Why **Zero Trust** should be at the forefront of your **IAM strategy**

ManageEngine
AD360

Introduction:

The Zero Trust framework follows a “never trust, always verify” policy. It doesn’t distinguish between internal and external users or devices; it treats everything as external. Hence, every individual or device that attempts to access a private network, whether it is located inside or outside of an organization's network, must be identified and authorized. Unlike other security models, which automatically trust individuals and devices that are already within the corporate network, Zero Trust advocates trusting no one at any time. Zero Trust should be part of any organization's identity and access management (IAM) solution.

Even though Zero Trust encompasses several factors, the only common denominator is the user. The underlying principle is to control who has access to which systems and data, and have well-defined policies to define when to allow or restrict access, and how to enforce it. The reasoning behind this framework is that there may be insider threats within the network in the form of a malicious employee who wants to compromise sensitive data, or privileged user credentials that have been breached by a threat actor outside the organization.

The traditional approach

Traditional security approaches were designed to protect the organization's perimeter. To get in, one had to be verified and trusted; but once inside the network, further verification was not required. This security model has been compared to a castle with a moat. The moat around the castle is designed to keep the attackers at bay, but once someone is trusted and let into the castle, there are no reasons to doubt their intentions. This assumption—that everything within an organization's network can be trusted—is outdated, especially in light of a new era of sophisticated attacks.

The Zero Trust approach: Security for a new world

The Zero Trust mindset operates under the assumption that all users and resources are untrusted, and always need to be verified. Adopting multi-factor authentication (MFA) and single sign-on (SSO) can go a long way in improving an organization's overall security posture. By granting people access only to the resources they need to carry out their tasks, organizations can minimize exposure. To prevent misuse of a former employees' user accounts, automatically disable accounts via HR-vetted directory identities. All said and done, it is wise to audit every activity, and any anomalies must be immediately flagged.

Steps to adopt a Zero Trust model

- Provide frictionless access with MFA and SSO
- Validate changes with a request and approve process
- Employ the principle of least privilege (POLP) and just-in-time (JIT) access
- Disable accounts of former employees automatically
- Monitor and audit privileged user activity

In this guide, we'll take a closer look at the challenges and how ManageEngine AD360 makes it easy to implement these five steps.

Provide frictionless access with MFA and SSO

If “trust” based on location or network segment is no longer sufficient, it follows that authenticating and authorizing users before granting access to any resources is a critical component of a Zero Trust initiative. Relying on usernames and passwords for authentication is a thing of the past. In many organizations, this outdated approach has been replaced with MFA, which needs multiple “factors” to prove an identity. By mandating several verification factors, hackers cannot brute-force their way into your enterprise network. The hope is that if an attacker has stolen the credentials from a breach, they will be denied access when challenged with MFA. SSO provides the ability for users to sign in once with their credentials, including a single password, and have access to all of their applications. In SSO, users authenticate once and then use that authenticated session to access all of the applications they’re authorized to use. By getting rid of passwords, this method suggests that usability and employee satisfaction are increased.

Validate changes with a request and approve process

For increased visibility, teams can implement multiple security checkpoints in the network to identify what is happening on their networks, and apply necessary restrictions on who can access the data to lower the risk of a data breach. For each request, it is important to know why somebody requires access to specific resources. Then, an IT admin must grant the user the necessary access rights only to the network areas or project the user needs access to. That way, even if an IT admin’s user credentials are compromised, the attack surface is limited.

Employ the principle of least privilege (POLP) and just-in-time (JIT) access

Insider threats and compromised user accounts are common concerns that can be mitigated if user access is limited in the first place. The concept of least privilege is to only grant the necessary level of privilege to a user to perform a certain task. By granting least privileges, it is possible to prevent lateral movement of the malware planted byattackers, reducing internal data exfiltration. The Zero Trust approach is to provide everyone with the minimal level of privileges they need. Another way to limit insider threats is applying the principle of just-in-time (JIT) access, and grant access for only a specific period of time on an as-needed basis. This can be used for contract employees and interns.

Disable accounts of former employees automatically

When an employee leaves an organization, their account should be stripped of its privileges, then deprovisioned; if this isn't done, that ex-employee's account will become stale. Malicious insiders could leverage stale accounts to access your organization's resources. It is a best practice to create a routine that periodically identifies stale user accounts and applies a deprovisioning policy to keep your infrastructure clean and updated.

Monitor and audit privileged user activity

Besides authenticating users and assigning privileges, it is essential to monitor and review all user activity across the network. With a documented record of all actions performed, the data can be used to identify any suspicious activity in real time. A good practice is to integrate this audit data with your existing security information and event management (SIEM) system for analysis so that risky activities can be identified and alerts can be triggered.

Get started with Zero Trust the ManageEngine way

To ensure successful implementation of Zero Trust architecture, stringent security and access policies must be in place. Rule-based role access, and governing and automating the provisioning of this access is an essential aspect of this architecture. This amplifies the need to have an effective IAM solution that can accelerate the efficiency of your Zero Trust policy.

ManageEngine AD360 is a comprehensive IAM solution that can help with implementing identity-driven security as the core of your organization's Zero Trust program.

Passwords are simply not enough

To mitigate password-related security risks, AD360 verifies users' identities using MFA via various authentication techniques, such as security questions and answers, Google Authenticator, YubiKey, fingerprint authentication, RSA SecurID, DUO Security, and more. To enjoy a consistent logon process across applications, users can secure access to all SAML-enabled cloud applications using the SSO capability; this includes Office 365, G Suite, Salesforce, SAP NetWeaver, and others.

Discover how AD360 can resolve the security gaps by consolidating identities across on-premises and cloud by configuring multi-factor authentication and single sign-on.

Implement proper authorization controls to avoid undesired changes

Making changes in AD permissions without having them reviewed first can unintentionally expose sensitive business data to security vulnerabilities. It is essential to have an access control policy in place for every critical action in AD to prevent users from gaining unauthorized privileges. The best course of action is to follow a review process where every user change request is evaluated by a manager before it's transferred to an IT admin. Each request, such as access to critical shares or changes to group membership, must be reviewed by an IT manager or team lead to ensure that enterprise resources are not compromised.

Using AD360, you can configure deprovisioning using an automation that identifies dormant objects, removes their privileges, moves them to a different container, removes associated Office 365 and G Suite accounts, exports the user's mailbox to a specified location, and revokes applicable software licenses before deleting them. Using AD360, you can automatically identify and clean up all inactive, disabled, account-expired users and computers in Active Directory.

Audit privilege use across your domain

With privileged users having free rein of the domain's resources, it is vital to monitor changes by auditing their file activities and receiving real-time alerts when there is unusual activity. By leveraging the privileged user activity auditing and user behavior analytics, you can verify that the actions of privileged users are in accordance with the normal standards. Besides that, it becomes easier to comply with various IT regulations by maintaining an audit trail of activities performed by privileged users across the network.

Using AD360, track privileged user access to data regulated by IT compliance policies, and instantly detect any accidental or willful violation of the data's integrity.

If your organization hasn't already, it's time to implement a Zero Trust model that puts identity and access management as the central theme of your IT security arsenal.