coevolve™

NextGen Series

Building cyber resilience through zero-trust

A guide to meeting your network security objectives through ZTNA and AI

January, 2025

Table of Contents

State of play: introducing zero-trust

Modern enterprises are under threat. Cyberattacks are relentless and rapidly increasing in number, making businesses more vulnerable than ever. Enterprises face dual security threats: malicious actors exploiting network vulnerabilities externally and employees inadvertently introducing risks internally. Securing enterprises requires a united effort, but Chief Information Officers (CIOs) must lead the charge. Zero-trust has emerged as a powerhouse approach, but it's not a solo solution. CIOs must navigate new ground and advance the zero-trust conversation to stay ahead.

Cutting through the noise: zero-trust hype or hope

With business risks rapidly multiplying, leaders are wondering how to safely operate and future-proof their enterprises in unchartered waters. The EY 2023 Global Cybersecurity Leadership Insights Study found only 48 percent of leaders were satisfied with the effectiveness of their enterprise's approach to cybersecurity and 54 percent with their ability to block the threats of tomorrow. There is still much work to do, and CIOs need to embrace fresh perspectives and modern strategies to drive meaningful change.

Enter zero-trust, the much talked about so-called foolproof solution. Yet, achieving "100% security" with zero-trust, while appealing in theory, remains a fallacy often perpetuated by vendors. According to Gartner, vendors continue to heavily promote zero-trust as the ultimate silver bullet to upgrading security, amplifying the noise and hype that CIOs must carefully navigate. While not a silver bullet per se, zero-trust enables greater cyber resilience than ever before possible, and CIOs that apply zero-trust with a strategic and pragmatic approach can seamlessly modernize and elevate their outdated cyber posture.

Today's savvy CIO must acknowledge that while zero-trust offers substantial advantages, no single product, solution, or paradigm can deliver "100% security" – instant solutions for network security are a myth. If a vendor makes such promises, recognize them as peddlers of illusion and immediately seek other partnerships. Still, defining zero-trust is a crucial starting point. As more enterprises adopt it without proper understanding, the likelihood of failure increases. Gartner research shows over 60 percent of organizations will deploy zero-trust by 2025, but more than half will struggle to realize its benefits.

> "The traditional concept of a secure network perimeter no longer holds in today's interconnected world. Firewalls and intrusion detection systems may guard the outer edges, but once inside, users often move freely – a major vulnerability. A zero-trust model challenges this, treating every user as untrusted until verified. No longer focusing on sites or locations and IP addresses, a zero-trust approach places a spotlight on the user and dynamically adapts based on user identity, device posture, and access needs - enforcing consistent protection whether at headquarters, a branch office, or working remotely."
>
> **Ciaran Roche**
> **Co-Founder and CTO, Coevolve**

Defining zero-trust and ZTNA for the modern CIO

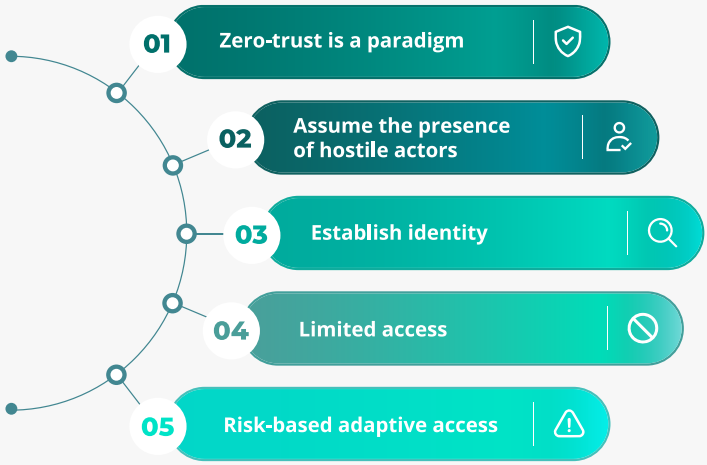
Even with a cloud of mystery surrounding zero-trust, according to Mordor Intelligence, the zero-trust market is expected to soar from USD$32 billion in 2024 to USD$73 billion by 2029. Whichever way you look at it, zero-trust is the next big thing, even if what it means is vague for businesses.

Zero-trust is challenging to define because it is not static. It continues to evolve, adapting to modern threats and current diverse organizational needs which in turn has opened the term up to misconceptions and misunderstandings.

