

EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 05

REVISED: JULY 24

ACCEPTED: AUGUST 08

PUBLISHED: AUGUST 27



Continuous Trust Evaluation Beyond the Perimeter

Carlos Mendoza

Asst Professor

Abstract— This paper defines continuous trust intelligence and situates it within the broader problem of identity-centric threat detection. We argue that this capability is especially relevant to hybrid, cloud-native enterprises, where identity has become a primary — and often under-monitored — attack surface. The paper outlines the scope of the work, states its research questions, and previews its anticipated contributions.

We offer provisional answers to the following questions: What key challenges arise from the capabilities of cloud-native services and applications? What properties must a system satisfy to support identity-centric trust intelligence and risk mitigation? And can trust itself be treated as a legitimate, measurable point within the enterprise attack surface?

Existing work on identity-centric risk avoidance is extensive, yet it largely fails to provide continuous, real-time visibility into identity-driven exposure within business-critical systems. This gap raises a practical question that enterprise architects and security officers routinely face: *When is it safe enough to consume partner, managed, and legacy identity-aware systems and resources without an additional layer of zero-trust controls?* Answering this requires a clear, ongoing assessment of how risky such usage actually is, paired with additional identity-centric safeguards that function as a last line of defense.

This matters because identity systems — generally assumed to be secure — often constitute the largest identity-centric attack surface in an organization, with both direct and indirect effects. Unlike conventional attack surfaces, which are typically measured and made visible through established tooling, identity-based attack surfaces can expand unchecked while remaining largely invisible, even when they involve strategic, high-value, or continuously active systems and connections.

Keywords—Hybrid Cloud-Native, Trust Intelligence, Identity-Based System, Identity-Centric Threat Detection, Trust Inference, Governance, Risk, and Compliance, Provenance, Digital Credential, Trust Score, Continuous Trust Intelligence, Identity-Centric Security, Threat Detection, Zero Trust Architecture, Hybrid Cloud Security, Cloud-Native Enterprises, Identity and Access Management, Behavioral Analytics, Continuous Authentication, Adaptive Access Control.

1. INTRODUCTION

Contemporary enterprise environments operate across multicloud and on-premises infrastructures, including cloud services, containers, and IoT devices. Adoption motives frequently revolve around agility, flexibility, and performance, but vigilance is often insufficient for achieving CyberFirst principles. Consequently, cloud providers suffer major security incidents at an alarming frequency. Attacks target cloud-native applications, with Cloud Security Posture Management maintaining full visibility of their configurations and Event Detection and Response systems collecting runtime telemetry. These telemetry signals feed Threat Attack Simulation and Threat Deception capabilities that encompass threat and risk modelling. However, teams face communication challenges, incidents often remain unsolved for long periods, and 40% occur during credential compromise. Consensus suggests shifting the monitoring focus from the infrastructure to the identities that access it.

Many organizations now embrace a risk-averse perspective where identity is the new perimeter. Symbolic representations of trust begin to reflect actors' real behaviour across all enterprise environment dimensions, allowing individuals to make informed decisions. Indeed, distinct actors behave according to their properties and roles, driven by business objectives, and privileges should be assigned accordingly. The selected approach assumes identity-related threats supported by intelligence sources capable of feeding

the entire detection life cycle. Identity-centric threat detection need not solely target the cloud but rather any of the enterprise risk exposure points. Its definition is essential to supporting identities and the corresponding processes in multicloud native scenarios. In Computer Science and Software Engineering, trustworthiness is the most relevant term as it specifies a property of a system rather than a belief.

