WHITE PAPER

Making Zero Trust Real

Enabling Unified Identity Security

What is Zero Trust?

A proven model for implementing robust and selective security, Zero Trust involves removing vulnerable permissions, unnecessary access and excessive access in favor of specific delegation and proper provisioning with fine granularity.

- Enabling Zero Trust eliminates the sharing of admin passwords and allows individual and dynamic authentication for every administrative action.
- Ensuring Least Privileged involves issuing just the permissions an admin requires to do their job – no more and no less.

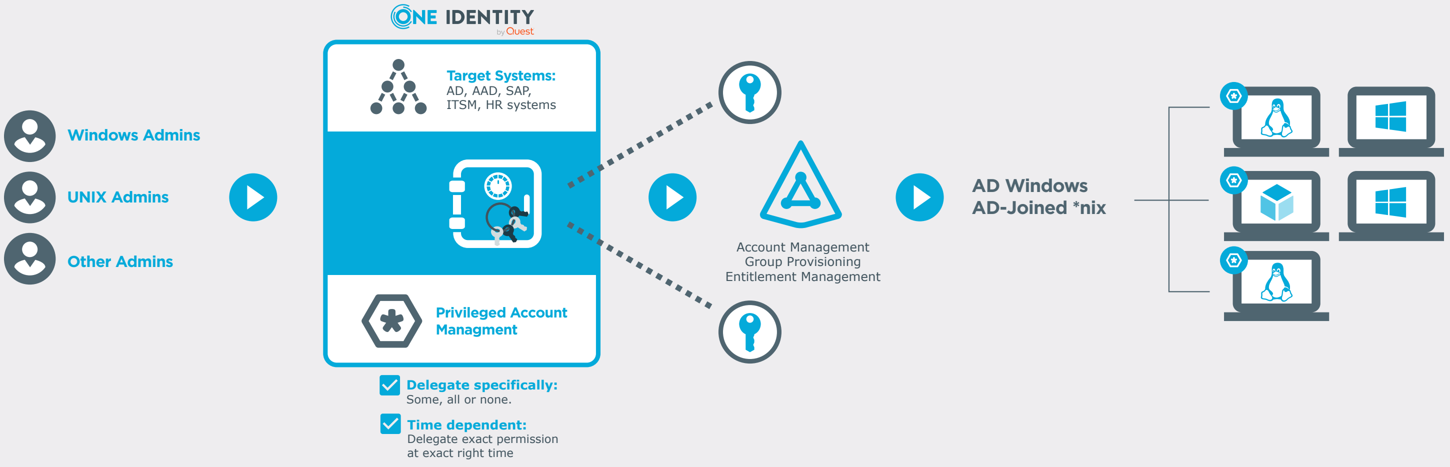
Overview

Zero Trust is rapidly becoming the security model of choice among IT leaders as it is a valid and trusted approach to identity security. With a more intentional method for security and privileged access management, Zero Trust's mantra of "never trust, always verify" differs from the least privileged model. This tech brief covers the components of achieving a robust security posture, including these points:

- Establishing 'identity as the perimeter' addresses many core tenets of this security model. Notably, that approach requires a unified solution for reliable provisioning, entitlement management, PAM, strong authentication, safe access and governance.
- In a Zero Trust model, all communication is secured but untrusted.
- Providing a 'single source of truth' – centralized and synchronized identity data – gives organizations complete control of the identities and resources. It can only truly be achieved when this concept of entitlement is nailed down first.
- No single piece of the puzzle delivers the complete security model but combining solutions well does.

For many organizations, Zero Trust is well within reach when they rely on modular and integrated solutions, including privileged access management (PAM), Active Directory (AD)/Azure AD management, event collection, and identity governance and administration (IGA). This integrated approach enables you to satisfy the core tenets of Zero Trust security while providing an optimal end-user experience.

Enabling Zero Trust with One Identity



Journey to the Zero Trust Security Model

As modernization efforts transform the fundamental ways computing technologies are applied, consumed, and accessed, identity security becomes increasingly important. Initiatives, such as application modernization, cloud-first mandates, networking innovations – like software-defined networking (SDN), and competitive business pressures – make it challenging to manage and protect access by users and other non-human resources. How does an organization safely implement cloud-based technologies while maintaining mission-critical resources on-premises?

As much as we'd all like to have clean and tidy processes, the reality is that most organizations will operate a hybrid mix of on-premises systems and cloud-based systems for the foreseeable future. Maintaining security, meeting compliance requirements and delivering a smooth user experience can seem like an impossible task.

It doesn't have to be. It can be achieved by introducing this security model as you move through your digital transformation. With the model in place, you can reduce complexity and define baseline metrics to create customized best practices for information security and identity security.

NIST Zero Trust Architecture

1. All **data sources and computing services** are considered resources.

2. All **communication is secured** regardless of network location.

3. Access to individual enterprise resources is granted on a **per-session basis.**

6. All resources authentication and authorization are dynamic and strictly **enforced before access is allowed.**

4. Access to resources is determined by a **dynamic policy** – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioral and environmental attributes.