Additionally, vendors present their own interpretation, further creating ambiguity. Despite this, the definition evolving, zero-trust is anchored in the principle of "never trust, always verify." Zero-Trust Network Access (ZTNA) refers to the strategic implementation of network devices and security services designed to enable a zero-trust model.

Phil Vachon, Bloomberg's Head of Infrastructure, highlights this variability and the importance of questioning vendors about their ZTNA definition during the sales process. He insists on asking, "I need an answer as to what [ZTNA] means to you at this point in time," as the explanation vendors provide will reveal their approach to zero-trust, which Vachon views as fundamentally a design philosophy.

The 5 zero-trust core principles



Source: Gartner

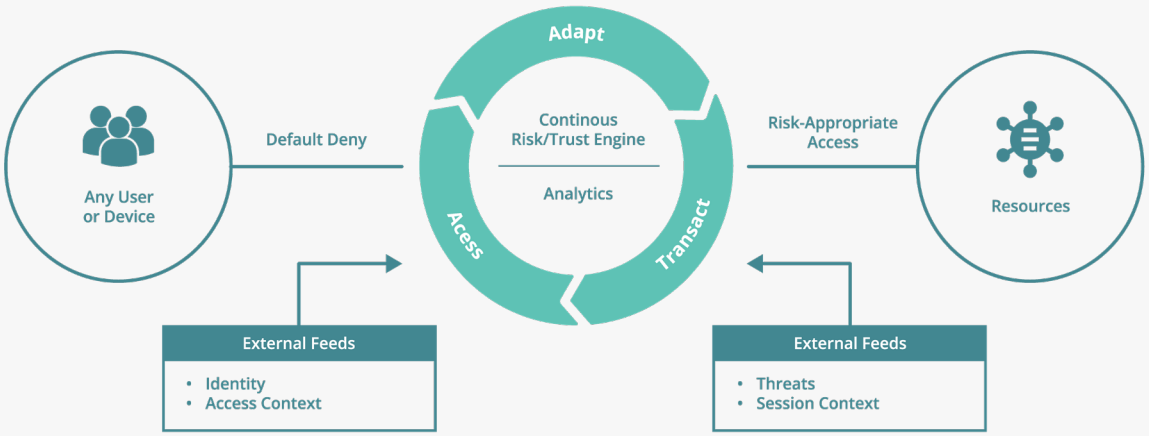
Breaches are inevitable but can be mitigated with ZTNA

As CIOs navigate their network security transformations, adopting zero-trust principles is essential for strengthening defenses. Because it is founded on 'never trust, always verify,' zero-trust ensures only authorized, necessary access is granted, and potential threats are immediately identified. It is an approach that is vigilant and ever-watchful, some might even call it appropriately paranoid, making it well-suited to meeting the demands of today's security landscape. Zero-trust capabilities can also be enhanced with AI to deploy algorithms to detect, analyze, and act upon threats in real time.

Before finalizing their security strategy, CIOs should assess their key challenges, such as legacy infrastructure, vulnerable devices, risk, hybrid working, compliance, cost, and skills gap, to ensure a tailored approach.

In this discussion paper, we invite CIOs to immerse themselves and discover the true capabilities of ZTNA – the myths, the truths, and the obstacles to success - to learn how to develop a robust security approach that unlocks the significant value of zero-trust. Now is the time for CIOs to move from a position of insecurity to proactively plan a future-proof security roadmap.

High-level zero-trust system



Source: Gartner

Key insights

In today's digital environment, CIOs are stressed, with shaken confidence, due to constant cyber threats and high expectations from their boards. According to PwC, 82 percent of CIOs struggle to realize value from technology investments. According to the World Economic Forum, for 45 percent of leaders, operational disruption in the event of a cyber event is also weighing on the minds of CIOs, further complicating their role in navigating this challenging environment.

