# ZERO-TRUST ARCHITECTURES AND THE TACTICAL DOMAIN: A SQUARE PEG IN A ROUND HOLE?

**The Zero Trust Architecture (ZTA) has rapidly become the hottest topic in cybersecurity. However, we have noticed that today's discussions inevitably focus on ZTA from the standpoint of the enterprise, ignoring the nuances and pitfalls of implementing ZTA in the tactical domain. Instead of driving the ZTA solely from the top-down, we see an operational benefit in constructing the enterprise ZTA from the bottom-up. This paper will delve into the potential issues with the industry's current approach and introduce the solution from ZKX.**

**ZKX changes the security dynamic by building assurance in rather than bolting it on. By combining proven cryptography with novel, next-gen authentication factors, ZKX delivers a swift, robust, and reliable authentication solution to all echelons of the DoD.**

## ORIGINS OF THE ZERO TRUST ARCHITECTURE

ZTA is a novel conception of network construction designed to eliminate the overall idea of "trust" from day-to-day network operations. Traditionally, networks of the past have been constructed without security at the immediate forefront, deciding instead to prioritize user-focused attributes such as speed and ease-of-use. Security, in its most rudimentary form, was relegated largely to the network's perimeter. If access was granted to a specific user's account, then that user was free to enjoy the privileges associated with said account.

The ever-evolving cyber threat landscape has shown us — rapidly and forcefully — that this philosophy of network construction is not feasible for sensitive and reliable operations, especially as more critical functions and infrastructures are rapidly falling victim to widescale digitalization.

As a product of the U.S. government's National Institute of Standards and Technology (NIST), the theoretical ZTA aims to eliminate these archaic network perimeters and the outdated concept of trust altogether from the

networks of tomorrow. From NIST SP 800-207 (the functional constitution of the ZTA), two distinct areas of the ZTA are highlighted which are crucial to its overall functionality: policy governance and authentication.

Policy Governance Architecture is defined as an ecosystem of three different theoretical network components: the policy engine (PE), the policy administrator (PA), and the policy enforcement point (PEP). These three components work in concert to facilitate policy governance — from understanding the access policies protecting a certain resource, to tracking a user's movements about the network — and work with other critical components (e.g., threat intelligence platforms, CDM, ICAM, etc.) intended to embody a "data-driven" course of network operations.

Authentication is critical to actualizing ZTA. The authorization of users and devices within a network requires a secure authentication system by which a minimum level of trust can be established before resources can be accessed. Under the zero-trust regime, authentication is a near-constant transaction which utilizes a variety of interactive and non-interactive sources of user input such as a user scanning their CAC or measuring the average time elapsed between mouse clicks. This ubiquitous authentication works in tandem with the policy governance architecture to alleviate the cumbersome burden of trusting the operators on your network.

## WHAT ABOUT THE TACTICAL DOMAIN?

While this brief description of the ZTA garners a lot of nodding heads from industry veterans and academics, there is a much less vocal — yet arguably more substantial — group within the military sure to be raising their eyebrows at this approach to eliminating trust. It is a fact of life that the doctrine which drives the strategic visions of the enterprise ecosystem will impact the tactical players and their sphere of operations in both expected and unexpected ways. In other words, *consequences are downstream from doctrine.*

As the ZTA continues to gain momentum and excitement among the research laboratories, it is important not to neglect the potential impacts that the enterprise-wide migration to zero-trust may have on those who operate out at the edge of DoD affairs. Those who conduct their day-to-day work in office or campus settings may be fine with one or two

or three extra authenticators supplemental to the CAC, but those who pull triggers, coordinate supply deliveries, and drop ordnance cannot be expected to handle two extra security tokens, a behavioral biometrics platform, and dedicated backhaul access to the cloud infrastructure alongside their already-necessary multitude of equipment. Similarly, while AI-fueled threat intelligence platforms may be instrumental to the military enterprise, there is likely little need or even capability to host said platform in the forward operating base.

