

The Zero Trust Architecture: A critical analysis of its principles, implementation challenges, and efficacy compared to traditional models.

Jacob Moseley
BSc Software Engineering
University of Wales Trinity Saint David
Swansea, United Kingdom
2317034@student.uwtsd.ac.uk

Abstract – With a shift towards cloud computing, remote work and distributed systems, traditional perimeter-based network security models no longer serve as comprehensive safeguards against cyber threats. The Zero Trust Architecture (ZTA) addresses these limitations by enforcing continuous authentication, least privilege access and the constant monitoring of all traffic within a network.

This paper aims to critically examine the core principles that make up the ZTA, the technologies it is made up of, challenges within its implementation. It further evaluates Zero Trusts efficacy against traditional models demonstrating its suitability within modern hybrid environments.

I. INTRODUCTION

In an increasingly complex digital environment characterised by cloud computing, remote work, interconnected systems have enabled modern organisations to be both more productive than ever before. While these developments work in favour of organisations, they also significantly increase the number of threats faced. Traditional security models that rely on implicit trust once a user or device is within a network are proving to be increasingly inadequate when faced with modern cyber threats. As systems continue to become more distributed, the assumption of a clearly defined and secure internal network can no longer be sustained.

In response to the limitations of legacy security architectures, the Zero Trust Architecture has emerged as a strategic approach that challenges implicit trust through policies, authentication, and the monitoring of network activity [1]. By treating every access request to an organization's network as potentially malicious, Zero Trust adopts a proactive approach to cyber security.

This paper aims to critically analyse the core principles of the Zero Trust Architecture, examining the technologies and challenges associated with its implementation, while also evaluating its effectiveness when compared to traditional security models.

II. TRADITIONAL SECURITY MODELS

Traditional security architectures have historically relied on clearly defined network boundaries and implicit trust. To provide context on the emergence of the Zero Trust Architecture, this section aims to examine these legacy security architectures, their approach to enforcing trust and their limitations within modern hybrid environments.

A. Trusted and Untrusted Network Boundaries

Traditional network focused security models are built upon the separation of trusted internal networks and untrusted external networks. This approach assumes that users, devices, and systems operating within the internal boundary of a

network can be trusted upon the completion of their initial authentication, with security primarily enforced at the perimeter of this boundary [2]. This typically means internal traffic is subject to fewer security checks, allowing for communication with minimal restrictions.

While this model was effective within older, centralized computing environments, it relies on the assumption that threats originate from outside an organisation's network. In modern environments where users, devices and applications operate across cloud platforms from remote locations, the distinction between trusted and untrusted networks can become harder to differentiate, reducing the effectiveness of a boundary-based approach to cyber security [3].

B. Firewalls, VPNs, and Perimeter Enforcement

Firewalls and Virtual Private Networks (VPN) are two common mechanisms used to enforce trust at a network's perimeter. Firewalls use a combination of hardware and software that both filters and prevents information from moving between trusted and untrusted networks through the use of policies. A VPN acts as a secure connection between systems that uses data communication capability of an unsecured and public network. Once authenticated, VPN users are often granted access comparable to that of being on site, extending trust outside the established network boundary [4].

This implicit trust within a network can be dangerous. If a trusted user's credentials were to be compromised, attackers may gain an opening into an organisations internal network. As a result, reliance on firewalls and VPNs alone are shown to be inadequate within cloud-based environments [5].

C. Limitations in Hybrid Environments

Hybrid environments introduce significant complexity by allowing users and applications to access organisational resources from multiple locations and devices, reducing the effectiveness of implicit trust. Reliance on perimeter-based controls can lead to inconsistent enforcement of security policies across these distributed environments, leaving networks exposed to internal threats such as credential misuse [6].

III. CORE PRINCIPLES OF THE ZERO TRUST ARCHITECTURE

This section aims to outline the core principles of the Zero Trust Architecture, explaining how they address the limitations of traditional network-centric security models within modern distributed environments.

A. Never Trust, Always Verify

The Zero Trust Architecture is a cyber security strategy built upon the principle of never trust, always verify. Rather than granting trust based on location or initial authentication, Zero Trust requires all access requests to be treated as potentially hostile. This approach directly challenges traditional perimeter-based security architectures where implicit trust is granted once a user or device is within a network's boundary. As a result, security within a network becomes dynamic, aligning more effectively with distributed, modern environments where a network's perimeter is harder to distinguish [7].

B. Least Privilege Access

Least privilege access is an information security principle that aims to reduce the attack surface within a network and minimise the impact of a potential security breach. This is achieved by limiting both users and applications to only the data and operations required to perform their roles [8].