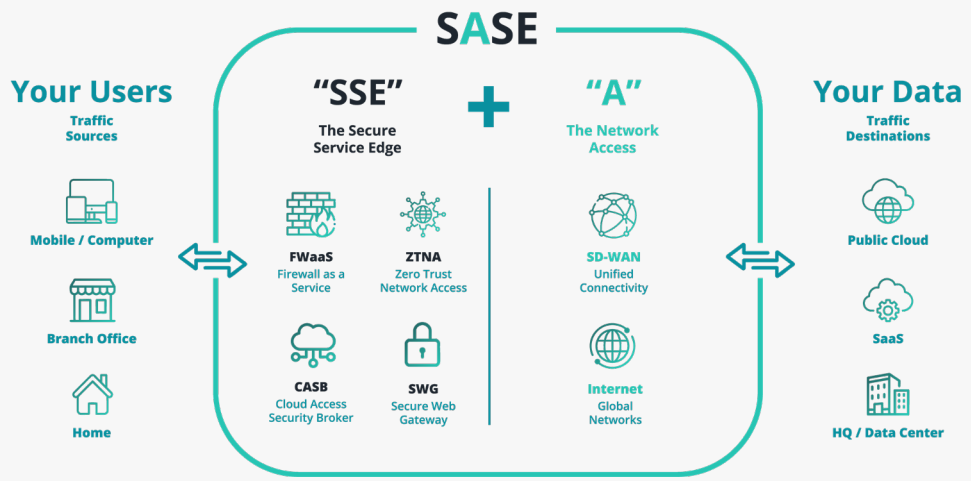
Key insight #1 – There is a lack of ZTNA intelligence

As Plato observed, these are strange times in which we live - an apt reflection of the complex cybersecurity challenges facing the modern CIO. In today's ever-evolving cybersecurity landscape, zero-trust misconceptions are widespread, primarily due to varying definitions that change depending on who you ask. Myths persist, such as that zero-trust adoption can instantly resolve all security issues. However, CIOs must recognize that cybersecurity requires ongoing refinement and adjustments to remain competitive, compliant, and secure. To navigate zero-trust complexity, enterprises must adopt best practices that address their unique cyber vulnerabilities while upholding a proactive stance. Leveraging industry experts and utilizing adaptive security technologies can further bolster implementation efforts.

Key insight #2 – The security divide must be closed

According to Gartner, a zero-trust strategy generally addresses up to 50 percent of an organization's security environment but only mitigates less than 25 percent of overall enterprise risk. It is essential for businesses to adopt a comprehensive security approach to address existing gaps. This involves integrating advanced measures such as AI-driven threat intelligence and incident response plans, as well as employing multi-layered frameworks like SASE (Secure Access Service Edge). By combining SASE with essential security technologies like ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Firewall-as-a-Service (FWaaS)—enhanced by Security Services Edge (SSE)—organizations can establish a more robust and future-ready defense against evolving cyber threats.

