STOIC: A Strategy for Pursuing Zero Trust

What Is Zero Trust (ZT)?

Zero Trust is a business strategy and IT/cybersecurity framework which reduces organizational exposure to increasing and evolving cyber threats by optimizing cloud, mobility, and other cutting-edge capabilities. Focused on five key elements, (***identity, devices, network, workflows,*** and ***data)***, ZT challenges traditional perimeter-based security models by embracing three principles for continuous, real-time security:

- ***Ongoing Verification*** – verify all authorization requests from users, devices, and applications,
- ***Least Privilege*** – only grant user, device, and application permissions for authorized activities, and
- ***Assume Breach*** – limit access to applications, services, networks, systems, and users by treating each as though they have been compromised.

Building Zero Trust Architectures (ZTAs) will require organizations to re-evaluate, refine, and sometimes redefine IT and cybersecurity strategies:

Anytime, Anywhere Computing – New, enhanced, and expanding technology is changing how people work and share information; users expect secure, on-demand access to networks, services, and data.

Advanced Persistent Threats (APTs) – Increased volume and sophistication of cyber-attacks, security breaches, and data compromises are threatening governments, businesses, and private citizens alike. Increased remote working, distributed networks, and more end points means additional opportunities and attack surfaces for malicious actors.

Zero Trust Architectures and Operations (ZTA/ZTO) – Governments and cyber-savvy organizations around the world are embracing an IT paradigm shift; empowering productivity by embracing technology while making enhanced security transparent to the end user.

How STOIC and Trinity Can Help Your Organization

Pressure to do more about cybersecurity, faster, and with limited resources, comes from all directions:

- Threats and vulnerabilities are increasingly dynamic, complex, and available
- Attacks, breaches, and compromises occur more frequently
- Breach impacts are more severe and widespread
- Laws, regulations, and recommendations are constantly changing, but rarely come with guidance, funding, or staff to implement viable solutions

Trinity created ***Strategy, Technology, and Operations Integrated with Cybersecurity (STOIC)*** to address these challenges as we advise clients, build realistic implementation plans, and support continuously evolving changes, priorities, and requirements. ***STOIC*** is built on tenets of Zero Trust, especially assumption of breach. First acknowledging the persistence of cyber-attacks, Trinity helps clients:

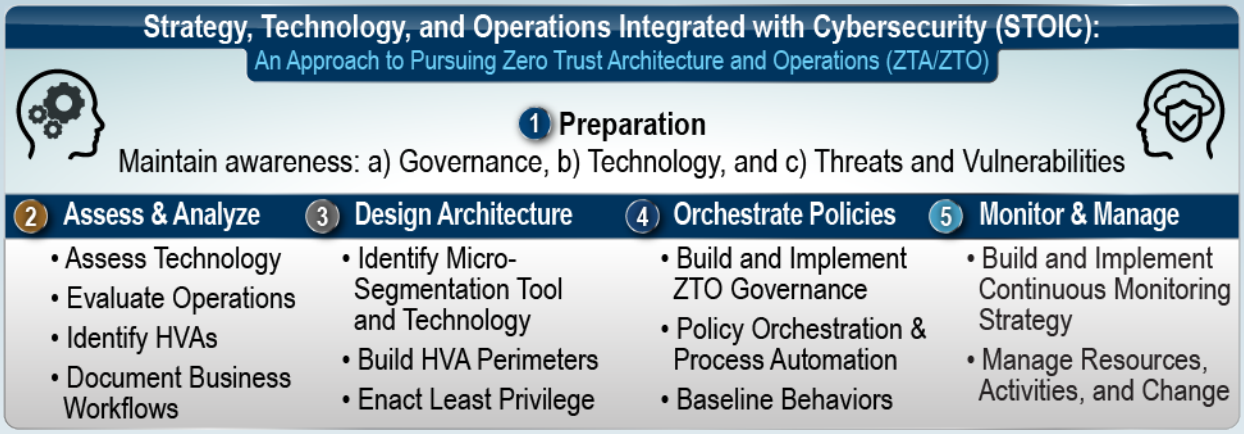
1) understand their needs and environments,
2) develop comprehensive strategies which anticipate threats,
3) wisely invest in current and future technologies, and
4) adapt to changes as they arise.