Over-privileged access control policies can leave networks vulnerable to insider threats, accidental misuse and compromised credentials, while under-privileged access controls may prevent users from performing their duties effectively. As a result, organisations must strike a balance between reducing risk and maintaining operational efficiency [9].

C. Assume Breach

The assume breach principle challenges traditional security architectures that treat internal network traffic as inherently secure. Within a Zero Trust model, it is assumed that a network is already compromised, and security measures are designed with this assumption in mind [10].

This approach shifts focus from solely preventing breaches to limiting their potential impact. By prioritising detection, containment, and response, the assume breach principle improves an organisation's ability to manage security incidents within modern distributed environments.

D. Continuous Authentication and Monitoring

Continuous authentication and monitoring of an organisation's network are key to the Zero Trust Architecture. Rather than relying on one-time authentication, Zero Trust enforces continuous verification for all platforms seeking access to a network's resources, including users, devices, and applications. Controls such as multi-factor authentication, device health checks and user behaviour analytics can all be used to evaluate access requests [11].

This continuous monitoring of distributed environments helps to improve the visibility of potential threat actors in real time. With this dynamic approach to network security, organisations can respond effectively to threats, mitigating the risk of prolonged unauthorised access to a distributed network.

IV. TECHNOLOGIES ENABLING ZERO TRUST

A successful implementation of the Zero Trust Architecture relies on a combination of continuous verification, ongoing monitoring, and least privilege access. Together, these technologies support the enforcement of security decisions through the assessment of risk, identity, and context. This section examines how these technologies collectively support Zero Trust principles within modern organisations.

A. Identity and Access Management

Identity and Access Management (IAM) forms the foundation of the Zero Trust Architecture by centralising the management of digital identities and access permissions. IAM systems control how users and applications authenticate, which resources they are permitted to access, and the conditions under which access is granted. Within a Zero Trust model, identity becomes the primary security perimeter, replacing traditional reliance on network location [12].

By enforcing consistent identity verification across all platforms associated with an organisation, including cloud services, on-site systems, and third-party platforms, IAM supports the principle of least privilege access. This reduces the risk associated with over-privileged access controls and compromised credentials, which is particularly important in hybrid and distributed working environments [13].

B. Multi-factor Authentication

Multi-factor authentication (MFA) enhances identity verification by requiring users to present multiple independent authentication factors before granting access. These factors commonly include something a user knows, such as a password; something they possess, such as a mobile device; and, in some cases, a biometric characteristic [14]. This multi-layered approach mitigates the risks associated with compromised credentials.

Traditional authentication methods that rely on passwords alone are particularly vulnerable to phishing attacks. By contrast, MFA significantly increases the difficulty for attackers attempting to gain unauthorised access, as possession of a password alone is insufficient [15]. When combined with contextual information, such as a device's location, MFA supports continuous verification and monitoring within a Zero Trust security model.

C. Zero Trust Network Access vs VPN

Zero Trust Network Access (ZTNA) has emerged as a response to the challenges associated with traditional VPN-based remote access. VPNs provide users with access to an organisation's internal network upon initial authentication, extending an organisation's network perimeter. This model increases the risk associated with compromised credentials by granting broad network-level access.

In contrast, ZTNA enforces access at the application level rather than the network level, providing users with access only to the specific resources they are authorised to use. Access decisions are based on the identity and the context of each request, such as device location. By minimising implicit trust and limiting the scope of access, ZTNA aligns closely with the principles of the Zero Trust Architecture [16].

D. Endpoint Detection and Response

Endpoint Detection and Response (EDR) refers to the continuous monitoring of endpoints, the many physical devices that may be connected to an organisation's network. Examples of such devices include mobile phones, laptops, and virtual machines. In hybrid environments, these endpoints can expand the attack surface available to threat actors. To combat this, EDR solutions log the behaviour of these endpoints at all times, this data is then analysed to reveal any potential threats [17].

Within the Zero Trust Architecture, EDR supports the principle of assume breach through the continuous monitoring of endpoint activity regardless of location. This capability remains significantly important in distributed environments

where users and systems may operate outside of a traditional network boundary.

E. Security Information and Event Management

Security Information and Event Management (SIEM) systems provide real-time analysis of security events within an organisation's network [18]. Key components of SIEM include log management, anomaly detection, event correlation and incident response [19].

Within a Zero Trust model, SIEM supports the principles of assume breach, and continuous authentication and monitoring by providing centralised monitoring of security events. When combined with automated response mechanisms, SIEM systems can reduce response times and limit the potential impact of security incidents, particularly in modern hybrid environments.

