ZKX HELIX™
CRAFTING CULTURE. CURATING CHAOS.

HELIX KEY BENEFITS

- Improves the cyber posture of your organization without introducing more friction
- Feels identical to existing MFA solutions, making user adoption seamless
- Zero training time for end users

INTRODUCTION

The relationships between our security technologies, the operators responsible for managing them, and the users that depend on them have never been worse. Cybersecurity technology, much like the federal government, has increasingly demanded more from those that supposedly "benefit" from its presence — all while delivering less consistent and more ineffective service at a higher price in a smaller quantity.

The creeping slog and burden of cybersecurity tools, techniques, policies, and procedures have made invocations of "cybersecurity" an automatic trigger for deep sighs and eye rolls amongst much of the modern American workforce. Likewise, the degree of technical knowledge and expertise needed actually to keep pace in the modern cyber environment has never been higher, especially for those whose job functions aren't centered around information technology or cybersecurity.

CYBER SLOG

Most everyone is familiar with cyber slog — the annual (or sometimes even quarterly) "security training", usually conducted by some subpar series of canned, soulless videos that get played on mute until it's time to brute-force the correct answers to the twelve-question quiz that follows dutifully after; a live seminar led by the least charismatic IT manager of all time reminding you that, no, your boss will never need three $500 Google Play Store gift cards in the middle of a board meeting; the constant, oppressive fear of "gotcha" spawned from the chance of clicking on a scam e-mail created by your organization just to test you; the continual coaching and challenge that comes with finally crafting a password up to whatever asinine, mythical standard has been set for those now, and countless other ingenious methods of gumming up the gears of progress with nuclear-grade banality.

CULTURE SHOCK

With how technologized the minutia of our daily lives have become, shouldn't there be a technological remediation to these issues? "These issues", of course, being the immediate consequence and impact of the shortcomings, the inefficiencies, and the outright gaps in function of the technologies (especially the "security" technologies) we've been coached, convinced, coerced, connived, conned into depending on.

This is precisely what we mean when we say "Culture" in cybersecurity: not just the way users interact with technology, but also the way technology interacts with users and how users interact with other users, especially when they do so through the available technology. Of course, users and technology aren't the only players in this game, as policy — the rules, tactics and procedures both technologies and its users must abide by — sets the stage for these day-to-day, minute-by-minute clashes between people and technology. In fact, policy often prescribes cyber slog, dictating and enforcing the inane procedures required to make ineffective technology work, leaving the people — the end user or the administrator — holding the bag when it comes to the heavy lifting of making sub-par technologies minimally effective. Bad technology begets bad policy. Bad policy begets bad culture.

FACILITATING GOOD CULTURE

Helix is a reimagining of what security technology can truly do for its constituents. Instead of shackling users and depending on their labor to sustain sub-par security effects, Helix frees the user's cycles, lessening the degree of raw effort one must exert to participate in today's cyber-driven ecosystem. An overwhelming majority of jobs depend on IT networks in some form or fashion, with more disciplines following suit every day. Why should we be content with the friction, the burden, and the slog that comes with this ever-creeping growth of the cybersphere and the bloated technology platforms that currently enable it?

Helix enables organizations to foster the culture they need to fulfill their goals. Much like people, organizations are entirely unique, and differ in terms of their goals, tactics, methods, ideas, makeups, strategies, etc. Attempting to force everyone into the same mold (shoving a square peg in a round hole) is unsustainable, and results in security gaps, which proficient threat actors can sniff out and *will* exploit. Helix's unrivaled flexibility and simple deployment foster your unique cyberculture and encourages it to emerge naturally, resulting in methods and practices (and, in turn, technologies and policies) that are organic to your organization, your organization's needs, your employees, and your overall business goals and mission objectives.

