axonpartnersgroup.com

Zero Trust: shifting the security architecture paradigm

July 2023

Authors

Samuel Tew
PRINCIPAL

Rafael Alés
SENIOR ASSOCIATE

AXON

As cyber threats grow in sophistication, traditional security measures are becoming inadequate.

The Zero Trust model addresses these challenges by ensuring security at every level of interaction. With its adoption becoming a global trend, governments are driving its take up. This paper explores Zero Trust, its benefits, challenges, and why government support is pivotal.

Abstract

The cybersecurity landscape has evolved with increasingly sophisticated and costly cyber threats that expose the limitations of traditional perimeter-based security measures and emphasise the need for a paradigm shift in security strategies. Zero Trust has emerged as a security framework that addresses these challenges by shifting the focus from network-centric to user-centric trust via the application of security measures at every level of interaction.

With the increase in the adoption of Zero Trust worldwide, it is evident that this security paradigm is here to stay and will continue to evolve to meet the ever-changing landscape of cybersecurity.

To drive the adoption of Zero Trust within critical sectors, governments are creating regulations and mandates for its implementation or establishing guiding frameworks for organisations to follow. This article focuses on exploring what Zero Trust is, its benefits and challenges, and explores the need for governments to help drive its adoption within government and critical infrastructure providers.

Contents

1.
Introduction

The alarming rise in the sophistication of cyber threats and attacks in the corporate cybersecurity landscape presents significant challenges for organisations and entities in safeguarding their networks and data. A key incident that emphasised the need for a paradigm shift in security strategies was the SolarWinds breach, which was plausibly one of the most damaging cyberattacks in US history. This highly sophisticated attack exposed vulnerabilities within traditional perimeter defences, highlighting the limitations of exclusive reliance on perimeter-based security measures.

The increasing adoption of digital transformation initiatives by organisations and entities has further magnified inadequacies of perimeter defences

The 'inside/outside' trust concept built into traditional defences relies on distinguishing between internal and external networks. This approach assumes that the network perimeter acts as a fortress, defending against the external threats while trusting internal users and devices. However, in today's dynamic threat landscape, attackers can infiltrate networks from both internal and external sources, rendering this concept obsolete.

At the same time, the increasing adoption of digital transformation initiatives by organisations and entities has further magnified inadequacies of perimeter defences by adding layer upon layer of attack surfaces to defend; with the proliferation of cloud services, remote work, and interconnected ecosystems, the network perimeter has therefore expanded beyond traditional boundaries.

The traditional approach to defence has become increasingly insufficient in today's dynamic threat landscape. In the case of the SolarWinds breach, these limitations were exploited to gain access to up to 18,000 of its customers, including Fortune 500 companies and several US government agencies. While the breach did not result in a complete shutdown, the affected organisations had to undertake extensive investigations, remediation efforts and implement enhanced security measures to address the breach and prevent further damage.

The lessons learned from this attack marked a turning point in how cybersecurity is considered for large organisations with heavy infrastructure, emphasising the need for a paradigm shift in organisational cybersecurity beyond traditional perimeter-based defence to something more continuous and robust.

Because of these challenges, the concept of "Zero Trust" has gained traction as a security framework that addresses the shortcomings of traditional security approaches by implementing more security checks and verifications at more stages than would have traditionally been considered necessary. This framework is now being used as a key design principle within network security architecture, and for good reason.

Recognising the urgency to enhance security measures and protect critical infrastructure, governments are increasingly considering regulations and mandates to promote the implementation of Zero Trust architectures. This article aims to provide policymakers with insights into the significance of Zero Trust as a security framework, exploring its principles, benefits and challenges.

Governments are increasingly considering regulations and mandates to promote the implementation of Zero Trust architectures

2.
What is Zero Trust?

Zero Trust is a modern security approach that challenges the traditional notion of trust within network architectures. It operates on the principle of ***never trust, always verify***, and assumes that every access request, whether from inside or outside the network, should be treated as potentially malicious.

In the past, organisations employed a castle-moat approach, whereby the network perimeter acts as a stronghold to protect valuable assets. Once crossed, trust is granted and the perimeter no longer offers this protection.

