

RESEARCH ARTICLE

 OPEN ACCESS | Double-Blind Peer Reviewed

Zero Trust Implementation Challenges in Financial Technology Organizations: A Systematic Review of Technical, Regulatory, and Organizational Barriers

Jamie Lee Gael¹¹ Economics & Finance Department, Creighton University, USA

*Corresponding author: Jamie Lee Gael | Email: jlgael@creighton.edu |

ARTICLE INFO

Article History

Received: 03 June 2026**Revised:** 08 July 2026**Accepted:** 03 August 2026**Published:** 19 August 2026

Keywords

Zero Trust Architecture, financial technology, cybersecurity, identity and access management, micro segmentation, regulatory compliance, NIST SP 800-207, open banking, systematic review.

How to Cite

J. L. Gael, "Zero trust implementation challenges in financial technology organizations: A systematic review of technical, regulatory, and organizational barriers," J. Appl. Technol., Intell. Comput. Syst. (JATICS), vol. 2, no. 2, pp. 26–37, 2026.

ABSTRACT

Traditional perimeter-based security model is no longer viable due to financial technology (FinTech) organizations running in hybrid cloud, open-banking application programming interfaces (APIs) and remote workforces. Zero Trust Architecture (ZTA), defined by the National Institute of Standards and Technology (NIST) in Special Publication 800-207, moves away from implicit network trust and toward continual, identity-based verification. The security advantages offered by Zero Trust are established, but their application within banks, payment processors, insurers and digital-native FinTech companies is significantly more complex than it is in most enterprise environments, thanks to legacy core banking systems, complex third-party API ecosystems, stringent and fragmented regulation, and high availability transaction needs. This paper attempts to systematically review the technical, regulatory and organizational challenges that FinTech can face when implementing Zero Trust. The review is based on peer-reviewed surveys, NIST publications, regulatory documents, and industry practitioner reports and highlights evidence of legacy-integration challenges, identity and access management (IAM) at scale, micro segmentation in multi-cloud environments, open-banking API exposure, performance overhead of continuous verification, budget and skills constraints, and third-party risks in the context of new regulations like the EU Digital Operational Resilience Act (DORA) and the Payment Services Directive 2 (PSD2). The review also presents empirical adoption and cost data derived from industry surveys, provides a composite severity evaluation of implementation barriers and recommends an implementation framework consisting of five phases that is specific to financial institutions. The paper concludes by highlighting open research challenges such as lightweight cryptography for constrained payment endpoints, adaptive trust scoring using AI and cross-jurisdictional harmonization of regulatory frameworks.

INTRODUCTION

Over the last ten years, the financial services industry has dramatically changed its architecture, transitioning core processes to public and hybrid cloud deployments, opening up account and payment services with open-banking application programming interfaces (APIs), and enabling an increasingly remote or hybrid workforce. This shift has broken the clear-cut boundary of the network that has been the foundation of security controls for decades in the banking industry [13, [15]]. A lack of awareness of access points in distributed digital journeys, lateral movement in low-technology internal networks, and compromised access control in customer-facing applications are all becoming common ways that attackers gain access in the era of distributed digital journeys [11, 12]. In a large asset-management firm in 2024, the internal lack of trust resulted in a breach where attackers opened fraudulent customer accounts and were able to breach a flawed access-control mechanism to access Social Security numbers, driver's license information, and financial account information for other customers [12].

But the dominant answer to this challenge is Zero Trust Architecture (ZTA). Zero Trust, which was formalized in NIST Special Publication 800-207, replaces the implicit trust associated with being inside the network boundary with continual access authorization checks for every access request based on identity- and context-aware data, whether the access is made from outside or in the traditional network perimeter [1]. The basic idea behind the paradigm is "never trust, always verify," which is based on the ideas of explicit verification, least-privilege access, and assuming that a breach has already taken place or will take place [1, [3].

But for financial technology firms, Zero Trust is more than just a technology upgrade; it's a transformation that cuts across decades-old core-banking systems, some of the most stringent data-protection and operational-resilience regulations of any industry, and transaction-processing environments where every additional millisecond of authentication latency has a direct impact on the business cost. Industry surveys indicate that 63% of organizations have implemented Zero Trust to some degree or the other, but for 78% of those who have adopted it, it has cost less than one quarter of the total cybersecurity budget, and general research suggests that a fully matured, continuously evaluated Zero Trust program is not commonplace even among regulated industries [20]. In the context of FinTech, however, the move to Zero Trust needs to comply with the prescriptive regulations, including the EU Digital Operational Resilience Act (DORA) [18], the Payment Services Directive (PSD2) [19] (in its latest version), and the Payment Card Industry Data Security Standard (PCI DSS) [28] (also in its latest version) that each have their own access-control, monitoring, and third-party risk requirements.

In this paper we present a comprehensive review of literature and industry stories on Zero Trust implementation in financial technology companies, organized around three overlapping challenge domains (technical, regulatory, and organizational) whose interaction in prior literature surveys has been almost completely ignored, often focusing on Zero Trust more generally across all industry verticals [3], [4], [7], [8]. This review does the following: (i) Gathers and synthesizes the technical hurdles associated with legacy core-banking integration, multi-cloud micro segmentation and open-banking API security and presents them in a unified format; (ii) Maps the key financial regulations to Zero Trust control objectives; (iii) Quantitatively synthesizes adoption, cost, and severity data from industry and academic sources in the form of purpose-built figures; (iv) Proposes a 5-phase implementation roadmap for financial institutions; and (v) Identifies open research gaps specific to financial institutions.

The rest of the paper is organized as follows: In Section II, the basics of Zero Trust and the review methodology will be reviewed. The FinTech threat and regulatory landscape is covered in Section III. In Section IV, technical implementation issues are discussed. Section V discusses organizational and cultural problems. An economic and risk analysis is provided in the Section VI. Section VII discusses industry case illustrations. You will find a Zero Trust enabling technologies comparison in Section VIII. The implementation plan outlined in Section IX is a staged approach. Finally, Section X lists open research directions and Section XI concludes the paper.

