TAG CYBER

A Process to Implement Zero Trust Access

A simple iterative process is introduced to help guide IT, network, and cyber security teams in the introduction of zero trust access to their enterprise. The process starts with quick win selection of systems, applications, or workloads, followed by a stepwise implementation toward the target goal.

Prepared by

Katherine Teitler
Senior Analyst, TAG Cyber
kteitler@tag-cyber.com

Edward Amoroso
Lead Analyst, TAG Cyber
eamoroso@tag-cyber.com

Introduction

Zero trust access involves protecting enterprise resources without reliance upon any firewall-based perimeter, although firewalls can still be helpful as part of your overall security strategy. With zero trust access, no user or entity is trusted by default to access enterprise resources based solely on their internal network positioning. Instead, access to enterprise applications, systems, and services requires explicit identification and authentication, even if such access is made laterally across an enterprise local area network (LAN). This approach greatly reduces enterprise security risk.

Because common IT and security initiatives such as cloud workload deployment and remote work-from-home support serve as building blocks, it turns out that implementation of zero trust access is often much easier than expected. This report provides a simple plan that can help develop an implementation framework to achieve zero trust. The plan includes four steps that iterate from a baseline architecture to one more consistent with improved security.

Plan to Implement Zero Trust Access

The process to implement zero trust access involves four simple, iterative steps that can be used as the basis for a local plan. The presumption is that the iterations would proceed from a series of initial quick win deployments in which select enterprise workloads, systems, or applications are transitioned from their legacy implementation to one supporting zero trust. The quick win approach is particularly well-suited here because it allows teams to build an experience based on simpler initial transition cases.

The four steps are designed specifically to avoid disruption throughout the zero trust transition, while also ensuring that positive changes are not offset by negative process issues which could have been avoided. These steps involve creating an inventory of assets involved in a given transition, identifying the applicable stakeholders, driving the transition based on an explicit plan, and then adjusting any applicable business processes (see Figure 1).

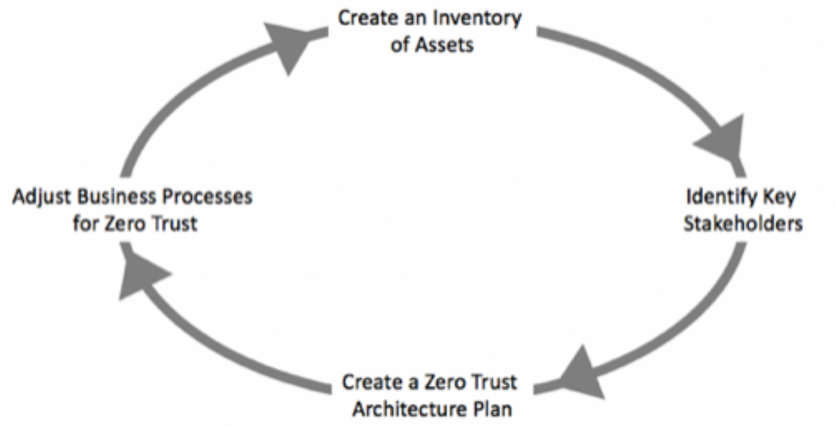

Figure 1. Iterative Steps for Managers Implementing Zero Trust Access

Each of these steps in the proposed iterative process toward zero trust are explained and illustrated in the sections below.

Step 1: Create an Inventory of Assets

Upon each iteration of the simple process for implementing zero trust access, it is necessary for IT and security teams to take a targeted inventory of applicable assets involved in the transition. The complexity of this inventory task will track directly with the scale, scope, reach, and features of the workload selected for transition to zero trust. By focusing the initial work on quick win projects with relatively simple functionality, this inventory step will likely be quite straightforward.

Typical assets to be identified in the inventory step include (1) the application, system, or workload selected for the transition step, (2) a list of applicable end users, (3) a list of all back-end system dependencies such as directories or databases, (4) a list of applicable existing security controls, and (5) identification of all policies in place for access to the target. Such inventory will help the IT and security teams ensure that the zero trust transition covers all relevant use cases for the targeted asset.

Step 2: Identify Key Stakeholders

While the IT and security teams tasked with managing to zero trust will always be key stakeholders in the process, each iteration will also require support from various other individuals and teams in the organization. The most common stakeholders include the owners of the application, system, or workload targeted for transition. They are necessary to provide the detailed context and support required to ensure a smooth shift from legacy to zero trust access.

Having disparate and unwieldy policies for each network segment can make managing the network complex and overwhelming.

While it might not be necessary to create formal advisory or governance groups to oversee the zero trust access transition process, teams should consider including some organizational structure during each iteration. IT and security management would be wise to focus on keeping stakeholders directly involved and informed during the transition step. This should be done consistent with the local norms for such cooperation, including use of any tools for information sharing.