V. IMPLEMENTATION CHALLENGES AND LIMITATIONS

While the Zero Trust Architecture offers clear benefits when compared to traditional cyber security models, it also presents a range of challenges within its own implementation. This section of the report aims to examine the key limitations associated with shifting to the ZTA, including integrational complexity, poor adoption, and financial impact.

A. Financial Challenges

The cost associated with implementing the Zero Trust Architecture can pose as a significant challenge to modern organisations. Organisations can expect to expend significant resources in areas such as enabling the monitoring of endpoints, data encryption, employing skilled workers, and staff training. Upon implementation, organisations can also expect ongoing operational expenses related to maintaining ZTA infrastructure [20].

As a result of the financial cost associated with Zero Trust, organisations must be careful to balance its security benefits with the resource availability of their business. Without clear guidance and long term planning, there is a risk that ZTA may be implemented in a fragmented manner, reducing its overall effectiveness.

B. Legacy System Integration

Integrating the Zero Trust Architecture into pre-established legacy systems represents a significant challenge for many organisations. Traditional network security typically uses a perimeter-based approach, where activity within this boundary is implicitly trusted, conflicting with the principles of Zero Trust. As a result, organisations may have to expend resources on areas such as bringing proprietary data formats up to date, identifying endpoints and removing implicit trust [21].

During the transition to ZTA, organisations may also experience disruptions to ongoing operations, ranging from affecting employee's ability to work to disrupting users accessing an organisation's service. In order to avoid these disruptions, organisations can implement a gradual roll out of ZTA standards, lowering the impact on organisational operations [21].

C. Risk of Superficial Adoption

When transitioning from legacy models to the Zero Trust Architecture, there is a risk of superficial adoption. This migration involves a multi-stage transformation of a network's

architecture, if organisations don't fully address underlying implicit trust, gaps within a network's security may persist [21].

This partial implementation can lead to organisations developing a false sense of security, when in reality, only select practices have been deployed. As a consequence, without a comprehensive approach to migration, the benefits of Zero Trust may be significantly diminished, leaving opportunities for threat actors to exploit remaining weaknesses within an organisation's network.

VI. EFFICACY COMPARED TO TRADITIONAL SECURITY MODELS

When compared to traditional perimeter based security models, the Zero Trust Architecture offers several advantages when addressing modern threats to cyber security. Traditional models operated within a clearly defined network boundary, providing implicit trust upon initial authentication of devices, systems, and applications. While this was effective within legacy environments, it is not an adequate solution in modern distributed environments.

With the introduction of cloud services, remote work and third party integration, Zero Trust has emerged as an answer to the challenges associated with legacy models. Instead of using tools such as VPNs and firewalls to protect and expand a networks perimeter, ZTA enforces continuous authentication, least privilege access and assumes a breach at all times. This approach enhances the visibility, allowing threats to be detected earlier and mitigating damage.

Despite these advantages, Zero Trust is not without trade-offs. Its effectiveness relies heavily on consistent investment and implementation, with superficial implementation hindering its efficacy. However, when implemented well, ZTA offers a much more robust solution cyber security within modern hybrid environments.

VII. CONCLUSION

In conclusion, this paper has critically examined the Zero Trust Architecture as a response to legacy network security models within modern distributed environments. By analysing its core principles and technologies, the report has demonstrated how Zero Trust enhances threat visibility, mitigates risks such as phishing and credential compromise, and reduces reliance on implicit trust.

The discussion of implementation challenges, including legacy system integration and financial barriers, highlights that adopting Zero Trust is neither simple nor cost-free. These challenges emphasise the need for careful planning and commitment when transitioning to a Zero Trust model.

Overall, Zero Trust introduces significant complexity within organisational networks but offers a more robust and adaptive security framework when compared to traditional approaches. Its effectiveness ultimately depends on the comprehensiveness of its implementation and the sustainment of ongoing investment.

VIII. REFERENCES

- [1] K. Olson and E. Keller, "Federating trust," Aug. 2021, doi: <https://doi.org/10.1145/3472716.3472865> (Accessed Dec. 31)
- [2] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wireless Communications and Mobile Computing*,