SASE framework example

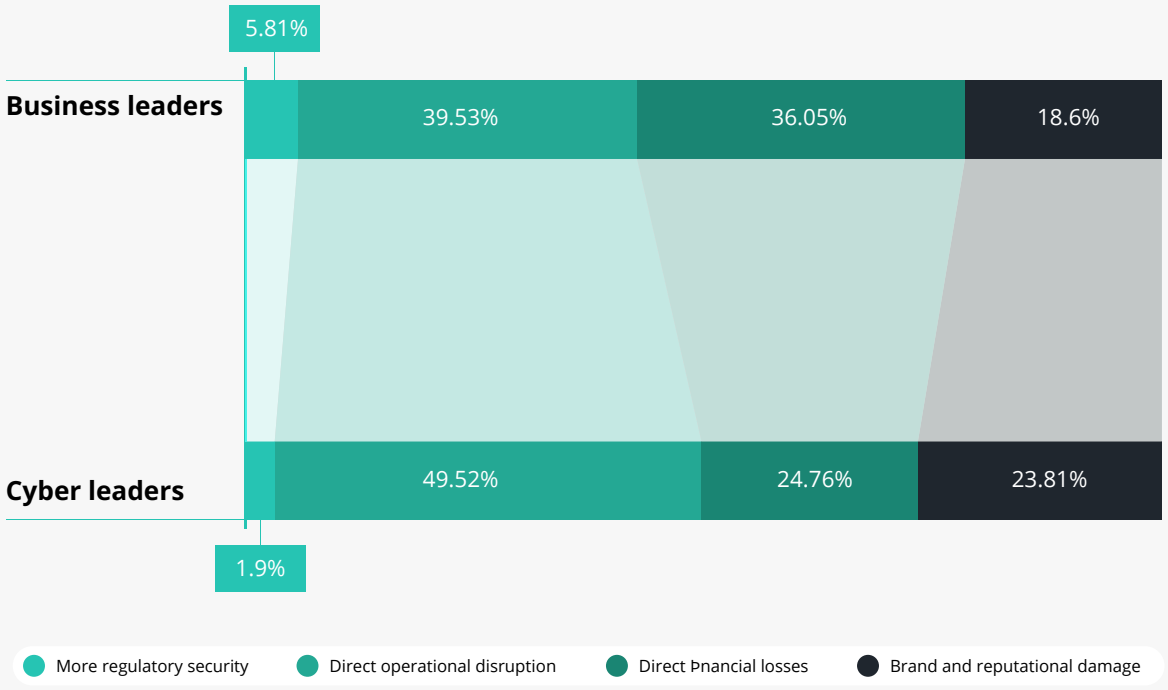


Key insight #3 – AI and zero-trust must work hand in hand

The influx of threat actors, including AI-enhanced threats, has made network security a top priority for CIOs, but they are torn between the competing challenges and priorities that they face across the full IT agenda. AI's rise is a dual challenge. It is both a powerful tool and a significant threat, making cyberattacks progressively cunning and harder to defend against.

Despite these critical obstacles to network security, there is a silver lining - AI can fight AI to secure digital infrastructure against attacks. Together with zero-trust, AI will enable enterprises to leverage adaptive and proactive defense mechanisms that mitigate and detect breaches before they happen. This synergy ensures a CIO's digital infrastructure is protected and has a security posture that adapts to emerging threats, safeguarding robust defense and shielding sensitive data and systems from malicious attacks.

What impact from a cyber attack are you most concerned about?



Source: World Economic Forum

Defining zero-trust: the myths, misconceptions and truth

The traditional approach to networking and security is no longer viable. In the ever-changing world of cybersecurity, CIOs need sophisticated solutions and thinking to advance forward. Zero-trust plays a key role in the future of security, but it requires continuous maintenance and adaptation. Zero-trust serves as a security paradigm, not a one-time integration solution. But despite the hype, CIOs must recognize the true potential of zero-trust and its weakness to effectively navigate the security journey.

What is zero-trust?

The term zero-trust was coined in the 1990s and was deemed the alternative to "castle-and-moat" network security models. Its model centers around strict access controls, continuous verification, and the "never trust, always verify" ideology. According to Gartner, zero-trust is defined as a security paradigm that begins from the "baseline of trusting no end user and explicitly identifies users and grants them the precise level of access necessary to accomplish their task."

As an example, think of traditional security models as an airport security checkpoint. Every passenger must show their identification and have their bags searched, after which they can move freely. Whereas a zero-trust model has the same initial checks, but in this highly secure airport, a security guard follows the passengers to their gate, ensuring they don't go anywhere risky and only allowing the minimum possible level of access.

A recent Gartner survey of chief security leaders uncovered that 56 percent of organizations are implementing a zero-trust strategy largely because it's deemed an industry best practice. However, as John Watts, VP Analyst at Gartner, observed, "Despite this belief, enterprises are not sure what top practices are for zero-trust implementations." To successfully implement this security approach, businesses should consider their scope first. "Scope is the most critical decision for a zero-trust strategy," he asserted.

Common zero-trust myths

Despite ongoing confusion, Statista, a global data platform, revealed that 56 percent of respondents rank the adoption of zero-trust paradigm as a top or high priority for their organization. There are several prevalent myths that are circulating about zero-trust that need to be discredited. We debunk the top four:

Myth #1 - Zero-trust is a product, service, or technology: Zero-trust is characterized as a security that eliminates the traditional perimeter-based security approach. The strength of the zero-trust method lies in its user identity focus; it can be tailored effectively to address unique and business-specific challenges, unlike traditional security structures.

Myth #2 - Zero-trust is a plug-and-play solution: It is a misconception that zero-trust can be applied quickly into a network, but it is a scalable approach that can be implemented incrementally. Instead, CIOs can start small—testing with specific users or sites. This gradual method helps refine policies, ensures strong security, and delivers a seamless user experience, steadily building a more resilient environment.

“Zero-trust is often misunderstood as simply adding another layer of technology. In reality, it represents a paradigm shift moving away from securing the traditional network perimeter to treating all traffic and users as untrusted until verified. Many still perceive zero-trust as being about network sites and IP addresses, when its true power lies in focusing on users, their identities, and the specific resources they need to access.”

Ciaran Roche,
Co-Founder and CTO, Coevolve

Myth #3 - Zero-trust means zero breaches: The nature of the modern cyber environment is ever-evolving, making the elevated amount and type of sophisticated cyberattacks hard to combat. zero-trust can significantly strengthen network security together with security solutions, but it is not bulletproof. It is designed to cut risk and restrict the impact of potential breaches, but no security model can offer absolute protection.

