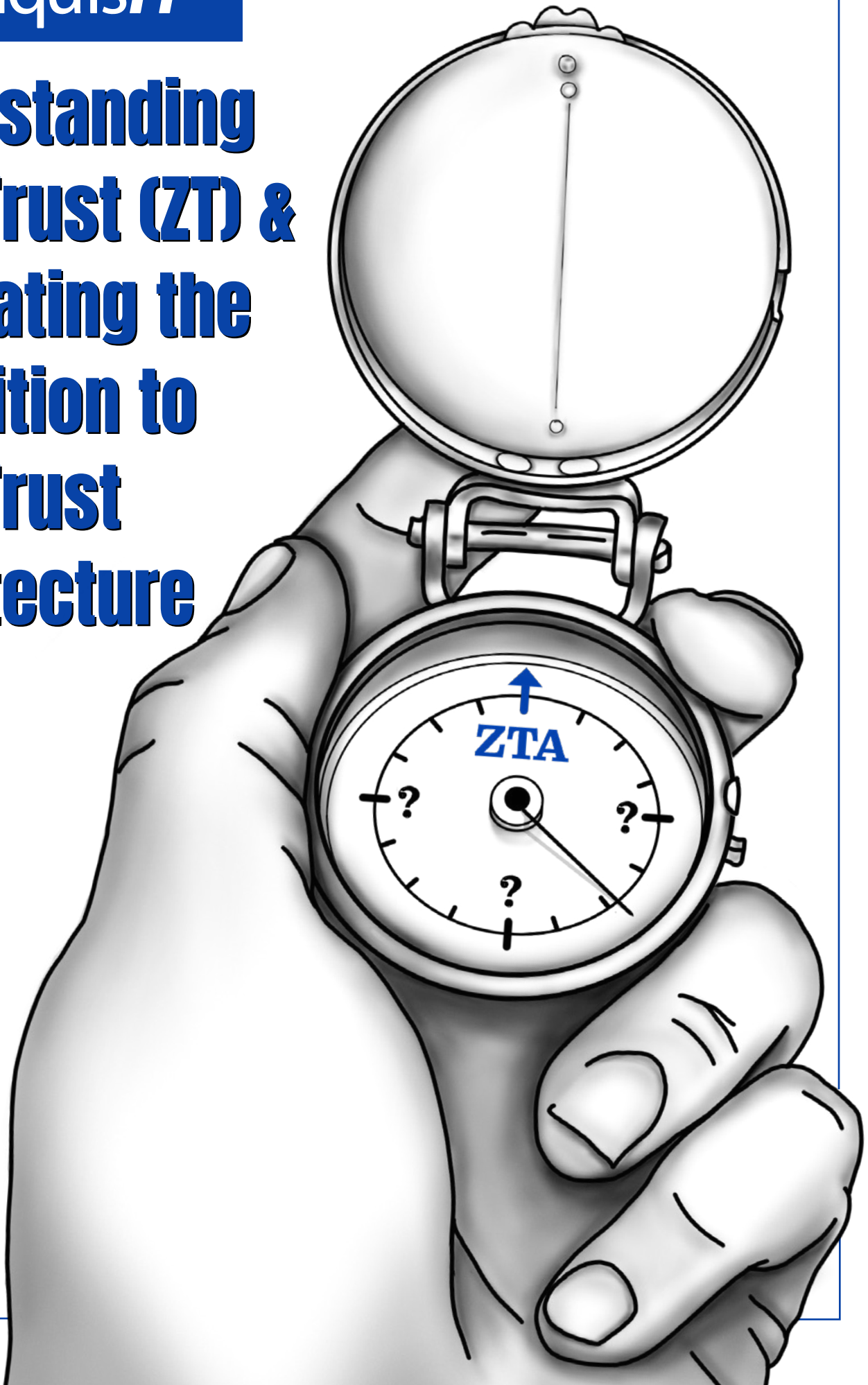
InquisIT

www.inquisitllc.com

Understanding Zero Trust (ZT) & Navigating the Transition to Zero Trust Architecture (ZTA)



We strongly believe that well-designed and properly implemented Zero Trust Architecture will improve your odds in the ongoing struggle with bad actors in cyberspace, and that it will also strengthen an agency-wide organizational culture of continuous improvement in cybersecurity.