To accomplish this, Helix contains novel and next-generation advancements in **usable security**. Typically in cybersecurity, usability and security are pitted at odds with each other and share an inverse proportionality. In other words, the more secure you want something, the less usable it becomes and vice versa. While security and usability will always be a balancing act in the larger cyber ecosystem, Helix offers a compelling

multi-factor authentication (MFA) and policy enforcement platform that achieves both characteristics — dynamic and robust security with ultimate usability.

The Helix platform intuitively combines technology and policy to create a usable cybersecurity experience. To detail exactly how Helix accomplishes the striking of this balance, we will briefly consider some of the core features of Helix and describe some of the security guarantees that come with them for both the end user and administrator alike.

MAXIMIZING USABILITY

From the perspective of the end user, the Helix client interface looks and feels nearly identical to the MFA clients we are all used to. As one of Helix's primary tenets is usability, it is vitally important that the introduction of Helix does not halt operations. When your organization deploys Helix, you will not have to deal with extensive training, unfamiliar interfaces, or an awkward UI.

For the administrator, this translates into zero training time for end users and ease of culturally migrating existing populations to a better technology. **Despite looking similar to competing MFA clients, the Helix client couldn't be more different under the hood.**

For starters, Helix can support an arbitrary pool of MFA credentials. Rather than prescribing credentials to you and your users, you can natively employ whatever best suits your people in your environment. Whether it's the reliable PIN and password, or more unconventional identity bindings like serial numbers and barcodes, Helix can ensure only the right credentials are used and verified.

Beyond simply employing whatever credentials you need supported, Helix goes one step further and secures those credentials in ways other solutions cannot. Helix uses patented technology to strengthen the confidentiality, integrity, and availability of each and every MFA credential employed by any user. Helix accomplishes this in three primary ways:

Exponentially boosting entropy of credential data. Entropy or, more colloquially, randomness, is the characteristic that makes something like a PIN or password powerful. Entropy is the reason why the obnoxious "password policy" – 12 characters, 2 special characters, at least 1 number, etc. – exists. Helix handles that piece for the user, especially if the user picks a traditionally "poor" or "weak" password. Helix's security boost to the randomness of credentials also extends to each individual instance that the credential is used – finally enabling user to safely utilize the same password across multiple accounts and websites. Finally – great security from great technology.

Strong identity binding, specifically between the user and the specific devices they are permitted to use on the network. The devices allowed to participate on a network may vary from organization to organization: some may support a BYOD policy, others may require multiple devices for multiple subnets, others may

have geolocation requirements, etc. Helix binds user identity to device identity, meaning that users can be considered differently based solely off of the device they're employing. Legitimate users, with legitimate credentials, holding legitimate privileges may still be denied access to certain resources on one device, but granted access on a different device. This stems from Helix's attribute-based method of building and using digital identity, and device-specificity is just one of the primary use-cases for how this system emboldens both cyber security and usability.

Session authentication. Authentication sessions (also known as "attestation" in Helix) continually authenticate users (and their devices) as they traverse the network and bounce between the potentially hundreds of resources they access during the course of their work. This is important, as emerging security frameworks such as zero-trust require near-constant authentication and authorization of users and their devices.

For other MFA solutions, this is a total nightmare! Imagine slowing down your workforce exponentially all so they can enter the same old MFA credentials into some client app a thousand times in one sitting, slowing the rate of progress to a crawl all in the good name of "security". On the other hand, if organizations don't adopt this more granular security structure, we wish them the best of luck with their upcoming recovery from being hacked.

Helix enables the best of both worlds via its session authentication as not only do the sessions enjoy all of the security guarantees that the MFA does, the sessions are also transparent to the end user – i.e., users and their devices are continually authenticated in the background of their operations; reverification requires no input from the user.

CONCLUSION

Helix technology technology is patented and totally exclusive to ZKX, making our security offerings truly one-of-a-kind. As a policy enforcement platform, you won't find another like Helix. Helix sustains total elevation of cyber culture via its other two foundational tenets – Superior Security and Precision Policies. Good technology begets good policy. Good policy begets good culture.

Create the culture you need. Don't let your needs be downstream from bad technology.