Clareus Scientific Science and Engineering
Volume 2 Issue 9 November 2025
DOI: 10.70012/CSSE.02.056
ISSN: 3065-1182

Current State of Zero Trust Assessments, Future Directions for Improvement

Citation: Shreekant Rangrej. "Current State of Zero Trust Assessments, Future Directions for Improvement". Clareus Scientific Science and Engineering 2.9 (2025): 07-16.

Article Type: Review Article

Received: October 18, 2025

Published: October 25, 2025

Shreekant Rangrej*

SAP GRC and Security Architect, Cybersecurity Expert, USA

***Corresponding Author:** Shreekant Rangrej, SAP GRC and Security Architect, Cybersecurity Expert, USA.

Abstract

The rapid advancement of digital ecosystems through the growing use of cloud, remote work, and intricate supply chains has posed a significant challenge to traditional, perimeter-based cybersecurity architectures. To address this challenge, the Zero Trust (ZT) model has emerged as a fundamental cybersecurity model based on the principles of "never trust, always verify," least privilege access, and continuous monitoring. This article provides a comprehensive examination of the status of Zero Trust implementation across industries, including the key strengths and entrenched weaknesses related to identity management, micro segmentation, telemetry, and automation. The results show that while inherent Zero Trust concepts have been widely embraced, their level of maturity remains variable due to disparate policy enforcement, legacy integration issues, and operational complexity. The convergence of DevSecOps initiatives, cloud-native applications, and benefits of artificial intelligence (AI) necessitates that Zero Trust be considered beyond the realm of static policies into adaptive, intelligence-driven architectures. Future work on developing Zero Trust principles focuses on continuous adaptive trust assessment, decentralized identity architectures, quantum-resilient methods for encryption, and privacy-preserving telemetry pipelines. The research concludes that the next generation of Zero Trust Security models must be cognitive, self-operational, and interoperable, to enable the integration of ethical design and human factors that can preserve usability in competitive marketplaces. This should be achieved in a way that provides a scalable and resilient connective infrastructure for securing digital enterprises in an increasingly dynamic threat landscape.

Keywords: Zero Trust; Identity Governance; Telemetry; Policy Orchestration; Micro-Segmentation; Phishing-Resistant Authentication; SBOM (Software Bill of Materials); Automation; Service Mesh; Credential Management; CARTA (Continuous Adaptable Risk and Trust Assessment); AI/ML (Artificial Intelligence / Machine Learning); Attestation Frameworks; Supply Chain Security; Trust Score Computation

Introduction

Zero Trust (ZT) has evolved from niche security construct to one of the most dominant engines by which one builds resilient enterprise security architectures. At its heart Zero Trust supplanting traditional “perimeter-based”, implicit assumptions with a theory of “never trust, always verify” - that is to say, all identity, device, and interactions are untrusted until proven otherwise. Yet, as it develops, the adoption of ZT has produced certain frictions: immature realizations of this theory; holes in its telemetry/automation; legacy systems which refuse modern adaptive identity constructs; and the tough tradeoffs between security and usability. The purpose of this paper is to examine the current state of Zero Trust theory and point out its immediate frictions and offer some definite technical and organizational way to sharpen the spear point of the theory within three to seven years. (The high-level references which underline the thought of this paper are the NIST Zero Trust Architecture, and CISA’s Zero Trust Maturity Model). This model [1, 3] is identified with five pillars namely devices Networks, Applications, workloads, data and identity which implies automation, transparency and governance.

By 2025 the surge of Zero Trust adoption is predicted as 60% wherein organizations will adopt the framework for cybersecurity [1] while if we see from the [3-5] the traditional model was perimeter based to continuous monitoring which in turn addresses the issues of rising cyber threats, regulatory mandates such as executive order 14028 for secure cloud adoption. A 75% of multicorporate have adopted Zero trust Principles which is up from 65% in 2023 is also indicated in global survey.

Applications in healthcare (blockchain for EHRs), finance (machine learning for fraud), IoT (micro-segmentation), and the military (inter-domain collaboration) are highlighted in a systematic evaluation of 91 publications published between 2016 and 2025. Sixty-three percent of enterprises are using Zero Trust Policy methods [6]. However, because to expenses and old systems, partial deployments continue [7].

