WHITEPAPER

Zero Knowledge Networking

XIID CORPORATION MAY 2023

CONTENTS

Abstract

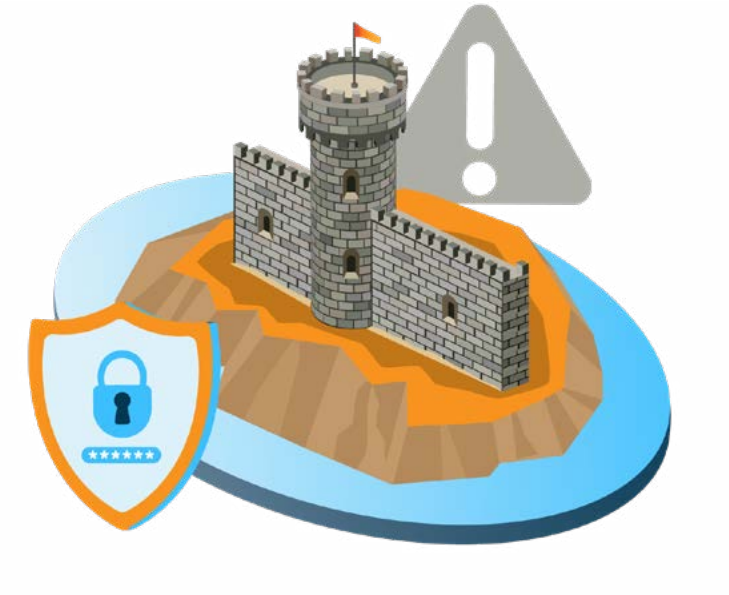
The growth and success of networking and IT architectures face obstacles due to the complexity and disparity of resources across enterprise networks and the diffusion of the network perimeter. To address security challenges, many organizations have adopted Zero Trust Network Access (ZTNA) solutions, which generally improve enterprise security posture.

Xiid is the leading pioneer of Zero Knowledge Networking (ZKN), which overlays and improves upon ZTNA by addressing common challenges such as third-party identity federation, “break-and-inspect”, and open inbound firewall ports. ZKN was designed and developed specifically to provide superior functionality at higher security levels and lower costs.

This paper defines the ZKN standard through the tenets and requirements that must be satisfied for a network architecture to be considered “Zero Knowledge”.

Xiid is the leading pioneer of Zero Knowledge Networking (ZKN), which overlays and improves upon ZTNA by addressing common challenges such as third-party identity federation, “break-and-inspect”, and open inbound firewall ports.

Zero Trust Attempted to Address the Challenges of Perimeter Security



For many years, network security was relatively straightforward. Preventative measures focused on protecting the private, internal enterprise network perimeter, since employees physically worked from the office and used digital resources located within the internal network. As a result, traffic inside the internal network was largely deemed "safe", and activity coming from the outside internet was untrusted and could be blocked. Over time, this "castle-and-moat" approach to cybersecurity, known as *perimeter security*, started to break down.

Market shifts and workplace trends expanded the network perimeter, complicating the cybersecurity landscape and exposing the vulnerabilities of perimeter security. The rapid adoption of cloud services, SaaS/XaaS offerings, and microservices led to a "hybrid cloud" enterprise infrastructure, with many key resources no longer residing within the internal network. Savings were realized through Bring Your Own Device (BYOD) programs, at the cost of relinquishing tight control over devices connecting to corporate resources and an increased risk of insider threats. More people began working remotely, and COVID-19 amplified a work-from-home trend that may never fully reverse.[1] With the vulnerable enterprise network "perimeter" becoming so diffused as to be rendered ineffective on its own, a new paradigm, *Zero Trust Network Access (ZTNA),* arose to deliver security without needing to assume a perimeter exists at all.

ZTNA, also referred to as *Zero Trust*, is a "never trust, always verify" approach to cybersecurity, distrusting users and devices equally and making no security distinction between the internet and intranet.[2] While perimeter security focused on connecting people to **networks,** in practice, Zero Trust instead connects people directly to the **resources** they need to use and re-authenticates them before each session.