Mathematical Formulas:

A. Risk and composite trust

Following the risk decomposition attributed to Thomas in Section 2, exposure attaching to an identity is the product of threat, vulnerability and impact:

$$R = T \times V \times I(1)$$

The continuous trust score of identity i at time t is a convex combination of normalised signal scores drawn from the telemetry classes of Section 5:

$$CTS_i(t) = \sum_k w_k \cdot s_k(t), \quad \sum_k w_k = 1, \quad s_k(t) \in [0, 1](2)$$

B. Temporal decay and evidential update

Trust established at a verification event is not durable; in an ephemeral cloud-native environment it decays until refreshed. For an identity in risk class r :

$$T_i(t) = T_i(t_0) \cdot \exp[-\lambda_r(t - t_0)], \quad \lambda_r > 0(3)$$

Evidence accumulated between verifications is absorbed through a Beta–Bernoulli update, with a compliant observations and b violations against prior (α, β) :

$$E[T_i | a, b] = (\alpha + a) / (\alpha + \beta + a + b)(4)$$

Behavioural deviation for signal k is expressed as a standardised departure from the baseline established for the identity's peer group, mapped monotonically to a trust contribution:

$$z_k = (x_k - \mu_k) / \sigma_k, \quad s_k = \exp[-\max(0, |z_k| - \tau)^2 / 2](5)$$

C. Adaptive access decision

The decision function is ternary rather than binary, which is what distinguishes continuous assessment from discrete authorisation:

$$a(t) = \text{allow if } CTS_i(t) \geq \theta(c); \text{ step-up if } \theta_{\text{low}} \leq CTS_i(t) < \theta(c); \text{ deny otherwise}(6)$$

The threshold is not fixed but context-adjusted by resource sensitivity and corroborating context, clipped to the unit interval:

$$\theta(c) = \text{clip}[\theta_0 + \gamma \cdot \text{Sens}(r) - \delta \cdot \text{Ctx}(c), 0, 1](7)$$

D. Latency, cost and drift

The architectural constraint of Section 4 is a budget on the end-to-end decision path:

$$L_{\text{total}} = L_{\text{col}} + L_{\text{tx}} + L_{\text{inf}} + L_{\text{enf}} \leq L_{\text{budget}}(8)$$

The evaluation framework called for in Section 6 must weight the two error types asymmetrically, since a false step-up and a missed takeover are not equivalent losses:

$$C(\theta) = c_{\text{FP}} \cdot \text{FPR}(\theta) \cdot N_{\text{b}} + c_{\text{FN}} \cdot \text{FNR}(\theta) \cdot N_{\text{m}}, \quad \theta^* = \arg \min_{\theta} C(\theta)(9)$$

Concept drift in the signal distribution is monitored by a population stability index over binned scores, with a review triggered above a governance-defined level:

$$\text{PSI} = \sum_i (p_i - q_i) \cdot \ln(p_i / q_i)(10)$$

2. Theoretical Foundations of Trust Intelligence

Trust has been defined in many ways. The Oxford English Dictionary defines it as the "firm belief in the reliability, truth, ability, or strength of someone or something", while Merriam-Webster suggests "assured reliance on the character, ability, strength, or truth of someone or something". In the context of intelligent trust, trust and trustworthiness can be seen as a rationing mechanism for critical resources—enabling an individual to efficiently direct activities, be they physical or virtual, toward others who have the capability or propensity to perform a certain action and have proven that they can be trusted to do so for the past, present, or future. Trust, whilst an analogy for security, involves what an entity behaves like rather than how secure it is. In the context of Cloud computing, trust determines the strength of the relationship between the Cloud provider and the Cloud user. The greater the trust, the stronger the relationship.

Intelligent trust extends the regular meaning of trust; it combines trust, assurance, security, and risk. Risk is the expectation of loss and is a function of threat, vulnerability, and impact, with Martyn Thomas proposing the following equation to describe risk: $R = T \times V \times I$. Assurance, on the other hand, is a broad notion usually associated with confidence on the part of a stakeholder that a service, product, or system possesses certain qualities—or the degree of assurance conferred by evidence.