It is our mission to help you get it right the first time.

Executive Summary

The basic principles of Zero Trust (ZT) are easy to understand because they require continuous access decision-making across the entire IT architecture. No user gets a pass to roam freely within the network simply because they have a tie to the organization and/or a password. Interrogating every request significantly reduces the risk a breach. Zero Trust Architecture (ZTA) is the implementation of ZT principles into an IT network, with all the necessary assessments, planning, policies, and controls on a constant basis.

To make this material as accessible, understandable, and interesting as possible for your agency, we use metaphors to communicate key elements of thinking about ZTA. We adapted recognizable cultural metaphors to present elements of ZT and ZTA. This helps to create a good foundation of initial shared knowledge within your agency. They are:

- *Zero Trust: The Organized Crime Metaphor*
- *Zero Trust Architecture: The Las Vegas Gaming Business Metaphor*
- *Agency Harmony on ZTA Transition: The Diplomacy Metaphor*
- *Initial Advice on ZTA Transition: The Sports Team Metaphor*
- *Designing ZTA for the Agency: The Custom Tailoring Metaphor*
- *Implementing ZTA: The Medical Metaphor*

As you read through each of our metaphors you will also see a method and philosophy behind assessing and planning a full Zero Trust Architecture.

Introduction

As a high-energy, forward-thinking, advanced technology company that provides our customers with an array of System Engineering, Enterprise Infrastructure, Cybersecurity, Software and Management services and solutions, we offer **tailored advisory services** to aid our customers in better understanding the concept of Zero Trust before navigating the transition to a Zero Trust Architecture for stronger cybersecurity.

Zero Trust has been used as a buzz phrase for many years, and it is only recently that official U.S. Government and Department of Defense documents have better clarified the form and structure of ZT and ZTA. A further complication is that each agency's approach to ZT will be unique. When that agency's ZTA transition is completed, their ZTA will also be as unique as the agency itself. There is no substitute for looking at every piece and part of your agency's unique IT architecture and deciding on the best way to incorporate ZT principles into your agency's enterprise architecture.

> *"Zero trust (ZT) provides a collection of concepts and ideas designed to **minimize uncertainty in enforcing accurate, least privilege per-request access decisions** in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is **an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies**. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan."*
>
> *- NIST Special Publication 800-207*

Cloud Technology has been prevalent in the commercial space since 2010, but is still being adopted by Federal agencies. Zero Trust represents a larger and far more urgent problem that puts American national security at risk by remaining exposed. This adoption cannot travel at the traditional pace of Federal technology adoption, and InquisIT is uniquely positioned with our commercial background to help make this transition quickly and efficiently.

The following six metaphors are widely recognized by many Americans, and form part of a shared set of cultural experiences such that the metaphor itself is usually a good starting point for most of us.

Our Role Within Your Mission

This white paper explains our approach to aligning a mutual understanding of complex ZTA concepts with your agency and then advising on navigating the various stages of the ZTA transition process. We see five primary roles:

1. **Provide Expertise & Communication Support**
   Briefing critical stakeholders on ZT and ZTA (regardless of their IT experience) in clear, understandable, and jargon-free language. Recommend communication strategies and tactics based on the overall changes to achieve ZTA.

2. **Provide Technology Experts**
   Our engineers incorporate their knowledge of a wide range of new and legacy technologies including how current licenses may be better leveraged for ZTA**.** For your agency, we bring unique insight in IT systems and products used to implement controls (and InquisIT's combined legacy experience with other organizations) into your agency's ZTA assessment.

3. **Create a Roadmap**
   After analysis of the architecture by our engineers, we advise your agency on the initial roadmap leveraging the DoD ZTA framework to get the ZTA transition off to a good start and how to get the most from current capabilities. This also directly supports agency deliverables.