Planning for worst case scenarios drives smart investments, focused training, and incident prevention, detection, and response preparation. Applying ***STOIC***, our cyber Subject Matter Experts (SMEs) help clients understand internal and external influences, challenges, and strategies to pursue ZTA/ZTO.

STOIC: A Strategy for Pursuing Zero Trust

STOIC In Action

STOIC integrates cybersecurity governance and operations with client's existing technology and current engineering and business processes to capitalize on previous investments and promote ZT principles. This awareness-driven, phased approach introduces enhanced cybersecurity protection and detection capabilities while building stakeholder buy-in to accelerate adoption of new processes and technologies.



Preparation – Our SMEs continuously engage the cybersecurity community to maintain awareness of ongoing changes to governance (i.e., laws, regulations, policies, and guidance), tools and technology, and trending threats vectors and vulnerabilities. Keeping our clients informed on Department of Defense (DoD), Cyber and Infrastructure Security Agency (CISA), and National Institute of Standards and Technology (NIST) ZTA/ZTO initiatives enables informed, prioritized strategy decisions and investments. As needed, we build and deliver briefings and training to help clients understand the value of ZT, what industry is doing, and how their organization can pursue ZTA/ZTO.

Assess & Analyze – Conducting comprehensive and objective analysis of client technology and operations enables discovery and documentation of High Value Assets (HVAs), business processes, and data flows. These are critical factors in developing project plans and schedules to manage ZT initiatives, designing micro-boundaries, and implementing least privilege.

Design Architecture – Combining tools and technologies, e.g., Active Directory (AD) groups, Internet Protocol (IP) segmentation, and next generation firewalls, we promote environment micro-segmentation to protect HVAs, minimize lateral movement, and enable least privilege across known communication paths. Implementing multiple perimeters and with layers of security protection is essential to enabling ongoing verification of user, device, and application credentials against up-to-date authorization policies.

Orchestrate Policies – Building ZT into organizational governance, e.g., policies, processes, standard operating procedures (SOPs); business processes, and training promotes stakeholder understanding and user adoption of updated roles and responsibilities. Trinity helps identify methods and tools to automate enhanced security measures, making new process and technology integration as seamless as possible.

Monitor & Manage – As a business strategy, ZT requires ongoing awareness, analysis, and adjustments to account for evolving cyber influences, i.e., governance, technology, and threats. We help clients build and implement IT and business processes which monitor their cybersecurity program and maintain its currency, effectiveness, and relevance. This includes processes and tools required to manage changes coming from internal and external cyber influences, resources, and activities.

*As your trusted advisor and strategic partner, Trinity is ready to support any and every facet of **STOIC** to help your organization manage its transition to ZTA and ZTO.*

TRINITY Technology Partners, Inc. Endless Possibilities

Trinity's Zero Trust Capabilities and Initiatives

Trinity uses ***STOIC*** to help clients plan for and transition to ZTA/ZTO. By incorporating leading edge technologies and industry-proven best practices we integrate Identity, Credential, and Access Management (ICAM), Computer Network Defense (CND), Continuous Diagnostics and Mitigation (CDM), Security Information and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR) solutions. Based on your specific needs in pursuit of ZT objectives, Trinity brings:

- ***IT, Business, and Process Analysts*** – Specialists to verify HW/SW inventories; map HVAs, business processes, connections, and user access requirements; and develop or update systems artifacts, training, and governance to accurately reflect ZTA configurations and ZTO rules and objectives
- ***Project Managers, Planners, and Coordinators*** – Detailed-oriented facilitators who create logical, viable, and action-oriented strategies, plans, and schedules which clearly outline critical paths, resources, and dependencies
- ***Network and Security Architects*** – Technical strategists to accurately capture and document 'As-Is' architecture while diagraming optimal components, connections, features, and functions of 'To-Be' ZTA environments
- ***Network, Systems, Application, Database, and Security Engineers and Administrators*** – Technical experts who design, develop, test, implement, integrate, and optimize IT and cybersecurity solutions which deliver ZTA and ZTO capabilities and capacity
- ***Cybersecurity Assessors and Analysts*** – Security professionals to thoroughly, objectively evaluate organizational security posture; assess implemented security and privacy control effectiveness; and calculate risk associated with known vulnerabilities and their potential impact to operations

Working with stakeholders responsible for leading ZT in your organization, Trinity will customize a strategy to optimize existing capabilities while building phased plans for ZTA and ZTO. These will include suggested investments in people, processes, and tools which promote ZT principles, build ZT capabilities, and meet compliance obligations. Our SMEs will distill ZT laws, regulations, policies, and guidance into actionable tasks with achievable timelines which account for your priorities, constraints, and resources. As your partners in this journey, Trinity stands ready to collaborate; guide and train; and execute and report back, as needed, to help achieve your ZT objectives and goals.

Zero Trust Initiatives and Updates

As the CISA, DoD, and NIST ZT models and guidance evolve and proliferate, government organizations have been tasked by Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, to develop and implement ZTAs and establish ZTO. In January 2022, the Office of the President at Office of Management and Budget (OMB) published a Federal ZTA strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 to reinforce federal defenses against increasingly sophisticated and persistent threat campaigns. Collectively, these reference models, laws, and governance lay the framework for effective ZTA. To develop an efficient and executable strategy to achieve ZT objectives, each organization must adapt their own policies, processes, and architectures as they adopt ZT principles and incorporate applicable standards.

- *Executive Order (EO) 14028 and associated Presidential Guidance,*
- *Cyber and Infrastructure Security Agency (CISA)'s ZT Maturity Model,*
- *Department of Defense (DoD) ZT Reference Architecture, and*
- *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, ZTA.*

Engaging the Right Stakeholders

Successfully transitioning to ZTA will be a true team effort.

Design – Architecting and engineering effective ZTAs will require input from Business Process Owners (BPOs), Systems Owners (SOs), Engineers, and End Users to identify and fully account for HVAs, business processes, and data flows.

Planning – Efficiently building and managing organizations' migration to ZTAs will benefit from detailed project plans and schedules, with dependencies, realistic timelines, and clearly defined due dates and deliverables, to facilitate timely communication and collaboration.

Resources – Early engagement with Acquisition and Human Resources (HR) teams will promote timely procurement of resources and personnel needed to design, develop, test, and implement ZTA initiatives.

Migration and Operations – As the migration progresses and ZTA features and functions are applied, organizations will need to refine their governance, i.e., policies, processes, procedures, roles, responsibilities, and training, to adopt and embrace ZTO.

STOIC is Trinity Technology Partners' comprehensive approach for planning and integrating technology and operations with cyber solutions to deliver ZTA and ZTO. We bring demonstrable experience and SMEs with hands-on success helping clients design, implement, and continuously improve their security posture, and we can do the same for your organization.

Trinity is Here to Help

When it comes to achieving ZTA and ZTO, there is no silver bullet or easy button. Cyber threats present a clear and present danger to national, business, and personal interests, and the time to address them is now. We are ready when you are. To discuss your ZT strategy and opportunities with one of our SMEs, please contact Trinity Technology Partners at www.trinitytp.com, info@trinity.com, or (301) 477-3008.

"…assume that what you fear may happen is certainly going to happen."
~ Seneca

*"In preparing for battle, I have always found that plans are useless, but **planning is indispensable**."*
~ Dwight D. Eisenhower

TRINITY Technology Partners, Inc. Endless Possibilities