TABLE I. NOTATION USED IN (1)–(10)

Symbo l	Meaning	Domain / illustrative setting
$CTS_i(t)$	Continuous trust score of identity i	$[0, 1]$
$s_k(t), w_k$	Normalised score and weight of signal class k	$s_k \in [0, 1]; \sum w_k = 1$ (Table III)
λ_r	Trust decay constant for risk class r	$0.010\text{--}0.050 \text{ min}^{-1}$ (Fig. 1)
α, β, a, b	Beta prior parameters; compliant and violating observations	$\alpha, \beta > 0; a, b \in \mathbb{N}$
z_k, τ	Standardised behavioural deviation; tolerance band	$\tau \approx 2$ (peer-group baseline)
$\theta(c), \theta_{\text{low}}$	Context-adjusted allow threshold; step-up floor	$\theta_0 \approx 0.60; \theta_{\text{low}} \approx 0.35$
γ, δ	Sensitivity and corroborating-context coefficients	$\gamma, \delta \geq 0$

L_budget	End-to-end decision latency budget	150 ms (Fig. 2)
c_FP, c_FN	Unit cost of a false step-up and of a missed detection	$c_{FN} \gg c_{FP}$
PSI	Population stability index over binned scores	> 0.25 triggers model review

3. Identity-Centric Threat Detection: Concepts and Requirements

Identity-Centric Threat Detection: Concepts and Requirements

Identity-centric threat models, together with attacker/persona personas, outline a new perspective on threats, their sources, related risks, and mitigations. In cloud-native and zero-trust environments, a focused perimeter approach based on traffic patterns is no longer viable. The detection process must therefore embrace a broader and more comprehensive view, where more actors than just the obvious attackers must assume the role of adversaries. Any legitimate user can potentially become an insider threat and should be able to take advantage of his relationships, indisputably stronger than any outsider, to conduct some form of malicious activities. Multiple layers of systems should then raise alarms when any behavior that deviates from the established base threshold levels is detected, regardless of the persona that initiates the action.

The continuous trust assessment process discussed in the previous section seems to explicitly match such requirements, provided that the defined monitoring scope embraces the identification of risky or even suspicious actions undertaken by valid users operating in an authorized manner and violating compliance constraints defined by baselines. Therefore, besides trust, a secondary focus on identity-centric threat detection emerges, meaning that identity-centric threat models, attacker/persona personas, the trust lifecycle, authentication and authorization problems, and compliance constraints must become in-scope elements for any identity-centric threat detection activities applied to cloud-native and zero-trust environments.

TABLE II. IDENTITY-CENTRIC ATTACK SURFACES MAPPED TO TELEMETRY AND TRUST COMPONENTS

Attack surface	Primary telemetry signal	Trust component affected	Target detection window
Credential compromise	Authentication context, impossible-travel, device posture	Authentication assurance	Seconds
Account takeover	Session behavioural biometrics, device fingerprint drift	Behavioural continuity	Seconds

Insider misuse	Access-pattern deviation from peer-group baseline	Behavioural continuity	Minutes
Lateral movement	Identity graph traversal, token exchange sequences	Provenance	Seconds – minutes
MFA fatigue	Push-approval rate, denial-then-approval sequences	Authentication assurance	Seconds
Workload / non-human identity abuse	Service-account call profile, secret lifetime, mesh identity	Provenance	Seconds
Privilege escalation	Entitlement delta, break-glass role assumption	Authorization compliance	Seconds
Posture regression	CSPM configuration change, policy-as-code violation	Environmental assurance	Minutes – hours

4. Architectural Paradigms for Hybrid Cloud-Native Environments

Architectural decisions fundamentally shape the design of hybrid cloud-native enterprises. Centralized architectures designed to monitor and enforce security policies across all workloads can incur prohibitive latency during operation, compromising the timeliness of identity-centric threat detection. Fully distributed architectures, meanwhile, may complicate the identification of anomalous risks. Examining common factors that accelerate the adoption of cloud-native patterns such as microservices, service mesh, and Kubernetes, these architectural paradigms and constraints assist in making informed and locally optimal deployment choices.

