ZKX HELIX™
HOLISTIC CYBERSECURITY FOR IT, OT, & IoT SYSTEMS

ZKX Helix ("Helix") is a holistic cybersecurity software platform designed to protect access to IT, OT, and IoT networks and their resources with pinpoint accuracy. Helix makes stronger security frameworks like zero-trust a reality, and extends heightened cyber protections to networked resources like user endpoints, SCADA systems, IoT sensors, and everything in between.

Helix is deployable in isolated edge environments and scalable to federated multi-enterprise networks. The Helix platform is a prototype, currently unreleased and actively undergoing agile development. Earlier proof-of-concept versions of Helix have been demonstrated and validated at various DoD technical field tests and exercises, including Cyber ANTX 2022 and Project Convergence 2022.

TOTAL CONTROL OF ACCESS

Helix enables secure, granular, and complete visible control of access to resources on any network. Helix is designed to prevent unintended access to any individual network resource, severely limit any degree of unchecked lateral movement on the network, and protect identity and multi-factor authentication (MFA) data for both the users and devices in the information ecosystem. Helix offers unmatched usability on top of these security benefits, speeding up cyber-enabled workflows by requiring little training to use and transparently authenticating users and their devices in continual fashion as they traverse the network.

Helix enables total, granular command of network access by providing three core capabilities:

- **Perimeters** – software-defined trigger points; the boundaries of privileged resources
- **Policy** – conditions that must be satisfied before privileged access to a resource is granted
- **Policy Enforcement** – patented MFA to securely and dynamically enforce access policies

These capabilities are the core offerings of the Helix platform and are built in large part from the identity attributes of the users and devices already in the network environment. Identity attributes are any characteristic relating to the identity of the user and/or device in question: organizational role, physical location, cryptographic suite, communication protocol, recent behavior, etc., can all be considered identity attributes in their own right and are used to construct and enforce access policies in the Helix framework.

RESILIENT SECURITY FOR CRITICAL NETWORKS

Helix is deployable to isolated or air-gapped network environments, is resilient enough to persist in contested, intermittent, and otherwise austere networks, and offers more granular and dynamic protection than that of traditional firewall + MFA solutions. Helix is agnostic to host compute platforms, communication protocols, and deployment form factors, making it suitable for cutting-edge enterprise networks, legacy manufacturing networks, lean critical infrastructure networks, and everything in between.

Helix consumes minimal compute and bandwidth, and has been proven feasible for both the tactical and operational networked environment, including over hybrid transport protocols like IP + RF. Likewise, the Helix user interface requires extremely minimal training, allowing for rapid uptake and migration to its superior security offerings.

Helix makes core principles of emergent cybersecurity frameworks like zero-trust a reality not just for well-resourced campus environments but also for leaner, austere, isolated networks.

Helix greatly minimizes the network's attack surface and offers unrivaled visibility and granularity in protecting access to networked resources of any kind, including IT, OT, and IoT assets. Helix simultaneously validates and verifies the identities of both the users on the network and the devices they are using, ensuring that only exactly correct access to any given resource is only ever granted to exactly correct clients with exactly correct privileges under exactly correct conditions.

HOW HELIX WORKS

Helix is a prototype software platform that enables the creation, deployment, and enforcement of cyber access policies at the macro and micro scale for networks of any kind and resources of any type.

Access policies are built from identity attributes – a conceivably boundless number of innate characteristics and properties carried by the users and devices that exist on a network. Attributes determine which access policies users and their devices are eligible to satisfy. They can be as broad or specific as needed to enforce specific access protections to varying degrees of granularity.

Trigger points for any access policy are deployed in the form of microperimeters, arbitrary boundaries that require authorization before a connection request is allowed to proceed past it. Microperimeters can be deployed around applications and services, as well as individual resources or functions within those applications and services, adding a new layer of depth to the network's existing security structure.

Via REST (or any other application-level process), Helix receives a request to authenticate via the microperimeter trigger point, as well as any information relevant to the access policy needing to be enforced for the specific client request and corresponding microperimeter.

After learning the details of the specific access policy, Helix enforces the access conditions on the entity requesting the connection with its patented MFA process. MFA is conducted on the basis of three characteristics of the user/device pair initiating the connection request:

- **MFA Artifact(s)** – what you have, what you are, what you know
- **Confidence Score** – a calculated measure of assurance in a claimed identity
- **Device Identity** – endpoint verification

Helix MFA simultaneously authenticates users and the device they're using – authentication will fail for correct users on incorrect devices and vice versa. Furthermore, Helix MFA is arbitrarily repeatable and can scrutinize claimed identities to varying degrees. This translates to the confidence score and can be used to authenticate user and device identities from low degrees of assurance (e.g., "five-9s" or 99.999%) to extremely high degrees of assurance (e.g., "twenty-9s" or 99.99999999999999999%). This enables more stringent verification for more sensitive network resources and vice versa.

Nearly any MFA artifact or credential can be supported by Helix. Whether it is conventional authenticators like PINs and passwords, or more unconventional identity bindings like ID cards, barcodes, biometrics, or hardware tokens, Helix MFA enables organizations to leverage whatever is already natural to their security environment.

MINIMIZING ATTACK SURFACES WITH NEXT-GEN MFA

The MFA used by Helix is patented and totally unique to the Helix platform. Not only is it the ideal tool for enforcing granular, attribute-based access policy schemes, it is safer, faster, and more usable than today's conventional MFA solutions.

Helix MFA is driven by zero-knowledge proofs (ZKPs) – functions that allow for the proving and verification of claims of knowledge without revealing what the knowledge in question is. In short, users can prove they know their password, have their CAC/PIV, can pass a biometric test, etc., without transmitting or storing that data anywhere on the network, in any form or fashion.

Helix MFA is not inherently sensitive – adversaries can intercept MFA traffic and they will learn nothing of substance. Similarly, nothing sensitive is kept on the device nor on any credential server on the network. A lost device or a compromised credential server has zero impact on the Helix security posture.

Even lost or stolen credentials have no impact on the security provided by Helix. A stolen CAC or a phished password still cannot undermine an organization's Helix-enabled security framework.

MFA transactions in Helix appear random each time they are conducted, concealing private information even if it is used hundreds of times a day. Furthermore, one of the patented processes of Helix MFA boosts

the entropy of user-supplied credentials, enhancing password and PIN-based authentication to previously unseen levels. With Helix, passwords – even traditionally "unsecure" passwords – become cryptographically rigid and perfectly viable to protect even the most sensitive network resources.

Lastly, Helix also contains a novel session authentication scheme that enables users and their devices to continually reauthenticate themselves in a fashion totally transparent to the end user. Because traversal of any one microperimeter may require authentication, enforcing hundreds of authentication challenges to every user/device pair on the network every day is infeasible.

This patented reauthentication method allows successful authentication at a certain security designation to persist and automatically apply to access policies with an identical or similar security distinction. Users and devices are re-authenticated in a non-interactive fashion when transversing microperimeters with similar access policy conditions – as long as they successfully passed the first interactive MFA check.

Both Helix MFA and Helix session authentication can be actively revoked or configured to expire on custom time or event triggers.

LEARN MORE ABOUT HELIX

Visit our website at **zkxsolutions.com** for more information on ZKX Helix and important use cases, such as:

- Establishing a Zero-Trust Architecture
- Zero-Trust Policy Enforcement
- Flattening the Tactical Network
- Merging Network Operations
- Tactical Cyber Defense
- Next-Generation MFA