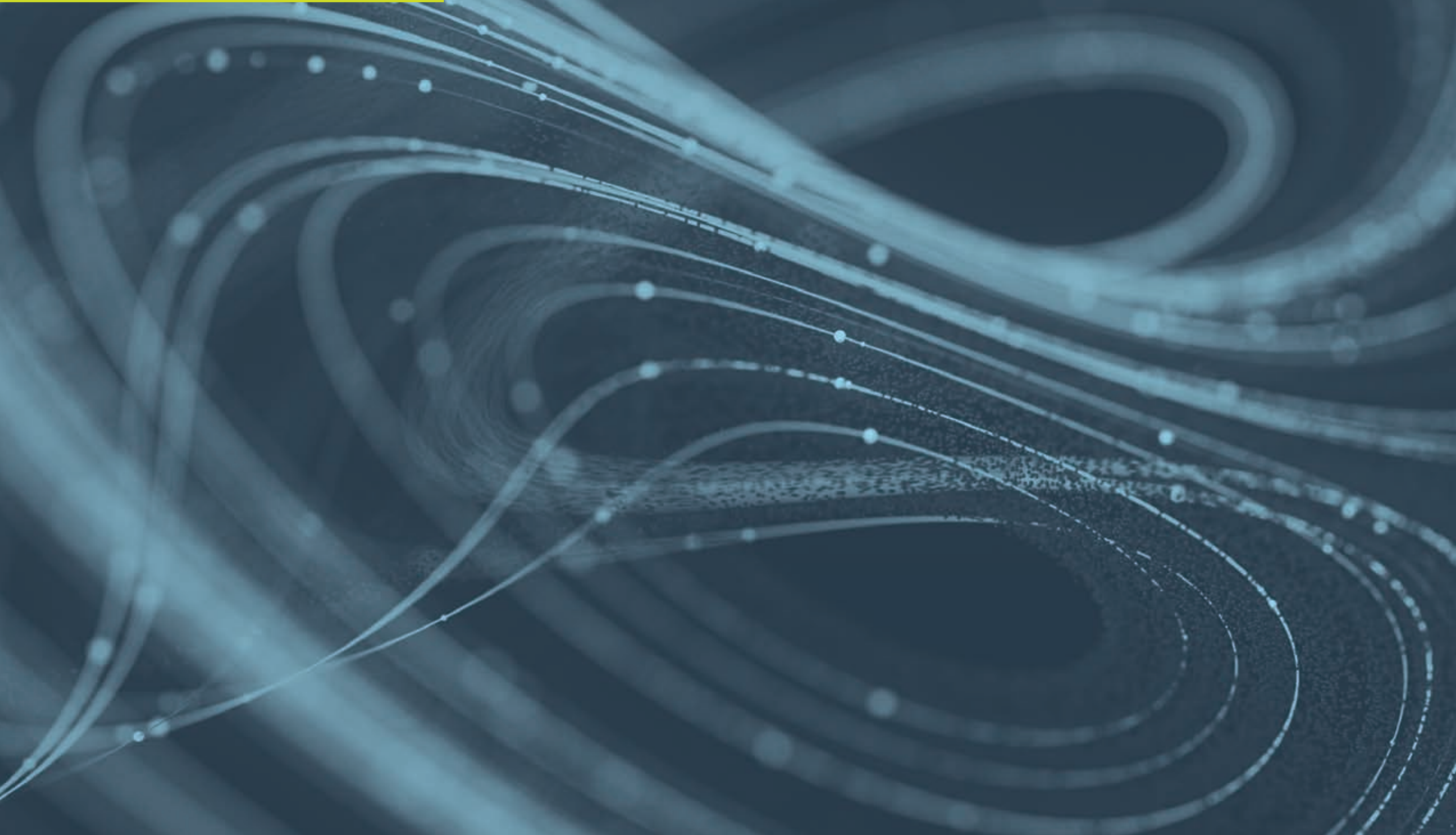
Booz
Allen®

How Enterprises Can Master Zero Trust

ZEROING IN



The Zero Trust rush is on, but achieving it is no small feat. *Don't buy into the cybersecurity product hype; Zero Trust isn't something you can purchase. Zero Trust Architecture (ZTA) is a framework and mindset that requires an enterprise estate-wide (identity, systems, application, network, and data) approach, where continuous verification is performed at all levels before granting access. This holistic security philosophy is far more effective at defending against today's advanced attacks than traditional defense-in-depth or perimeter-based models.*

ZERO TRUST ISN'T SOMETHING YOU CAN PURCHASE

Zero Trust Architecture is a framework and mindset that requires an enterprise estate-wide approach.