Myth #4 - Implementing zero-trust means adopting a full SASE architecture: While there may be benefits that come from a single set of policies and end-to-end context for every connection attempt, a zero-trust architecture can be implemented in phases. Technologies like software-defined wide area network (SD-WAN) enhance zero-trust frameworks by aggregating diverse connectivity options for reliable performance, providing overlay benefits like optimization and visibility, and bridging legacy devices without compromising security. Its flexibility supports hybrid setups, ensuring seamless operations for both modern users and traditional network elements. Businesses can also implement zero-trust without a full migration to all SASE components.

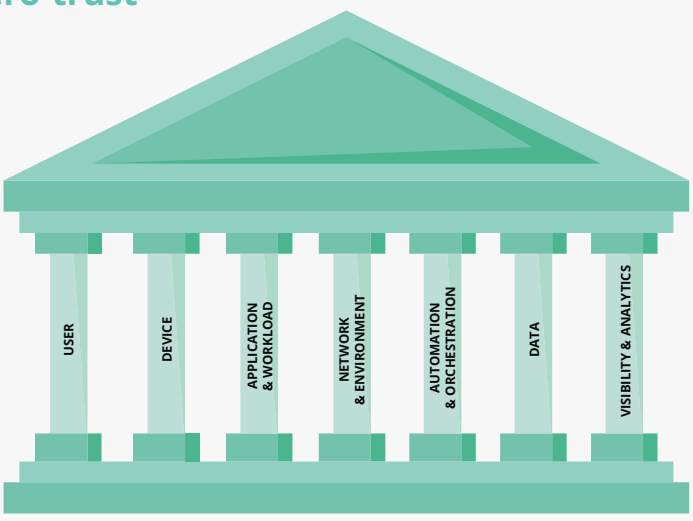
Aligning zero-trust ambitions with vendor realities

In the cybersecurity realm, there is tension between the zero-trust goals of enterprises and the capabilities of security vendors. CIOs must ensure they understand that zero-trust requires a complex adoption process before engaging with a vendor. Otherwise, they could face implementation failure. Unfortunately, Gartner has indicated the majority of zero-trust approaches safeguard 50 percent or less of an organization's environment and, worse, mitigate only up to 25 percent of overall enterprise risk. This is a stark contrast from the information circulating in terms of zero-trust effectiveness.

Zero-trust is gaining traction as a critical strategy to reduce risk despite a lack of knowledge surrounding the security paradigm. By 2026, roughly ten percent of large-scale businesses will have mature zero-trust initiatives in place – an increase from one percent last year. The increase of zero-trust combined with deep knowledge gaps is a recipe for security failure.

Navigating your zero-trust journey will undoubtedly pose challenges, but there are third-party partners, such as Coevolve, who can serve as a guiding light, steering you away from disinformation, hype, and the confusing narratives surrounding zero-trust perpetuated by other vendors. Instead, Coevolve provides support, knowledge, and guidance focused on positive outcomes for your business.

7 pillars of zero-trust



Source: National Security Agency (NSA)

From insecure to secure network security – how to bridge the divide

Cyber insecurity in business has reached epidemic proportions. An EY survey revealed approximately half of leaders are worried about their network security posture. Leaders can overcome insecure network security, but it will take ingenuity and a comprehensive security framework. Ambiguity is a leader's enemy; achieving clarity in all areas impacting the IT agenda, including cybersecurity, is essential to move forward. CIOs must dare to define zero-trust in the context of their enterprise to deliver digital value and an ROI on new security measures.

The path to future-proof network security

In a perfect digital world, a clear path toward network security would exist without any ambiguity, and it would be a one-size-fits-all approach for all enterprises. CIOs would immediately know what type of approach to take and the solutions to adopt. The zero-trust paradigm could be dropped into an enterprise's current network security environment without any errors and immediately ward off all attacks from today, tomorrow, and forever.

In reality, nothing could be further from the truth. Instead, vendors continue to falsely market zero-trust as a security technology that can transform cyber security for organizations, and the majority of leaders are still unclear in terms of zero-trust can achieve.

To ditch cyber uncertainty and elevate cybersecurity, CIOs should concentrate on gaining a comprehensive understanding of zero-trust's capabilities and how to best implement a contemporary network security roadmap while adopting a human-centric approach to security. Additionally, enterprises should not shy away from AI but embrace it and employ next-generation technologies, such as SD-WAN, that will optimize security and network performance. Lastly, lean on the expertise of a trusted partner like Coevolve to benefit from their expertise and guidance throughout your zero-trust journey.