- vol. 2022, no. 1, pp. 1–13, Jun. 2022, doi: <https://doi.org/10.1155/2022/6476274> (Accessed Dec. 31)
- [3] T. N. Nisha, D. Pramod, and R. Singh, “Zero trust security model: Defining new boundaries to organizational network,” Aug. 2023, doi: <https://doi.org/10.1145/3607947.3608067> (Accessed Dec. 31)
- [4] C. Campbell, “*Security Technology: Access Controls, Firewalls and VPNs*,” Lecture 6, University of Wales Trinity Saint David, Swansea, UK, Aug. 2025 (Accessed Dec. 31)
- [5] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, “Theory and Application of Zero Trust Security: A Brief Survey,” *Entropy*, vol. 25, no. 12, Dec. 2023, doi: <https://doi.org/10.3390/e25121595> (Accessed Dec. 31)
- [6] M. Ayedh, A. W. A. Wahab, and M. Y. I. Idris, “Enhanced Adaptable and Distributed Access Control Decision Making Model Based on Machine Learning for Policy Conflict Resolution in BYOD Environment,” *Appl. Sci.*, vol. 13, no. 12, Art. no. 7102, Jun. 2023, doi: <https://doi.org/10.3390/app13127102> (Accessed Dec. 31)
- [7] Microsoft, “Zero Trust implementation guidance,” *learn.microsoft.com*, Apr. 12, 2024. <https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview> (Accessed Jan. 1)
- [8] Microsoft, “Increase application security with the principle of least privilege - Microsoft identity platform,” *learn.microsoft.com*, Oct. 23, 2023. <https://learn.microsoft.com/en-us/entra/identity-platform/secure-least-privileged-access> (Accessed Jan. 1)
- [9] M. W. Sanders and C. Yue, “Mining least privilege attribute based access control policies,” *Proceedings of the 35th Annual Computer Security Applications Conference*, Dec. 2019, doi: <https://doi.org/10.1145/3359789.3359805> (Accessed Jan. 1)
- [10] N. Nahar, K. Andersson, Olov Schelén, and Saguna Saguna, “A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks,” *IEEE Access*, vol. 12, pp. 94753–94764, Jan. 2024, doi: <https://doi.org/10.1109/access.2024.3425350> (Accessed Jan. 1)
- [11] S. Ghasemshirazi, G. Shirvani, and M. Alipour, “Zero Trust: Applications, Challenges, and Opportunities.” Available: <https://arxiv.org/pdf/2309.03582> (Accessed Jan. 2)
- [12] Microsoft, “What is Identity Access Management (IAM)? | Microsoft Security,” *www.microsoft.com*. <https://www.microsoft.com/en-gb/security/business/security-101/what-is-identity-access-management-iam> (Accessed Jan. 2)
- [13] A. Sharma, S. Sharma, and M. Dave, “Identity and access management- a comprehensive study,” *IEEE Xplore*, Oct. 01, 2015. <https://ieeexplore.ieee.org/abstract/document/7380701/> (Accessed Jan. 2)
- [14] NCSC, “Recommended types of MFA,” *Ncsc.gov.uk*, 2024. <https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/recommended-types-of-mfa> (Accessed Jan. 2)
- [15] NCSC, “Why MFA matters,” *Ncsc.gov.uk*, 2024. <https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/why-mfa-matters> (Accessed Jan. 2)
- [16] V. Mavroudis, “Zero-Trust Network Access (ZTNA).” Available: <https://arxiv.org/pdf/2410.20611> (Accessed Jan. 2)
- [17] Microsoft, “What Is EDR? Endpoint Detection and Response | Microsoft Security,” *www.microsoft.com*, 2025. <https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response> (Accessed Jan. 3)
- [18] G. G. Granadillo, S. G. Zarzosa, and R. Diaz, “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures,” *Sensors*, vol. 21, no. 14, p. 4759, Jul. 2021, doi: <https://doi.org/10.3390/s21144759> (Accessed Jan. 3)
- [19] Microsoft, “What is SIEM? | Microsoft Security,” *www.microsoft.com*, 2024. <https://www.microsoft.com/en-gb/security/business/security-101/what-is-siem> (Accessed Jan. 3)
- [20] Z. Adahman, A. W. Malik, and Z. Anwar, “An analysis of zero-trust architecture and its cost-effectiveness for organizational security,” *Computers & Security*, vol. 122, Sep. 2022, doi: <https://doi.org/10.1016/j.cose.2022.102911> (Accessed Jan. 3)
- [21] S. Teerakanok, T. Uehara, and A. Inomata, “Migrating to Zero Trust Architecture: Reviews and Challenges,” *Security and Communication Networks*, vol. 2021, pp. 1–10, May 2021, doi: <https://doi.org/10.1155/2021/9947347> (Accessed Jan. 3)

Case Scenario: Designing a Zero-Trust-Aligned Security Programme for ResilientIntellect Ltd.

Jacob Moseley
BSc Software Engineering
University of Wales Trinity Saint David
Swansea, United Kingdom
2317034@student.uwtsd.ac.uk

Abstract – This report proposes a Zero Trust Aligned security program for ResilientIntellect Ltd (RI), a threat intelligence organisation specialising in the production of AI-powered threat analysis software. RI employs a fully hybrid workforce that relies heavily on third party services and cloud platforms. The design of the proposed security programme aims to implement fine-tuned access control features, continuous monitoring, relevant policies as RI expands into the European Union (EU). The implementation of these features aligns closely with the Zero Trust Architecture (ZTA), a cyber security model that aims to eliminate implicit trust. This is further supported through compliance with local regulations such as the Digital Operational Resilience Act (DORA) and the Network and Information Systems 2 (NIS2) Directive.