5. The enterprise **monitors and measures** the integrity and security posture of all owned and associated assets.

7. The enterprise collects as much information as possible about the **current state of assets, network infrastructure and communications** and uses it to improve its security posture.

Reference: NIST SP 800-207 "Zero Trust Architecture"

Identity is the New Perimeter

With more networking functions becoming part of a virtual networking environment, traditional on-premises firewalls and static routing has been replaced with virtually coupled resources. Identity security is the new perimeter. Protecting identities requires strong authentication, safe access and governance. In a Zero Trust security model, all communication is secured but untrusted.

A robust identity security foundation that dynamically adapts and provides unified policies and access control for on-premises or cloud-based resources is a critical component of this new model. Providing a 'single source of truth' (centralized and synchronized identity data) to ensure rights, attributes and entitlements throughout the lifecycle of the identity gives organizations complete control. Zero Trust can only truly be achieved when this concept of entitlement is nailed down first.

The Seven Core Tenets

A Zero Trust model has defined core tenets per NIST SP800-207. These tenets help vendors design solutions so that technology users can adopt services that enable them to implement the security model in an efficient and predictable way.

The NIST tenets include:

1. **All data sources and computing services are considered resources.**

2. **All communication is secured regardless of network location.**

3. **Access to individual enterprise resources is granted on a per-session basis.**

   This key concept of identity security specifically focuses on managing elevated privileges. If a person or account needs elevated privileges to do a specific task, they probably don't need that permission all the time. One Identity Manager, Active Roles, and One Identity Safeguard (with Just-in-Time provisioning) make this possible.

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.**

   The key word here is "dynamic." Dynamic policy enables the capability for access to change to meet specific, real-time needs of the user. Both Identity Manager and Active Roles provide this capability as well as an elaborate audit trail to prove where access was granted (or denied), who requested it, where it was granted, and when it was removed.

5. **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.**

   The "assets" of the enterprise encompass many things. Visibility into who has access, how it was granted, and even calculated security vulnerabilities based on a privilege model provide critical decision-making information to the enterprise. One Identity Manager focuses on the identity both as an asset and a subject to be managed so accurate information is used to make access decisions and provide reports.

6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.**

   The strict enforcement of access control is an absolute necessity for any system. One Identity solutions layer in the ability to make access control dynamic to meet any regulatory or business need by detecting identity changes and instantly manipulating end systems to reflect the required access change.

7. **The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.**

   Visibility is key to ensure the security of any system. Whether looking at current state of access or events generated by change, One Identity solutions cover this core tenet. While One Identity Manager provides visibility and governance into access states and changes, Active Roles audits changes to Active Directory objects, and Safeguard controls privileged access; One Identity syslog-ng collects all the event data to ensure complete situational awareness of the enterprise.

No solution provides a "magic button" for implementing a Zero Trust model. It should become a mindset when implementing new systems, applications, networks, and even physical security. Embracing and combining these concepts provides a framework to ensure enterprises are utilizing all possibilities to secure their infrastructure. Identity security plays a significant role in the modern workforce.

While no single piece of the puzzle delivers Zero Trust, combining the pieces in a powerful manner will. Leveraging One Identity's unified identity security platform, including our privileged access management (PAM), Active Directory (AD)/Azure AD management, event collection and identity governance and administration (IGA) offerings is the path to implementing the security model while providing a satisfying end-user experience.

How do we make Zero Trust real?

To make it achievable for organizations, an integrated approach with a unified identity security platform is required. Creating well-thought-out practices to secure and manage identities can be a very complex task, but the critical piece of the security pie is how they are implemented.

One Identity solutions allow enterprises with diverse environments to implement identity-centric practices that follow the NIST Zero Trust Architecture. NIST arms us with solid technology guidelines to help make significant strides toward securing critical information. While they don't specifically address securing on-prem or cloud, it is critical that we apply them to the systems that provide access decisions every day for every organization.

One Identity provides the solutions to squarely address the specific NIST tenets. Our solutions include:

Control Access with One Identity Manager, which is specifically designed to control access, ensure the least privilege model is implemented, and dynamically remove access when no longer required for any connected system.

Enforce least privileged access with Active Roles, which allows Zero Trust concepts to be applied to Active Directory by providing account lifecycle management, dynamic roles and access control, and strictly enforcing the least privilege model for access to Active Directory and all attached systems.

Manage privileged access with Safeguard, which provides the complete range of privileged access management solutions to ensure the powerful identities and accounts that run the enterprise are under strict control, and this can be proven through detailed audit trails and reports.

Collect logs with syslog-ng for flexible and scalable log management across the enterprise to ensure the most efficient and cost-effective use of SEIM.

About One Identity

One Identity by Quest, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of the program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com

WhitepaperAD-MakingZeroTrustReal-RS-65397