The human-centric approach to cybersecurity

Enterprises must understand that their people have the capacity to make or break their network security success. For Bloomberg, Phil Vachon, Bloomberg's Head of Infrastructure, said that they took a human-centric approach and that the identity concept must be "baked" from the start. "The moniker we use is the principle of least privilege. You should only be privileged just enough to do your job and nothing more. So that might sound like some paranoid spy nonsense, but it's about a mindset of, 'Hey, would I be comfortable putting this system, this service, this functionality out on the open internet.' And if not, why?"

According to Forrester, a research and advisory company, predicts that 90 percent of data breaches have some aspect of a human element in 2024. Most breaches are unintentionally facilitated by employees, underscoring that employees must be taken on the security journey. Humans are crucial to zero-trust implementation, and enterprises must recognize their pivotal role in ensuring its success throughout the network security process.

Ultimately, a human-centric approach is vital for robust cybersecurity, as employees play a critical role in both the success and vulnerability of network security.

SD-WAN and ZTNA – a dynamic security duo

The human aspect of an enterprise's security posture is critical and ensuring hybrid teams are safe and secure within a zero-trust framework presents opportunities and challenges for CIOs due to the complexity of aligning diverse technologies.

When applied successfully, the zero-trust approach allows enterprises to realize the highest level of security in borderless IT environments. ZTNA, however, does have limitations. A common question is whether SD-WAN is necessary when ZTNA is already in place. The answer is a yes – this two-tier security approach unlocks significant benefits, and organizations can deploy SD-WAN at any stage of their transformation, granting them the ability to secure access to distributed applications for their dispersed and global workforce.

Additionally, an SD-WAN network excels at aggregating various connectivity options, such as broadband, 4G, and 5G, while abstracting the underlying network infrastructure. This setup ensures users have reliable connections, failover capabilities, and seamless performance, which are critical even in a zero-trust environment. By combining SD-WAN with zero-trust principles, organizations benefit from underlay application components and overlay capabilities like configuration management, network optimization, and enhanced visibility into network health and performance.

The five key ways that SD-WAN can work together with zero-trust to combat risk:

1. Multi-tier security model for a stronger cyber defense
2. Enhanced network visibility and performance monitoring
3. Aggregated connectivity for reliable operations
4. Efficient support for legacy and non-compliant devices
5. Gain overlay features to boost security and flexibility

SD-WAN actively enhances zero-trust by providing granular access control and secure, sustainable connectivity through encrypted tunnels, ensuring that users access only the necessary resources. By partnering with a trusted advisor like Coevolve, enterprises gain expert guidance and tailored solutions, ensuring that SD-WAN and zero-trust architectures are seamlessly integrated, optimized for current demands, and prepared to adapt to future challenges, providing a robust and sustainable approach to network security.

Redesigning network security with a ZTA approach

While IT leaders want to believe that zero-trust is the antidote to their security challenges, there is a disconnect between what leaders want ZTNA to do and the reality. To close the security gap, CIOs need to fully understand what zero-trust is and gain strategic guidance and help on the best path forward, which includes a comprehensive, multi-layer security approach with zero-trust and innovative cyber solutions.

The 5 step ZTNA-ready security methodology

Partners like Coevolve provide CIOs with the chance to turn zero-trust concepts into tangible realities, bridging the gap between theory and implementation. This proven, proactive security program unlocks the network security enterprises that are indispensable in today's digital world. To ensure your security transformation is successful, Coevolve acts as a trusted advisor, seamlessly integrating with your internal departments and team. They will facilitate an in-depth assessment of security vulnerabilities and goals before they tailor their effective 5-step methodology to your business. Let's explore how to get your enterprise ZTNA an-ready:

Step 1: Start with a comprehensive understanding of the cyber environment and your enterprise's current security posture

Gain a deep understanding of the existing security environment, with a focus on where the full capabilities and applications of zero-trust could deliver benefits. Ensure you also assess the security posture of your enterprise by asking:

- What are my enterprise's vulnerabilities and strengths?
- What security solutions have already been integrated, and how do they fit with zero-trust?
- How can the security culture be improved?