The ZTA and its ancillary components are certainly an exciting field of cybersecurity and network operations, but it is haphazard to think of this as a blanket solution for all players across the echelon. While the principles of the ZTA have been rigidly defined (and its value proposition certainly well understood), the numerous mechanical questions and various discrepancies would forge a chasm between the strategic and tactical ways of life if both sides of the echelon are not considered in the ZTA conversation. Features such as input tracking and gait analysis may do very well in thwarting the next would-be Edward Snowden, but may also be an extreme hindrance in situations with live fire.

## ACTUALIZING ZTA AT THE TACTICAL EDGE

The benefits of the ZTA can be actualized both at the enterprise and the edge simply by considering from the start how the fundamental principles of the ZTA can be integrated into tactical operations. Distributed command posts will not always have dedicated access to services reliant on cloud infrastructures. Likewise, the warfighter should not be encumbered with excess authenticators, or denied access to a critical communications channel due to an unexpected change in her gait brought on by an encounter with the adversary. Operations conducted at the tactical edge can not afford to be lost in the conversation surrounding ZTAs, for the sake of both the edge and the enterprise.

The ZKX Solutions Group is a leading voice in the conversation on actualizing the ZTA at the tactical edge. Our new disruptive authentication technology offers seamless and frictionless multi-factor authentication designed to embody the foundational principles of zero-trust. This is done by its lightweight construction and intentional “bottom-up” philosophy — integrating the enterprise with the edge, not the other way around. With ZKX, networks at the edge or in the enterprise reap the benefits of the

zero-trust philosophy, without the need for excess materiel, burdensome authentication artifacts, or increasing the footprint of existing architectures.

ZKX can utilize many forms of traditional and non-traditional forms of identifying data: from CAC to call sign to weapon serial number. ZKX features a nested design which does not require dedicated cloud access or network backhaul in order to be fully functional even in denied environments. This nested approach to authentication allows a portion of the garrison authentication framework to be detached, allowing forward-deployed personnel to utilize the authentication they're used to without needing to be tethered to the mothership.

ZKX is designed atop a foundation of zero-knowledge proofs — longstanding mathematical functions which are used to prove one's knowledge of secret information without revealing what that secret information is. We have taken these functions and applied them to the complex issue of multi-factor authentication in zero-trust regimes, and has created a ZTA-friendly authentication solution which eliminates the network's need to trust its users and also the users' need to inherently trust the host network. ZKX relies primarily on public data to authenticate users, enabling dynamic and rigid authentication even in environments surveilled by the adversary. Secret authenticating information is stored neither on the user's endpoint nor a network's data storage system, making ZKX impervious to endpoint breaches, data theft, or information leaks.

In the interest of usable zero-trust, ZKX features many quality-of-life features for the end user, including seamless expansion techniques for increasing the available amount of authenticating data and a proprietary method for attestation of user identity. Together these special features deliver seamless, zero-knowledge authentication and session management to both the office and the command post.

## ZERO TRUST ARCHITECTURES FROM THE BOTTOM-UP

The ZTA is an exciting theoretical approach to total information security, but it is just that — an approach. While the technologies and methodologies meant to actualize the theoretical foundations of the ZTA are being developed, tested, and implemented, it is important not to lose sight of the ripples which changes in the enterprise will cause downstream to the edge.

Instead of driving the ZTA solely from the top-down, ZKX believes a bottom-up approach to constructing the enterprise ZTA will deliver decisive operational benefits. The ZKX engine is our first concrete offering to bring ZTA not just to the strategic and operational echelons, but to the tactical domain as well. The ZTA is a noteworthy and significant step toward mitigating all sorts of threats emergent in the cyber landscape, but the lack of conversation surrounding down-echelon and cross-echelon zero-trust interoperability is troubling, especially for those operating at the edge.

If you are interested in a sensible methodology for bringing zero-trust architectures to the tactical edge, reach out to the ZKX Solutions Group for more information about our technology.