Overview of Zero Trust Principles

The principles of the Zero Trust model are based on the philosophy that no user, device, or system should be inherently trusted. There are continuous and contextual checks of trust rather than one-time checks of trust only based on static factors like an identity credential, for instance. Elements of the approach include strong identity verification, least-privilege access, and isolation of workloads to reduce exposure to attack. Determining trust is based on dynamic elements such as device posture, user behavior, and session context as opposed to based only on static credential factors. Each principle works with and reinforces the others. Automation and telemetry operate as key components of the approach to facilitate the effective reinforcement of policy and detection of anomalies in real time. This refinement of the strategy recognizes that the patronage of perimeter-based security is being supplanted by a more relevant model founded upon a dynamic intelligence-driven protection of data, adapted for a contemporary cloud and hybrid-data environment.

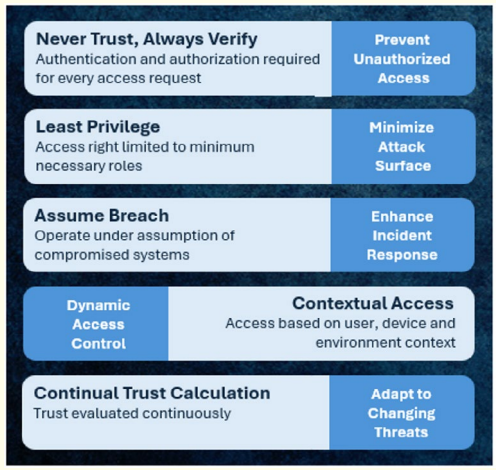

Figure 1: Zero trust principles to operating goals.

The figure 1 Illustrates the operating goals of principles of Zero Trust, such as "never trust, always verify," translate into operational outcomes such as continuous authentication, adaptive access control, and telemetry-driven decisioning. These outcomes drive achieving such things as phishing-resistant credentials, micro-segmentation, and automation of policies that cut across identity, network, and workload layers. Ultimately, Zero Trust operationalizes security through the technical alignment of security controls with dynamic risk posture, enabling strong and scalable enterprise security.

Where Zero Trust Is Today: Adoption, Maturity, And Core Patterns

Adoption Vs. Maturity

Across sectors, Zero Trust is increasingly being embraced by organizations as a guiding doctrine. Yet, adoption is frequently not the same as maturity: many of the programs are partial (identity first, or network segmentation-only) rather than holistic, and many of the programs are in "Zero Trust-in-flight" rather than accomplished. The lacuna which produces is greater conceptual acceptance in ZT, and relatively incomplete end-to-end realization of same. Thus, the organizations have a patch work of risk posture: some of the controls being sound (e.g., MFA), and some being weak, (e.g., limited telemetry to the end of effective continuous decisioning).

- Approximately 72% to 81% of companies worldwide have embraced or are in the process of putting in place Zero Trust frameworks, versus only 44% in 2022.
- 52% report having achieved full deployment with 38% of companies partially implemented.
- Larger enterprises exhibit the most maturity (86%); mid-sized companies, 68% and small firms 41%.
- Mature companies emphasize automation, integration, identity-based access control, and micro-segmentation.
- Major barriers include, amongst other things, legacy infrastructures, cultural resistance, and the failure of unified visibility around hybrid environments.

Mature ZTA decreases occurrences by 83% and breach costs by 42% ($2.83M vs. $4.88M), with recovery times being 87% faster [1, 8]. With a return on investment from reduced cleanup and enhanced user experience, regulatory demands and cyber threats that cost $10.5 trillion yearly make investment justifiable [8-10]. These advantages highlight the necessity of ongoing funding for scalable ZTA solutions.

Common Architectural Patterns

Practically, the deployments steadily shift toward compatible holdings on a handful of architectural choices:

- ***Identity Controls***: strong authentication, and identity governance as primary control plane; multi factor (MFA), single sign-on (SSO), and growing interest in "password less" tactics resistant to phishing.
- ***Micro Segmentation, ZTNA/SASE***: Network segmentation of workload, or session context: cloud-based points of policy enforcement.
- ***Telemetry driven enforcement***: logs, event, traces, metrics, and control IO data to feed risk engines to evolve and allow adaptive assessment of decisions about access.
- ***Policy orchestration***: a central policy/control plane which can enforce across a diverse number of enforcement modes (i.e., identity, endpoint, network, API gateways).