BACKGROUND AND REVIEW METHODOLOGY

ZERO TRUST ARCHITECTURE FUNDAMENTALS

According to NIST SP 800-207, Zero Trust is an emerging group of cybersecurity principles shifting focus from static, perimeter-based defense to one which emphasizes individual resources, users, and devices, and that access to a resource is only granted when the resource is needed and user and device are authenticated and authorized for that session [1]. The reference architecture logically distributes the control plane and the data plane into three main components: the Policy Engine (PE) that decodes a trust decision based on an organization-defined trust algorithm; the Policy Administrator (PA) that defines and removes communication path between subject and resource; and the Policy Enforcement Point (PEP) that enables, monitors and terminates connections between subject and enterprise resource [1]. The figure below (Fig. 1) depicts a simplified version of this architecture as applied to a financial services deployment, where continuous contextual signals from identity, telemetry and threat-intelligence sources inform the trust decision that is made for each access request.

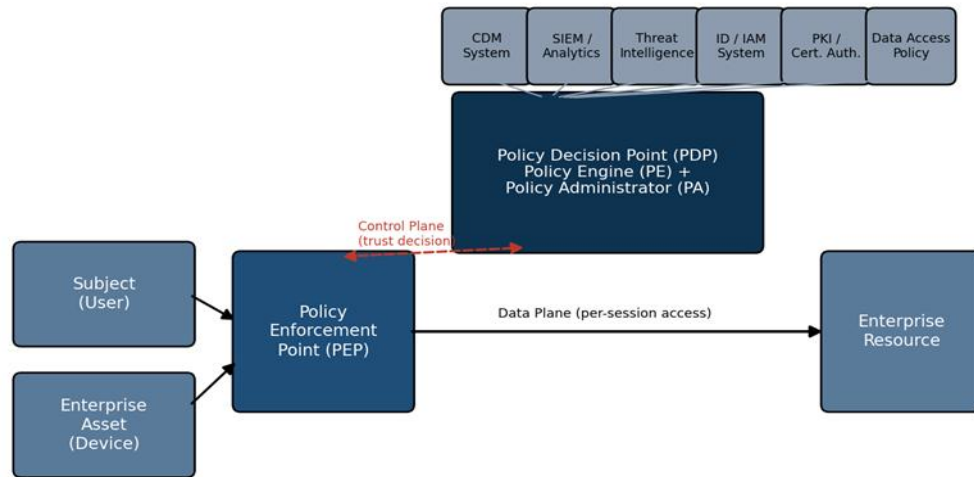


Fig. 1: Simplified NIST SP 800-207 Zero Trust logical architecture adapted for financial services [1]

The NIST model has seven fundamental principles, including the treatment of all data sources and computing services as resources; secure all communications, irrespective of network location; grant access on a per-session basis as needed, based on the principle of least privilege; continuously monitor and measure the security posture of all enterprise-owned and associated assets [1]. A companion publication, NIST SP 800-207A, is an extension of this reference model to cloud-native applications that span multiple cloud service providers, and outlines an application-level policy enforcement architecture based on service identities, API gateways, and sidecar proxies, which is relevant to FinTech companies whose core payment and ledger services are increasingly deployed as micro services across multiple cloud regions and cloud service providers [2].

EVOLUTION OF ZERO TRUST RESEARCH

This is because academic interest in Zero Trust has grown rapidly since the publication of SP 800-207. Based on a comprehensive survey on the IEEE Access, the technologies which enable Zero Trust can be divided into four groups: identity-based access control, micro segmentation, software-defined perimeters, and continuous trust evaluation, and the authors mention that identity-based access control is often too coarse-grained for today's dynamic subject and object populations in distributed environments [3]. Later studies have explored the development of Zero Trust and trends going forward [4], the problem of transitioning legacy architectures to a zero-trust approach [5] and if the approach really achieves better security results than what is achieved in terms of the implementation cost and complexity [6]. The literature is dominated by studies on cloud computing (24 studies), Internet of Things (11), healthcare (7), and enterprise/remote-work systems (6), with only 74 studies published between 2016 and 2025, and the most frequently studied ZTA components include authentication, authorization, and access control; auditing, orchestration, and environmental perception are still comparatively under-explored areas, and the cross-domain analysis revealed that there are persistent scalability limitations, a lack of lightweight cryptography for small-size systems, and weak alignment with regulatory frameworks [7]. A comprehensive survey of applications and challenges provides a more general look at cultural issues and technical challenges, highlighting that they are the major hurdles for the successful implementation of Zero Trust's promise, not the lack of enabling technology [9].

Compared to the cloud and IoT research is still relatively light in the financial sector. When present, it typically centres around identity and access management, device and network security, and data protection via mechanisms like multi-factor authentication, intrusion detection, data-loss prevention, and network segmentation; reported challenges are largely related to integration with legacy systems, and maintaining user experience; some work has proposed machine-learning-based trust-level evaluation models to integrate with the policy engine of a financial-sector Zero Trust deployment [7]. This review fills the gap and brings together the financial-sector specific evidence in the academic and practitioner literature.

REVIEW METHODOLOGY

This review is done in a narrative systematic method. Four sources were used to obtain sources: (1) peer-reviewed academic surveys and systematic literature reviews on Zero Trust Architecture [3]–[9]; (2) primary standards and regulatory documents, such as NIST SP 800-207 and 800-207A [1], [2] and the EU Digital Operational Resilience Act [18] and the revised Payment Services Directive [19] and PCI DSS v4.0 [28]; and (3) practitioner and industry analyst publications covering the Zero Trust adoption in financial services and capital markets [10–17, 23, 24, 26, 27]; and (4) quantitative industry survey and market-research data on adoption rates, budget allocation, and breach economics [20–27, 29]. Sources were selected to meet the criteria of their recency (2020–2026), relevance to financial services, and for quantitative claims, their ability to be traced to a named primary survey or standards body. The results were first organized thematically in three categories of technical, regulatory, and organizational challenges, as suggested in the previous cross-domain Zero Trust surveys [7], [9].