4. **Secure Systems Development & Testing**
   Engineers will map current controls, map policies, prototype, and test ZTA principles on a relevant subset of your agency's IT systems to validate policy, technical, and security approaches to your agency's ZTA transition.

5. **ZTA Transition Oversight**
   Our team is available for project support and oversight to assure ZTA is implemented properly coordinating security, infrastructure, software, and operational elements of the organization. Providing short-term, collaborative, programmatic support for ZTA implementation to your agency while you need it.

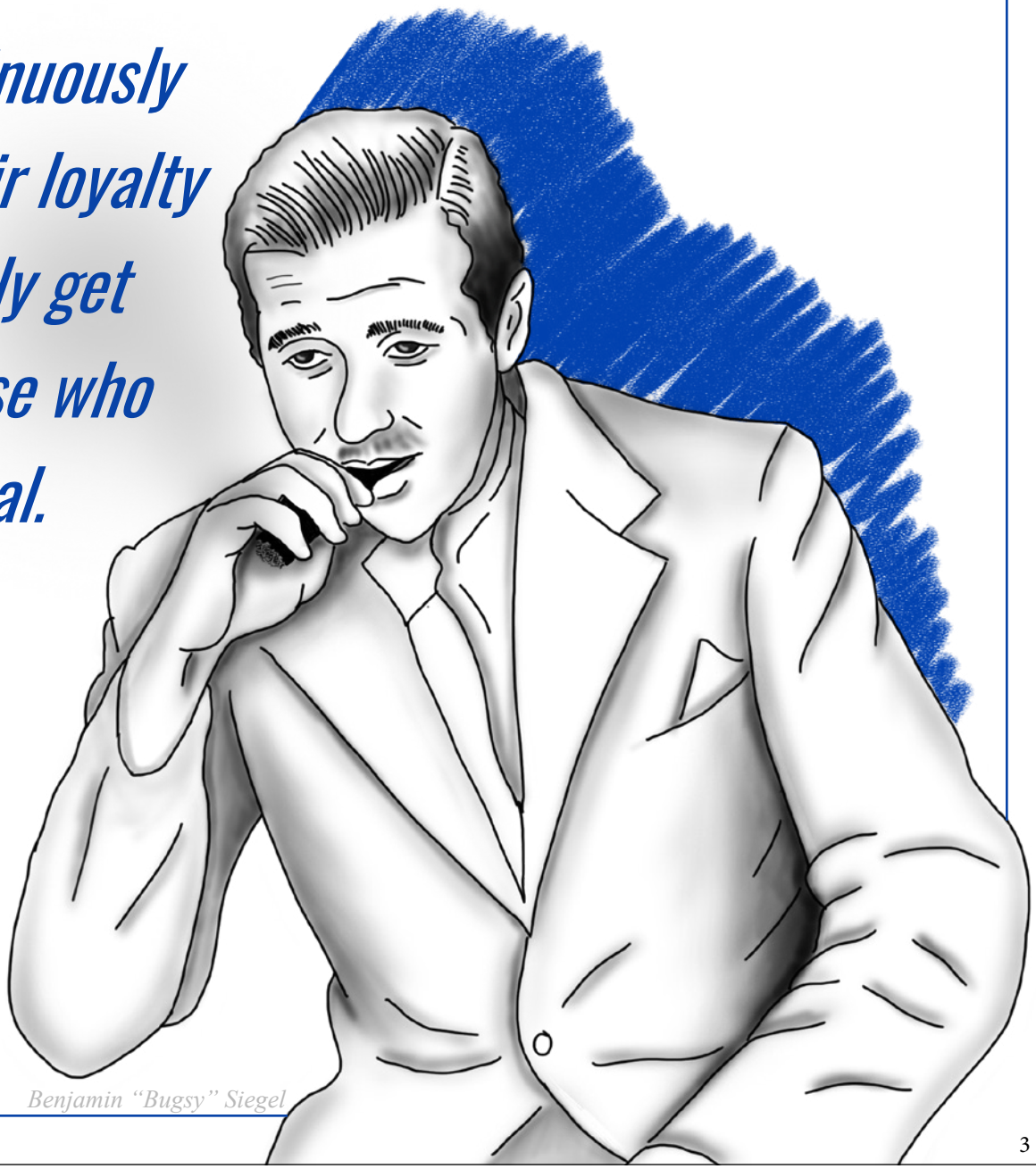
What is Zero Trust?