> While perimeter security focused on connecting people to networks, in practice, Zero Trust instead connects people directly to the resources they need to use and re-authenticates them before each session.

Over the past decade, the number of ZTNA solutions available in the market skyrocketed, as numerous vendors launched products claiming to quickly make an organization's architecture "Zero Trust". In 2021, an Executive

[1] https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/
[2] https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

Order issued in the United States directed Federal Government agencies to "...advance toward Zero Trust Architecture", further demonstrating a recognition of the increase in cyber risks and advanced cyber adversaries and the growing demand for ZTNA in both the public and private sectors.[3]

Many Commercial ZTNA Products May Still Have Vulnerabilities

To standardize the meaning of *Zero Trust* industry-wide, the National Institute of Standards and Technology (NIST) published a set of tenets that an architecture should follow to be considered Zero Trust. These tenets include controlling access on a per-resource basis, securing communication regardless of a device's location, using a dynamic security policy, and monitoring the integrity of devices that use enterprise resources.[4] Unfortunately, many ZTNA solutions in the market do not fully meet this NIST standard.

While most ZTNA implementations offer substantial improvements over perimeter-based security models, they are not "one-shot fixes" to all cybersecurity concerns. The architectural designs of many ZTNA products, even those meeting the NIST standard, often suffer from several common, significant vulnerabilities:

Third-Party Data Federation

To provide authentication services, vendors frequently require organizations to entrust them with full copies of LDAP directories to store in the vendor's data centers. Trust must be placed in the vendor to protect this highly sensitive enterprise data not only at-rest, but also in-transit, both during the servicing of authentication requests and the syncing of directory data to and from the organization. A misconfigured sync could accidentally expose sensitive data, and holding volumes of sensitive data from multiple organizations in vendor clouds makes the vendors themselves an alluring target for cybercriminals.

Use of "Break-and-Inspect"

Many vendors tout their capability to defeat the encryption of enterprise web traffic to scan it for malware or other undesired content, and if done well, this feature can be valuable and effective, albeit risky. Enabling "break-and-inspect" allows the vendor, and any attacker who has breached the vendor, to have full access to all secrets, secure communication, and other sensitive enterprise information traveling across the internet or private network.

Requiring Open Inbound Firewall Ports

To provide authentication services, sync directories to the vendor's data centers, or enable other functionality like tunneling or remote desktop, nearly all vendors require the enterprise to open inbound firewall ports on their private network, such as the often-exploited port 443.[5] Open inbound ports represent a substantial vulnerability and are among the first places attackers attempt to breach when trying to infiltrate an organization. To mitigate this, ZTNA vendors offer "AI-enabled" firewall products that attempt to manage a complex set of firewall rules to thwart attackers. However, these "AI" models are often black-box and

[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[5] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=443

imprecise, and an organization must entrust the security and reliability of their enterprise networks to the decisions the models make.

These aspects of many commercial ZTNA products conflict with the implication of "Zero Trust" – that no entity is trusted. Instead, **nearly limitless trust must be placed by an enterprise or agency in the ZTNA vendor themselves.** While the original intent of Zero Trust – "never trust, always verify" – is laudable, not all ZTNA solutions in the market are successful at achieving this goal.

A new framework, Zero Knowledge Networking, has emerged to conform to, overlay, and dramatically improve upon the NIST Zero Trust Architecture standard, delivering the initial promise of ZTNA while solving the fundamental security concerns with real-world ZTNA solutions.

