Zero Trust Authentication and Identity and Access Management: How They Work Together

The zero trust model for enterprise security is quickly becoming a necessity in the fight against cybercrime. One of the critical components of this model is Zero Trust Authentication. Rather than implicitly trusting login requests, Zero Trust Authentication denies access until both the user and device are vetted. It then continuously authenticates throughout the user session.

Zero Trust Authentication aims to prevent bad actors from gaining entry through lost or stolen credentials, which are by far the most common means of access for cybercriminals. A recent study attributes roughly half of all external breaches to credential theft. Reduce your risk of attack by instituting an authentication architecture that keeps attackers from accessing your resources.

Another critical component of the model is Identity and Access Management, an important part of Zero Trust Authentication. Let's look at the roles of each and how they work together to protect your resources.

What is Zero Trust Authentication?

Zero Trust Authentication is a set of requirements meant to ensure access is granted only to authorized users on trusted devices. To achieve this, your authentication architecture must be:

- **Passwordless.** Eliminating passwords removes the single largest source of ransomware and other cyber attacks.
- **Phishing-resistant.** No passwords and continuous device checks make it impossible for criminals to use stolen credentials.
- **Able to validate user devices.** Binding user identity to the device ensures an unauthorized third-party device can't access company resources.
- **Capable of assessing device security posture.** Security checks keep compromised devices off your network and SaaS platforms.
- **Able to analyze many types of risk signals.** Data from endpoints, security platforms, and IT management tools are analyzed before granting access.
- **Equipped with continuous risk assessments.** Continuous assessments prevent compromise during a session by analyzing risk signals throughout the session.
- **Integrates with your existing security infrastructure.** Connecting authentication data with other security tools helps speed up detection and response to suspicious behaviors and provides data for audit and compliance reports.

Four Zero Trust Authentication mechanisms help companies meet these architecture requirements.

1. **Multi-Factor Authentication (MFA):** A key component of login security, MFA requires users to verify their identity with two or more factors. Common verification methods include a PIN or one-time password. But these methods are susceptible to phishing, which is why asymmetric cryptography and biometric data are considered the gold standard of MFA.

2. **Risk-Based Authentication (RBA):** With RBA, the number of security questions or checks increases for access to high-risk systems. These extra layers of protection keep valuable company data and infrastructure safe.

3. **Device Trust:** As remote work and the IoT landscape have grown, so has the need for device checks that verify the presence of firewalls, antivirus software, biometrics, and more. These checks for managed and unmanaged devices determine in real-time whether a device is trustworthy.

4. **Continuous Authentication:** Screening for changes in location, device posture, and behaviors is critical when login credentials and devices are so vulnerable. This tool lets you monitor user activity in the background without impacting the user experience.

In this current threat landscape where bad actors can easily steal credentials, impersonate an authorized user, or infect an authorized device, Zero Trust Authentication ensures each user is fully verified. By mitigating credential-based attacks, you reduce the attack surface, which leads to enhanced security and protection against breaches.

If you want to deploy Zero Trust Authentication, one of the first steps is creating a framework of policies and technologies for managing digital identities called Identity and Access Management (IAM). Your organization's IAM has two roles in the authentication process: 1) check login identity against a repository of user identities and 2) verify that the person requesting access has permission to access that resource.

The role of Identity and Access Management (IAM)

Authentication begins with the user. Each user must have a unique digital identity to which roles and access can be assigned and devices bound. An IAM automates managing these identities and assigning permissions based on role and company policy. Because of this, IAM allows companies to not only protect their digital perimeter like an access control gate might do around a corporate headquarters, but also protect individual network resources and cloud-based platforms.

Whether deployed onsite, in the cloud, or in a hybrid model, IAM technologies reduce the risk of breaches and improve user access controls. One example of improved control is the ability to view real-time logs of each user session and quickly identify the breached account and revoke access. Without an IAM, companies can burn through precious time identifying the source of compromise and, once they do, may be unable to revoke access. The more time bad actors have in critical systems, the more damage they can do.

