White Paper

Zero Trust

What Is It and Why You Should Care

cbi
Cybersecurity Solutions

Dan Gregory
VP | Systems Engineering

Overview

Traditional networks allow users to attach devices and access their data, systems, applications, and services. This process may include the verification of access during one or two of the following critical checkpoints:

- WHO IS CONNECTING?
- WHAT DEVICE ARE THEY USING?
- WHERE ARE THEY PHYSICALLY CONNECTING?
- WHAT METHOD ARE THEY USING TO ATTACH?
- HOW ARE THEY BEING CHALLENGED DURING THE AUTHENTICATION PROCESS?

There are many examples, but traditionally networks typically only challenge a few of these checkpoints during the connection process. Once a connection has been established and verified, it is allowed to operate unchallenged.

What is Zero Trust?

Zero Trust ("ZT") is a "Cybersecurity Model." It flips the script on the traditional network security model. It operates under a single rule: "Anything connecting to the network should not be trusted by default."

ZT enforces this approach for all objects, including users, devices, endpoints, systems, and applications. ZT securely verifies the connection before they are allowed to access the network. Once connected, ZT continues to challenge and verify the object to ensure it has the minimum level of authorization and access needed to do its job but no more.

Verification can vary based on the type of object. The operational protocols for ZT use a set of rules to govern the amount of access granted based upon the type of user, job title, device, location, and other variables.

Some of the Primary Principles and Strategies Needed to Implement a Successful ZT Model

Network Segmentation

The ability to separate your network into smaller enclaves ensures devices, servers, and services containing sensitive data are isolated from the rest of the network. This process keeps a potential attacker contained within the network segment they've accessed.

IT Security Hygiene

The ability to ensure the asset requesting access to your network adheres to a predefined minimum-security baseline standard. The standard significantly lowers the risk to the end-user as well as the organization's critical assets.

Vulnerability and Patch Management

The ability to scan an endpoint before connecting to the organization's network and automatically mitigate vulnerabilities associated with a lack of software patching is a critical component to any ZT model.

Continuous Risk Monitoring

Continuously monitoring the state of devices, systems, applications, and services to identify and address security vulnerabilities or act on their access privileges accordingly in real-time.

Dynamic Network Monitoring

Controlling and monitoring all traffic access for approved. If an asset no longer meets a minimum set of security-based criteria, it should automatically be shunted to a secure, off-line network where automated remediation is applied before allowing it access the corporate network and or assets.

Data Risk Management

Knowing where all of your sensitive data is, classifying it based on a set of metrics aligned with the organization's goals and objectives to monitor for unwanted or unauthorized access.

Why Should I Care About ZT?

The increase in remote or work-from-home (WFH) users has driven most organizations to flip their network security model inside out. Organizations have shifted from managing most risks from within their on-prem, cloud, and hybrid environments to a primarily external model with hundreds and possibly thousands of remote endpoints running out of insecure home office networks. These remote endpoints operate outside of the protected corporate perimeter.

Meanwhile, IT teams are tasked with the ultimate responsibility of protecting the organization's critical data, intellectual property, and to some extent, its brand and reputation.

ZT models are highly applicable in this scenario and are quickly becoming a component for enabling secure, scalable networks and systems.

A ZT model assumes everything trying to connect and or access an organization's network should not be trusted until verified. Until recently, this approach would have been highly complex and cost prohibited. Advances in technology and the continued adoption of communication standards across the IT industry now make it possible to implement a ZT model.

Some of the Use Cases That a ZT Model Addresses

Defense against the potential loss of critical and or customer data

Defense against the potential loss of intellectual property

Validation of remote connections into the corporate network

Implementation of a highly defensible position for the network and its connected assets

Highly effective defense against malicious activity

Proactive identification and defense against insider threats

Monitoring and enforcement of minimum-security baseline standards for all network-connected assets

Organizations that are looking to build a Secure Access Service Edge ("SASE") program

The CBI logo is a registered trademark of Creative Breakthroughs, Inc.

How Does a ZT Model Operate?

If the security status of any connecting endpoint or user cannot be resolved, the ZT model denies the connection by default. If the relationship can be verified, it will be subjected to a restrictive policy for the duration of its network access.

The ZT model also operates under the “least-privilege” principle, which states all programs, processes, devices, and users are limited to the minimum privileges required to carry out their functions. Least-privilege access rights can range from full access to no rights at all, depending on the verification results when accessing or connecting to a device, data, system, application, or service.

