DELL Technologies

Supporting Zero Trust Goals

Without redeveloping your cybersecurity framework

By Daniel Carroll

A key element of Zero Trust principles is the verification of assets within the enterprise prior to providing access, and continued verification prior to execution of processes or lateral movement within the network.

An increase in ransomware, security vulnerability exploitations, and supply chain attacks has generated renewed interest in Zero Trust principles for cybersecurity. There have been a number of U.S. federal and DoD directives on the topic and a recent reference architecture by the National Institute of Standards and Technology (NIST).

This has helped organizations reassess their current approach to and application of Zero Trust principles. These organizations face the challenge of how to understand where they are in their journey and whether their current cybersecurity framework will help them achieve the best outcomes.

Old is new again.

The principles defined by Zero Trust are not new. Zero Trust is built on the definition of "never trust, always verify." This is based on the idea that all identities within an architecture should be validated prior to allowing them to execute a function or access a resource (object). The concept dates back to 1994, when Stephen Paul Marsh introduced it in his doctoral thesis.[1] Over the years these principles have been adopted into security control guidance and architectures defined by various cybersecurity industry leaders like NIST.

What is Zero Trust?

NIST defines Zero Trust in their Special Publication 800-207 (SP 800-207) as an approach primarily focused on data and service protection, but one that can and should be expanded to include all enterprise assets.[2] It is not a single architecture but a set of guiding principles for workflow, system design, and operations. A key element of Zero Trust principles is the verification of assets within the enterprise prior to providing access, and continued verification prior to execution of processes or lateral movement within the network.

A variety of publications and media outlets have discussed Zero Trust, but how do you separate the noise from sound guidance? The truth is, if your organization already has strong cybersecurity practices and a defined roadmap, you don't need to start over. New government guidance and directives can be used to assess the models already in place and the room for improvement.

The Dell Technologies goal is to help U.S. federal customers meet their missions. Cybersecurity attacks have gotten bolder and more brash, and the President's Executive Order on Improving the Nation's Cybersecurity aims to tackle that challenge directly.[3]

How Dell Technologies looks at the Zero Trust model:

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resource is granted on a per-session basis.
- Access to resources is determined by dynamic policy.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

[1] Stephen Paul Marsh, Formalising Trust as a Computational Concept, University of Stirling, April 1994.

[2] Scott Rose et al., Zero Trust Architecture, NIST, August 2020.

[3] The White House, Executive Order on Improving the Nation's Cybersecurity, May 2021.

Discover how Dell Technologies can secure your infrastructure and advance your federal initiatives. Contact us at DellFederalSales@federal.dell.com or 855-860-9606.

- All resource authentication and authorization are dynamic and strictly enforced before access is permitted.
- The enterprise collects as much information as possible related to the current state of assets and uses it to improve its security posture.

Dell Technologies has developed a derivative model called the Seven Pillars of Cybersecurity. The goal of the Seven Pillars model is to make it easier for cybersecurity leaders to assess their current framework, and to explain how Zero Trust principles enhance the security model.

The Seven Pillars are set up to allow for the visualization of distinct assets and communication flows:

1. **Device Trust** is defined as any physical device within the enterprise. Examples would include user devices (such as smartphones, tablets, and laptops), data center devices (such as servers, storage, and network switches), and IoT devices (such as sensors, cameras, and kiosks).
2. **User Trust** is defined as end user, administrator, and service level accounts.
3. **Transport/Session Trust** is defined as the communication path used to move into, across, and out of an enterprise network.
4. **Application Trust** is defined as local and cloud applications that enter, work within, or leave the network for data access.
5. **Data Trust** is defined by the organization as key assets used to execute the function and mission of the organization that can be held within the enterprise and extended into cloud services.
6. **Visibility Analytics** are defined by the resources from the previous five pillars that should be enabled, to the fullest extent, to allow for analysis of the secure state and function of the pillar definition.
7. **Automation and Orchestration** are defined through the use of the visibility and analytics output to perform policy enforcement, baseline configuration definitions, automated remediation, and conditional access models.

Why seven pillars?

By organizing the NIST SP 800-207 model into a Seven Pillars model, Dell Technologies helps make the concept more accessible to organizations—from tech to legal. The Seven Pillars can be viewed as a communication flow from left to right: A device is accessed by a user to cross a communications path to access an application to obtain data. Logging and alerts should be configured to feed visibility analytics, to help improve automation and drive orchestration of policy enforcement.

Data governance

The most critical aspect of a Zero Trust principle–driven cybersecurity architecture is data governance. Who owns the data, how sensitive and critical is the data, and who should have access? These are key questions not often well defined in many enterprises. This is due to the evolution of enterprise infrastructures over the decades and the massive amount of data being generated in modern infrastructures because of the advent of cloud and edge/IoT solutions that makes it hard to define an owner.

An effective path to success

The key to effective improvement within a well-established cybersecurity framework and defined roadmaps is to ensure there are clear targets for improvement that assess the components and how they build out into the whole. As an example, there are usually departments, or split duties within an enterprise, focused on delivering IT services that support a particular outcome or mission. One team may be charged with managing the application infrastructure, separate from compute and storage management, separate from end-user management. These management teams need to work together to improve the total organizational cybersecurity framework adoption of Zero Trust principles.

About the author: Dan Carroll

Dan Carroll leads the cybersecurity practice development for the Office of the CTO, Dell Technologies, Federal. He focuses on designing and implementing cybersecurity frameworks to help federal customers meet their diverse cybersecurity missions. Dan served in the U.S. Marine Corps Base Quantico.

DELL Technologies