Operational Problems Being Experienced

- ***Friction with Legacy Systems***: Old applications and legacy protocols frequently don't possess telemetry hooks, or new flows of authentication leading to the expensive rewrites or brittle intermediate proxy creations.
- ***Tool sprawl, and policy drift***: Multiple, overlapping tools produce operational difficulty and withdrawn complexity and inconsistency of policies.
- ***Usability, and developer resistance***: Overly strict tracking, and slow-user behavior with CI/CD leads to concentrating users' great effort to come up with circumventions for controls.
- ***Lack of Automation***: Failure of automation in remediation, and identity lifecycle, lead human operators required to stay involved for the purpose of slowing meaningful responses.

These realities lead to Zero Trust projects producing gains but lead generally to underperformance vis-a-vis expectation, and thus demands for better road maps, better metrics, and better integrative frameworks.

Technical Pillars of Improvement

To Facilitate the Shift from Incomplete Zero Trust Implementation to Full Robust Sustainable Zero Trust Implementation.

Five technical pillars of improvement must support such a shift. They are identity, telemetry/observability, policy automation/orchestration, workload isolation, secure supply chain practices.

Identity: Passwords To Phishing Resistant Managed Credentials

Why it is important. Identity is the new perimeter as credential compromise is the cause of most breaches. Improving identity strength provides a hedge against the largest class of risk, to wit: credential theft and re-use.

Actions to take next are accelerating the widespread adoption of phishing resistant authentication (FIDO2/passkeys and hardware tokens). The large public or vendor-led initiatives which are already underway provide demonstrable evidence of this movement. Use of passkeys, and FIDOs, provides cryptographic phishing resistant attestation which materially abates the risk of credential attacks.

Accelerate automated provisioning, de-provisioning and certification of entitlements; embed in DevOps identity lifecycle governance of ephemeral developer identity provision and JIT privilege elevation.

Heighten secrecy management and wipe out all unmanaged credentials (i.e. unmanaged or local service accounts, long-lived API keys). Vaults, and the effectuation of rotation and attestable (secrets management) are valuable.

Telemetry & Observability: From Logs to Real Time Trust Signal

The Zero Trust decisions rely upon strong and timely signals about the actors, devices and behavior involved. If there is not good rich complete telemetry the rules revert to being static.

- ***Actions to take next***: Create a telemetry pipeline, which collects logs, metrics, traces, endpoint posture and network flows, assimilated in a scalable analytics layer. Instrument the applications and infrastructure with structured telemetry, and correlate identity and session metadata. Use Streaming Analytics and Feature Stores for Speed of Risk Model Creation
- ***Why This is Important:*** Streaming technology allows trust rates to be created in real time. In addition, threat intelligence and contextual enrichments (geolocation, device posture) can be intermixed in the data pipeline.
- ***What to do:*** Create measurables SLAs for telemetry completeness and latency. Only as good is the policy decision as the signals that provide it.

Policy Orchestration and Automation: Move Decisions into Code

Manual policy creates latency and discrepancies. Automation allows for swift reactions and lessens discrepancies.

Model access and enforcement policies in declarative fashion (policy as code) and store in a version-controlled repository. Adopt CI/CD for policy alterations with automated validation and canary rollouts.

Get a policy decision point (PDP) and decentralized policy enforcement points (PEP's) architecture to separate out the decision logic from the enforcement mechanism.

Create automated remediation playbooks, if trust rate is dropped below a threshold, then step-up authentication is called for automatically, sessions are quarantined and/or credentials are revoked, through approved process.

Workload Isolation and Micro-Segmentation: Decrease Blast Radius

If the intruder is successful damage containment should be assured. Micronized segmentation assures that the lateral disposition of the intruder is less.

In this case, adopt workload level segmentation through network policies, host-based controls or service meshes for east-west traffic control. Utilize identity and service to service authentication (mTLS, mutual attestation) to obviate the inherently trust worthiness between services. Couple segmentation with strong observability so as to make detection/containment fast and accurate.