Various considerations impact how trust-related decisions can be made and enforced across cloud-native environments. Localization of data collection or processing can optimize latency, resource utilization, and privacy-preservation and thereby make the task of modelling supported; approaches must be resilient to incomplete or faulty data sources; sensitive personal data stored in persistent databases, transmitted across external networks for correlation, or kept outside corporate control may breach data regulations; post-hoc models must faithfully decouple the training from deployment spaces, or otherwise amplify drift detection; service-monitoring infrastructures must remain used by remaining resources to ensure observability; and actors' identities must federate across clouds to validate inter-tenant communications.

TABLE III. ILLUSTRATIVE SIGNAL WEIGHTING AND REFRESH SCHEME FOR (2)

Signal class k	Weight w_k	Refresh interval	Principal governance constraint
Authentication context	0.25	Per event	Retention of device identifiers
Behavioural / session biometrics	0.20	10–30 s	Biometric data protection regimes
Access-pattern deviation	0.20	1–5 min	Peer-group definition fairness
Identity graph and provenance	0.15	1 min	Cross-tenant federation scope
Entitlement and policy compliance	0.12	On change	Segregation-of-duties rules
Environmental / posture signals	0.08	5–15 min	Cross-border telemetry transfer
Total	1.00	—	—

5. Data Sources and Signals for Continuous Trust Assessment

Identity-centric threats manifest in diverse attack surfaces, including credential compromise, identity theft, account takeovers, internal threats, lateral movement, and multifactor authentication fatigue. Addressing these requires a comprehensive telemetry architecture that generates and correlates signals reflecting security, privacy, and policy violations, and can support a range of identity-centric governance and control requirements, such as risk-based access controls, zero-trust authentication, network or data-mining user behaviors, and real-time detection of abnormal behaviors. Signals must be obtained with minimal latency and be amenable to continuous assessment, but excessive generation or data deluge can contravene compliance, governance, or data privacy constraints.

Realistic latency and accuracy thresholds are dictated by the context of use, acceptance criteria, and expected trade-offs among the risks of alert overload or missing real attacks. Well-calibrated scores also contribute to operational trust; the risks posed by the level of trust must be kept low relative to the benefits. Users, applications, and services are unlikely to use or react to trust signals that cannot be understood, so efforts to make output meaningful, even simply through adding textual descriptions, are important. Detecting conceptual drift is crucial for environments with high variance or volatile data distributions, e.g., in the context of models for intrusion detection or malware classification.

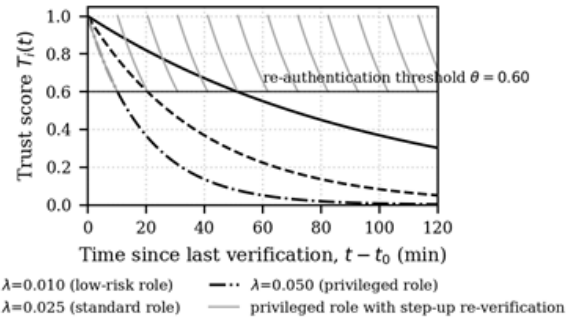


Fig. 1. Illustrative trust decay under (3) for three risk classes, with the step-up trajectory of a privileged identity re-verified whenever the score crosses $\theta = 0.60$. Synthetic; parameters assumed, not measured.

6. Models and Methodologies for Trust Inference

A diverse arsenal of modeling and methodological approaches support the attribution of trust to distributed identities. Rule-based systems fit well within the declarative nature of policy mechanisms. Parametric models express probabilistic relationships and provide natural integration points for different formalisms. Machine learning and AI techniques excel at handling unstructured data and differentiating complex concepts, albeit at the cost of interpretability. Causal models expose the underlying drivers of a phenomenon but demand costly data-collection efforts. Commonsense reasoning lends an additional layer of assurance to predictions. Methods from the decision sciences allow for the explicit quantification of uncertainty and risk.

Pipelines for trust inference can span multiple methods operating in sequence. The calibration of probabilistic models and the adaptation of all models to the evolution of identities, their capabilities, and the threat landscape merit dedicated consideration. The assessment of model quality can useholdout sets or dedicated benchmark datasets, but such evaluations remain narrow in scope compared with the myriad external threats or internal errors of an enterprise. A comprehensive performance framework must capture the different types and effects of false positives and negatives encountered in a continuous-trust-assessment context. Such considerations—including vulnerability to adversarial examples—extend naturally to the evaluation of ML/AI models and demand particular scrutiny in other approaches as well.

