SteelCloud

# Realizing the Promise of Zero Trust

*Prior to designing a Zero Trust Architecture, a baseline protection level must be implemented which is in compliance with existing IT security policies and standards.*

Source: DoD Zero Trust Reference Architecture v1.0

September 2023

The term "Zero Trust" refers to a set of cybersecurity initiatives and strategies that assume no actor/service/system can be trusted—regardless of their location or ownership—and, therefore, the concept of cyber defense moves from the perimeter to, or closer to, the individual data repository or application. Equally important, Zero Trust increases the breadth and depth of continual verification versus the traditional single verification at the network perimeter.

Government agencies have been moving toward Zero Trust philosophies for years, through policies and capabilities such as the FISMA (Federal Information Security Modernization Act), RMF (Risk Management Framework); FICAM (Federal Identity, Credential, and Access Management); Trusted Internet Connections; and CDM (Continuous Diagnostics and Mitigation) programs.

As an umbrella of cyber technologies/initiatives, Zero Trust relies on and builds on many traditional cyber best practices and technologies. As stated in NIST 800-207, Zero Trust Architecture, "Organizations need to implement comprehensive information security and resiliency practices for Zero Trust to be effective." These would include firewalls, IDS/IPS, anti-virus/malware, two-factor authentication, secure endpoint configurations, and NAC (network access control). Zero Trust also dictates additional capabilities to support its new paradigm and specific changes in the implementation of traditional cyber technologies/best practices.

So, at a high level, think of Zero Trust as a roadmap that first dictates that cyber leadership fully implements its traditional cyber technologies and best practices as a foundation in preparation to layer on new Zero Trust-specific cyber capabilities. Of these, secure and compliant baselines are imperative because the implementation of Zero Trust will rely on/build on the blanket of protections provided by a STIG compliant environment.

Undoubtedly, the most significant change prescribed by Zero Trust is the depth and frequency of validation of both user identity and configuration of the endpoint/system accessing the infrastructure. As mentioned earlier, a foundational concept of Zero Trust is that validation moves from a single instance at the perimeter of the network to individual validations at each data source.

Before the initiation of Zero Trust, organizations might only remediate their infrastructures once a quarter and validate compliance monthly. With Zero Trust, configurations will most likely be validated multiple times per day. These system validations will include both patch levels and security policy configurations using industry standard STIG or CIS benchmarks.

## SteelCloud's Zero Trust Initiative


The success of Zero Trust depends upon it being built on top of a secure and compliant baseline. SteelCloud's ConfigOS software has been used across the federal government to automate the remediation of endpoint STIG/CIS compliance at the lowest cost/effort and the highest level of consistency. Military components and civilian agencies are currently using ConfigOS in development, integration,authorization/RMF, and sustainment use cases in cloud, on-prem, and classified environments.

SteelCloud follows the federal government's Zero Trust initiative closely. The DoD Zero Trust Reference Architecture document dated July 2022 introduces the Zero Trust Framework. This framework identifies the "Pillars" that surround the protection of data. Over the last year, much of the ZTA focus has been the "users" Pillar. However, this DoD ZTA framework document