WHAT IS ZERO TRUST ARCHITECTURE?

At its core, Zero Trust requires that trust is earned, not given. Sometimes described as 'just in time' security (JIT), every entity attempting to access an enterprise's systems and data is scrutinized. In a Zero Trust Architecture (ZTA), the focus is on protecting and providing secure access to an organization's data–regardless of where the data resides. As enterprise technology ecosystems and adversaries evolve, how we think about deploying security and technology capabilities must follow suit. However, the true challenge lies in taking deliberate actions that not only reduce cyber risk but also revolutionize the way various IT silos and enterprise technology teams collaborate and adapt to the ever-evolving security landscape. This 'never trust, always verify' paradigm shift can empower organizations to meet the unique challenges of the digital age while safeguarding their assets and ensuring operational continuity.

THE FOUNDATIONS OF ZERO TRUST

ASSUME BREACH

In an "assume breach" model defenders must adapt to operating in an adversarial environment where the threat actors are assumed to be present.

NEVER TRUST, ALWAYS VERIFY

All requests to access Data, Applications, Assets, and Services are denied by default and require explicit verification using authentication and authorization mechanisms.

USE LEAST PRIVILEGE ACCESS

Access privileges are restricted to the minimum necessary to perform specific roles within the organization. Elevated privileges are aligned to specific functions and are time-bound.

WHY THE COUNTDOWN TO ZERO TRUST IS ON

The ubiquitous nature of connectivity across the digital ecosystem demands that teams work together to do more to defend against multi-dimensional cyber attack schemes. Enterprise IT and Security teams are often funded in silos, with each group prioritizing their own needs and agendas. While IT teams typically look to provide the most frictionless experience, those on the security side of the business take a security-first approach. Today's threat landscape requires a holistic, cross-business defensive strategy that provides greater visibility, control, orchestration, and automation across all Zero Trust pillars. While ZTA is not (yet) federally mandated in the public sector, critical infrastructure compliance is a hot topic in Washington. As the journey to Zero Trust is a multi-year process, businesses need to start rearchitecting their security strategies now in order to keep pace with what's to come.

IT PAYS TO ADOPT ZTA

Zero Trust is a mindset change, architectural approach, and cultural philosophy shift that drives an enduring horizontal security journey yielding a variety of positive impacts across the business.

REDUCES RISK

By enabling continuous assessment and response to threats across the entire digital estate, Zero Trust acts as an insurance policy against substantial potential loss.

STAKEHOLDER-DRIVEN ADOPTION

From CEOs focusing on business value to IT and security teams implementing technical solutions, all stakeholders benefit from improved risk management and user experience.

BUSINESS-ALIGNED STRATEGY

CIOs ensure the Zero Trust approach aligns with organizational goals, while CTOs champion technology adoption from infrastructure to applications.

ENHANCES PRODUCTIVITY

As Zero Trust maturity increases, defense and remediation tasks become more automated, resulting in more agile and productive IT and cybersecurity teams.

SAVES TIME AND MONEY

ZTA cuts down on the reaction time required to combat threats and helps avoid the steep costs associated with data breaches.

SIMPLIFIES COMPLIANCE

The granular access control required in a ZTA also aligns with data privacy regulations like GDPR, CCPA, CMMC, HIPAA, and PCI, making it easier and less costly to meet regulatory requirements through streamlined processes and enhanced visibility.

DRIVES OPERATIONAL EXCELLENCE

Enhances operational efficiency by streamlining access to resources while protecting identities, managing authentication, and enforcing authorization.