I. INTRODUCTION

The expansion of an organisation's operations into highly regulated and distributed environments can pose as a significant challenge. ResilientIntellect Ltd is a fast growing threat intelligence and consultancy company, developing its own AI-powered threat analysis software while employing a fully hybrid workforce. As the organisation plans to expand into the EU, it must comply with current regulations according to both DORA and NIS2.

Due to the nature of RI's operations, they stand as a valuable target to threat actors, leaving the protection of sensitive AI training data and client information of the highest priority. Furthermore, the reliance on cloud platforms, remote access, and Software as a Service (SaaS) applications significantly expands their attack surface. Taking this into account, the implementation of traditional security models can be considered inadequate.

This report aims to present a comprehensive design of a Zero Trust security model tailored to RI's requirements. By building upon research findings from Task 1, the proposed design adopts a strategic implementation of policy, risk management and security controls while supporting regulatory requirements.

II. CONTEXT, DRIVERS, AND SCOPE

The design of an effective Zero Trust information security architecture must be aligned with both the regulations enforced by local governance and the needs of RI. The organisations expansion into the EU introduces new compliance requirements while increasing exposure to threats associated with distributed networks.

This section aims to examine the key regulatory and security drivers of RI's network, using its findings to further assess the scope and complexity of the required network security solution.

A. Regulatory Drivers

RI's expansion into the EU introduces new regulatory obligations that directly affect the design of a proposed solution. The two key frameworks that shape these policies are:

1) *Digital Operational Resilience Act*: DORA requires organisations follow stringent guidelines regarding the safeguarding against Information and Communication Technology (ICT) incidents. These requirements include risk management; the reporting and sharing of incidents with relevant authorities; resilience testing and the management of third party risk [1]. Together, these requirements expand RI's responsibilities regarding network security, and align with the adoption of ZTA.

2) *Network and Information Systems 2 Directive*: The NIS2 Directive is an established legal framework that aims to uphold cyber security across the EU. Policies enforced place a heavy emphasis on supply chain security, vulnerability management and cyber security education and awareness [2]. These requirements are particularly relevant to RI due to its reliance on cloud services, SaaS, and a hybrid workforce. Mandating security controls consistent with ZTA, NIS2 supports the continuous enforcement of security policies, ensuring the resilience of critical infrastructure [3].

B. Security Drivers

Other than regulatory obligations, RI faces several security drivers. As a threat intelligence organisation developing AI-powered threat analysis software, the protection of intellectual property (IP) relating to AI training data, legacy models, and source code is of high importance. The organisation's reliance on cloud infrastructure and third-party services introduces significant risk, particularly from supply chain attacks, insider threats, and misconfiguration [4]. These risks are amplified within networks that contain poorly configured access controls and superficial authentication and monitoring.

In parallel, a fully hybrid workforce increases the attack surface of RI's network, raising the risk of compromised credentials and unauthorised access. This distributed environment also increases the risk of phishing, one of the most common forms of cyber-attacks [5]. This signifies the need for a security solution that removes implicit trust, enforces least privilege access, and enables continuous monitoring of user and system activity, which are key pillars of Zero Trust.

C. Aim and Scope

The goal of the proposed security programme is to design a Zero Trust-aligned approach that allows RI to operate securely within a distributed, hybrid environment while complying with EU standards established by both DORA and NIS2. This approach aims to enhance RI's ability to detect, respond to, and recover from cyber threats, while protecting critical resources such as their IP and user information.

By focusing on governance and security controls, this design aims to adopt a forward-thinking approach to network security. Furthermore, the implementation of access controls, increased resilience to threats, and active monitoring across RI's network

aims to reduce potential reliance on implicit trust and improve the organisation's overall security posture.

III. DESIGN ASSUMPTIONS AND THREATS

The proposed design for the security programme is based on a set of assumptions that relating to RI's threats exposure. Within a distributed environment, phishing attacks and credential compromise pose a significant risk to operations. In addition to external threats, intentional and unintentional insider threats are also taken into consideration. The organisation's reliance on cloud platforms, third party services and SaaS further introduce exposure to potential supply chain attacks and cloud misconfiguration risks.

In order to combat these threats, policies that prioritise detection, containment, and recovery are essential to RI's security programme. Preventative measures are also considered, placing network wide monitoring, strong access authentication and least privilege access at the forefront of the proposed solution.