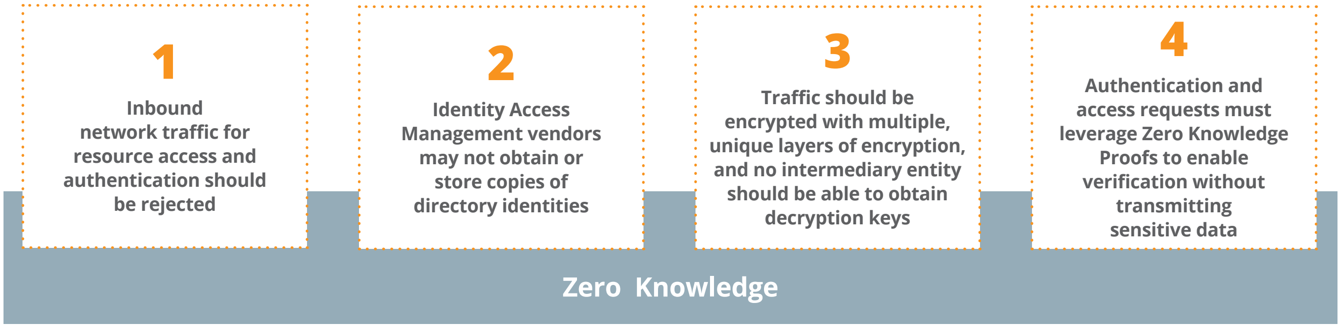
Zero Knowledge Networking Overlays ZTNA and Addresses Key Vulnerabilities

Tenets of Zero Knowledge Networking

Zero Knowledge Networking (ZKN) guarantees that all parties – the endpoints and the vendor in-between – have no excessive knowledge of each other's sensitive data or location, eliminating vulnerabilities in a way that's proactive, rather than reactive.

Whereas ZTNA solutions in the market largely utilize "break-and-inspect" and AI-enabled firewalls to react to incoming attacks and exploits, ZKN fundamentally re-architectures the network to be naturally and proactively resistant to a wide range of attacks.

To be considered Zero Knowledge, networks must adhere to the following tenets regardless of the type of network traffic:



1 Inbound network traffic for resource access and authentication should be rejected

2 Identity Access Management vendors may not obtain or store copies of directory identities

3 Traffic should be encrypted with multiple, unique layers of encryption, and no intermediary entity should be able to obtain decryption keys

4 Authentication and access requests must leverage Zero Knowledge Proofs to enable verification without transmitting sensitive data

Zero Knowledge

Inbound network traffic for resource access and authentication should be rejected

Client devices and the enterprise private network should not require open inbound firewall ports for authentication or resource access. Attackers frequently target open ports for vulnerabilities. All access to resources, no matter the resource, should be achieved using outbound-only traffic on both endpoints. Further, since all traffic is outbound-only, neither endpoint should require or need to share a public IP address.

Identity Access Management vendors may not obtain or store copies of directory identities

Authentication requests should be processed and actioned efficiently without federation to a third-party service. Copies of sensitive identity information in Identity Access Management (IAM) vendors' data centers are extremely risky and dramatically increase the enterprise attack surface. Taking this risk should not be necessary for an organization to securely authenticate its users.

Traffic should be encrypted with multiple, unique layers of encryption, and no intermediary entity should be able to obtain decryption keys

All traffic should be encrypted with multiple layers of encryption, with the encryption algorithms used varying across the layers. This variation is key, as is it far more difficult for an adversary who can defeat one type of encryption to defeat multiple. There must be at least two layers of encryption, and one of the inner layers must use an Authenticated Encryption with Associated Data (AEAD)-type encryption method.

In addition, decryption keys should not be shared with any entity that could be positioned to intercept network traffic. These measures prevent man-in-the-middle attacks, adversaries, and potentially-compromised "break-and-inspect" vendors from deciphering traffic and enterprise data.