The inside/outside approach to security architecture is limited as it means that an organisation's overall protection is only ever as strong as its weakest link

Figure 1: Castle-moat security model illustration [Source: Axon, based on Cloudflare]

However, as the SolarWinds breach demonstrated, with this approach an organisation's overall protection is only as strong as its weakest link. An attacker only needs to find a way to breach the perimeter defences, i.e. compromising the castle walls, and all critical data and networks are exposed.

"Zero Trust" approach does not assume trust based on network location or user identity but instead treats every access request as potentially malicious

The "Zero Trust" approach does not assume trust based on network location or user identity but instead treats every access request as potentially malicious. This approach is aligned with the evolving cybersecurity landscape, where threats can originate from both internal and external sources. In contrast to the "castle moat" model, which grants broad privileges once a user has gained access to the network, Zero Trust, applies security measures at every level of interaction, emphasising continuous verification of user identities, assessment of device health, and consideration of contextual factors to determine access privileges within the network or application security architecture.

This shift in mindset is essential as the increasing sophistication of cyber threats and the adoption of cloud services have made the traditional perimeter-based security model inadequate for protecting sensitive data and networks. However, it is important to understand that Zero Trust is not a silver bullet for all cybersecurity challenges or a single technology, product or service that will enable companies to redefine their cybersecurity approaches and practices. At its core, Zero Trust is an identity-centric security approach that challenges traditional models by shifting the focus from network-centric to user-centric trust.

This shift in mindset behind Zero Trust is essential as the increasing sophistication of cyber threats have made the traditional perimeter-based security model inadequate for protecting sensitive data and networks

2.1. Guiding principles of Zero Trust

Zero Trust is based on a set of guiding principles that challenge traditional notions of trust and security. While "never trust, always verify" may be the most cited Zero Trust principle, the security model is also based on a broader set of guiding principles, some of which have been provided by the NIST or National Institute of Standards and Technology (SP 800-207) and the United States National Security Agency (NSA):

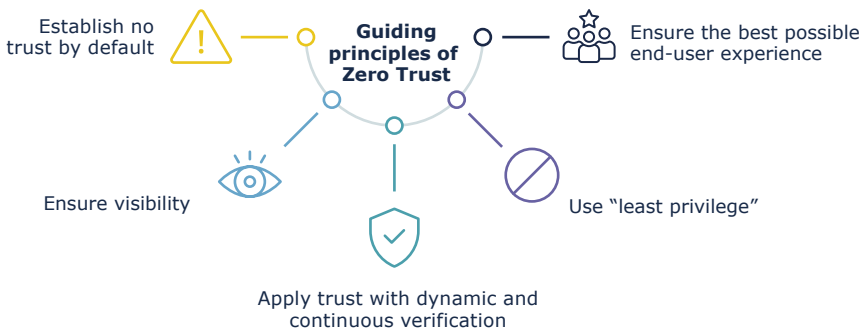

Figure 2: Guiding Principles of Zero Trust [Source: Axon, based on NIST and NSA]

- **Establish no trust by default:** In a Zero Trust model, trust is not automatically granted based on network location or user identity. Instead, all access requests, whether from inside or outside the network perimeter, are treated as potentially malicious.
- **Ensure visibility:** A critical aspect of Zero Trust is maintaining complete visibility of the network's 'protection surface'. This includes identifying and mapping critical applications, data, devices and users. By having automated and continuous visibility, organisations can effectively monitor and detect any anomalies or unauthorised access attempts.
- **Apply trust with dynamic and continuous verification:** Zero Trust emphasises continuous verification and validation of access for all users and devices to all resources. Rather than granting access based on pre-established trust, Zero Trust continuously verifies the legitimacy and authorisation of access requests in real-time. This dynamic verification ensures that only authenticated and authorised users and devices can access specific resources.
- **Use "least privilege":** Least privilege is a fundamental concept in Zero Trust. It involves granting users and devices access rights only to the resources they need according to their specific role or responsibilities. By minimising unnecessary access privileges, organisations reduce the potential attack surface and limit the impact of compromised accounts or devices.
- **Ensure the best possible end-user experience:** While security is paramount, Zero Trust recognises the importance of maintaining a positive end-user experience. Security controls should be implemented in a way that does not hinder productivity or interfere with the user workflow.