Together, these assumptions make up a security programme that enforces least privilege access, minimises implicit trust and supports the continuous monitoring of users, devices, and services.

IV. ZERO TRUST ARCHITECTURE OVERVIEW

This section covers the proposed Zero Trust aligned security architecture for RI. The architecture outlines how access to organisational resources is managed, with Figure 1 providing a visual representation of the proposed architecture.

A. Identity and Access Management

As shown in Figure 1, Identity and Access Management (IAM) forms the foundation of the proposed Zero Trust aligned security architecture by centralising the management of digital identities and access permissions. IAM governs how users and applications authenticate, which resources they are allowed to access, and the conditions under which they are permitted access. This aligns with the core principles of Zero Trust by using identity as a primary security parameter, reducing reliance on implicit trust [6].

Throughout RI's network, consistent identity verification via Multi Factor Authentication (MFA) is proposed across all platforms, including cloud dependencies and third party services. This supports the principle of least privilege access by ensuring systems, applications and users are only granted the permissions necessary to perform their roles. This reduces risks associated with over privileged access controls and compromised credentials, two key threats within RI's distributed network [7].

B. Access Enforcement

As illustrated in Figure 1, the implementation of access enforcement is integrated through the use of a dedicated enforcement layer. This layer dictates access to organisational resources through the use of Zero Trust Network Access (ZTNA).

Unlike traditional VPN based approaches, extending privileges outside a network's perimeter upon initial authentication, ZTNA enforces access at the application level [8]. This approach reduces the scope of threat actors that have potentially gained access to RI's network, reducing the damage in cases involving compromised credentials.

To further support this, the monitoring of endpoints such as users, devices and systems is also proposed. This allows for the

detection of malicious behaviour, improving the visibility of threat actors [9]. This approach supports the principle of assume breach within ZTA, allowing for constant monitoring of RI's distributed network.

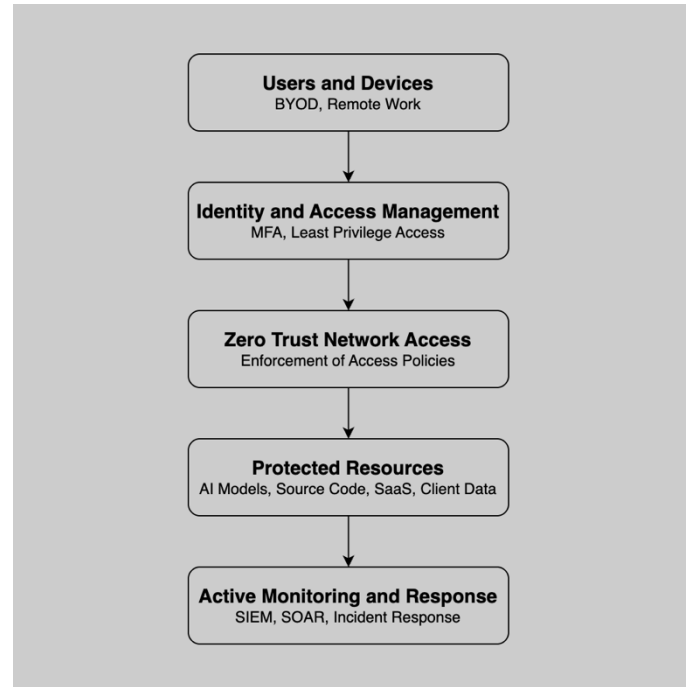
C. Security Monitoring and Response

As shown in Figure 1, continuous security monitoring and response forms the final layer of the proposed Zero Trust aligned security programme. Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) systems enable the collection of data related to security events in real time.

These systems are further supported through Security Orchestration, Automation and Response (SOAR), enabling automated incident response and recovery. Together these proposed controls improve RI's ability to detect, respond, and contain security incidents. This approach aligns closely with the ZTA principle of continuous monitoring and assume breach [10].

D. Proposed Zero Trust Architecture

This section provides a diagram presenting a top down overview of the proposed Zero Trust aligned architecture.



[Figure. 1]

V. ORGANISATION, GOVERNANCE AND POLICY

This section aims to outlines the governance approach, organisational roles, and policies underpinning the proposed Zero Trust aligned security programme.

A. Organisational Structure

To support the proposed security programme, a Cloud Security Architect should be instated. This role would involve the implementation access management via MFA, enforcing secure configurations using Cloud Security Posture Management (CSPM), and enabling continuous monitoring of and threat visibility through SIEM tools [11]. Together, this would reduce the exposure to misconfiguration and supply chain related threats.