THE FINTECH THREAT AND REGULATORY LANDSCAPE

THREAT LANDSCAPE AND BREACH ECONOMICS

Financial institutions are still in the top 10 industries for the highest costs of data breaches. The Cost of a Data Breach Report by IBM [22] showed that the financial sector had an average cost of \$5.56 million, behind only healthcare at \$7.42 million but ahead of industrial, energy, and technology at \$5.38 million, respectively, though the latter figure was down 8.6% from \$6.08 million in 2024. The financial sector remains consistently exposed compared to other sectors, as shown in Fig. 2. The top costliest attack category reported was malicious insider, averaging \$4.92 million per incident, reinforcing the importance of Zero Trust's "least privilege" and "continuous verification" tenets to an industry where privileged access to payment rails and funds held by internal personnel is common [22].

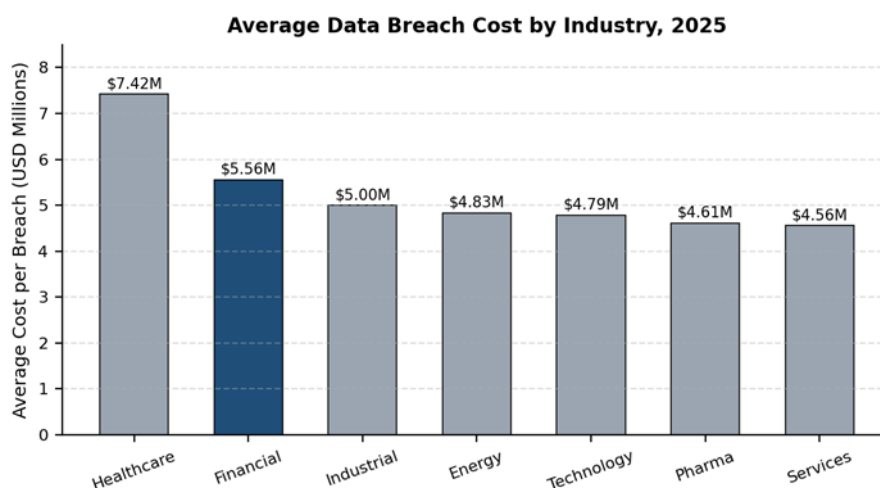


Fig. 2: Average data breach cost by industry, 2025, showing the financial sector's elevated exposure relative to most other verticals [22].

In addition to direct breach costs, financial institutions have a growing attack surface as a result of remote workforces, cloud operations, and increased use of APIs that link banks to FinTech partners, payment processors and third-party data aggregators [15], [16]. The failure to adhere to the concept of "least privilege" is precisely the type of access control violation that Zero Trust seeks to prevent, as evidenced by a large investment management company that was breached in 2024, where attackers employed fraudulent accounts to access other customers' personal and financial information [12].

REGULATORY FRAMEWORKS SHAPING ZERO TRUST ADOPTION

Unlike many industries, FinTech firms have to deal with multiple overlapping regulatory frameworks when implementing Zero Trust. The EU Digital Operational Resilience Act (DORA) entered into force in January 2023 and will be applicable in January 2025, and sets out uniform requirements for the ICT risk management framework for over twenty categories of EU financial entities, including credit institutions, payment institutions, e-money institutions, investment firms, and crypto-asset service providers, as well as ICT incident reporting and digital operational resilience testing, and crucially, ICT third party risk management, which includes contractual oversight of cloud and other technology providers [18]. Continuous risk assessment of the entire technology estate, from all third-party ICT providers, aligns with the Zero Trust principle: "Do not trust a provider by default" [1] [18].

Strong Customer Authentication (SCA) is a new requirement in the revised Payment Services Directive (PSD2) for electronic payments, and the banks must allow third parties to access their account and payment services through secure and standardized APIs, typically using OAuth 2.0 authorization flows [16], [19]. PSD2 explicitly places the responsibility on providers to properly authenticate transactions, which provides explicit regulatory incentive for the identity-centric, continuously verified access model that Zero Trust prescribes [16]. The so called open-banking API standards like NextGenPSD2 by the Berlin Group and the Open Banking Standard by the British banking regulator Bank of England, along with the aforementioned SCA, need to be complemented by multi-layered security architectures involving OAuth 2.0 authorization as well as in-transit and at-rest encryption [17]. Although not part of the DORA or PSD2 frameworks, the Payment Card Industry Data Security Standard (PCI DSS) 4.0 edition still requires network segmentation, robust access controls and regular monitoring, and thereby reinforces several key Zero Trust network controls [28]. Table I shows how four significant regulatory instruments relate to key Zero Trust control goals.

Regulation	Primary Scope	Related Zero Trust Control Objective	Ref.
DORA	EU ICT risk mgmt., incident reporting, third-party oversight	Continuous asset/vendor risk assessment; assume-breach resilience testing	[18]
PSD2	Strong Customer Authentication; open-banking API access	Explicit per-transaction identity verification; least-privilege API scopes	[16], [19]
PCI DSS v4.0	Cardholder data environment protection	Network segmentation; least-privilege access; continuous monitoring	[28]
GDPR (general reference)	Personal data protection across EU operations	Data minimization; access logging; breach notification	[7]

Table I: Mapping of Financial Regulations to Zero Trust Control Objectives

ZERO TRUST MARKET AND ADOPTION TRENDS

Industry surveys indicate that Zero Trust adoption is gaining momentum across industry, but not evenly. When it comes to the financial industry as a whole, the surveys are mixed in terms of the rate at which Zero Trust is being adopted, but the growth is a steady pace. In fact, 63% of organizations globally had deployed a Zero Trust approach to at least some degree in 2024, with only 78% of those that have adopted spending less than 25% of their cybersecurity budget on it, and 35% of adopters facing a failure that hindered full or partial deployment. ((Gartner, 2024)) When asked separately, 91% of organizations surveyed said that identity is a critical component of their Zero Trust efforts, while 80% of those organizations indicate that their Zero Trust budgets are expanding annually despite overall security budgets shrinking [27]. These indicators of adoption and maturity are summarized in Fig. 3.