Such principles serve as guiding factors when designing a modern security system. Better positioning the architecture to address the specific threat landscape that Zero Trust is intended for in the most sensible way. The integration of such principles within a Zero-Trust network/application security architecture at the earliest stage (wherever possible) is highly advised as part of a wider secure-by-design approach to ensure that the correct measures are embedded into the design from the outset. However, transitioning to such a system may instead be required, in which case careful planning may be needed to integrate such principles while avoiding any weakening of the current security posture along the way.

Zero Trust is based on a set of guiding principles that challenges traditional notions of trust and security. Such principles serve to better position the architecture to address the specific threat landscape that Zero Trust is intended to protect

2.2
Benefits and challenges

Implementing a Zero Trust security model offers numerous benefits that contribute to improved cyber security and the protection of critical assets. However, as with any significant strategy or paradigm shift, organisations must overcome several challenges when adopting a Zero Trust security model.

Embracing Zero Trust provides organisations with clear enhancement to their security measures that minimises the attack surface and reduces the likelihood of potential breaches

First and foremost, embracing Zero Trust provides organisations with clear enhancement to their security measures that minimises the attack surface and reduce the likelihood of potential breaches. This is achieved by implementing strong access controls, segmentation and continuous verification of user identities and device health at all stages, regardless of whether they are inside or outside the network perimeter. The resulting reduced attack surface not only limits the exposure of critical assets, but also reduces the potential impact of a successful breach by systematically assuming that every entry point is potentially exploitable, and therefore applying checks, controls and monitoring mechanisms throughout the user journey.

Mobile banking is a good example of where these types of security measures are implemented. Within the banking sector, security is at the forefront. Firstly, no device is stored as trusted, which means a user must always log in, in many cases using advanced techniques such as biometrics. Even after logging in, if a user wishes to make a transaction, there are further Multi-Factor Authentication (MFA) checks to confirm the user's identity again using an SMS or other coding system. Finally, upon confirming a transaction, there are active monitoring practices to identify suspicious behaviour. Even at this stage the transaction and the entire account could be temporarily blocked until further identification and authorisation takes place, e.g., via human correspondence such as a phone call. This approach significantly reduces the potential impact of an initial breach and puts many barriers in the way of a cybercriminal achieving their goal.

Integrating such controls and processes requires serious investment in key technologies, such as micro-segmentation and identity and access management (IAM) solutions. However, such costs will at least be somewhat offset by the reduction in investment and overheads assumed by an overdependence on perimeter security appliances such as firewalls or intrusion prevention systems, and, in some cases, may lead to long-term cost reduction benefits. When we consider the reduction in future costs of potential data breaches also, there is potential for more cost savings.

Governments deploying regulation surrounding Zero Trust adoption must also be careful to align with existing or upcoming data protection laws in their territory

Zero Trust architectures also improve incident response capabilities by focusing on continuous monitoring and real-time detection of security incidents. By closely monitoring user behaviour, device health and contextual factors, organisations can quickly identify and respond to potential threats, enabling rapid mitigation and reducing the potential impact of security breaches. However, this benefit assumes a thorough understanding of an organisation's IT infrastructure and security requirements, so it is essential to establish clear policies, ensure seamless integration across different systems and platforms, and maintain ongoing monitoring efforts.

On an organisational level, implementing Zero Trust can come with another challenge, resistance to change. Employees may be reluctant to change their working habits and adopt stricter security measures, unaware of the benefits that such an "annoyance" may provide. To deal with this resistance, organisations would be wise to employ tech solutions that avoid being overly obtrusive and are easy to use to reduce the overall hindrance to productivity. In addition, organisations can also benefit from developing a security mindset within their teams at all stages of workflow, for example, by engaging employees through training or awareness programs.

A further potential challenge of Zero Trust adoption comes from a regulatory perspective. The Zero Trust model's focus on identity recognition and close monitoring of user activity means that it involves a significant amount of data handling. If personal data is involved, this can bring the model under the scope of personal data protection laws such as the General Data Protection Regulation (GDPR), particularly in regions such as the European Union (EU). Organisations implementing a Zero Trust model must therefore navigate these legal and regulatory frameworks with care, and governments deploying regulation surrounding Zero Trust adoption must also be careful to align with existing or upcoming data protection laws in their territory. Nonetheless, both governments and organisations should see this as an opportunity to improve both security and privacy practices. Zero Trust can be implemented in a way that prioritises privacy while still providing the security measures.