Secure Software Supply Chain: Left-Sift Zero Trust

Trusting build artifacts or dependencies with no verification creates very large systemic supply chain risk as evidenced by such attacks as malicious dependency injection show that supply chain compromises can go around perimeter solutions.

Action plan would be, require signed artifacts, reproducible builds and SBOM's for critical software releases.

Integrate SBOM checks, provenance checks and vulnerability scanning into CI/CD pipeline as mandatory gates. Utilize attestation frameworks (binary signing + metadata) so that the runtime environments can interrogate the security of artifacts before evaluation.

Emerging Enabling Technologies: AI/ML, CARTA and Decentralization

Continuous Adaptable Risk and Trust Assessment (CARTA)

Gartner's approach to CARTA: Continuous Adaptable Risk & Trust Assessment is a conceptual cousin of the Zero Trust paradigm of which most security professionals are aware. CARTA more than anything stresses the risk and trust assessment on a real time basis, it elaborates also the idea that continuous controls reduce the need for static policy. Zero Trust has a futurity in systems which will in-

nately look more like the CARTA concept, or the techniques of streaming telemetry technologies will be utilized to leverage automated decisioning of the greatest potential to cause action without human intervention.

AI/ML as Driver (and Risk)

AI and ML can be applied to aid in anomaly detection, influential in speed of trust-score computation, and predicts risk before the fact for the risk manager. Concrete and practical examples of use are:

- Behavior anomaly detection based on session activity.
- Continuous automated classification of device posture and software inventory.
- Predictive techniques to aid in credential abuse or credential compromise identification.

It must be stated that AI and ML can create risk (model bias, poisoning of models, black-box management). Defensive design is undertaken with area of defensive techniques involving model transparency, robust training pipelines, and continuous verification. It is an increasingly commonplace theme in various industry articles which AI is spoken of as a necessity for the effectiveness of Zero Trust and sometimes as a matter of Good Governance.

Decentralized and Privacy-Preserving Identity

Some longer-range directions include the further use of decentralized identity models (self-sovereign identity) and increased usage of telemetry based on privacy-preserving principles (differential privacy, federated analytics), to reduce centralized points of the controllable vulnerabilities, so also allowing for greatly increased levels of user privacy as the level of monitoring increases.

Governance, Regulation, and Human Factors

Regulatory Mapping & Verification

Zero Trust must not be merely a technological exercise, map the entirety of each control to compliance and business objectives.

- Govern its compliance with requirements (data residency, SOX, GDPR, etc.). Consolidate Evidence Gathering and Attestation in Automation Playbooks to be less destructive and quicker in audits.
- CISA and NIST frameworks (for example NIST SP 800-207, and CISA Zero Trust Maturity Model) have governance established vernacular and maturity criteria that organizations should be in tune with.

Human Behavioral, Usability & Cultural Acceptance

Technical controls work greatly, provided they are accepted by users and developers. Reduce friction with:

- Phishing resistant authentication and SSO focused on ensuring secure access is less time consuming than unsecure methods.
- Security embedded into developers' workflows (pre-commit checks, policy gates in CI/CD) where security is facilitative rather than roadblocking.
- Communicating controls "why" and carrying exception workflows to amplify shadow IT risks.

Metrics that Matter

More bucketed around measurable, rather than check box compliance:

- Mean Time to Detect (MTTD) and Mean Time To Remediate (MTTR) policy violations.
- Percent of privileged actions requiring JIT elevation.
- Telemetry coverage and alert fidelity (signal-to-noise ratio).
- Percent phishing resistant cred.

A Pragmatic Roadmap: Short-term, Mid-term, and Long-term Moves

Below is a pragmatic phased roadmap for improvement of zero trust principles applicable to an organization.