How Do I Implement a ZT Model?

It may help to look at ZT as a set of instructions for designing and implementing a secure network infrastructure versus an actual product that can be purchased.

That said, your ZT plan will still need to include the acquisition of some automated technologies, especially in the following key areas:

Asset type detection

Dynamic policy enforcement and network segmentation

Automated remediation capabilities

Automated workflow orchestration

Access security broker

Access rights management and policy enforcement

Authorization and authentication enforcement

Where Do I Start?

Now that we’ve defined the ZT model, how it operates, and why you should consider implementing one within your organization, we can talk about the steps you should consider when implementing it.

As stated earlier, ZT is not a single thing you can purchase, install, and turn on. It is an approach to handling enterprise-wide security. Like most projects, the more time you invest in developing a project plan, the easier it will be to implement.

Your project plan will need to include an initial set of assessments, planning, architecting, designing, piloting, and implementation.

Your Roadmap Should Include the Following

1. **Alignment**. In this initial phase, you should be trying to answer the following fundamental questions:
    - What are your overall business goals and objectives?
    - Have you included business unit managers and explained the benefits that a ZT model will have on their part of the organization?
    - Which networks will you target? Begin by creating a prioritized rollout plan based on the criticality of the system(s), the asset type(s) within them, and their overall level of risk to the organization.
    - Map goals of the ZT model rollout to known or historical cyber threats that may have already impacted the business.

2. **What, Where, Who.** Your approach should clearly define what data, applications, and systems you need to protect based on their criticality to the organization. Next, you need to focus on locating, identifying, and classifying your organization's data, where it's going, how it's getting there, and most notably, the levels of access and permissions your end-users have to those data, applications, and systems. Make sure to include an evaluation of on-prem, data center, and cloud-based networks.

3. **Prepare.** Start by evaluating any pre-existing ZT elements that you already have in place. It might not be obvious in some cases, but some systems can be repurposed or upgraded to address portions of a ZT model. Also, keep in mind the policies, procedures, and workflows you may need to create and or modify as a result of implementing a ZT model. This step is crucial for allocating the proper resources, time, and budget to your ZT model. A ZT model is typically broken into two technical domains, cloud and on-prem. As stated previously, a ZT model is "Anything connecting to the network should not be trusted by default." ZT enforces this rule for everything (a.k.a. objects), including users, devices, endpoints, systems, etc. ZT implies a method to properly verify all items before they are allowed to access the network or to have anything access them. Since these objects are found in the cloud as well as on-prem networks, you need to implement technologies that can enforce ZT principles within both of those network types.

4. **Build.** Your ZT model should accommodate traditional local and wide area networks, software-defined networks, and dynamic segmentation based on asset type as well as verified end-user identities.

   In the previous steps, you located, identified, and classified your organization's data, where it's going, how it's getting there, and most importantly, the levels of access and permissions your end-users have to that data.

   Start by building your ZT policies. These policies will govern the level of scrutiny you place on assets attempting to gain access to your networks and data based on a set of predefined rules. Create groups of user types based on their minimum level of access needed to perform their job function. Once you have these policies, you can acquire the automated technology that best fits your needs. You should create a test environment to adjust your group policies.

5. **Improve.** You will want to capture as much quantifiable data as possible as you continue to expand your ZT footprint. Rely on first-hand feedback from your test users as well as data collected from security information event monitoring ("SIEM") and end-user behavioral analytics platforms. Adjust your ZT program policies as needed.

Technical Recommendations

Scrutinize which users truly need an account that allows them to access your network via traditional VPN.

This review will shift the administrative workload associated with the support of resource-intense legacy network connections to one based in agentless-identity and device-aware access.

Your ZT program must include an integrated multi-factor authentication capability.

This feature significantly decreases the risks associated with identity-based authentication and context-based adaptive access control networks.

Consider a cloud-based ZT network architecture if your traditional VPN is limited in capacity or bandwidth.

If possible, replace applications that expose services directly to the internet.

Online services that require partner accessibility should be included in early testing phases.

Ensure your ZT program aligns with it any Secure Access Service Edge ("SASE") model that you may already have or plan to implement in the near future.

Summary

ZT programs have a lot of moving parts, and they require a wide array of security and risk management disciplines. If you are considering a ZT model and need assistance in developing your policies, selecting the appropriate technologies, or want some advice on where to start, please Contact CBI today.