A DevSecOps lead should also be instated. This role would entail the integration of security controls into development pipelines, the establishment of disaster recovery and response

plans, the embedment of security testing, and the implementation of monitoring tools [12].

Together, these roles would ensure that security is applied consistently throughout RI's infrastructure, reducing reliance on implicit trust while supporting the foundations of a Zero Trust Architecture.

B. Governance Model

Governance of the proposed security model is based on the NIST Cyber Security Framework (CSF) 2.0. This framework provides a structured approach through the principles of Govern (GR), Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC) [13].

Within RI, CSF aligns with both their business objectives, and their cyber security goals by prioritising the protection of IP, implementing regulatory compliance, and supporting organisational resilience. By integrating governance across these sectors, RI can maintain awareness of risks and enforce the implementation of Zero Trust aligned controls.

C. Policy Model

The proposed security programme is further supported by policies aligned with NIST CSF. Policies regarding AI usage align with ID.AM (Asset Management) and PR.AA (Access Control), defining ownership, classification and restricted access to AI models and training data. This further reduces the risk of unauthorised access to models and data leakage by enforcing strict access controls.

In addition, the implementation of a Bring Your Own Device (BYOD) policy aligns with PR.AA and GV.PO (Policies, Processes and Procedures) by defining acceptable device usage and enforcing access controls. This is particularly important within RI's hybrid workforce, where unmanaged devices may introduce credential compromise.

Finally, a proposed security monitoring and logging policy should also be considered, mandating centralised logging, real time event analysis and threat visibility across endpoints and cloud environments. This policy is further supported by DE.CM (Continuous Monitoring) [14]. The use of a continuous monitoring policy aims to enable earlier threat detection while supporting organisation resilience and reporting obligations.

VI. COMPLIANCE AND RISK MANAGEMENT

This section aims to outline the proposed security programme aligns with regional standards such as DORA and NIS2. This compliance is further supported by an assessment of key risks and mitigation strategies.

A. DORA and NIS2 Alignment

Compliance with both the DORA and NIS2 frameworks are supported through the implementation of organisational resilience, continuous response and incident detection and response into RI's proposed security programme. DORA's requirements for ICT risk management are addressed through the application of continuous monitoring of RI's network and automated threat response via SOAR and CPSM systems. The reporting and sharing of information pertaining to security incidents is also mandated by organisational policy. Together, these measures ensure compliance with DORA standards and reduce the likely hood and impact of potential breaches [1].

Compliance with NIS2 is also accounted for, with supply chain security and vulnerability management being at the forefront of RI's proposed security programme. This compliance is achieved through the implementation of IAM,

authentication within third party services and clearly defined governance and policy models. Together, these measures ensure RI's compliance with local regulations and further strengthen the proposed Zero Trust aligned security model [2].

B. Risk Management

With RI's expansion into the EU, several key threats to their network must be managed to maintain both their security and compliance with local governance. A primary concern is supply chain risks, including vulnerable cloud dependencies and poisoned AI models, where outputs are manipulate by modifying training data [15]. These risks are mitigated through the use of tools such as MFA, IAM and the continuous monitoring of third party services, reducing implicit trust and improving the visibility of potential threat actors.

In addition, cloud misconfiguration poses as a significant threat to RI's infrastructure, potentially exposing sensitive data and services. A Cloud Security Architect plays an essential role in mitigating these risks, enforcing secure configurations via CSPM systems, and enabling continuous monitoring of cloud services through the use of SIEM tools [11]. These measures allow RI to respond to supply chain threats, supporting Zero Trust while reducing the risk to ongoing operations.

VII. CONTINGENCY PLANNING

To support RI's operational resilience, a contingency and disaster recovery plan is included in the proposed security programme. A potential scenario facing RI's network is a ransomware attack, encrypting AI training data and source code repositories. In order to mitigate the related risk, recovery is supported through secure, disconnected backups, enabling recovery upon the elimination of the threat [16]. This is further supported by the continuous monitoring of the network through an implemented SIEM system, enabling early detection and containment of the attack, reducing the total data compromised.

In addition to recovery, the proposed contingency plan also supports compliance with local governance. Incidents are assessed, documented, and reported to the appropriate authorities. These reports are further supported by logs from both EDR and SIEM systems, displaying transparency with regulators. Together, these measures ensure that RI can recover and contain disasters while complying with regulations and upholding organisational resilience.

VIII. CONCLUSION

In conclusion, this report has presented a comprehensive design for a proposed Zero Trust aligned security programme for ResilientIntellect Ltd. The proposed model adopts key principles of ZTA, including fine-tuned access controls, least privilege access, and the continuous monitoring in response to risks associated with distributed, hybrid environments.