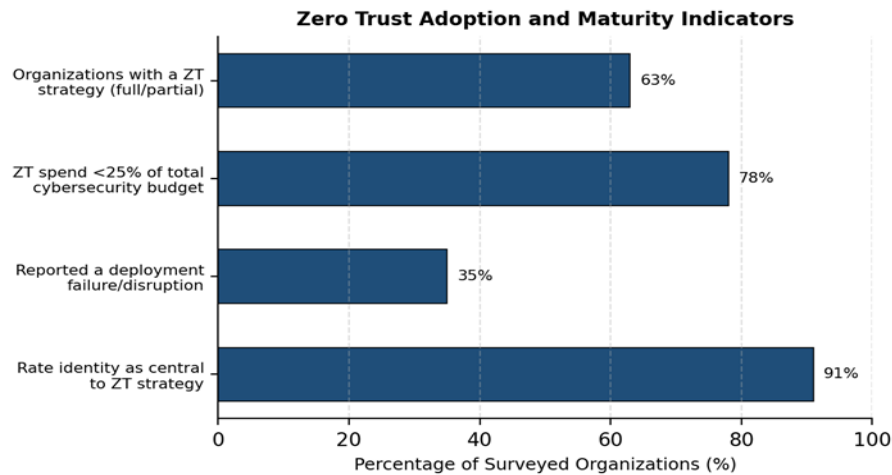


Fig. 3: Zero Trust adoption and maturity indicators compiled from industry survey data [20], [27].

The global Zero Trust security market is estimated to be valued at USD 38.37 billion in 2025 and will reach USD 86.57 billion by 2030 at a CAGR of around 17.7%, while large enterprises currently account for 76% of the market revenue [21]. Fig. 4 shows this projected growth. While that may be the case, maturity is still quite limited, with less than 10 percent of large enterprises expected to have a fully mature and continuously evaluated Zero Trust program by 2026, compared to less than 1 percent in 2023, suggesting most organizations, including financial institutions, are still at an early or partial stage of implementation [27].

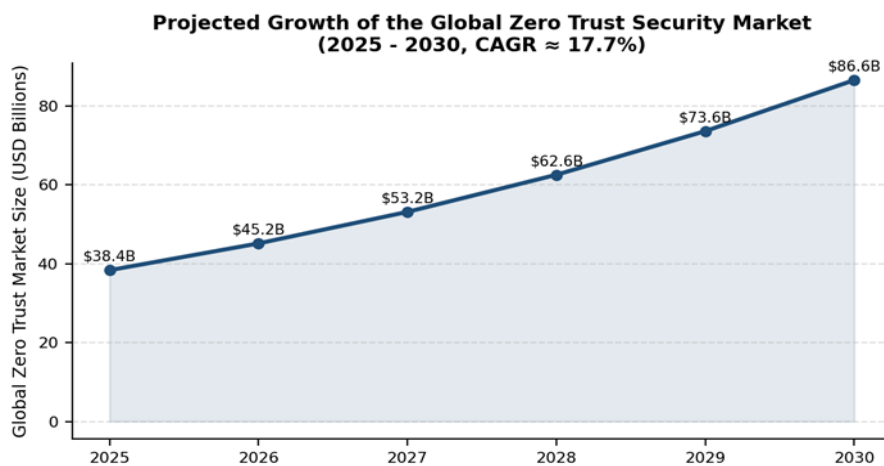


Fig. 4: Projected growth of the global Zero Trust security market, 2025–2030 [21].

TECHNICAL IMPLEMENTATION CHALLENGES

LEGACY CORE-BANKING SYSTEM INTEGRATION

The most common technical challenge to Zero Trust in financial services is the use of legacy core banking systems that were not built for session-by-session identity-based authorizations. Core banking platforms have typically been developed in the past decades, are monolithic, and rely on implicit trust between tightly coupled components within the platform; introducing continuous verification on such systems could create potential for disruption to transaction processing pipelines with extremely high availability requirements [14]. The need for legacy system integration and the potential for operational disruption are the most frequently cited challenges in transition, even when the focus is on the technological aspects of transition [14]. This challenge is exacerbated by open-banking: Exposing modern, standardized APIs (including those that meet NextGenPSD2 requirements, as specified in PSD2, and also the UK Open Banking Standard) over legacy cores generally requires an intermediary integration layer between legacy and modern systems, adding an extra layer of trust boundary that needs to be secured and monitored on an ongoing basis [17].

IDENTITY AND ACCESS MANAGEMENT AT ENTERPRISE SCALE

By moving away from network-based to identity-based access control, Zero Trust also provides vulnerabilities in access-control-list and role-based access-control schemes that are less scalable for the

large number of employees, contractors, service accounts and third-party integrations that are common in a financial institution [3]. In practice, financial-sector Zero Trust IAM deployments are based on a strict “least privilege” model, built on multi factor authentication, device fingerprinting and posture checking, geolocation analysis, and privileged access management, with continuous monitoring via user and entity behavior analytics (UEBA) that can lower a session's trust score, based on risk, if it matches known patterns for data-exfiltration. One of the difficulties with such adaptive, partially automatable decision-making is that the system may turn off or deny access to legitimate activities, but industry input guidance suggests that such systems are supposed to be “conservative” [10]—that is, they are not intended to grant any more access than is already permitted.

MICROSEGMENTATION IN HYBRID AND MULTI-CLOUD ENVIRONMENTS

While micro segmentation — small isolated network or workload environments that limit the spread of lateral movement in the event of a compromise — is one of the core enabling technologies for Zero Trust, it is architecturally challenging to implement in many financial institutions' hybrid, multi-cloud environments [3, 4]. But modern micro segmentation frameworks are increasingly identifying policy by workload identity, enabling consistent policy enforcement as workloads migrate between on-premises data centers and multiple cloud providers [3]. In this case, the organization created an internal certificate and service-identity management system, adopted mTLS for all internal service-to-service connections, and deployed micro segmentation to separate workloads, thereby maintaining high volume transaction processing while also significantly lowering the risk of lateral movement [23]. Micro-segmentation of networks specifically to isolate critical payment and ledger systems and automation of threat detection and incident response with AI-driven tooling are recommended best practices for financial institutions moving toward this model [14].

