FOUR POINTS TECHNOLOGY

Zero Trust Overview

Overview

Threat actors, specifically those who are state-sponsored, have redefined the threat landscape with their creative exploitation of vulnerabilities. In response to these ever-increasing and evolving attacks on Federal agencies, we have seen Executive Orders (EO), mandates from the Office of Management and Budget (OMB), new security archicture standards from the National Institute of Standards and Technology (NIST), and guidance on creating a Zero Trust Architecture (ZTA) from the Cybersecurity and Infrastructure Security Agency (CISA).

An assessment of your organization against CISA's ZTA compliance structure is critical in understanding your current security posture and figuring out where the gaps lie.

ZTA Self-Assessment: Where Do You Stand?

- Are you continuously monitoring and validating your organization's security posture?
- Do you continuously verify identitities and applications across your organization's environments?
- Is there a single identity perimeter for your cloud, on-prem, and hybrid environments?
- Are you able to quickly, or automatically, disperse security policy actions across your organization?
- Can you successfully categorize, inventory, and encrypt data, and provide dynamic access to it?
- In DevSecOps pipelines, are you able to scan and fix vulnerabilities in your code and executables?
- Is your network segmented to protect critical data and workflows?
- Do you employ any Artificial Intelligence (AI) or Machine Learning (ML) models to detect anomalies?

The CISA Zero Trust Maturity Journey

CISA defined a maturity model for ZTA, represented in *Figure 1*, with four states -- Traditional, Initial, Advanced, and Optimal. This model serves as a road map for agencies by identifying their current state and what they need to do to get to an optimal state.

As you advance to the next stage, you can expect an increase in both the level of effort and the benefits received. These stages are dynamic -- your plan to progress to the next state, and its scope and impact, may change over time.

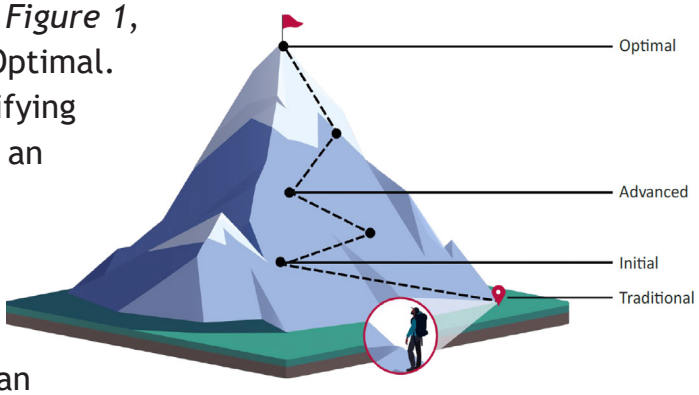

Figure 1, Zero Trust Maturity Journey
© CISA, 2023

The CISA Zero Trust Maturity Model

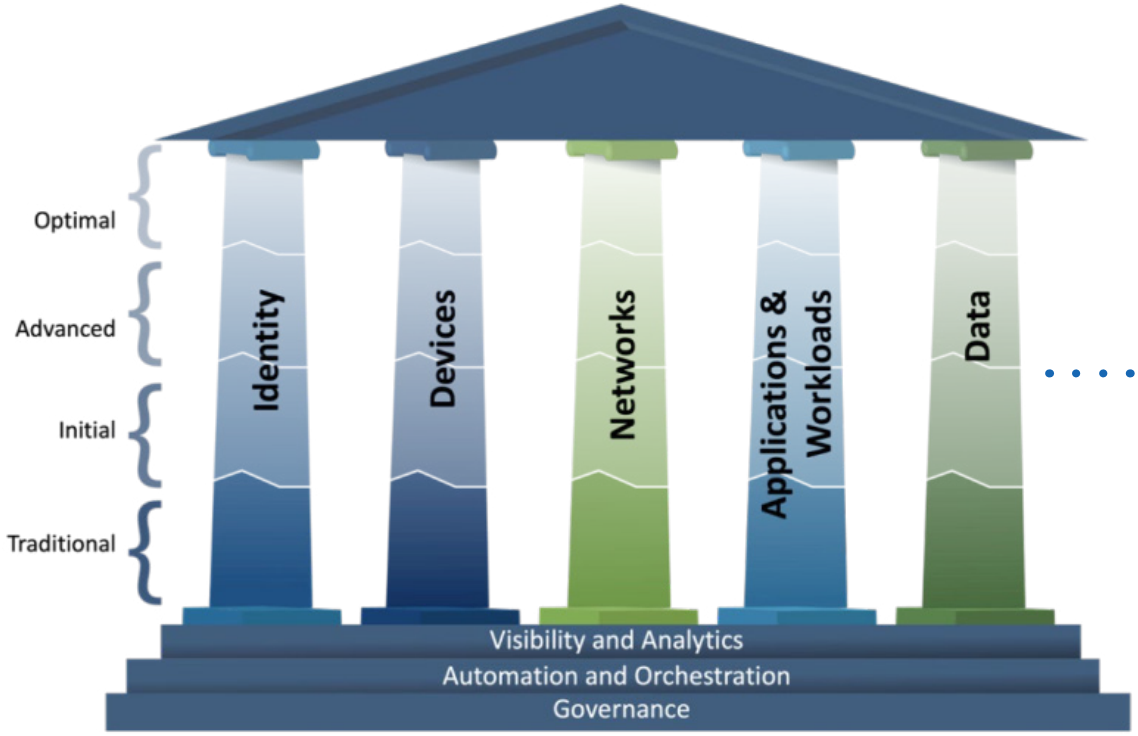

Figure 2, Zero Trust Maturity Model © CISA, 2023

In today's technology landscape, agencies are faced with the daunting task of modernizing their architecture to keep up with rapidly evolving environments. In response, CISA created the Zero Trust Maturity Model (ZTMM) to provide agencies with a clear path forward as they transition to, and, ultimately, evolve their architecture.

The ZTMM, shown in *Figure 2*, incorporates five pillars, three cross-cutting capabilities, and the maturity states from *Figure 1*. As you progress through the model, you move closer toward optimal zero trust implementations -- characterized by automated solutions and fully integrated, dynamic systems. Each pillar can progress at its own pace, which allows for a gradual evolution to zero trust.

Getting Started

It is normal to find this process overwhelming, or to not know where to start. That is where Four Points Technology comes in. As a Service-Disabled Veteran-Owned Small Business (SDVOSB) Value-Added Reseller (VAR), we have experience with helping Federal customers across all ZTMM pillars and capabilities. Our team is here to help you understand the process, identify your security challenges, and solve your pain points. Contact us to learn more!

FOUR POINTS TECHNOLOGY

CONTACT US FOR MORE INFORMATION:
sales@4points.com | 703-657-6100

Four Points Technology, LLC
13221 Woodland Park Road, Suite 400, Herndon, VA 20171 • www.4points.com