Kickstart Zero Trust with Active Roles and OneLogin MFA

Introduction

As cyberattacks and data breaches become more commonplace, Zero Trust has become a sought-after security strategy among IT leaders. Organizations should view Zero Trust as a journey, not a destination, and the journey begins with the protection of identities, many of which reside in Active Directory (AD) and Azure Active Directory (Azure AD). As such, organizations must start taking the necessary steps to unify their cybersecurity approach and begin making Zero Trust a reality.

What is Zero Trust?

Zero Trust is a collection of cybersecurity initiatives that remove vulnerable permissions, unnecessary access and excessive access in favor of least privilege, per-request access delegation. In short: "never trust, always verify." Zero Trust takes a completely different form within each organization based on its IT environment and industry compliance and regulatory standards. Regardless of the individual requirements of an organization, Zero Trust aims to always provide a holistic view of security risks, as well as complete control of an organization's identities and resources.

The core tenets of Zero Trust include:

1. **All resources (data sources and computing services) are strictly enforced:** Ensures only authorized actions are performed after authentication
2. **All communication is secured, regardless of network location**
3. **Access to individual enterprise resources is granted on a per-session basis:** Each operation must be authenticated and authorized before it can be carried out
4. **Access to resources is determined by dynamic policy – including the observable state of client identity, application/service and the requesting asset – and may include other behavioral and environmental attributes:** Enables the capability for access to change to meet specific, real-time needs of users
5. **Collect as much information on the current state of assets, network infrastructure and communications as possible:** Visibility is key to ensure the security of any system

To make Zero Trust achievable for organizations, an integrated approach with a unified identity security platform is required, as well as gradual upgrades and changes that will need to be made to an organization's entire infrastructure over time.

Together, One Identity Active Roles and OneLogin multi-factor authentication (MFA) can help you **kickstart your journey to Zero Trust**.

The Role of Active Roles within Zero Trust

Active Roles helps satisfy three of the core tenets of Zero Trust:

- Allows the privileges of one person or account to be elevated to do specific tasks and then return to their basic privileges afterward (Tenet 3)
- Changes user access to meet specific, real-time user needs (Tenet 4). Additionally, the solution provides an elaborate audit trail to track where access was granted (or denied), who requested it, where it was granted and when it was removed
- Audits changes to Active Directory objects (Tenet 5)

Overall, Active Roles allows Zero Trust concepts to be applied to AD and Azure AD by providing account lifecycle management, dynamic roles and access controls. The solution also strictly enforces the least-privilege model for access to AD, Azure AD and all AD-joined systems.

The Role of OneLogin MFA within Zero Trust

Why multi-factor authentication? In short, MFA secures your applications and data by preventing unauthorized access. OneLogin MFA offers policy-based MFA with flexible authentication factors, including:

- OneLogin Protect: One-Time-Password (OTP) app, email, SMS, voice, Web Authentication for biometric factors, plus a range of third-party options
- SmartFactor Authentication: Uses machine learning to evaluate the risk and context of each login and adapt accordingly

The Zero Trust tenets that OneLogin MFA helps satisfy are:

- Enhancing cybersecurity with system-level checks and only lets authorized users access assets (Tenet 1)
- Reducing the security gaps of distributed workforces and infrastructures (Tenet 2)

Active Roles and OneLogin MFA Together Aid Zero Trust

Together, Active Roles and OneLogin MFA satisfy all the highlighted core tenets of Zero Trust. The two solutions can also be seamlessly integrated as part of the One Identity Unified Identity Security Platform. Adding OneLogin MFA to Active Roles secures authentication of Active Directory and Azure Active Directory, ensuring all users only access what they need to get their work done, preventing unauthorized access to data, passwords, etc. At the same time, Active Roles provides foundational identity management capabilities for AD and Azure AD, enabling organizations to easily create the necessary access permissions for cloud and legacy applications which are in turn granted access to using OneLogin MFA.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing 500-million-plus identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.

ONE IDENTITY by Quest