API SECURITY AND OPEN-BANKING EXPOSURE

Under the open-banking mandate in PSD2 banks are required to share account details and payment initiation capabilities via APIs, which means that the bank's attack surface is significantly extended [16, 19]. While industry security architecture for open banking generally includes Strong Customer Authentication, OAuth 2.0 authorization, in some cases federated identity via Open ID Connect, and end-to-end encryption, there are unique risks with APIs that can't be mitigated by perimeter controls, such as data loss, identity theft, account takeover, and API-specific security vulnerabilities outlined in the OWASP API Security Top 10 [16], [17]. It is widely thought that Zero Trust is a good fit for securing open-banking API traffic as it never trusts the network from which a call originated, but standardizing and managing the consent lifecycle, along with managing OAuth scope granularity, across all third-party integrations is not trivial [16], [17].

CONTINUOUS VERIFICATION, LATENCY, AND PERFORMANCE OVERHEAD

The per-session verification step adds computational and latency costs that may be important in transaction processing systems where milliseconds can mean the difference between a wonderful customer experience and a terrible one, and, in trading scenarios, between good and bad financial results. Comparative studies of Zero Trust network models point to the known security/performance trade-offs, with finer-grained, continually re-evaluated trust decisions typically resulting in more time-consuming authentication and authorization processes compared to perimeter-based static trust [8]. The security gain offered by Zero Trust is a live debate in the literature; in fact, at least one well-publicized study suggests that it is not about Zero Trust, but about how well it is implemented and how mature the organization is [6].

AI- AND MACHINE-LEARNING-BASED TRUST EVALUATION

Researchers have developed a variety of techniques for integrating machine-learning-based trust-level evaluation directly into the Zero Trust policy engine, so that behavior and context risk signals are also part of the access decision-making process, a technique that is especially relevant for financial institutions, where access is particularly critical and threats are sophisticated [7]. In the broader literature on Zero Trust, AI and machine learning is one of the most rapidly growing and relatively under-explored areas of Zero Trust research, with the potential for significant productization and research in the financial sector in this space [7].

ORGANIZATIONAL AND CULTURAL CHALLENGES

EXECUTIVE BUY-IN, BUDGET JUSTIFICATION, AND ROI

In addition to technology, the most successful Zero Trust migrations have included continued executive backing and a multi-year budget commitment, which can prove challenging for financial institutions since as many as 78% of the organizations that have adopted invest less than a quarter of their cybersecurity budgets in Zero Trust and the ROI is long-term and comes with reduced risk versus tangible revenue [14, 20]. Industry guidance for banking and capital-markets firms highlights that Zero Trust is not just another set of point products or solutions, but a shift in the way security is viewed and must be adopted across the business, and therefore, it is important to ensure cross-functional collaboration between security, compliance and business-line teams to ensure its success [15].

CYBERSECURITY SKILLS SHORTAGE

There are few or no financial services practitioners with the ability to apply this to Zero Trust implementations, given the need to master identity engineering, cloud-native networking, policy-as-code, and regulatory compliance — a mix of skills that is challenging in the wider cybersecurity job market and even more so for financial services, due to additional domain-specific requirements in this space [9, 24]. Workforce and skills challenges are consistently cited as a top two barrier to the paradigm's security potential, ahead of cultural resistance, in reviews of the barriers to Zero Trust adoption [9].

CHANGE MANAGEMENT AND WORKFORCE RESISTANCE

At the heart of Zero Trust is the shift in how users interact with systems, which comes with increased authentication prompts, device compliance checks, and, in some cases, session re-verification. For financial institutions that already have a perimeter-based security mindset, it is important to carefully manage the transition to minimize productivity friction and employee circumvention of perimeter security controls; recommended practice includes a staged rollout, robust and visible leadership support, cross-functional coordination between the IT department, security department and business units, and continuous employee education to engender acceptance of the new access model [14] [15]. There is also a broader body of Zero Trust literature that defines the movement beyond legacy trust assumptions as a cultural transformation that organizations must undertake, which means changing their methods from perimeter thinking to continuous verification as the norm, rather than the exception [23].

THIRD-PARTY, VENDOR, AND SUPPLY-CHAIN RISK

External ICT providers, cloud platforms, and FinTech partners via open-banking APIs are all trust boundaries that must be constantly monitored rather than simply trusted to be secure [16], [18]. DORA institutionalizes this concern by laying down common principles for the prudent management of third-party risks and specific contractual obligations for financial entities and technology providers, and a monitoring system for technology providers considered critical to the financial system [18]. For most financial institutions, having continuous — and Zero-Trust consistent — oversight of dozens or hundreds of third-party integrations instead of a one-time vendor security questionnaire is a significant new capability that is still in its early stages of development.

ECONOMIC AND RISK ANALYSIS

Based on the technical and organizational results summarized above, the authors have developed a composite severity index for the key Zero Trust implementation challenges reported in the literature, as represented in Fig. 5, which was created from the relative frequency and level of emphasis assigned to each challenge across the literature surveyed by the authors in the above technical and organizational sources [3], [7], [9], [10], [14], [15], [23]. Legacy core banking integration and multi-jurisdictional regulatory complexity are again the highest ranked barriers, as both practitioner and academic sources list them as the top two barriers to implementation, before latency and performance overhead, which ranks as the third highest barrier despite their reality but are significantly mitigated by modern edge-deployed policy enforcement points and hardware-accelerated cryptography.