In addition to key stakeholders, organizations should also seek vendor partners with the desired types of zero trust access functional support. It is important to note that new technologies may have stronger security capabilities that should be evaluated for inclusion in the new zero trust access solution. For example, teams might require more refined access control policies in the platforms they select. In many cases, having disparate and unwieldy policies for each network segment can make managing the network complex and overwhelming, whether on-premises or in a cloud, hybrid cloud, or multi-cloud setting, so selecting a vendor partner who can help simplify and consolidate your access security can be a significant advantage.

In addition, vendor solutions might be selected that unify access control using single sign-on, with consistent enforcement policies across networks and support for administrators to audit policies from a central console. Zero trust access controls that continuously assess the validity requests based on multiple attributes such as IP address, device type, and OS will help remove the need for humans to approve or deny each request manually.

Step 3: Create a Zero Trust Architecture Plan

An important consideration in the process toward implementation of zero trust is that the target architecture will be achieved in an iterative, stepwise manner. This implies that the existing perimeter-based legacy (perhaps already in a hybrid cloud mode) will follow a series of transitions for select applications, systems, and workloads – eventually arriving at the desired state. This is helpful, because it supports early quick wins and allows for experience-based adjustment to the process.

The most important property to be maintained through transition to zero trust access involves dissolution of any default authorizations based on local positioning on the enterprise network.

While each step will require a plan that takes into account the specific functionality, user base, functional controls, and mission purpose of the selected application, system, or workload, some generic guidelines can be identified to assist IT and security engineers during the transition. Such generic assistance usually involves clear description of the existing precondition state along with guidance on the target state with zero trust access. This is especially important because zero trust access can have more comprehensive security policies that will better protect your resources.

Regardless of the specific plans created for each successive step, the most important property to be maintained through transition to zero trust access involves dissolution of any default authorizations based on local positioning on the enterprise network. That is, every step in the proposed process to zero trust will begin with a perimeter-based access architecture and will result in a zero trust arrangement devoid of reliance on a perimeter. The diagram in Figure 2 shows a typical generic transition.

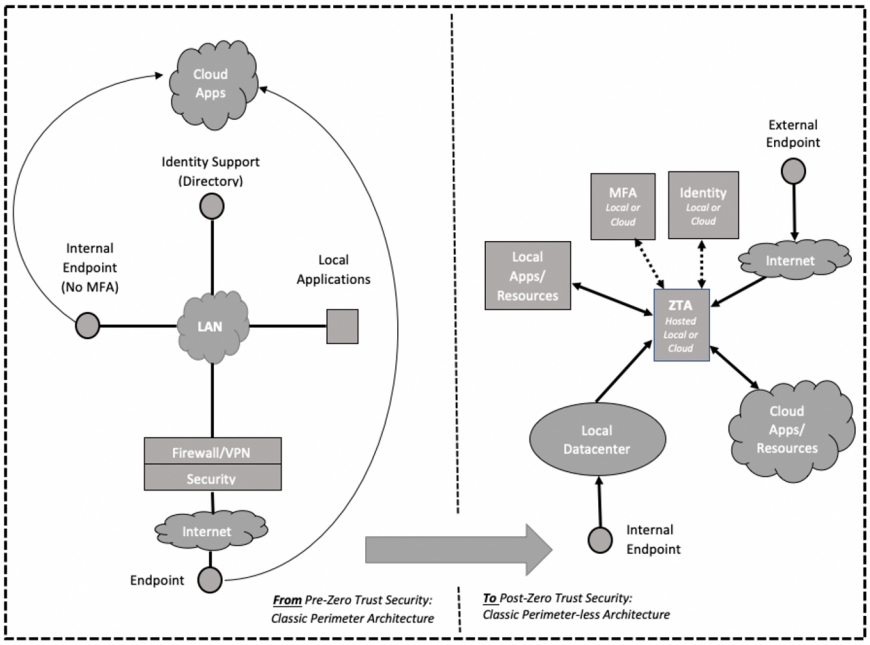

Figure 2: Typical Zero Trust Access Architecture Plan Transition for an Application

Step 4: Adjust Business Processes for Zero Trust

While it might be tempting to consider the zero trust transition complete once the new functionality has been achieved, IT and security teams have the obligation to ensure that any changes do not require adjustments to applicable business processes. Training and user support teams, for example, must be made aware of any new zero trust set-ups, and this could require that they amend or adjust applicable processes that support the user base.

Teams should expect, as the early quick wins are completed during the stepwise implementation of zero trust, that this business process adjustment step will gradually become a lesser concern. That is, once support teams such as help desks and IT administration groups are made aware of the ongoing transition, it will become easier to provide information on successive applications, systems, and workloads undergoing a shift to zero trust.

The Bottom Line: Simplify, Consolidate, Strengthen

As resources are moved to a zero trust access architecture, teams will be able to greatly reduce the complexity of their infrastructure and close more ports to the outside world, strengthening security across the enterprise. Stronger controls created by zero trust access will provide targeted and secure microsegmentation of resources that make the lives of both end users and admins alike easier. Finally, for the first time, teams will be able to provide centralized reporting and auditing of all access to local and cloud resources and applications.