Governments and organisations should see Zero Trust as an opportunity to improve both security and privacy practices, implementing it in a way that prioritises privacy while still providing adequate security measures

3.
Zero Trust adoption

As briefly explained in the previous chapter, the benefits offered by Zero Trust in terms of preventing and mitigating the effects of cyber-attacks can make a positive impact on organisations, both in terms of business continuity and overall cost savings.

Cybersecurity is a costly business, especially for those who are less prepared for attacks and breaches. Referring back to the SolarWinds attack in 2020, the true cost to US organisations was staggering. Governments and Fortune 500 companies were left scrambling to assess the extent of the breach and expel the hackers from their computer networks, requiring significant resources. Some estimates put the total insured losses of the breach up to $90 million.[1]

While any such wide-scale breach will have significant economic impact, data tells us that organisations that have adopted Zero Trust have seen a significant reduction in both data breaches and their associated costs. For example, IBM's Cost of a Data Breach Report 2022 shows that organisations without Zero Trust incur an average cost of $5.1 million from a data breach, compared to an average cost of $4.15 million for those that have it.[2]

Organisations without Zero Trust incur an average cost of $5.1 million from a data breach, compared to an average cost of $4.15 million for those that have implemented Zero Trust

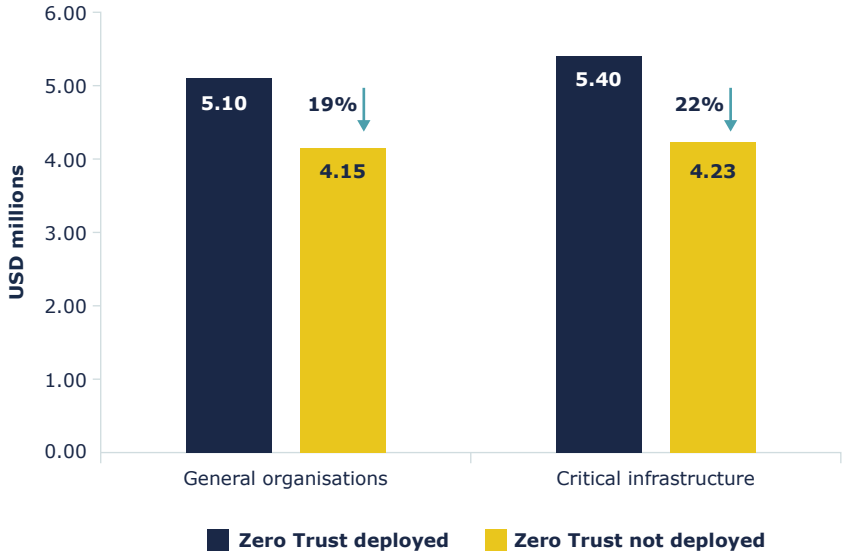

Figure 3: Impact of Zero Trust on average cost of a data breach for General and Critical Infrastructure organisations [Source: IBM's Cost of a Data Breach Report 2022[4]]

For critical infrastructure organisations, which include industries such as financial services, communications, healthcare, technology, energy or transportation, the cost of breaches is even higher

Furthermore, Zero Trust maturity is inversely correlated with breach costs. Organisations with a mature level of Zero Trust security architecture, where Zero Trust is applied consistently across all domains, experience an average breach cost of $3.45 million. At the mid-stage, where Zero Trust has been applied to many but not all areas of the organisation, the average cost of a data breach is $3.96 million. For low-maturity adopters that are just beginning to implement Zero Trust practices, the average cost of a data breach is $4.96 million, roughly $1.5 million (or 43%) more than those of mature organisations.[4]

Low maturity Zero Trust adopters that are just beginning to implement a few practices see an average cost of a data breach roughly $1.5 million (or 43%) more than those of mature adopters

Figure 4: Average cost of a data breach by zero trust maturity deployment in USD million [Source: IBM's Cost of a Data Breach Report 2022[4]]

These statistics highlight the importance of Zero Trust in reducing data breaches and associated costs. At the government level, this concept is being taken seriously. Okta's report, The State of Zero Trust Security 2022, shows that 72% of Government organisations have defined or plan to define a Zero Trust security initiative, compared to 55% of private organisations globally.[3]

72% of Government organisations have defined or plan to define a Zero Trust security initiative, compared to 55% of private organisations globally