By aligning the security programme with regulatory frameworks such as DORA and NIS2, the design supports operational resilience and compliance with EU governance. Finally, the proposed security program provides RI with a forward thinking approach to network security, enhancing its ability to detect, respond and recover from cyber threats while protecting sensitive resources such as AI training data and IP within a modern hybrid environment.

IX. REFERENCES

[1] "Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554," [www.digital-operational-resilience-](https://www.digital-operational-resilience-act.europa.eu/)

act.com. <https://www.digital-operational-resilience-act.com/> (Accessed Jan. 4)

[2] European Commission, “Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe’s digital future,” *digital-strategy.ec.europa.eu*, Sep. 14, 2023. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> (Accessed Jan. 4)

[3] M. Ortmann and R. Schmitt, “Zero trust architectures for interconnected industry.” Accessed: Jan. 04, 2026. [Online]. Available: <https://www.ipt.fraunhofer.de/content/dam/ipt/en/documents/whitepaper-studies-broschures/einzelkapitel/zero-trust-architectures-for-interconnected-industry-10-24406-publica-3778.pdf> (Accessed Jan. 4)

[4] D. K. Sharam, R. Sharam, and S Peng. “Proceedings of International Conference on Next-Generation Communication and Computing,” *Google Books*, 2024. https://books.google.co.uk/books?hl=en&lr=&id=c3FrEQAAQBAJ&oi=fnd&pg=PA115&dq=how+do+ai+companies+protect+their+models&ots=KWnDibIdyK&sig=K94ZrZ-GrQ7gn8XhDxbmEVALc4&redir_esc=y#v=onepage&q=how%20do%20ai%20companies%20protect%20their%20models&f=false (Accessed Jan. 4)

[5] S. M. Zohaib, S. M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb, and Z. Muhammad, “Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work,” *Information*, vol. 15, no. 11, p. 734, Nov. 2024, doi: <https://doi.org/10.3390/info15110734> (Accessed Jan. 4)

[6] Microsoft, “What is Identity Access Management (IAM)? | Microsoft Security,” *www.microsoft.com*. <https://www.microsoft.com/en-gb/security/business/security-101/what-is-identity-access-management-iam> (Accessed Jan. 4)

[7] A. Sharma, S. Sharma, and M. Dave, “Identity and access management- a comprehensive study,” *IEEE Xplore*, Oct. 01, 2015. <https://ieeexplore.ieee.org/abstract/document/7380701/> (Accessed Jan. 4)

[8] V. Mavroudis, “Zero-Trust Network Access (ZTNA).” Available: <https://arxiv.org/pdf/2410.20611> (Accessed Jan. 2)

[9] Microsoft, “What Is EDR? Endpoint Detection and Response | Microsoft Security,” *www.microsoft.com*, 2025. <https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response> (Accessed Jan. 3)

[10] IBM, “SOAR,” *Ibm.com*, Feb. 08, 2023. <https://www.ibm.com/think/topics/security-orchestration-automation-response> (Accessed Jan. 5)

[11] EC-Council, “How to Become a Cloud Security Architect: A Complete Career Guide,” *Cybersecurity Exchange*, Feb. 07, 2025. [https://www.eccouncil.org/cybersecurity-exchange/cloud-](https://www.eccouncil.org/cybersecurity-exchange/cloud-security/how-to-become-a-cloud-security-architect-career-and-role-guide/)

[security/how-to-become-a-cloud-security-architect-career-and-role-guide/](https://www.eccouncil.org/cybersecurity-exchange/cloud-security/how-to-become-a-cloud-security-architect-career-and-role-guide/) (Accessed Jan. 5)

[12] “Lead DevSecOps Engineer,” *Alooba.com*, 2026. <https://www.alooba.com/roles/lead-devsecops-engineer/> (Accessed Jan. 5)

[13] NIST, “The NIST cybersecurity framework (CSF) 2.0,” *The NIST Cybersecurity Framework (CSF) 2.0*, vol. 2.0, no. 29, Feb. 2024, doi: <https://doi.org/10.6028/nist.cswp.29> (Accessed Jan. 5)

[14] “Policy Template Guide NIST Cybersecurity Framework: Policy Template Guide.” Available: <https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2024/08/cis-ms-isac-nist-cybersecurity-framework-policy-template-guide-2024.pdf> (Accessed Jan. 5)

[15] “What is AI data poisoning?,” *Cloudflare.com*, 2025. <https://www.cloudflare.com/learning/ai/data-poisoning/> (Accessed Jan. 5)

[16] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, “A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions,” *ACM Computing Surveys*, vol. 54, no. 11s, Feb. 2022, doi: <https://doi.org/10.1145/3514229> (Accessed Jan. 5)