ClearArmor Zero Trust Architecture Resource Planning (ZTRP)

Move Beyond Discussion….Successfully Implement a Zero Trust Architecture and Manage Your Zero Trust Program

Introduction

Despite having implemented scores of specialized cybersecurity tools over the past decade, government and commercial enterprises are continuing to see uncontrollable waves of costly network and data breaches. As a result, the U.S. Federal Government is mandating the implementation of the Zero Trust Architecture. This mandate includes all Government agencies, and will all include all vendors who provide goods and services to the U.S. Government.

The Zero Trust Architecture is a reality, but few organizations have implemented it to date due to several factors:

- First, **there has been a tremendous amount of discussion about the concept and goals, but no prescriptive framework or guidelines for what to do, how to do it, and what a successful program would look like have been defined until now.**
- Secondly, **many vendors have created confusion by offering tools with niche functionality that address some aspect of the Zero Trust Architecture concept.** They claim to offer Zero Trust Architecture solutions, when in fact they are one piece of a larger process.
- **Zero Trust is a clearly defined, managed and continuously evolving process, it is not the random application of technology.**
- Finally, **most organizations cannot implement zero trust because they are not utilizing discovery technologies that provide the scope, accuracy and quality of data** that will be required as a foundation for Zero Trust activities. An enterprise-level discovery process that covers 100% of physical and virtual endpoints, servers, installed and cloud software, application and SBOM vulnerabilities, and more is essential and mandatory. Many discovery tools are focused on supporting a particular function like license management or security and in the end, are too restricted for the wide-ranging but stringent requirements of Zero Trust Architecture.

Implementing a Zero Trust Architecture Initiative

To move beyond the discussion and successfully implement an effective Zero Trust Architecture program, you need:

- A prescriptive set of guidelines
- An automated, continuous, and repeatable management process
- Tools that automatically provide all required data, a method for managing activities and process workflows, and a means of reporting on progress.
- The implementation of a continuous auditing and verification process – Zero Trust is not “one and done”.

To successfully plan and implement a program, you need to know:

- What are the specific objectives and goals of your Zero Trust program?
- What networks, endpoints, systems and people are involved?
- What activities and tasks need to be defined, implemented, automated, and verified?
- How the activities will be completed (process)?
- Who is responsible for completing each task?
- How will progress be measured (method and metrics)?
- What work has been done to date?
- What work remains to be completed?
- What are the highest risks and priorities?

Eracent's ClearArmor Zero Trust Resource Planning (ZTRP)

Process – Tools – Data Analysis – Management and Audit

Eracent offers and complete and unique comprehensive framework management process to support and expedite the implementation of a Zero Trust Architecture initiative. No matter what tactical tools you are using, ***the ZTRP solution pulls together your tasks, processes, teams and systems. The result is complete visibility into your program, a single management and reporting platform, and automated, repeatable processes.***

ZTRP includes a set of best practices for establishing a Zero Trust Architecture program that can be adopted and followed as-is or they can be modified to meet your organization's specific requirements.

The ZTRP platform provides intuitive framework management capabilities.

- All major activities are mapped out in a tree structure
- All systems, endpoints, installed software, vulnerabilities and people are linked to any other entities as appropriate.
- Tasks, activities, specific action items and policies are described and tracked throughout
- People responsible for each activity or process are assigned
- The frequency of each activity is designated
- Metrics and reporting contents are defined and can be modified to meet your organization's needs.

Many activities in the ZTRP solution are automated and replicated, like following an instruction manual. This will save time and establish protection and results in an accelerated manner, while reducing the risk that any steps or systems have been overlooked. These controls ensure that your Zero Trust program is fully auditable, and it can seamlessly fit into a larger Risk Management program.

Summary

The ClearArmor ZTRP solution consolidates and transforms the concept of Zero Trust Architecture into a complete implementation within an organization. ZTRP distills the theoretical implementation of Zero Trust into a structured and auditable process that brings together all of your networks and endpoints, their components, software applications, organizational data, policies, and audit and risk analysis into one streamlined, automated management tool.

To learn more about the ClearArmor ZTRP solution, contact Eracent today or visit www.eracent.com.

Eracent, Inc.
519 Easton Road, P.O. Box 647
Riegelsville, PA 18077 USA

info@eracent.com
+1- 908-537-6520

www.eracent.com