Zero Trust: The Organized Crime Metaphor

Whether you watch The Godfather, Goodfellas, Boyz n the Hood, A Bronx Tale, Eastern Promises, Bugsy, Scarface, Gomorrah, American Gangster, The Departed, Donnie Brasco, or any other quality movie in the genre, the notion of trust is never far from the center of the plot line – and successful mobsters trust very few people, even those closest.

A visionary leader in American organized crime, Benjamin "Bugsy" Siegel, is credited by many for establishing the post-World War II gaming industry on the Las Vegas Strip as the modern, sophisticated, big business that it became. The *'trust only those who continuously prove their loyalty and quickly get rid of those who are disloyal'* paradigm is an easily recognizable real-world analog form of Zero Trust, which leads us directly to the next metaphor.

Trust only those who continuously prove their loyalty and quickly get rid of those who are disloyal.



Benjamin "Bugsy" Siegel

Zero Trust Architecture: The Las Vegas Gaming Business Metaphor

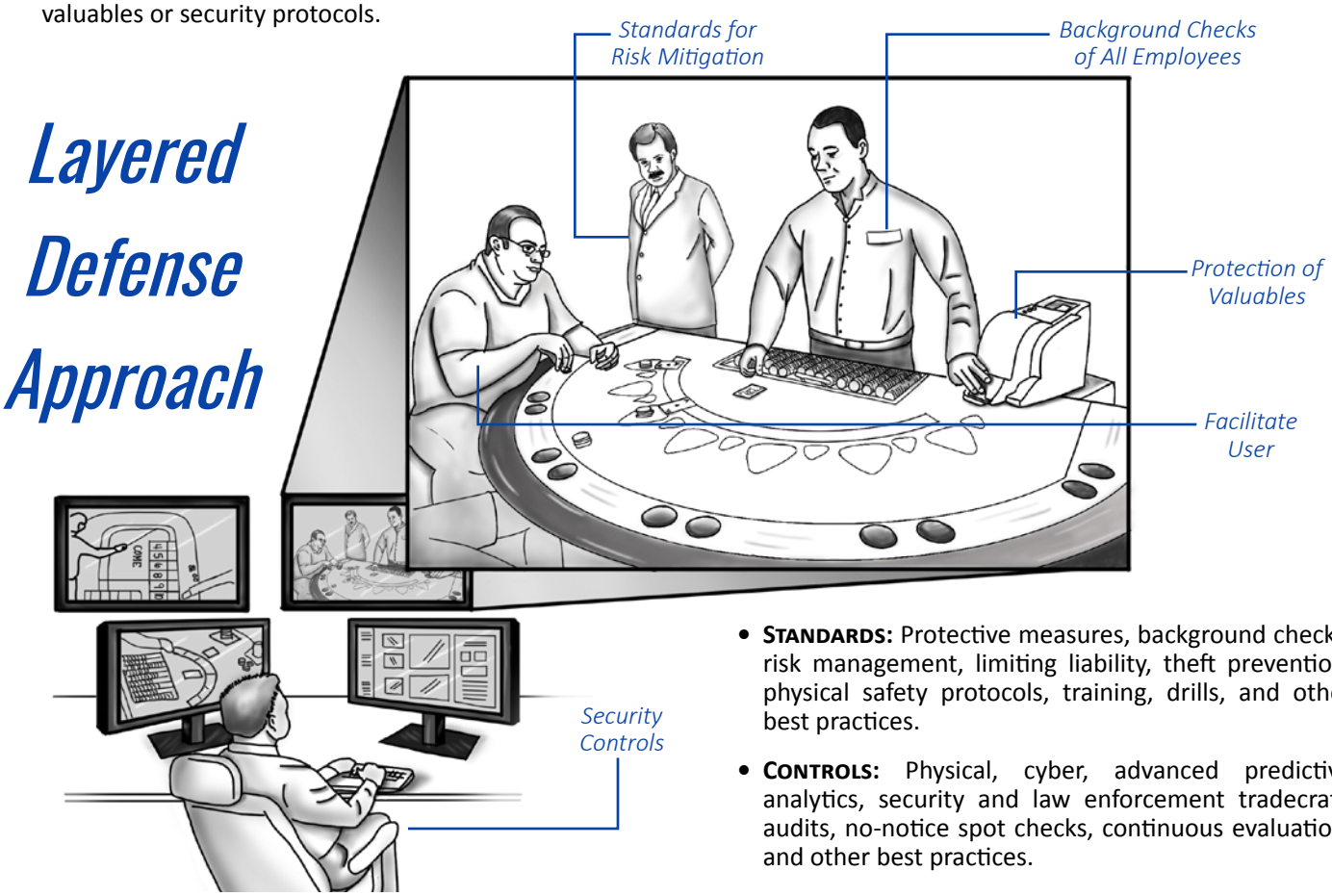
A good metaphor for ZTA is a resort hotel in Las Vegas that offers extensive gaming, dining, entertainment, shopping, and other attractions.