Authentication and access requests must leverage Zero Knowledge Proofs to enable verification without transmitting sensitive data

Stealable credentials (e.g., usernames and passwords) should never be sent over the internet as part of the authentication process. *Zero Knowledge Proofs* make it possible to exceed the level of authentication used by Multi-Factor Authentication (MFA), which still requires the transmission of credentials, by securely authenticating users without sharing credentials at all. Zero Knowledge Proofs, until recently, only existed in academia. These algorithms now make it possible to prove a piece of information – such as an identity – without transmitting any sensitive knowledge to the verifier.[6]

[6] https://codethechange.stanford.edu/guides/guide_zk.html

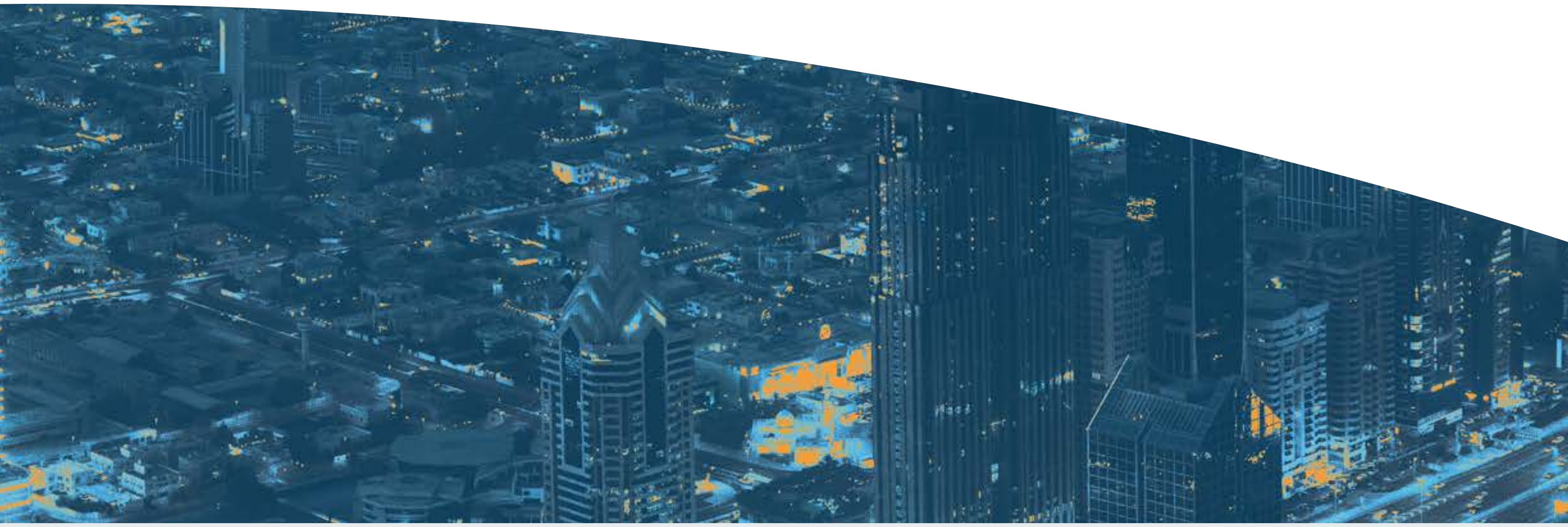
Compliance with these tenets, in addition to the NIST Zero Trust Architecture, forms the highest-security commercial networking paradigm on the market. Ideally, a ZKN network should also take a decentralized approach to resources, where no resource or system has authority over the entire network.

As cybercriminals become increasingly sophisticated, it may be tempting to implement "AI-enabled" products in an attempt to outsmart adversaries. ZKN achieves a higher level of security without needing black-box AI algorithms by fundamentally redesigning the network in a way that **structurally** reduces the enterprise attack surface, offering security, efficiency, transparency, and simplicity.

Xiid is the Leading Pioneer of Zero Knowledge Networking

Predominant players in the authentication and digital resource access market largely arose out of a need for *functionality* – that is, they delivered an urgently needed service in an evolving market. However, this meant that mitigating security concerns were an afterthought and many products' designs became vulnerable as cybercriminals grew more sophisticated and new angles of attack emerged. Even those who fit the ZTNA model may still leave wide security gaps in their architecture. Xiid is unique in that its products were designed from the ground up with a security-first architecture that pioneers and defines Zero Knowledge Networking, in addition to meeting all NIST ZTNA guidelines.