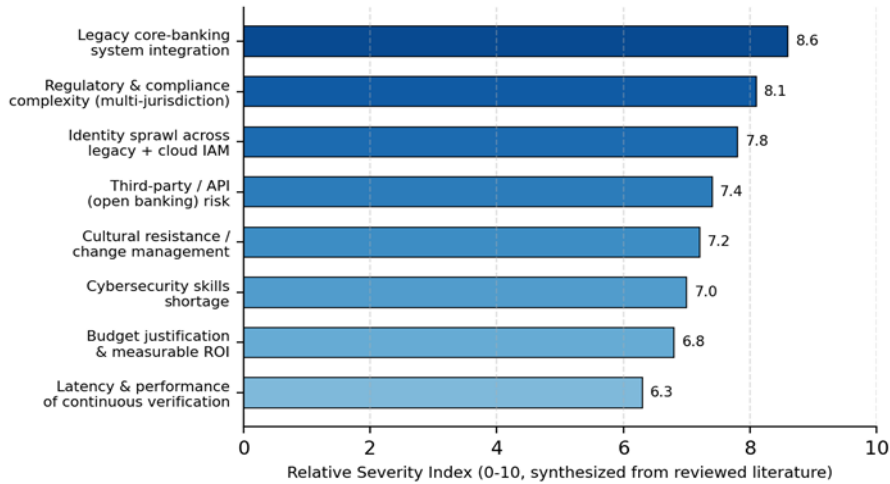


Fig. 5: Composite severity of reported Zero Trust implementation challenges in FinTech organizations, synthesized from the reviewed literature [3], [7], [9], [10], [14], [15], [23].

From a cost-benefit perspective, IBM's 2025 findings indicate that organizations using extensive security artificial intelligence and automation — capabilities central to a mature Zero Trust continuous-monitoring layer — realize substantially lower breach costs and faster containment than organizations without such tooling, reinforcing the economic case for investment even where the return is realized as avoided loss rather than direct revenue [22]. Concurrently, a lack of sequenced deployments is a genuine operational risk in Zero Trust, as 35% of those that have adopted Zero Trust report a failure or disruption in their deployment [20] further underscoring the need for the phased deployment strategy suggested in Section IX.

CASE ILLUSTRATIONS FROM INDUSTRY PRACTICE

The following are some of the documented industry cases that illustrate the challenges that have been identified above. First, the 2024 breach at a large investment-management firm was the result of another breach of access control that was not expected: Attackers successfully exploited the access control flaw by creating fake accounts and then accessing other customers' sensitive information, something that per-session authorization does not prevent [12]. Second, a large cloud-native financial services organization's internal identity and certificate management system, using mutual TLS for all internal communications and micro segmenting workloads across a multi-cloud environment, provides a more mature technical implementation pattern that maintained transaction throughput for millions of transactions every day while significantly reducing lateral-movement risk, showing that performance and security don't have to be mutually exclusive, but can be engineered at the workload-identity level instead of retrofitting onto legacy network segmentation [23]. Third, adaptive, continuously monitored identity controls can be added on top of existing investments in IAM without replacing infrastructure, as seen in banking-sector Zero Trust deployments that integrate device fingerprinting, geolocation, privileged access management, and UEBA-based dynamic trust scoring [10]. Last but not least, a pattern from Open-Banking API gateway implementations based on OAuth 2.0 and Strong Customer Authentication (SCA), combined with existing identity providers, illustrate a concrete approach for fulfilling the requirements for third-party facing APIs introduced by PSD2 [16] and embedding Zero Trust principles.

COMPARATIVE ANALYSIS OF ZERO TRUST ENABLING TECHNOLOGIES

Table II compares the principal technology categories used to implement Zero Trust in financial institutions, summarizing their primary function, financial-sector-specific value, and the implementation challenge most closely associated with each, drawn from the surveyed literature [3], [4], [8], [10], [23].

Technology	Primary Function	FinTech-Specific Value	Principal Challenge
IAM / MFA	Identity verification and authorization	Satisfies PSD2 Strong Customer Authentication	Legacy directory integration
Micro segmentation / SDP	Workload isolation, lateral-movement containment	Isolates core-banking and payment systems	Multi-cloud policy consistency

ZTNA / API Gateway	Per-request access brokering	Secures open-banking third-party API access	OAuth scope and consent governance
UEBA / Behavioral Analytics	Continuous, risk-based trust scoring	Detects insider fraud and credential misuse	False positive / negative tuning
CASB / EDR	Cloud access control and endpoint monitoring	Extends control to remote/hybrid workforce	Tool sprawl and integration overhead

Table II: Comparative Analysis of Zero Trust Enabling Technology Categories in FinTech

PROPOSED PHASED IMPLEMENTATION FRAMEWORK FOR FINTECH ORGANIZATIONS

With the challenges and enabling technologies identified above, this review outlines a five-phase framework to sequence the adoption of Zero Trust in a way that balances operational risk to systems with a high impact on transactions and gradually meets compliance requirements in line with DORA, PSD2 and PCI DSS [1], [14], [15], [18], [28].

PHASE 1. DISCOVERY, DATA CLASSIFICATION, AND REGULATORY MAPPING

Inventory all data flows, applications and third party integrations; classify data and systems by sensitivity and scope of regulation (such as cardholder data under PCI DSS, payment data under PSD2); and map existing controls against DORA's ICT risk-management requirements to build a baseline and prioritized gap list [18], [28].

PHASE 2. IDENTITY FOUNDATION

Combine identities into consistent identity providers, deploy multi-factor and posture-aware authentication for all identities (including services), and use least-privilege and privileged-access-management as the basis for the later phases: access is granted per-session and per-resource [1], [10] as per NIST principles.

PHASE 3. MICROSEGMENTATION OF CRITICAL SYSTEMS

Developing the highest value assets first: payment rails, core ledgers and cardholder data environments, then segmenting the rest of the estate, like the workload-identity-based approach shown in cloud-native financial services deployments [3], [14], [23].

PHASE 4. API AND THIRD-PARTY ACCESS GOVERNANCE

Implement a Zero Trust Network Access or API gateway as a layer in front of all open-banking and third-party integrations, with the requirement to implement OAuth 2.0 scopes and Strong Customer Authentication, and to have contractual and technical oversight of ICT third-party providers as per DORA [16, 17, 18].