Step 2: Craft a comprehensive, enterprise-specific security roadmap

With Coevolve as your trusted advisor, we will jointly develop a future state network security roadmap to evaluate, plan, and adopt zero-trust principles seamlessly. Our methodology for a comprehensive roadmap to zero-trust excellence is underpinned by:

- **Adopt a human-centric approach:** Most breaches are caused or triggered by humans. CIOs must recognize the pivotal role of people in ensuring the success of implementing zero-trust.

- **Prepare for the implications of adopting a zero-trust architecture:** Many organizations lack sufficient data on access requirements for various roles or groups. Documenting the required access will make it easier to extend security inside the perimeter.

- **AI deployment in key areas only:** Utilize AI as a complementary tool within the zero-trust framework to enhance security measures and adapt to evolving threats.

Step 3: Develop customized hybrid solutions

Deploy tailored integrated solutions that leverage technologies like SD-WAN to optimize security and network performance and ensure these three actions are included:

- **Focus on a vendor-agnostic framework, avoiding technology lock-in:** To ensure your enterprise is not dependent on any one vendor or solution, consider using a vendor-neutral SASE framework for flexible network security.
- **Use the co-managed model to augment internal skill sets:** Simplify security management by selectively outsourcing or out-tasking with a co-managed model.
- **Ensure cloud-first strategies are adopted:** Review and deploy cloud-first strategies and modern remote access solutions for hybrid work models to improve user experience.

Step 4: Build comprehensive incident response plans

Ensure business resilience by strengthening security with zero-trust principles and a comprehensive incident response plan for advanced threat detection and mitigation. We advise in this stage of the planning:

- **Zero-Trust integration:** Introduce this paradigm only with a tailored approach with applications specific to meeting business requirements.
- **Advanced Incident Response:** Proactively minimize downtime, enhancing overall security and resilience against cyber threats with a comprehensive incident response plan.
- **Leverage external expertise:** Specialist partners like Coevolve can help CIOs access industry experts and advanced vendor tools to mitigate the most complex threats.

Step 5: Adapt to the changing needs of the business

In terms of business continuity, the IT infrastructure landscape must adapt to changes in the internal business environment, such as mergers, acquisitions, and segmented environments, while also accounting for external influences. We recommend:

- **Ongoing dynamic training and continuous improvement:** Empower employees with thorough, dynamic compliance and cybersecurity training.
- **Evaluations of security strategies:** Ensure that these steps are taken to tighten security policies - identify risk, tighten policies, and optimize solutions.
- **Correlate data from multiple sources:** Network security doesn't happen in isolation. There can be real value in the insights that come from collecting and correlating data from other relevant sources, including endpoint detection and response (EDR) systems, mobile device management (MDM) platforms, and application security products.

In conclusion

Implementing zero-trust without a strong understanding of the paradigm or explicit knowledge of your enterprise's vulnerabilities is like setting out on a cross-country road trip without GPS. A planned route is compulsory; otherwise, enterprises risk getting lost, wasting time and money, and ending up in the wrong destination, ultimately leading to an inefficient zero-trust implementation.

It is evident that an enterprise's network security must evolve to adapt to today's cybersecurity demands. Many CIOs have already steered their teams through adopting cloud technologies, embracing hybrid remote-work environments, and expanding mobile access to business applications. However, these changes necessitate the adoption of innovative solutions to support and safeguard the modern workplace.