> Xiid was the first to leverage Zero Knowledge Proofs in the authentication and access markets, protecting credentials, identities, and enterprise data from theft, and is also one of the only companies to offer ZTNA functionality without requiring the federation of data to third-party data centers or infrastructure.

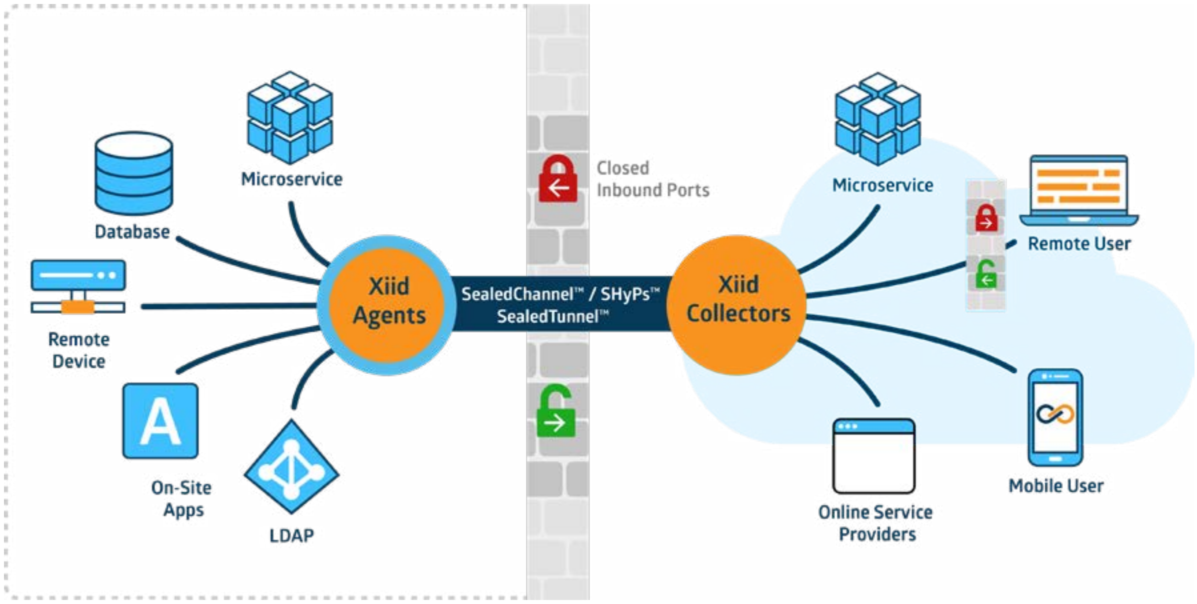


Xiid also devised low-level security innovations that stop attacks before they happen or make them impossible altogether, such as Xiid's patented Smart Hybrid Protocols (SHyPs™) that maintain unbreakable, multi-layer, end-to-end encryption while still guaranteeing that authentication requests do not contain extraneous malicious payloads.

Xiid Zero Knowledge Networking In-Practice

Backed by Xiid's ZKN Identity Access Management solution, Xiid.IM, Xiid delivers ultra-high security access to enterprise resources, such as through the Xiid SealedTunnel™, delivering low-latency, double-encrypted, process-to-process tunneling between remote resources over any type of IP communication, including SSH and Remote Desktop Protocol/Virtual Desktop Infrastructure (RDP/VDI). In addition, **since Xiid does not need to operate large data centers, it is able to offer solutions at a far lower cost than traditional ZTNA vendors.**

Sample Xiid ZKN Implementation



Xiid agents are installed behind the firewall that connects out to the cloud.

Closed firewall ports block incoming traffic.

Multi-layer encryption protects all connections.