Like the IT world, Las Vegas is open for business and operating 24 hours a day. Anyone can wander onto a gaming property through unguarded entrances. Activities in the city are optimized to welcome guests and proceed to relieve those guests of their money. However, properties also go to extraordinary lengths to protect their revenue streams, their valuable assets (personnel, physical, cyber, financial, intellectual property, marketing), and their favorable reputations. To accomplish this, they employ an analog equivalent of ZTA with the following characteristics:

- It starts with the assumption that you trust no one, if you do not know them, trust them only as much as you need to if you do, and constantly maintain high security standards at the individual person and individual location level depending on the presence of valuables or security protocols.
- A 'layered-defense' approach is used to make it significantly harder to access sensitive areas or storage for valuable items the closer you get to them.
- Another approach to layered defense or 'defense-in-depth' is the personal protection of VIPs with national name recognition. The closer one gets to their suites the more obstacles need to be navigated and cleared.

Las Vegas security protocols are then structured roughly as follows:

- **GOAL:** Get people to spend their money in Las Vegas.
- **FACILITATION:** Make it easy and inexpensive to get there and spend money, while having a good time and not hurting themselves while enjoying the excitement, glamour, fun, shows, food, amusement, and other delights.



- Rigorous background screening of all employees and contractors (mandatory in Nevada for any property with a gaming license – particularly with all the cash in play).
- Other than entrances to the hotel, restaurants, and certain recreational and retail spaces, almost everything is behind at least one locked door, and frequently many locked doors and meaner security personnel in front of them.
- **STANDARDS:** Protective measures, background checks, risk management, limiting liability, theft prevention, physical safety protocols, training, drills, and other best practices.
- **CONTROLS:** Physical, cyber, advanced predictive analytics, security and law enforcement tradecraft, audits, no-notice spot checks, continuous evaluation, and other best practices.

The ***Goal*** and ***Facilitation*** bring in the customers, and the ***Standards*** and ***Controls*** protect assets that have varying levels of public exposure. These protocols are recognizable to Zero Trust practitioners, and casino executives would have no difficulty following a Zero Trust briefing even if they had limited knowledge of cybersecurity. All agencies have a Goal and Facilitation leveraging technology is the charge of nearly all CIO's in some capacity. They too use Standards and Controls and with ZTA do so at the lowest level possible (users) and validating prior to entering any area of the infrastructure.

InquisIT's Approach to Zero Trust Advisory Support

Agency Harmony on ZTA Transition: The Diplomacy Metaphor

The best diplomats are those who want to resolve disputes and problems fairly and equally with agreements that give each party much to be pleased with, and also leaving each party with something to grumble about – but not enough to break the agreement. Fallible humans who disagree with each other will seldom construct perfect treaties or perfect agreements, so any document that all parties can live with and present to their superiors for signature is usually a good thing. We know the dynamic of how things get done in agencies is much the same.