PHASE 5. CONTINUOUS MONITORING, AUTOMATION, AND GOVERNANCE

Implement UEBA, security information and event management (SIEM), and automated incident-response tooling in order to achieve the "assume breach" principle by continuously detecting and quickly containing breaches, and implement recurring digital operational resilience testing to meet DORA and effectively communicate measurable risk reduction to decision makers and close the gap in the budget justification process from Section V-A [1], [10], [18], [20].

OPEN RESEARCH CHALLENGES AND FUTURE DIRECTIONS

There are a number of research gaps that are prevalent across the broader zero trust literature, but are even more significant for the financial services industry. There is still a long way to go, however, in the development of lightweight cryptographic solutions for resource-constrained endpoints, such as point-of-sale (PoS) terminals and embedded payment devices, compared to the demands on cryptography for continuous mutual authentication [7]. Third, orchestration and auditing mechanisms covering a variety of policy enforcement points across diverse and multi-cloud environments are comparatively under-explored compared to authentication and access control, even though key to showing continuous compliance in the event of DORA [7] [18] is in play. Third, the research field of adaptive trust scoring, used to dynamically evaluate the trust level of a session according to behavioral and contextual signals, is also active but still emerging, and shares direct relevance with the detection of insider-driven and credential-based frauds that account for the bulk of the costs of financial-sector breaches [7], [9], [22], [24]. Fourth, regulatory harmonization across jurisdictions is still an open policy and engineering challenge: Multinational financial institutions need to align DORA, PSD2, PCI DSS, and banking regulation

requirements within a single technical control framework; and academic tooling to formally validate the compliance of a given Zero Trust policy configuration to multiple overlapping banking regulatory requirements is not yet at maturity [7], [18]. Lastly, there is a need for industry studies over a longer time period to take a significant look at the return on investment of Zero Trust, beyond the concept of avoided breach cost, as adoption becomes more widespread beyond the current partial-implementation phase reported across the industry [20], [21].

CONCLUSION

For financial technology firms, the threat environment and technology has outpaced a perimeter-based approach to security, which Zero Trust Architecture provides a principled answer. However, as shown in this paper, implementation in financial services is significantly more complicated than general enterprise deployment guidance suggests, due to the unique and complex nature of the legacy core-banking infrastructure, overlapping and stringent regulatory regimes, high-availability transaction needs and an ever-growing open-banking API surface. In this review, we have compiled technical challenges from legacy integration, identity and access management at scale, multi-cloud micro segmentation and open-banking API security, as well as organizational challenges such as budget justification, skills shortage, change management, and third-party risk governance, to highlight the financial industry as a highly compelling and constrained target in which to apply Zero Trust. The five-step model provided a risk-progressed roadmap for financial institutions starting from identity foundation and moving forward continuously with regulation-aligned monitoring. Financial technology companies are poised to gain from a body of evidence in Zero Trust that is evolving from the basic architectures and into domain-specific considerations like lightweight cryptography, AI-driven trust evaluation, and cross-jurisdictional compliance automation, thereby turning Zero Trust from a desired future state (currently covering, on average, just 50% of a typical organization's environment) into a measurable and real-world reality.

REFERENCES

- [1] U. A. Kithran, S. Ilyas, K. Amber, H. Abbas, and S. Zahid, "AI-based collision prediction and prevention systems in urban traffic," *Spectrum of Engineering Sciences*, vol. 3, no. 12, pp. 1907–1920, 2025.
- [2] M. R. Islam, I. A. Badhan, M. H. Rahman, and M. N. Hasnain, "The economics of global renewable energy supply chains: Opportunities and vulnerabilities for the U.S.," *International Journal of AI, Engineering and Management Studies (IJAIEMS)*, vol. 1, no. 1, pp. 108–136, 2026.
- [3] U. Imtiaz, "Ghost signals: Ethical RF adversarial testing of consumer alarm ecosystems," in *Data Science and Security*, S. Shukla, H. Sayama, K. Tiwari, J. P. George, and J. V. Kureethara, Eds. Cham, Switzerland: Springer, 2026, *Lecture Notes in Networks and Systems*, vol. 1945, doi: 10.1007/978-3-032-24075-0_21.
- [4] S. M. Ali, M. Hadi, F. Usama, M. S. Khan, M. Iqbal, and S. Ahmad, "From artificial to quantum intelligence: The next frontier of low-carbon energy systems," in *Proc. 2026 Int. Conf. Integrated Intelligence and Cognitive Engineering (ICIICE)*, Dubai, United Arab Emirates, 2026, pp. 1–6, doi: 10.1109/ICIICE69672.2026.11565487.
- [5] A. Badhan, M. N. Hasnain, M. H. Rahman, I. Chowdhury, and M. A. Sayem, "Strategic deployment of advance surveillance ecosystems: An analytical study on mitigating unauthorized U.S. border entry," *Inverge Journal of Social Sciences*, vol. 3, no. 4, pp. 82–94, 2024.
- [6] M. Delshadi, N. Ahmad, M. D. Rasheed, M. S. Sardar, and U. Aslam, "Deep learning-based network traffic analysis for cyber threat detection," *Spectrum of Engineering Sciences*, vol. 3, no. 12, pp. 607–614, 2025.
- [7] K. Khaliq, M. S. Khan, S. Sajid, I. Shahbaz, M. W. Iqbal, K. S. Siddiqui, et al., "A study on the application of deep learning and machine learning in adaptive intelligent tutoring," *Spectrum of Engineering Sciences*, vol. 4, no. 3, pp. 818–835, 2026.
- [8] U. A. Kithran, A. Khanam, S. Ilyas, R. Yaqoob, and M. Hannan, "Demand forecasting in transportation networks using deep learning," *Spectrum of Engineering Sciences*, vol. 3, no. 11, pp. 687–700, 2025.
- [9] U. Iqbal and Y. Bhutto, "Digital transformation through artificial intelligence and advance business analytic in American operational management," *Journal of Theoretical and Applied Econometrics*, vol. 3, no. 1, pp. 37–50, 2026.
- [10] M. M. Islam, "AI-driven fraud detection and prevention using human behavior analysis to enhance U.S. social and financial security," *International Journal of Applied Mathematics*, vol. 38, no. 8S, pp. 861–871, 2025.
- [11] D. Safiullah, A. A. Khan, N. Ahmad, M. Danish, and S. Rana, "Integrating artificial intelligence and soil ecology to enhance plant resilience under environmental stress," *ASSAJ*, vol. 4, no. 2, pp. 3508–3516, 2025.
- [12] R. Singh, "Brønsted-acid-guided esterification: Mechanistic and kinetic insights for long-chain fatty acid to alkyl ester conversion on a heterogenized porous acid platform," *International Journal of Clinical Research and Medical Sciences*, vol. 1, no. 1, 2026, doi: 10.67231/rzakra50.

