ZKX HELIX™

PERVASIVE POLICY. PREMIUM PERFORMANCE.

HELIX KEY BENEFITS

- Granular, flexible, and customizable access policy
- Adaptable into any standardized framework, including commercial, Federal, and military systems
- Defined by device identity, authentication artifact, and calculated confidence
- Policy enforcement can extend beyond the enterprise level, out to the tactical edge or other networks

INTRODUCTION

In the context of cybersecurity, policy serves one absolutely essential function: to tie specific technology to specific action(s). Policy is the backbone upon which security operates. Policy dictates critical parameters of a network, including the definition of secure access and risk tolerance.

Yet policy – in all of its forms – is often seen as restrictive, a hindrance whose sole purpose is to arbitrarily stand in the way of optimal process and prevent quick and easy solutions from permeating the workplace. This perception – especially regarding cybersecurity – didn't come from nowhere, and in fact has done quite a bit to earn this reputation. Whether its requiring MFA to access a certain resource on the network, or having to communicate over a specific flavor of encryption, to ensuring your users' BYOD devices are compliant with some body of standards – policy has the ability to deflate any and every one of our cyber operations.

POLICY DEFINED

It's important to arrive at a succinct answer for the question, "What exactly is policy?" before we continue this conversation. In the context of cybersecurity, policy serves one absolutely essential function – to tie specific technology to specific action(s). Whether it's "capital-P" Policy (formalized, written standards like FIPS 140-3 or CMMC) or "lowercase-p" policy (access policies; usage policies), the driving motivation behind any prescriptive policy is to define in what form, method, and scope any piece of technology should or must be used. Take, for example, this verbatim line from the FIPS 140-3 requirements document:

> *"Cryptographic modules that conform to this standard shall employ Approved security functions…"*

If we dissect this, we can see the core elements of what constitutes a policy in action:

> *"Cryptographic modules (specific technology) that conform to this standard shall employ Approved security functions (specific action)…"*

Now, take an example access policy:

> *"All laboratory terminals must be configured to require an employee's badge and unique passphrase for login."*

We see again the core elements at play in this hypothetical policy:

> *"All laboratory terminals (specific technology) must be configured to require an employee's badge and passphrase for login (specific action)."*

In essence, all cyber policies (both Policies and policies. . .) accomplish this core task: tying technology to action.

Even though it may be one of the most disliked pieces of the cybersecurity environment, policy is the backbone by which security can stand and operate. Often, policy dictates critical parameters of a network, including the defining of relative terms such as "secure access" (the standards of which may vary by organization) and how tolerant of risk certain areas of an organization's ecosystem are (which in turn dictates how much money, time, and resourcing needs to be applied to said areas).

ADAPTABILITY IS KEY

When it comes to policy (both Policy and policy) ZKX Helix is an extremely flexible tool for the cyber operator, the security practitioner, and the on-the-ground tactician alike. In cases where Policy considerations are a primary concern, Helix can be molded and adapted into most any standardized framework and can live happily alongside the latest and greatest post-quantum encryption engines, as well as within the boundaries of locked-down-tight intrusion detection systems and other staples of federal, military, and commercial Policies and practices. Furthermore, the algorithms that drive the internal functions of Helix's MFA can be customized and fine-tuned to your organization's specific Policy needs, ensuring that whatever you may need – be it end-to-end encryption, the latest communication protocol, post-quantum cryptography – can be included in your own personalized Helix environment to give your network exactly the support that it needs.

GRANULAR, FLEXIBLE, AND CUSTOMIZABLE

Policy is where ZKX Helix truly shines. Granular, flexible, and customizable access policy is a necessity not only for new and emerging initiatives like zero-trust networking, but for keeping pace with the alarming rate

of increased attacks. In Helix, network administrators are able to define access policies on the basis of three main parameters that Helix uses to drive its core MFA functions:

- Device identity
- Authentication artifact
- Calculated confidence

These three parameters form the basis of the toolkit network administrators have at their disposal to set and enforce their exact access policy requirements within Helix. Helix policies are arbitrarily enforced, meaning that even as access policy requirements change in real-time, they are still faithfully executed in an exact fashion.

HELIX POLICY EXAMPLE

Say an e-mail server has been configured with Helix to require users to log in to their accounts using a PIN and password, achieve a confidence score of eight 9's (99.999999%) or greater, and allow them to do so on their own endpoints. The three Helix parameters at play here are again:

- Device identity (BYOD)
- Authentication artifact (PIN; password)
- Calculated confidence (eight 9's – 99.999999%)

Helix then enforces this access policy on users signing into the e-mail server until instructed otherwise. To continue our example, let's say that a significant security event has transpired: a vulnerability in the e-mail server's architecture has been discovered and has yet to be patched. A network administrator (or automated security tool) can reconfigure the Helix policy definition to more stringently vet those attempting to access the server until it is patched. A more stringent Helix policy may require users to now login with their PIN and employee badge, achieve a confidence score of fourteen 9's, and restrict connection only from enterprise-provisioned devices. The three Helix parameters have now been updated:

- Device identity (Enterprise Only)
- Authentication artifact (PIN; Employee Badge)
- Calculated confidence (fourteen 9's – 99.999999999999%)

This new policy – without any intervention on the end of the user, their device, or the client MFA software – will instantaneously begin being enforced, ensuring that your need for responsive, flexible protection of your network resources is met by Helix – an equally flexible, unthinkingly responsive, brutalist enforcer of access policy.

The example above is just the tip of the iceberg with regard to how Helix can enhance your inherent ability to enforce your exact specifications for protecting resources, as there are even more utilities in the Helix toolbox to provide your organization with a more visible, more granular, and more effective method by which to enforce access policy: session management, varying degrees of user and device revocation, policy chaining, and much more.

POLICY ENFORCEMENT AT THE EDGE

The most critical of these added capabilities is Helix's unique and native policy deployment, which enables your organization's enterprise policies to follow you in tactical or forward-deployed situations, and can even extend past your network's boundaries to that of the networks of your federated partners. Because MFA and policy enforcement for ZKX Helix are driven almost exclusively by publicly available data, users and devices that don't natively belong to your networked ecosystem can enter your network and have your access policies enforced upon them as they access your network – even if you didn't enroll them, their devices, or provision them any specific equipment.

This flexible and powerful characteristic exclusive to the Helix platform ensures that need-to-know is always enforced on your network — even in situations when multiple organizations meld together, network conditions are changing all the time, and dedicated backhauls to larger enterprise structures are denied or intermittent. Ensuring security is deployable (and policies are transferable) is only one of many assurances that come with ZKX Helix.

CONCLUSION

Policy, for all of its negative connotations, is a core driver and backbone of the cyber ecosystem. Policy helps to define the goals and boundaries of your network, and prescribes how the technologies that exist in your cyber environment must be deployed, configured, used, and managed in order to achieve goals and achieve mission success. ZKX Helix breaks new ground in terms of what policy (and Policy) mean to you and how your organization benefits from more granular, more dominant control of both policy management and enforcement.

Policies that permeate networks, boundaries, and the most hostile conditions. Helix protects your network exactly how it needs to be.