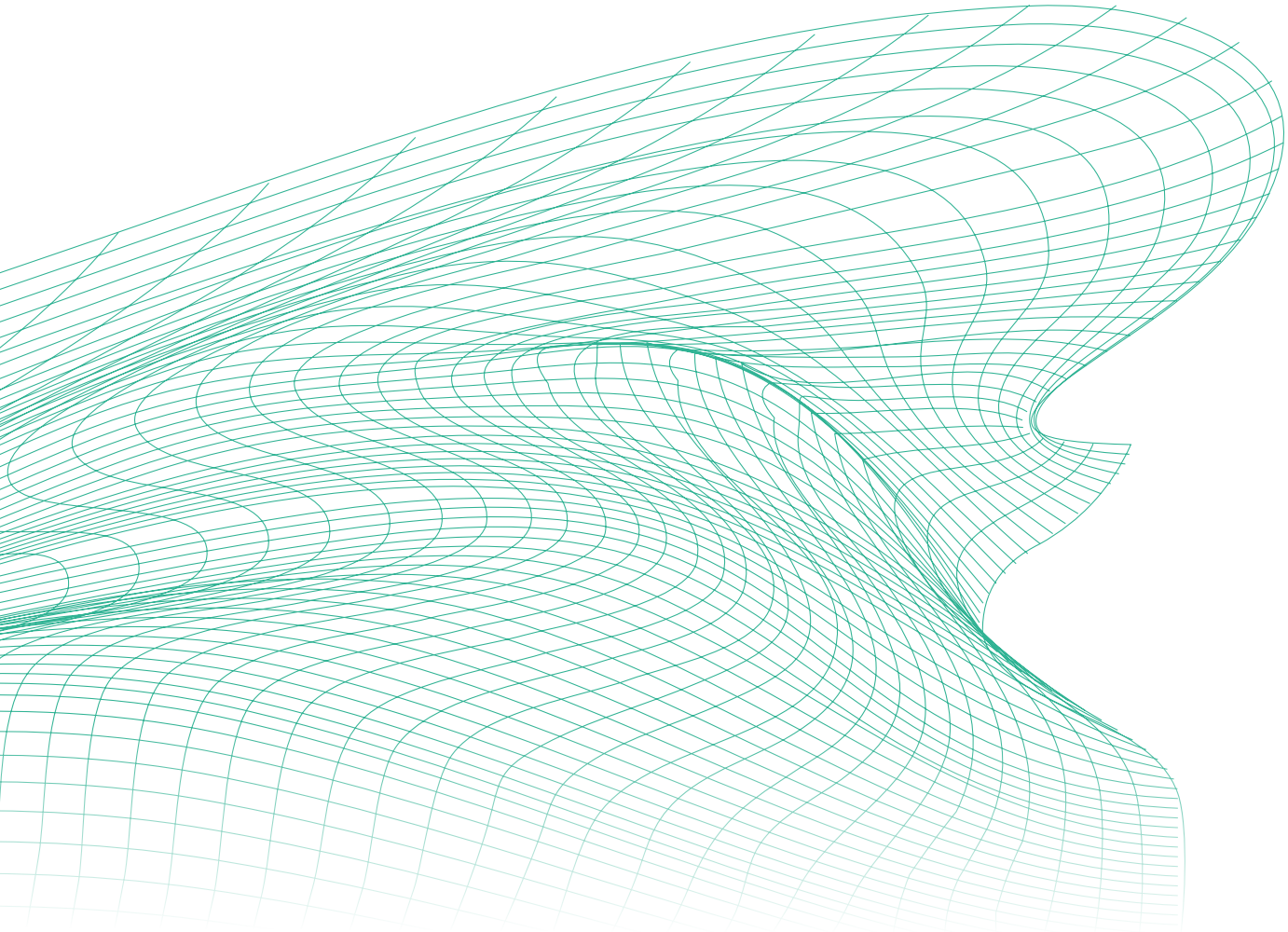
As cyber threats adapt and change, CIOs must navigate intricate webs of vulnerabilities within their networks. A comprehensive zero-trust framework is not just beneficial, it's critical to support them along the way. CIOs armed with a comprehensive zero-trust integration plan will ensure their business has elevated cyber defenses by continuously validating every user and device, thereby mitigating risks and enhancing protection across the digital landscape.

As the noise around zero-trust amplifies, partnering with a trusted advisor, such as Coevolve, helps you focus on what matters, enabling you to streamline your network security transformation. They can guide you through zero-trust complexities, ensuring your business is secure against threats while maintaining budget and delivering ROI on security updates. CIOs must act swiftly to future-proof their networks by embracing the zero-trust model, and with Coevolve's expertise, the barrier to entry for zero trust is removed. CIOs can begin to implement customized strategies to ensure they have achieved the fortified network security they require to create a strong defense against threat actors.

About us

At Coevolve, we understand that there is no one-size-fits-all solution to cybersecurity. To address the current challenges within the cyber landscape today, we have developed a unique approach to zero-trust that is both consultative and iterative, tailored to meet the specific needs of each organization. Our strategy incorporates the entire network life cycle, ensuring that security measures evolve alongside your business.

Coevolve delivers an experienced, real-world approach for clients implementing a zero-trust model. As a trusted advisor, we've been part of the network security and zero-trust conversation for over a decade. We offer historical knowledge and deep insights into the network security segment, pioneering globally in the co-managed services space. Throughout this time, we've ensured quality is at the heart of everything we do, earning the trust of our partners. Contact Coevolve today to learn more, enhance your enterprise's agility, and unlock greater network security potential with tailored strategies backed by our extensive expertise.



Contact us

www.coevolve.com

Coevolve

@coevolvetech

coevolve™