Future Makers
Research Community

Zero-trust networking: Is it worth the cost?

Atos

Introduction

In the ever-evolving landscape of cybersecurity, zero-trust networking (ZTN) has emerged as a transformative approach to securing enterprise networks.

Traditional security models — which often rely on perimeter defenses and the assumption that internal network traffic is inherently trustworthy — are becoming increasingly obsolete in the face of sophisticated cyber threats and a rapidly expanding attack surface. Zero-trust networks challenge this notion by adopting a "never trust, always verify" stance, fundamentally altering how security is implemented and maintained within an enterprise.

While implementing ZTN should be considered a journey, there comes a point at which each organization can consider itself to have implemented as much technology and cultural change as is necessary.

A key challenge that most organizations face when considering a ZTN implementation is the cost associated with reaching this point, and what will be gained and lost along the way. The intention of this paper is to define these net gains and losses, as well as to provide a logical framework for thinking about ZTN and deciding if it is the right way forward for your organization.

What is zero trust?

Zero-trust networking (ZTN) is a modern security and connectivity model where no user or device is trusted by default, even if they are within the corporate network. Instead, zero trust requires continuous verification for each request to access data or systems.

Unlike other models which rely on defending the perimeter of the organization, ZTN uses the latest network security and connectivity technologies to continuously monitor and dynamically adapt security policies at a per-user/per-device level.

The ZTN model significantly enhances an organization's cybersecurity posture by limiting access to only those users who genuinely need it and delivering in-depth visibility of network activities. Such enhancements mean a reduced risk of cyber breaches and improved productivity through streamlined access.

Adoption of ZTN is accelerating because the model addresses two of the biggest concerns of the modern cybersecurity landscape: An increasingly large and dangerous threat landscape, and seamless access to corporate resources regardless of resource or user location.

Table of contents

The benefits

To begin, let's consider the gains which can be achieved. As with any paradigm shift, zero-trust networking brings a wealth of potential value if implemented correctly.

Zero trust improves the security posture, preventing cyber incidents and reducing breach costs.

- The average global cyber incident cost for a large enterprise is $4.88 million.[1]
- 70% of enterprises report significant or very significant business disruption as the result of a data breach.[1]
- The average period from a breach occurring to it being detected and contained is 250+ days, and recovery takes even longer.[1]

It enables your organization to more readily stay in compliance with regulations.

- Increasing industry and governmental legislation on cybersecurity is expensive because data and reports take time to find and generate.
- Existing compliance requirements such as GDPR, HIPAA and PCI-DSS are evolving, and new regulations are coming soon in Europe and the US.[2]
- ZTN helps control compliance costs by capturing a wealth of deep-level data, which is immediately available for compliance audits.

It reduces operational costs over the long term.

- Automation and AI are key components of ZTN technologies, enabling support activities to shift-left and reducing overall operational costs.
- ZTN enables seamless remote working, creating savings potential by downsizing office space.
- Scaling up or down is a non-issue, eliminating the costs associated with rapid increases in IT, as well as amortizing investments in hardware.

It enables improved productivity and accessibility.

- Although ZTN requires more user authentication and authorization, they can largely be hidden from view for a "single-sign-on" experience.
- ZTN's **"Anything from Anywhere"** approach gives users the same application access experience regardless of location. It requires less training, improves accessibility, and reduces time wasted switching between apps.
- ZTN provides seamless remote and blended working models, with studies showing increased productivity.[3]

[1] ibm.com/reports/data-breach
[2] cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia
[3] gallup.com/workplace/398135/advantages-challenges-hybrid-work.aspx

The challenges

Despite all its advantages, zero-trust networking has some challenges. True ZTN is a mindset change as well as a digital transformation, and one that will impact many facets of the enterprise. These impacts include:

Initial investment

Any ZTN implementation will require investment in new technologies.

Strategic planning is needed, with most organizations choosing to work with experienced technology consultants and partners to ensure they are on the right track and are getting the most value from their plan.

Transformational complexity

Whatever ZTN means to each enterprise, there is a period of transformation required, during which there will be some business disruption.

ZTN often requires integration with new and existing technologies, which come with their own IT skills challenges.

Changing operational requirements

ZTN involves continuous monitoring, policy management and updates, requiring a team of multi-skilled resources.

To make the most of the data and insight that ZTN technology provides, additional tools are often needed to optimize policies and identify issues.

Ongoing user adoption

Users will need training on how to use the new technologies and obtain support.

IT teams need to re-train and re-skill to operate ZTN's converged network and security technologies.

Mindset changes take time, and the entire enterprise will need time to embrace the "security in everything" paradigm.

Phases of investment

The costs of implementing ZTN

Of course, any significant change of this nature will have certain costs associated with it. When it comes to zero-trust networking, these costs can be broken down into three primary categories, which we have outlined below.