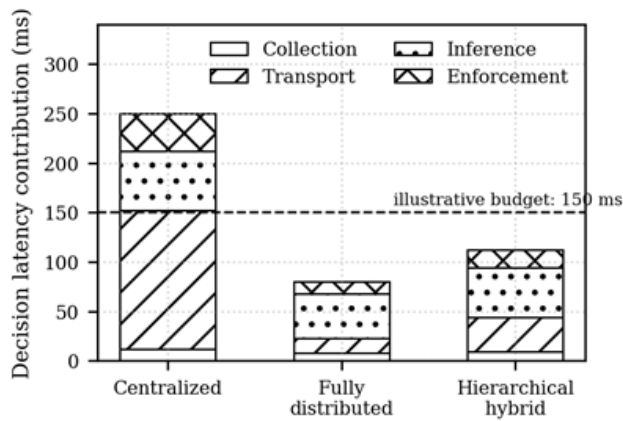


Fig. 2. Illustrative decomposition of the decision-path latency budget in (8) across the three architectural paradigms of Table IV. Values are assumed for exposition and are not benchmark measurements.

7. Conclusion

Continuous trust intelligence continuously assesses confidence in trusted identities—human users, machines, applications, and microservices. Discrete trust management has become impractical in cloud-native enterprises. Threat scenarios include insufficiently justified accesses, externally visible identity or access management data, and diverging login behavior. Cloud-native architectures rely on ephemeral resources; low-latency detection of serious incidents, such as identity theft, accounts under external control, failed compromising, or unauthorized privilege escalation, is essential.

Novel approaches for continuous trust assessment have emerged, drawing on models and methods from statistical, machine-learning, and knowledge-graph communities. Most approaches cover only specific types of trust signal or only specific aspects of trust management. Continuous trust assessment for trusted identities—human users, machines, applications, and microservices—and for actual trust management remain unexplored. Such mapping is vital for practical implementation, including the combination of ground truth with detection systems or metrics for evaluation and guided deployment. Real-time ability to recognize counterproductive signals, while also meeting the demands of policy-as-code, is essential.

REFERENCES

1. Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, 27, Article 101227.
2. Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, 110, Article 102436.
3. Kumar, S. S., Gadi, A. L., Sheelam, G. K., Kummari, D. N., Reddy Koppolu, H. K., & Pamisetty, A. (2026). AI-Driven Compliance and Audit Framework for Manufacturing Infrastructure in Automotive Connected Services and Financial Ecosystems. In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–6). IEEE. 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON). <https://doi.org/10.1109/i3ctcon68242.2026.11507231>
4. Chandramouli, R., & Butcher, Z. (2023). A zero trust architecture model for access control in cloud-native applications in multi-location environments (NIST Special Publication 800-207A). National Institute of Standards and Technology.
5. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A review and comparative analysis of relevant approaches of zero trust network model. *Sensors*, 24(4), Article 1328.
6. Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, 89, Article 103832.
7. Krishnan, M., Yandamuri, U. S., Recharla, M., Challa, K., Kolla, S. H., & Valiki, S. (2026). Adaptive Machine Learning Ecosystem for Personalized Medicine and Digital Finance: Leveraging Azure Cloud, Data Engineering, and Workflow Automation. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1–6). IEEE. 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0. <https://doi.org/10.1109/otcon69332.2026.11629728>
8. Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. *Entropy*, 25(11), Article 1595.
9. Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero trust cybersecurity: Procedures and considerations in context. *Encyclopedia*, 4(4), 1520–1533.
10. Nahar, N., Andersson, K., Schelén, O., & Saguna, S. (2024). A survey on zero trust architecture: Applications and challenges of 6G networks. *IEEE Access*, 12, 94753–94764.
11. Phiyura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to Zero Trust Architecture. *IEEE Access*, 11, 19487–19511.
12. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.
13. Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. *Sustainability*, 14(18), Article 11213.
14. Shetty, T. S., Gorle, R., Malani, S. R., Mattaparthi, R., & Kalra, M. (2026, August). AI-Driven Self-Healing Infrastructure Using Predictive Material Intelligence. In 2026 7th International Conference On Computational Vision and Bio Inspired Computing (ICCVBIC) (pp. 1876–1883). IEEE.
15. SumanPrakash, P., Ramana, K. S., CosmePecho, R. D., Janardhan, M., Churampi Arellano, M. T., Mahalakshmi, J., Bhavsingh, M., & Samunnisa, K. (2024). Learning-