In your zero trust architecture, the IAM becomes the single source of truth for verifying identity. The principle of least privilege access, meaning users are assigned the least privilege needed to perform a specific task, is also applied to its policy engine. There are several other functions an IAM performs that are worth reviewing.

Identity lifecycle management - IAM systems are connected with other company databases to manage employees, contractors, and sometimes visitors' changing roles. For instance, when an individual joins the company, the IAM system sets up a user identity and permissions. If two years from now, that individual gets promoted, their access levels will automatically be updated based on their new role.

Access provisioning and deprovisioning - IAM systems automatically manage the setup of new employee access and revoke access for those who leave the company.

Single sign-on (SSO) - SSO is a feature of IAM systems that replaces individual passwords for each company platform with a single username and password that grants access to all applications. An SSO significantly reduces IT requests for password help and improves workforce productivity.

MFA - As previously mentioned, MFA requires multiple sources of identification to authenticate and authorize a user. IAM systems store or manage these other sources of identification.

Role-Based Access Control (RBAC) - Also called role-based security, RBAC restricts access based on a user's role within the company. Assigning access by role is less error-prone than setting by each user.

Privileged Access Management (PAM) - Some users need access to critical systems, infrastructure, and data. PAM manages privileges for these users, which often include network administrators and users within the Finance and HR departments.

Integrating Zero Trust Authentication and IAM

Zero Trust Authentication can't be achieved without robust IAM. The identity and device data stored in an IAM system is the source of truth needed to authenticate. Another way to think of it is that IAM handles a big part of the verification process in the zero trust motto of "never trust, always verify."

Conversely, Zero Trust Authentication influences the policies and permissions used by IAM systems, such as least privilege access. It also requires that IAM systems bind devices to identity and manage passwordless mechanisms for authentication.

Because Zero Trust Authentication integrates into your existing security architecture, you can tighten your whole ecosystem. The benefits of integrating Zero Trust Authentication and IAM are clear:

Implementing a passwordless approach in IAM eliminates the primary source of ransomware and cyber attacks, enhancing security by removing the vulnerabilities associated with password use. This simultaneously boosts user experience, as it simplifies and expedites the authentication process.

Incorporating phishing-resistant factors into IAM systems provides an additional layer of security. Without passwords and with continuous device checks, it becomes virtually impossible for criminals to exploit stolen credentials, reducing potential security breaches and strengthening the integrity of your IAM system.

Validating user devices within the IAM framework enhances the system's security and trust levels. By binding user identity to specific devices, the system ensures unauthorized devices cannot access sensitive resources, providing an additional layer of control and protection.

The ability to **assess device security posture** within IAM helps keep potentially compromised devices off your network and SaaS platforms. This not only protects your resources but also mitigates the risk of internal breaches, contributing to a more secure and reliable system.

By integrating the ability to **analyze multiple types of risk signals** within IAM, the system can make more informed decisions before granting access. This ensures that only secure and trustworthy endpoints gain access, enhancing overall security.

Continuous risk assessments paired with IAM prevent potential compromises during a session by constantly monitoring and analyzing risk signals. This dynamic and responsive approach ensures ongoing security, even after initial authentication.

Integrating Zero Trust Authentication with IAM enhances the security ecosystem, enabling efficient detection and response to suspicious behaviors, and providing comprehensive audit and compliance data. This means it not only improves your overall security, it also helps you meet regulatory requirements and maintain a compliant posture.

The return on investment with Zero Trust Authentication

Distributed and hybrid work environments that allow remote work and access to cloud-based resources have shifted the security perimeter. Companies are more at risk than ever. And with the cost of a data breach reaching $4.35 million per incident in 2022, failing to implement a zero trust model could jeopardize your business.

Zero Trust Authentication is critical for IAM because it strengthens security, continuously detects and adapts to evolving threats, and it ensures regulatory compliance.

Beyond Identity's Zero Trust Authentication offers a unique approach to phishing-resistant, passwordless authentication that is simple for both users and IT teams. By reducing friction and supporting easy adoption, we give enterprises a powerful tool to implement zero trust initiatives. Book a demo today.