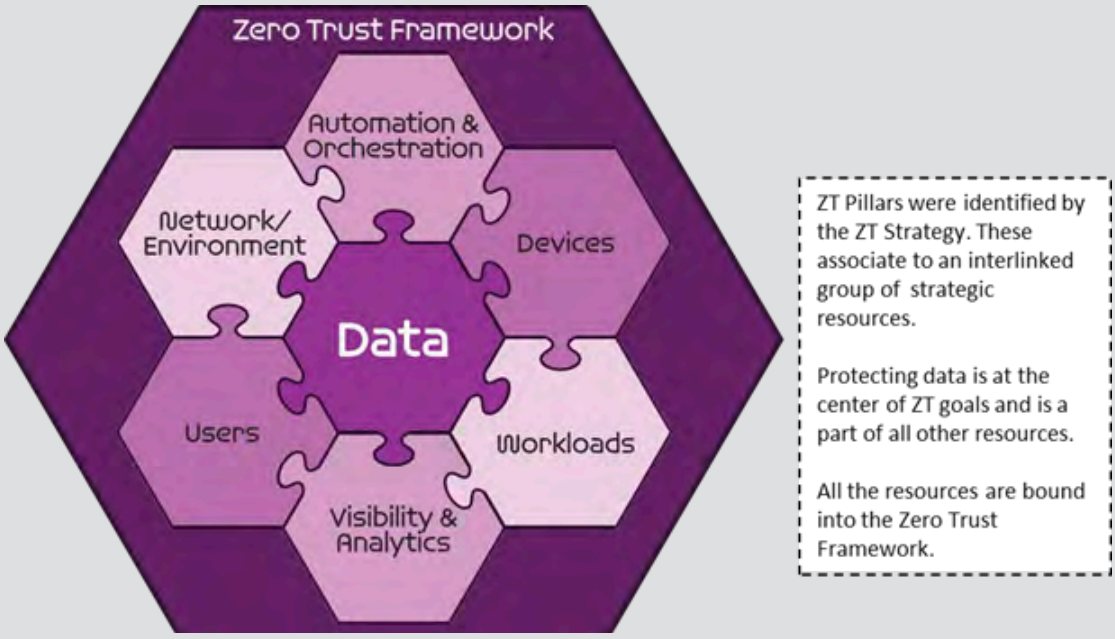
also focuses on the "devices" and "workloads" Pillars. In that discussion, configuration compliance is a baseline objective of any ZTA effort. SteelCloud has added significant new capability to ensure the automated continuous compliance of infrastructure endpoints. Additionally, our new ConfigOS MPO (Master Policy Object) software application was designed to address the complexities of workstation compliance for transient and hybrid workforces connected through VPNs and other bandwidth-constrained communications. ConfigOS MPO provides our customers with the most efficient mechanism to address the ZTA device pillar for workstations.

ConfigOS MPO supports Zero Trust implementation in two ways. First and foremost, its agent is semi-autonomous, able to scan and/or remediate systems both on and off the network. Thus, endpoints will be in continuous compliance without the need for scheduling separate remediation or scanning activities. Secondarily, the agent will make detailed security configuration information available for validation by a NAC for a "comply-to-connect" capability at the endpoint, eliminating the need to drill back into some central repository for this information. When considering the millions of endpoints within federal organizations that will have to be validated, most multiple times per day, this approach is infinitely scalable and less fragile than other approaches. Gartner concurs that, whenever possible, it is preferable to make ZT decisions based on information that can be retrieved locally from the system.

So, with SteelCloud, the same technology utilized to establish a securely perfect baseline and keep endpoints continuously in compliance is also used for simple, scalable Zero Trust validation.

A byproduct benefit of the implementation of a semi-autonomous compliance agent is that it reduces network traffic by 90%+ for scan and remediation compliance activities. This advantage becomes even more critical as more and more endpoints are connected to the enterprise via lower bandwidth VPNs.

## Operational Activity Model




Source: DoD Zero Trust Reference Architecture v2.0

## About SteelCloud

SteelCloud develops ConfigOS, a family of STIG and CIS compliance software products for government and commercial customers. Our software reduces the complexity, effort, and expense of testing, building baselines, and implementing system-level controls into virtually any infrastructure. ConfigOS has been implemented in use cases addressing cloud migrations, OT/SCADA infrastructures, weapon systems, and classified environments. ConfigOS can also be a valuable tool to support Zero Trust and RMF while driving compliance throughout every stage in the Development, Authorization, and Operations processes. SteelCloud products are easy to license through our GSA Schedule 70 contract or other GWACs. SteelCloud can be reached at 703.674.5500 or info@steelcloud.com. Additional information is available at www.steelcloud.com.

*SteelCloud's ConfigOS software helps you STIG FASTER!*

SteelCloud
20110 Ashbrook Place, Suite 200
Ashburn, VA 20147
1.703.674.5500
info@steelcloud.com | **steelcloud.com**