1 Bitsight and Kovrr, "The Financial Impact of SolarWinds Breach"; Available at: https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided

2 IBM, "Cost of a data breach 2022"; Available at: https://www.ibm.com/reports/data-breach

3 OKTA, "The State of Zero Trust Security 2022"; Available at: https://www.okta.com/resources/whitepaper-the-state-of-zero-trust-security-2022/

4 Gartner, Press release; Available at: https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026

However, private organisations are lagging behind public agencies. For example, Gartner estimates that less than 1% had a mature and measurable Zero Trust program in place as of 2022, and further predicts that this will reach just 10% by 2026. But perhaps more concerning is the rate at which the critical infrastructure provider segment is adopting Zero Trust. IBM indicates, 79% of critical infrastructure providers have not implemented a Zero Trust architecture, showing a lower prevalence of Zero Trust security approaches compared to the global average.[4]

79% of critical infrastructure providers have not implemented a Zero Trust architecture

In response to this, governments have begun to issue mandates and guidance to accelerate this process. For example, in May 2021 the US government issued an executive order.[5] The order mandated that all US federal agencies must adhere to NIST Special Publication 800-207, the US government's Zero Trust Architecture (ZTA) guideline, with an implementation plan for full adoption by the end of 2024. This ambitious three-year implementation timeframe shows the urgency with which the US government perceived the required shift in approach to federal security and serves as a strong commitment to strengthen cybersecurity defences and address the cybersecurity threats at the government level. Since then, the NIST 800-207 standard has become the de facto reference for organisations looking to build their own Zero Trust systems.

Mandates and guidance, such as guidelines, frameworks, and executive orders, have contributed to higher rates of Zero Trust adoption in government organisations

The UK has also taken a proactive stance on Zero Trust by publishing a set of eight design principles for Zero Trust architectures as part of the National Cyber Security Centre's guidance.[6] Similarly, other countries such as Canada have recognised the importance of Zero Trust as a model for addressing modern security challenges and are providing information and guidance to organisations.[7]

With government organisations at the forefront of adopting Zero Trust initiatives mandates and guidance documents, such as those mentioned above, have contributed to higher rates of Zero Trust.

5 White House (USA), "Memorandum for The Heads of Executive Departments and Agencies"; Available at: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

6 National Cyber Security Centre, "Zero Trust Architecture Design Principles"; Available at: https://www.ncsc.gov.uk/collection/zero-trust-architecture

7 Government of Canada, "Zero Trust Security Model"; Available at: https://www.cyber.gc.ca/en/guidance/zero-trust-security-model-itsap10008

4.
Conclusion

The cyber security landscape has evolved because of an alarming increase in the sophistication of cyber threats and attacks, posing significant challenges to organisations and entities in protecting their networks and data. These attacks have exposed vulnerabilities within traditional perimeter defences, highlighting the limitations of relying solely on perimeter-based security measures and emphasising the need for a paradigm shift in security strategies.

Zero Trust has emerged as a security framework that addresses these challenges by shifting the focus from network-centric to user-centric trust by applying security measures at every level of interaction. Zero Trust is critical for organisations looking to improve their defences against cyber threats, reduce data breaches and limit their potential impact and cost. While there are challenges to adopting Zero Trust, the benefits far outweigh the risks.

This is especially important for critical infrastructure organisations, which hold strategic significance for governments and incur higher costs associated with data breaches compared to other sectors. Despite this, Zero Trust adoption is lower among critical infrastructure organisations, which indicates a need for action in these sectors by governments.

This calls for government-led action to drive critical infrastructure providers and large enterprises towards acting on their approach to security architecture. Governments can play a key role in this by exploring the support or mandate they can give to entities either through guidance or regulation.

About
Axon Consulting

Axon is an international firm founded in 2006 that provides investment and advisory services to a broad client base in the ICT and digital space in more than 70 countries across the world.

Axon's cybersecurity practice is central to its business and an increasingly important service area for clients. Its work in this field includes strategy, policy/regulation, and research at the business and governmental level. Axon works closely with national representatives to help them understand their cybersecurity needs and to define actionable recommendations aimed at improving their cybersecurity ecosystems.

Tel: +34 913 102 894
Email: marketing@axonpartnersgroup.com

AxonPG
axon-partners-group