driven continuous diagnostics and mitigation program for secure edge management through Zero-Trust Architecture. *Computer Communications*, 220, 94–107.

16. Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security*, 133, Article 103412.
17. Mashetty, S. M. S., & Schneider, D. S. D. (2026). Continuously Delivered Lakehouse Analytics on Azure Databricks. *European Journal of Advances in Artificial Intelligence*, 4(03).
18. Yan, X., & Wang, H. (2020). Survey on zero-trust network security. In *Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Proceedings, Part I* (pp. 50–60). Springer.
19. Itodo, C., & Ozer, M. (2024). Multivocal literature review on zero-trust security implementation. *Computers & Security*, 141, Article 103827.
20. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A comprehensive survey. *IEEE Access*, 10, 57143–57179.
21. Chandramouli, R. (2021). Attribute-based access control for microservices-based applications using a service mesh (NIST Special Publication 800-204B). National Institute of Standards and Technology.
22. Rose, S., Borchert, O., Kerman, A., & Souppaya, M. (2025). Implementing a Zero Trust Architecture: High-level document (NIST Special Publication 1800-35). National Institute of Standards and Technology.
23. National Institute of Standards and Technology. (2022). Implementation of DevSecOps for a microservices-based application with service mesh (NIST Special Publication 800-204C).
24. Subramanian, G., Premalatha, V., Peddi, R. K., Qidwai, T., Krishnamoorthi, M., & Swetha, B. (2026, August). Explainable Consumer Behavior Forecasting Using Dynamic Knowledge Graphs. In *2026 7th International Conference On Computational Vision and Bio Inspired Computing (ICCVBIC)* (pp. 579-586). IEEE.
25. National Institute of Standards and Technology. (2024). Service mesh proxy models for cloud-native applications (NIST Special Publication 800-233).
26. National Institute of Standards and Technology. (2024). A data protection approach for cloud-native applications (NIST Interagency Report 8505).
27. National Institute of Standards and Technology. (2024). Guidelines for API protection for cloud-native systems (NIST Special Publication 800-228).
28. Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A systematic literature review. *arXiv*.
29. Pigola, A., & De Souza Meirelles, F. (2025). Zero trust in cybersecurity: Managing critical challenges for effective implementation. *Journal of Systems and Information Technology*. Advance online publication.
30. Aitha, A. R., Pamisetty, V., & Recharla, M. (2026). Letter to the Editor re: “Implementation of deep learning for measurement of penile curvature on real 2D intraoperative images.” *Journal of Pediatric Urology*, 22(5), 106036. <https://doi.org/10.1016/j.jpuro.2026.106036>
31. Pigola, A., & Souza Meirelles, F. (2024). Unraveling trust management in cybersecurity: Insights from a systematic literature review. *Information Technology and Management*. Advance online publication.
32. National Institute of Standards and Technology. (2021). Zero trust networks. In *2020 cybersecurity and privacy annual report*.
33. National Institute of Standards and Technology. (2023). A zero trust architecture model for access control in cloud-native applications in multi-cloud environments (NIST Special Publication 800-207A).
34. National Institute of Standards and Technology. (2020). Zero trust architecture: Initial public draft (NIST Special Publication 800-207).
35. National Institute of Standards and Technology. (2025). Implementing a Zero Trust Architecture: Practice guide (NIST Special Publication 1800-35).