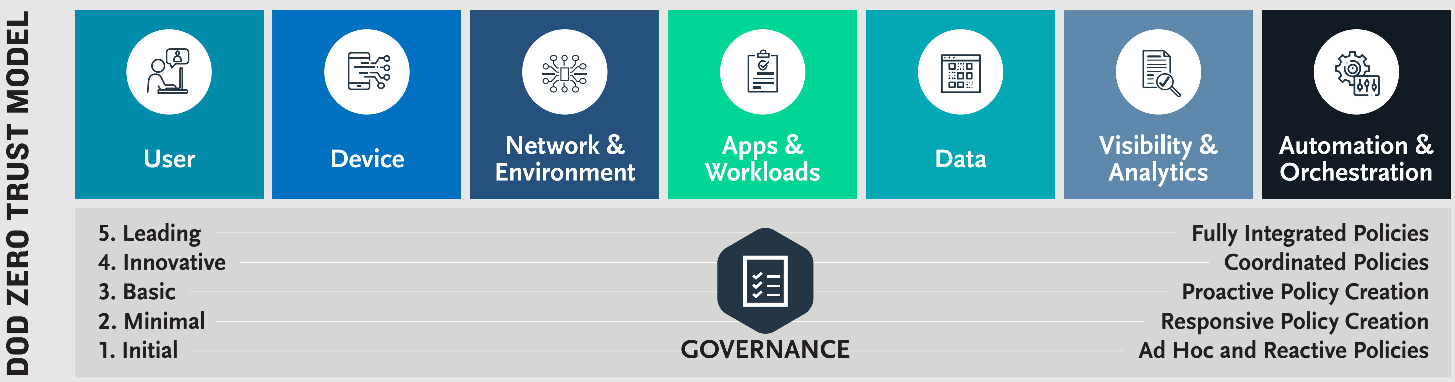
ZERO TRUST VS NIST CSF

One of the most frequently asked questions from business leaders considering moving to a ZTA is: *“Why do I need Zero Trust if I’m already leveraging the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)?”* Put simply; Zero Trust is the ‘what’ of security, and NIST CSF is the ‘how-to’. Zero Trust offers focus by providing a more prescriptive set of principles to guide your security strategy, while NIST CSF enables a flexible approach that you can tailor to achieve those security objectives. Implementing Zero Trust enables organizations to withstand today’s most sophisticated cyber attacks.

NEXT STEPS IN THE JOURNEY TO ZERO TRUST

Ready to start moving towards a state of Zero Trust? Remember: this transformation is a marathon, not a sprint. Baselining and prioritization are key as you reveal your organization’s current state and get the insight you need to take meaningful action.

Booz Allen has developed a Zero Trust Maturity Approach that enables enterprises to systematically enhance cybersecurity within the framework. Informed by both the DoD Zero Trust Model and the CISA Zero Trust Model, it provides a thorough and pragmatic assessment of the organization’s current state. This in-depth analysis enables us to identify and roadmap opportunities strategically to modernize services across the base ZTA pillars and reach a prescribed target state maturity. We empower clients with targeted Zero Trust solutions, driving down operational risk and enhancing overall cybersecurity resilience.