We are experienced honest brokers in good faith efforts to bridge the gaps in understanding between technical and non-technical personnel and explaining the interests and focus of each group to the other, while helping create a higher-level focus on a 'whole-of-organization' approach to the issues being addressed.

We will communicate with your agency's stakeholders to identify significant **policy**, **priorities**, and **trade-off** decisions involved in the ZTA transition process. As part of the initial step in the ZTA engagement, we will prepare an internal Memorandum of Understanding (MOU) with your agency to solidify action plans and ensure that expectations are met throughout implementation. These initial deliverables are then refined and expanded for final delivery.

To make this a better experience for your agency's personnel, all the advisory and facilitation efforts will be done with full transparency within your agency and with a visible metrics-driven approach so everyone can see where we are in a particular process.

Our people have broad, varied, and extensive experience in multiple organizations across government service, military service, industry, academia, and nonprofits. We bring all this combined talent to our customers.

Initial Advice on ZTA Transition: The Sports Team Metaphor

In rough chronological order of presentation and consultation:

Team Approach: Plan a 'team approach' the way successful sports franchises do, with the equivalent of scouting, strategic draft picks, recruitment, coaching, PR, practice, a playbook, a strategy, and a commitment to winning.

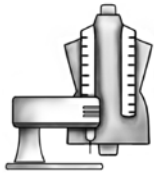
Team Owners: Your agency's most senior leadership, as the equivalent of team owners, need to understand ZTA's many benefits and all the diligent work to come.

Boosters: Identify all agency stakeholders who need to have an informed layperson's understanding of ***Zero Trust 101 and Zero Trust Architecture 101*** and get them comfortable with thinking about it and discussing it with their colleagues.

Fitness, Training & Practice: With broad input from your agency, develop an evaluation plan on the status quo of your agency's IT systems, with recommendations for where to focus starting. Test it and improve as needed.

The Players: Work with the CIO organization to translate those focusing decisions into a 'gameplan' and provide ongoing advice to CIO personnel.

Designing ZTA for the Agency: The Custom Tailoring Metaphor



No two agencies and their respective IT architectures are exactly alike, and each agency's approach to ZTA will be unique. Your agency needs a ZTA solution designed uniquely for it, with the engagement of agency stakeholders and leaders.

Custom tailoring of quality garments is a good way to think about this issue. Experienced designers make the effort to learn their customers' interests, tastes, goals, and many other attributes before designing a new garment. Armed with this knowledge, they can prepare a menu of choices and advise their customer on options. It is then important for the customer to wear it for a bit. This shows the designer where final adjustments are needed to achieve the perfect fit.

Tailoring a solution to your agency's fit is how we will provide quality advice and support on ZTA, with the added advantage that our knowledge of your agency's goals, stakeholders, infrastructure, and tools strengthens our capability to best apply Zero Trust principles to your agency's environment.