Xiid's products meet all Zero Knowledge Networking requirements:

ZKN Requirement	Xiid Compliance
Inbound network traffic for resource access and authentication should be rejected	Xiid products do not require any use of inbound network traffic at any time and are capable of efficiently handling large numbers of concurrent users. As a result, endpoints using Xiid products do not require public IP addresses. In practice, two endpoints interacting via Xiid services are "triple-blind" in that neither party nor Xiid knows excessive information about the other nor the endpoints' locations.
Identity Access Management vendors may not obtain or store copies of directory identities	Xiid's cloud services can action IAM requests without collecting or requiring copies of enterprise data.
Traffic should be encrypted with multiple, unique layers of encryption, and no intermediary entity should be able to obtain decryption keys	Multiple layers of end-to-end encryption with varying algorithms between devices and enterprise infrastructure prevent Xiid, adversaries, or other "break-and-inspect" solutions from deciphering network traffic. Xiid's inner encryption layers leverage AES-GCM in the AEAD family. At no point does Xiid require copies of encryption keys, ensuring that enterprise traffic stays safe even in the event of Xiid itself being compromised.
Authentication and access requests must leverage *Zero Knowledge Proofs* to enable verification without transmitting sensitive data	Xiid's XOTC™ Authenticator leverages Zero Knowledge Proofs and SHyPs™ to deliver secure, credential-less authentication.

As an example, RDP and VDI are widely used by call center and Managed Service Provider (MSP) employees who work remotely and need to access specialized enterprise tools and customer data.[7] ZTNA products and VPNs currently used to facilitate remote resource access are vulnerable to the interception of highly-confidential customer information, and companies must trust the vendors of these products with safeguarding that information. In addition, adversaries that breach these vendors may gain access to large quantities of customer PII or even the enterprise tools themselves. Xiid's SealedTunnel™ secures RDP/VDI without VPNs or the need for open inbound firewall ports on either the client machine or server.

[7] https://www.ibm.com/cloud/blog/what-is-virtual-desktop-infrastructure

Financial

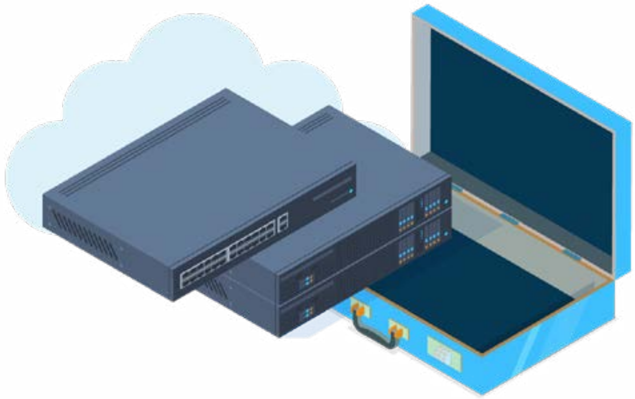
Healthcare

Military

The SealedTunnel ensures that neither Xiid nor cybercriminals, even if Xiid's services were breached, would be able to decrypt the multiple layers of end-to-end encryption securing the RDP/VDI session.

Xiid's product suite has been penetration tested by the U.S. Air Force Research Laboratory (AFRL), and **not only was the AFRL unable to breach Xiid's encryption, but their tests also demonstrated the "...near invisibility of the product externally."** As a result, Xiid's products are now in use by several U.S. Government agencies in the field to secure extremely sensitive data.

For instance, one agency's in-theater field operatives faced significant challenges in securely logging and transmitting highly sensitive health information with limited internet and command center access at remote sites. Xiid worked with the agency to create "flyaway kits" (briefcase servers) equipped with Xiid Identity Access and Management (IAM) for secure authentication and access to medical record software through an Xiid-hosted Single Sign-On (SSO) portal. Field operatives are now able to securely authenticate and log medical information through the flyaway kits, with Xiid ensuring the confidentiality, integrity, availability, and in-transit security of sensitive data from anywhere in the world.



Xiid's suite of NIST-compliant ZTNA products overlays Zero Knowledge Networking to address the security gaps of other ZTNA offerings while delivering higher levels of functionality at a lower cost.

Engineered by longtime industry cybersecurity experts, Xiid offers the leading framework for secure access to an organization or agency's most sensitive assets from anywhere in the world.

Prepared by Full Depth Consulting

xiid.com