Technology investments

- Implementing Identity and Access Management (IAM) systems
- Expenses for deploying micro-segmentation networking technology
- Investment in endpoint detection and response (EDR) solutions
- Secure cloud environment implementation
- Costs of implementing data encryption

Operational costs

- Investment in training employees and IT staff on ZTN principles and practices
- Costs related to developing and enforcing new security policies
- Ongoing updates and maintenance of ZTN technologies

Cultural change costs

- Management costs associated with enabling a cultural shift towards a zero-trust mindset
- Potential initial loss of productivity as users adapt to new security measures

The synergies

Fortunately, there are three important areas of synergy which can be harnessed to help offset some of the challenges and costs of implementing ZTN:

1 Ability to leverage existing investments.

- While the concept of ZTN is new, some of the technologies it uses are already mature and may be in place at your organization. If this is the case, the initial investments may be lower than expected, or there's a chance to avoid some costs along the ZTN implementation journey.
- Similarly, the IT team may find that they already have some of the skills required through training on existing investments.
- Any investments which have been committed to (such as cloud migration or hybrid cloud) are complimentary to ZTN, so there's no duplication of costs or re-work required.

2 Relying on partners to help reduce the required investments.

- Zero-trust networks can be separated into modules of service and delivered in a blended approach. For example, you can keep the governance aspect in-house to maintain control, but outsource the technology management.
- Buying technology or managed services through existing providers can yield economies of scale (cheaper licenses, for example) which wouldn't be available to individual organizations.

3 Time is a gift.

- ZTN requires some big changes in the mindsets of users and IT teams. Resistance to change is normal, so using the technology implementation period to obtain user buy-in and train IT teams will improve adoption.
- Rather than bombarding users with constant change, ZTN technology can be implemented gradually, while keeping major changes to work habits unaltered.
- Rather than a greenfield approach, most organizations will choose to implement ZTN as a journey. Doing so allows time to identify synergies and adapt.