Implementation

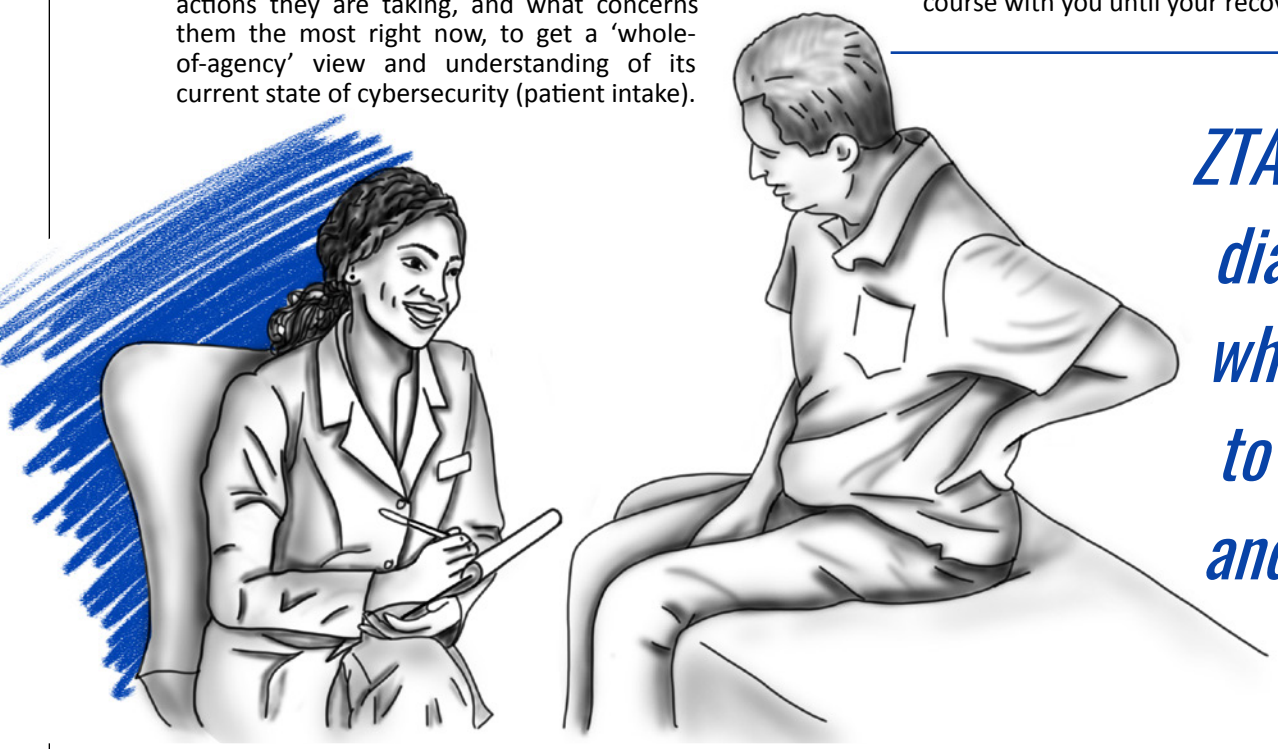
Implementing ZTA: The Medical Metaphor

Diagnosing what needs to be done and in what order for implementing ZTA is much like how a doctor would design and implement a treatment plan. By figuring out exactly where the health of your current architecture stands, we leverage our expertise in ZTA to improve the health of your current architecture and monitor and follow up as needed to keep everything in good health.

NIST 800-207 indicates an understanding that all ZTA efforts are agency-specific because they represent a series of agency decisions based on many elements of their IT infrastructure. This is something ZT and ZTA have in common with the practice of medicine as shown below.

Our process looks something like this, with appropriate modifications as needed based on your agency's feedback:

- Ask your agency's personnel a variety of inquisitive questions that reveal important and relevant information, how they are doing now, what corrective actions they are taking, and what concerns them the most right now, to get a 'whole-of-agency' view and understanding of its current state of cybersecurity (patient intake).
- We do not pass judgment on any information shared with us since we are trying to help your agency get to the best possible ZTA (Hippocratic Oath).
- Based on your agency's history and known areas of improvement, we will suggest a series of tests to quantify your agency's current cybersecurity readiness (draws, samples, testing).
- We will then review the test results with agency stakeholders and recommend a course of action (what we see, and our opinion on what works best for you).
- Throughout the process, we also serve as an interpreter/translator of complex terminology and phrases into clearly understandable conversational words, grammar, and language for the benefit of non-technical or non-IT stakeholders (we can make this less scary and don't need fancy words to do so).
- Once your agency decides what to do, we will prepare a recommended plan and schedule to be implemented, with frequent reviews to help ensure desired outcomes (the road to getting better).
- We are also your partner in assessing, prioritizing, planning, scheduling, and following up/following through with what needs to be done to reach an optimum Zero Trust Architecture (we will stay the course with you until your recovery is complete).



ZTA requires diagnosing what needs to be done and in what order

We nurture a partnership that provides full disclosure, full accountability, and a shared desire by all parties to emerge from the process with a modern cybersecurity posture capable of protecting IT assets from all attack vectors.■

When would you like to start?

Contact us at info@inquisitllc.com