- [13] U. Iqbal, "AI-enhanced network optimization for electric vehicle charging infrastructure expansion in the United States using graph theory and demand analytics," *Journal of Engineering and Computational Intelligence Review*, vol. 2, no. 2, pp. 112–129, 2024.
- [14] M. Chaudhari, "Hydrophilic nanofiber barrier coatings for aluminum: Waterborne crosslinking, microstructure–property links, and EIS-based protection," *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3017, Jul. 2026, doi: 10.4238/rhd2k915.
- [15] R. Singh, "Smart prediction of molecular behavior in liquid chromatography for better compound detection," *International Journal of Clinical Research and Medical Sciences*, vol. 1, no. 1, 2026, doi: 10.67231/v3jyx227.
- [16] R. Parveen, "An explainable AI framework for ethical fraud prevention in U.S. federal welfare programs," *International Journal of Applied Mathematics*, vol. 38, no. 11S, pp. 1425–1435, 2025.
- [17] M. N. Amjad, "Machine learning for renewable energy forecasting and smart grid optimization," *Journal of Engineering and Computational Intelligence Review*, vol. 2, no. 2, pp. 130–145, 2024.
- [18] U. Imtiaz, "Dynamic security certification framework for evolving distributed architectures," in *Data Science and Security*, S. Shukla, H. Sayama, K. Tiwari, J. P. George, and J. V. Kureethara, Eds. Cham, Switzerland: Springer, 2026, *Lecture Notes in Networks and Systems*, vol. 1947, doi: 10.1007/978-3-032-24360-7_32.
- [19] M. Chaudhari, "Epoxy barrier coatings reinforced with solidified-waste microfillers for aggressive acids," *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3020, Jul. 2026, doi: 10.4238/96y1s945.
- [20] Kumar and K. K. S. Nair, "The impact of cloud-based business analytics on operational efficiency in U.S. small and medium-sized firms," *Spanish Journal of Innovation and Integrity*, vol. 49, pp. 303–318, 2025.
- [21] S. T. Hasan, "Labor market intelligence using natural language processing for the U.S. direct care workforce: Predicting skill gaps, recruitment needs, and emerging healthcare workforce demand," *American Journal of Multidisciplinary Knowledge Insights*, vol. 3, no. 1, pp. 1–16, 2024.
- [22] S. Mirza, S. Butt, A. Arif, and N. Jahangir, "COVID and post-COVID e-learning reforms in higher education institutions: A systematic review of literature," *Journal of Business Insight and Innovation*, vol. 5, no. 8, pp. 364–383, 2026.
- [23] M. N. Amjad, "Artificial intelligence-based voltage stability assessment in modern power systems: Edge intelligence for real-time monitoring of smart electrical networks," *Journal of Business Insight and Innovation*, vol. 3, no. 1, pp. 102–115, 2024.
- [24] M. A. Jawed, "Uncertainty-aware geostatistical reconstruction of regional groundwater hydraulics under sparse monitoring conditions: A case study of the Evergreen Underground Water Conservation District (EUWCD), Texas, USA," *Bishop International Journal of Mathematics and Computer Science*, vol. 1, no. 1, pp. 57–71, 2025.
- [25] W. Reese and D. Sinclair, "Bridging the digital divide: Digital inequality and socioeconomic outcomes in the United States," *American Journal of Multidisciplinary Knowledge Insights*, vol. 5, no. 1, pp. 1–8, 2026.
- [26] A. Kumar, "The role of banking credit access in healthcare analytics-driven practice growth: Implications for regional economic development in the U.S.," *Journal of Computational Systems & Engineering Insights*, vol. 2, no. 2, pp. 15–28, 2024.
- [27] N. J. Mercer, "Enhancing organizational performance through strategic cloud computing in management," *International Journal of Business Integrity and Technology Advancements*, vol. 1, no. 1, pp. 11–17, 2025.
- [28] K. Hamdan, "AI-powered cyber resilience strategies for modern organizations," *Journal of Computational Systems & Engineering Insights*, vol. 4, no. 1, pp. 1–10, 2026.
- [29] R. M. Cachart, F. Ahmed, S. Pochincharla, V. Gummadavelli, R. S. Ganapathy, and A. Devineni, "Adaptive program governance platform using reinforcement learning and policy optimization," in *Proc. 2026 Int. Conf. Intelligent and Sustainable AI Systems (ICOSAAS)*, Bali, Indonesia, 2026, pp. 1563–1570, doi: 10.1109/ICOSAAS68663.2026.11648756.
- [30] M. S. Uddin, A. Khan, I. Alim, and D. Khan, "The evolution of cybersecurity in the digital age: Contemporary threats, technologies, and future directions," *Journal of Computational Systems & Engineering Insights*, vol. 4, no. 2, pp. 12–29, 2026.
- [31] T. Boz et al., "Large-scale online science and engineering professional learning for rural elementary teachers," *Research in Science Education*, vol. 56, no. 3, pp. 891–914, 2026.
- [32] R. J. Hammack, J. Robinson, T. Boz, et al., "Supporting elementary engineering instruction in rural contexts through online professional learning and modest supports," *Teaching, Leadership & Professional Practice Faculty Publications*, no. 40, 2024. [Online]. Available: <https://commons.und.edu/tlpp-fac/40>