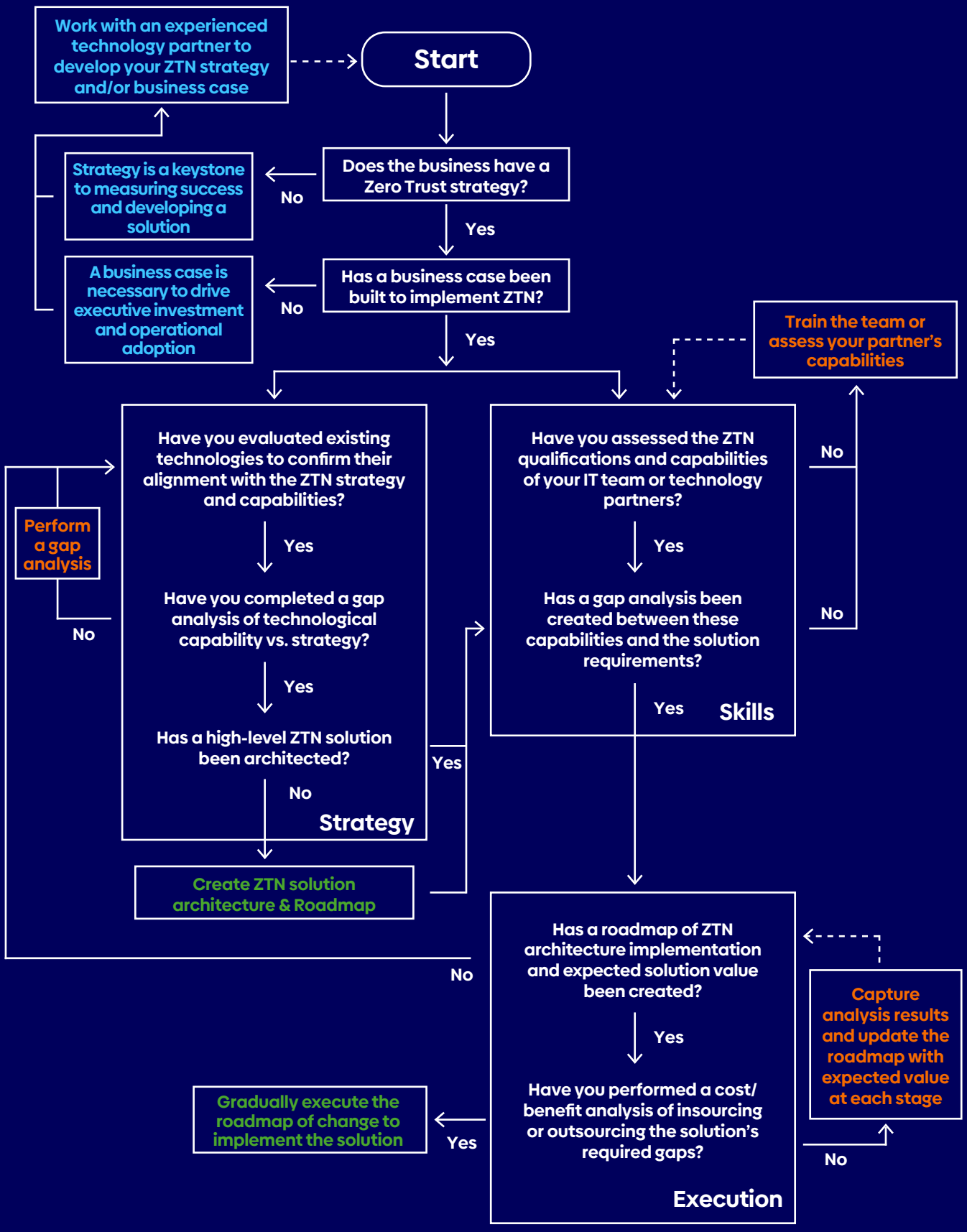
Conclusion

Implementing zero-trust technology is not just a security measure; it is a strategic investment in the future of the enterprise. By adopting ZTN, you can significantly enhance your enterprise security posture, ensure regulatory compliance, improve operational efficiency, and support business agility.

Zero-trust networks can be a worthwhile investment for many organizations, particularly those with a high risk of cyberattacks or stringent compliance requirements. While the initial and ongoing costs can be substantial, the long-term benefits in terms of enhanced security, improved compliance — and the potential cost savings from avoiding breaches — can outweigh these expenses.

Each organization should conduct a thorough cost-benefit analysis considering its specific needs, risks, and resources to determine which aspects of zero-trust networking can be adopted and which bring the most value.

Below is a representative decision model to help guide your organization's thinking on whether the investment in ZTN makes sense compared to the costs of implementation.



Of course, this model is merely intended to be a general representation of the decision-making process. The exact decisions that determine the pathway to ZTN will vary for each organization.

What is universally true, however, is that a detailed up-front analysis will accelerate time-to-value and focus your investments on delivering value rather than investing in unnecessary technologies.

Offsetting the higher operational costs through strategic partnerships and services delivered by partners means that the total costs are often outweighed by the initial and ongoing costs.

As with any major initiative, there is a give and take in terms of costs. With ZTN, many of the costs are front-loaded but if implemented correctly, they should pay off in the long run. Below, we have listed a few of the typical gains and losses for comparison.

Net Gains:	Net Losses:
Security Posture: Significant improvement in overall security posture	**Initial Investment:** Up-front costs for technology and training
Compliance: Easier and more robust compliance with regulatory requirements	**Cultural Resistance:** Potential resistance to change from employees
Operational Efficiency: Streamlined operations and reduced IT overhead	**Initial Productivity Dip:** Temporary productivity loss as users adapt to new systems
Cost Savings: Long-term savings from reduced breach costs and improved efficiency	

Despite the investments required, zero-trust networks are usually a good financial choice for large enterprises. Focus on the synergies available to the organization, and partner with trusted providers to reduce investments, deliver value sooner and maximize overall value and cost savings.

Assessing your current security posture and developing a strategic roadmap aligned with your business objectives will not only enhance operational excellence during the transition period, but also ensure cost efficiency throughout the implementation. It will also go a long way to removing future operational roadblocks, allowing continuous evolution and network improvements.

Proper planning and strategic allocation of resources are essential to achieving the desired outcomes and mitigating potential risks associated with the transition to a zero-trust model – providing additional monetary savings.

Before beginning any such project, it is essential to make the proper investments in consulting and advisory. The CIO and IT leadership must lay a strong foundation and provide an ongoing push for the implementation of ZTN to succeed.

If you need help building the case for zero trust in your organization,
you can learn more at atos.net/ztn

About Atos

Atos Group is a global leader in digital transformation with c. 72,000 employees and annual revenue of c. € 10 billion, operating in 68 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start discussion together

About the Future Makers Research Community (FMRC)

The Future Makers Research Community is a global network of our Future Makers - exponential thinkers and forward-looking technology thought leaders - across Atos.

Our Future Makers are united by profound curiosity, a strong growth mindset and a passion for shaping the future through exponential technologies applied in a deep industry context. We collaborate on thought leadership, (co)-innovation and R&D across all innovation horizons, and our ambition is to elevate organizations and drive lasting impact.

In close co-creation with our clients and partners, we deliver bold ideas and industry use cases, by anticipating trends and market needs that will reshape businesses and society.

Together, we're not just imagining the future — we're building it.

106482 - JS + GR - Zero-trust networking