WHAT IS THE ZERO-TRUST ARCHITECTURE? WHAT DOES IT MEAN FOR THE MILITARY?

The Zero-Trust Architecture (ZTA) is not in itself a specific technology. Instead, it is a cutting-edge operational philosophy that security architects utilize to preserve the networks of today. Traditionally, the security of the network has been focused mainly on its perimeter. If access to the network is heavily guarded, less scrutiny is given to accessing the network's resources.

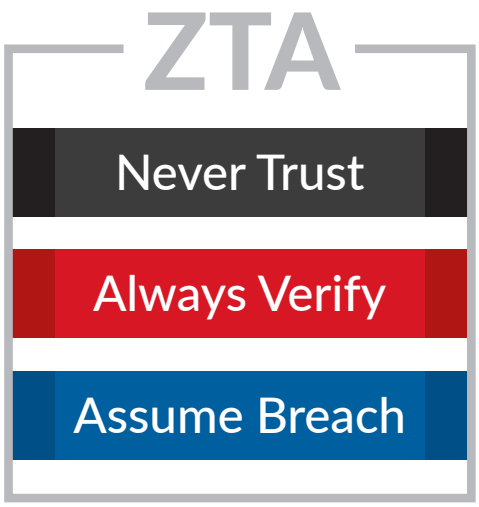
Current Gaps in Network Security

Recent cybersecurity incidents (especially major ones such as the Snowden data leaks and the more recent SolarWinds supply chain attack) have shown current systems are not working. Executives, security practitioners, and customers alike see that a perimeter-focused approach to network security is not stable or effective for today's networks and certainly not for the networks of tomorrow. The modern network includes vastly more endpoints, technologies, applications, geolocations, and communication protocols than those of yesterday. It is challenging to define a logical perimeter when considering the monolithic size and capability of the modern (and future) network.

Furthermore, considering the numerous different endpoints, BYOD policies, and the potential use of cloud-based third-party tools and services, defining such a perimeter may be a near impossibility for your network and its assets. Cyber adversaries have used this emerging trend to their advantage, and zero-trust is cybersecurity's response to this.

Primary goals of Zero-Trust

Zero Trust is, in its essence, a "never trust, always verify, and assume breach" thought process for modern cybersecurity. To be clear, removing the concept of "trust" is the primary goal of zero-trust. As an example, users do not connect to the network as untrusted and authenticate themselves to a trusted state to utilize resources. In ZTAs, the concept of trust does not exist, so users are required to constantly prove their identities to the network's governance structure to conduct their daily business.



The National Institute of Standards and Technology (NIST) has formalized the theories of the ZTA, its fundamental tenets and assumptions, and its overall mission. Similarly, some preliminary guidance has been drafted (also by NIST) for government

REDCOM™

RESEARCH, ENGINEERING, & DEVELOPMENT IN COMMUNICATIONS

ONE REDCOM CENTER, VICTOR, NY 14564, USA | 585.924.7550 | WWW.REDCOM.COM | SALES@REDCOM.COM

organizations seeking to implement zero-trust principles into their existing networks. Still, many questions about the practical ZTA remain, especially for government and military entities. This has slowed organizations' willingness and ability to adapt or re-architect their networks to match this zero-trust model of cybersecurity. However, various pilot programs and pieces of practical guidance have emerged to help different organizations construct zero-trust architectures, most recently (and perhaps notably) DISA's Reference Zero Trust Architecture explicitly tailored for the DoD.

Government and Military vs. Commercial Industry

Zero-Trust in the government and military space is a unique problem set versus the issues faced by the rest of the commercial industry. Similar trends with other technical developments like 5G infrastructure, methods, technologies, and strategies for actualizing effective zero-trust networking will be starkly different between industry and the government & military. Similarly, there are unique implications for designing and enforcing organizational policies in a zero-trust regime regarding the homogeneous zero-trust information enterprise.

REDCOM, ZTA, and the DoD

Like the rest of the contracting and subcontracting market, REDCOM has been eagerly studying the foundational principles of zero-trust. REDCOM is looking to help produce a zero-trust network operationally secure at the enterprise level and includes some considerations for how zero-trust principles can be actualized in forward-deployed environments, bringing security to even the most fringe areas of the DoDs operations. REDCOM has been engaged in conversations with the DoD and the larger federal government to assist in bringing the security of the zero-trust model to all levels of the military without the need for overloaded architectures, infeasible computational requirements, or sacrifices of operational security.

Operational Freedom for Digital Identity

After reviewing the DoD Reference ZTA put forward by DISA (available at https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf), we identified many notable trends and significant findings — some promising and others daunting. First is the open-standards approach to the construction of the ZTA. From almost every standpoint, the architecture relies on open standards, policies, and technologies as frequently as possible. This is critically important for actualizing enterprise-wide, interoperable zero-trust frameworks, especially regarding policy. As there are doctrinal sources of government and military policy, simply adhering to those guidelines is not enough to ensure an organization's security and ability to interoperate with other separate (albeit similar) organizations. For example, documents such as NIST SP 800-63 provide a great deal of operational freedom in how different organizations could structure their overall digital identity and authentication solutions — as granular as specific technology an organization employs. While other organizations could use different solutions certified under a given level of SP 800-63, technical interoperability between the two solutions remains an independent consideration if the two entities were ever to collaborate on a specific mission. Reliance upon open standards, technologies, and policies is an excellent approach to ensuring this, but it is not the complete picture. Phenomena such as "vendor lock-in" still has the potential to wreak havoc on large, complex, multi-faceted systems like the ZTA.

Minimizing technological footprint

The next consideration which arises from the DISA reference architecture is that of computational overhead or technological footprint. While the fundamental mechanics of zero-trust require a magnitude of computational

architecture and platforms, it is still critically important to minimize unneeded or ancillary architecture and focus on critical assets. This is especially necessary for environments where cloud access is unavailable and employable, compute architecture is severely limited. Although limited in their cyber capabilities, these environments are often overlooked in strategic conversations about bringing zero-trust to the different military settings. As the cyber domain will serve as a new battlefront in the next great conflict, failing to address this oversight would be a critical misstep appropriately. Indeed, many believe that this "next great conflict" has already begun.

Why implement ZTA?

The last central theme, and perhaps most obvious, is the desired adherence to the fundamental principles of zero-trust. The cybersecurity benefits of zero-trust emerge from how its basic principles are defined and implemented. However, to receive these benefits at all echelons, utmost importance must be placed on minimal cyber footprints and interoperability between technologies and policies. Overcoming this challenge while retaining the integrity of the original vision of zero-trust is no small feat and must not be considered lightly.

While the primary benefits of zero-trust will significantly boost the security posture of any organization, the lifecycle of its different components and experiences of its various users must remain highly efficient. This must be done for the zero-trust model of networking to see ubiquitous long-term use and evolution. Especially in environments where personnel can only carry a limited volume of equipment, actualizing the maximum amount of zero-trust benefits with the least amount of different technological (hardware and software) components is critical for long-term and successful ZTA adoption.

Conclusion

REDCOM's cybersecurity business unit is already working on a multi-factor authentication system for the strategic, operational, and tactical levels of the U.S. government and military. Our solution, called ZKX Helix™, leverages the Zero Trust Architecture to overcome the fundamental flaws in traditional authentication systems in use today. ZKX leverages open standards, is resistant to popular attack vectors, and is adaptive to local policies.

To learn more about REDCOM's Zero Trust research and development efforts, email sales@redcom.com or visit www.zkxsolutions.com.