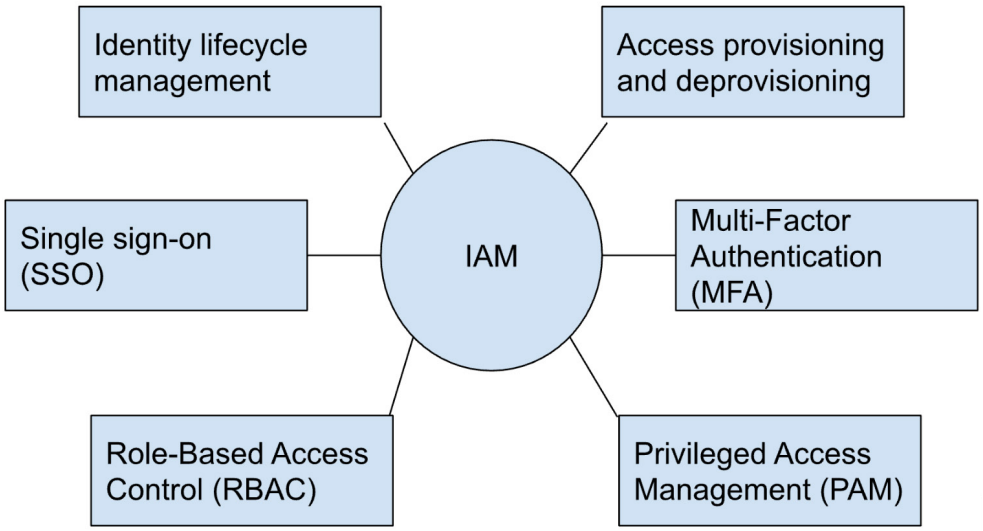
Because Zero Trust Authentication relies on secure validation of user identities, an integrated authentication and Identity and Access Management (IAM) solution provides a holistic mechanism of protection.

IAM solutions enable the management of user identities across the identity lifecycle. During the authentication process, the IAM checks the login identity against a repository of users and verifies that the person requesting access has permission for that resource.

The role of IAM

In a zero trust architecture, the IAM solution is the single source of truth for user and device checks. Its foundation is the principle of least privilege access, which says users are assigned the least privilege needed to perform a specific task.

Key functions of IAM



Identity lifecycle management: Oversees employee, contractor, and consultant user identities throughout their time at the company, keeping a record of access, devices, and sessions.

Access provisioning and deprovisioning: Automatically manages new employee and exiting employee access.

Single Sign-On (SSO): Replaces individual platform login credentials with a single credential that grants access to all company resources.

MFA: MFA requires multiple sources of identification to authenticate and authorize a user. These sources are stored in and managed by IAM solutions.

Role-Based Access Control (RBAC): Assigns access by user role, which is less error-prone than setting per user.

Privileged Access Management (PAM): Manages privileges for users who need access to critical systems, like network administrators and HR executives.

The benefits of integrating Zero Trust Authentication and IAM

Remote work, cloud-based resources, and Bring-Your-Own-Device (BYOD) policies have increased the attack surface for every company. Moving your security architecture to a zero trust model is the best way to avoid a data breach today, which costs $4.35 million or more per incident.

Integrating Zero Trust Authentication with IAM makes it possible to stop bad actors from accessing your corporate environment by providing the necessary validation of identity and device prior to access and continuously. With an integrated solution in place, you'll be able to prevent breaches before they occur.

Zero Trust Authentication with IAM

Reduces the main source of attacks by eliminating phishable credentials	Protect against advanced, modern credential attacks to keep your security ahead of evolving tactics, techniques, and procedures (TTPs)	Enhances security and trust levels by also validating device security posture
Keeps compromised devices off your network with real-time and continuous device security checks	Allows for more informed decisions before granting access by analyzing multiple risk signals	Prevents compromises during a session with continuous risk assessments

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.