DOD ZERO TRUST MODEL

User

Device

Network & Environment

Apps & Workloads

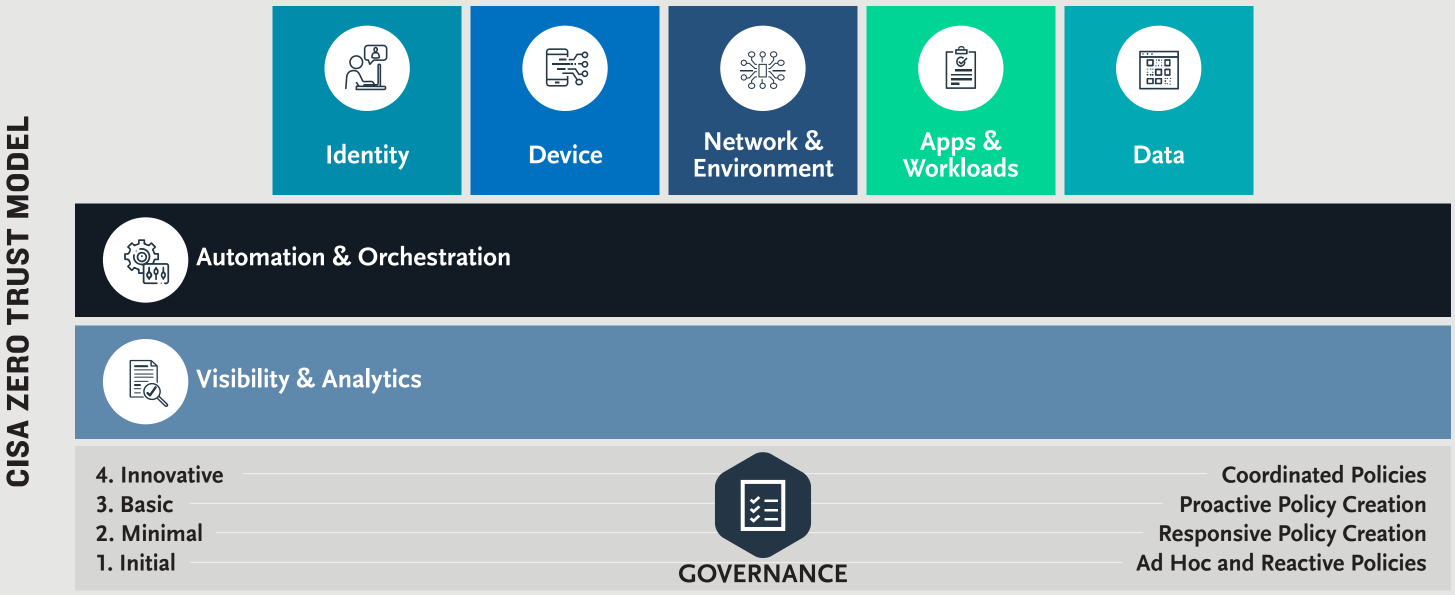
Data

Visibility & Analytics

Automation & Orchestration

5. Leading — Fully Integrated Policies
4. Innovative — Coordinated Policies
3. Basic — Proactive Policy Creation
2. Minimal — Responsive Policy Creation
1. Initial — Ad Hoc and Reactive Policies

GOVERNANCE



CISA ZERO TRUST MODEL

Identity

Device

Network & Environment

Apps & Workloads

Data

Automation & Orchestration

Visibility & Analytics

4. Innovative — Coordinated Policies
3. Basic — Proactive Policy Creation
2. Minimal — Responsive Policy Creation
1. Initial — Ad Hoc and Reactive Policies

GOVERNANCE

THE BOOZ ALLEN DIFFERENCE

We developed proprietary tools and intellectual capital, informed by hundreds of assessments for the public and private sectors, to help our clients move strategically to buy down risk quickly.

ZERO TRUST DIAGNOSTIC ANALYTICS:
To control subjectivity, we employ analytics that model capability baseline data against threat scenarios to uncover and prioritize gap-related risks.

ZTA DESIGN SOLUTIONS:
We accelerate your ability to close critical gaps and formulate a multi-year roadmap by drawing on a library of ZTA design solutions that span the pillars of DoD and CISA's Zero Trust models.

CROSS-DISCIPLINE EXPERIENCE:
Talented subject matter experts across the firm in the vertical pillars and horizontal ZTA pillars of analytics, visibility, systems integration, orchestration, and program governance.

PRODUCT AGNOSTIC:
Unlike industry-specific product vendors that have dominated the commercial narrative by focusing on one pillar of Zero Trust, we take a holistic approach to address each organization's unique requirements, risk tolerance, and business goals across all ZTA pillars.

LEADING THE WAY IN ZTA:
Our ground-breaking work leading the federal government's most critical ZTA reviews resulted in DISA awarding us the opportunity to spearhead the DoD Thunderdome.

For general inquiries, please contact: **infosec@bah.com**

About the Author

Thor Draper

Thor is a Principal at Booz Allen Commercial practice, he oversees the firm's Commercial Zero Trust Cyber practice, Enterprise Hardening, and Attack Surface Management, delivering capabilities that help commercial clients reduce operational and business risk. He brings more than 35+ years of industry leadership experience in information technology (IT) across various aspects of infrastructure engineering, enterprise architecture, and solution architecture.

For general inquiries, please contact: **infosec@bah.com**