- ***Short-term (0-12 months):*** An integrated security initiative is underway that includes; inventorying key assets, data flows and identities, piloting phishing-resistant MFA whilst testing high-risk and administrator credentials, the use of telemetry agents on key workloads, a just-in-time telemetry ingest with a data ingest platform, and establishing policy-as-code repositories with version access controls applied.
- ***Mid-term (12-36 months):*** The tactical roadmap includes the rollout of micro-segmentation to high-value workloads, intra-service authentication, mandatory SBOM generation and signed artifact release for all the CI/CD pipelines, a centralized PDP/PAP architecture integrated with enforcement points at IDP, ZTNA and service mesh level, with machine learning based anomaly detection with good model governance.
- ***Long-term (3-7 years):*** The strategic roadmap includes; moving to adaptive, continuous trust-scoring across sessions and services through CARTA-style automated workflows; considering decentralized identity to protect partner ecosystems and privacy-preserving telemetry reducing the surveillance risk, investing in post-quantum encryption technology for credentials and other long-lived keys and artefacts and evolving our metrics to be business risk indicators as part of a zero-trust posture that is integrated into board level reporting.

Strategies and Techniques for Tech-Hardware Compliance Trustiness

The advanced elements of the Zero Trust strategy are many and are focused toward improving the security posture overall of the enterprise. At the fundamental level, dynamic trust scores will be computed, based on continuous updated inputs, such as device posture, identity risk, session context, behavior analytics, and threat intelligence. These trust scores will be produced via streaming feature extraction and online scoring models applied to achieve levels of risk for low, medium, or high, which can then result in access actions of normal access, denial of access, session kill, or incident response workflows. CI/CD workflows will gain significance from the integrations of pre-merge static analysis, SBOM-generate, production signed builds, runtime attestation flows, and post-deploy integrity checking. Micro-segmentation will be enforced via a service mesh, which takes advantage of mutual-TLS and per-route policies, while short-lived, rotating certificate authorities are distributed from a central authority. Telemetry from the mesh is integrated into centralized analytics to provide detection of lateral movement of attack and response could be automated in abilities.

All these components work to continue real-time monitoring, authentication, and governing of both infrastructure and software development workflows, a continued alignment to the modern Zero Trust philosophy and supporting scalable, secure workflows across disparate environments.

Risks, tradeoffs, and failure modes

Zero Trust is not a one-size-fits-all solution. Common failure modes include:

- Over-reliance on a single signal (e.g. ‘device’ posture alone) leads to false negative, false-positive situations.
- Poor telemetry leads to blind-spot and brittle policy management.
- Model drift/poisoning in ML-driven decisions if training datasets are not refreshed/verified.
- Privacy-creep - admin spending excessive personal data ordering unnecessary amounts of legal supervision, and minimization.
- Operational overload resulting from having too many enforcement points carrying contradictory policies.

Risk mitigation requires layered controls, transparency in governance, and continuous measurement.

Research and Standardization Gaps That Need Work

To improve the usefulness and interoperation of Zero Trust within the community, the following standardized interfaces for trust-scores are required so that the enforcement vendors can work together to put forth uniform decisions.

It will also be necessary to adopt shared SBOM and attestation standards for legacy and cloud native aspects of the systems, and to provide detailed guidance in such areas as ML governance, this covering idea explainability, poisoning resilience, privacy-preserving telemetry and the like. Each of these can define various best-practices which will assist in legacy integration of technologies standing on proxy patterns or lightweight attestation layers for non-modern apps, while at the same time working in conjunction with the emerging public standards from such standards bodies as NIST and CISA and vendor consortia, like the FIDO Alliance/OpenSSH, assuring scalable, safe and consistent implementation in diverse environments.

Business Case: Why Go Forward Investing in ZERO Trust?

- ***Reduced breach impact***: segmentation and dynamic enforcement reduce blast radius and speed up containment.
- ***Faster incident response***: telemetry driven automation reduces MTTD/MTTR.
- ***Compliance efficiency***: automated evidence gathering and policy as code reduces audit efforts.
- ***Developer productivity***: assign by default pipelines reduce rework and permit faster releases with less manual gating.

Several market studies now produce measurable reductions in incidents and remediation costs for organizations who adopt mature ZERO Trust practices that validate the investment produces both security and operational benefits.

Future Directions of Zero Trust Improvements

Machine Learning for Trust Scoring and Behavioral Analytics

Zero Trust will increasingly be underpinned by machine learning that will be used to compute real-time trust scores based upon telemetry, context of sessions and behavioral patterns. These models will give rise to predictive risk types based upon objects that can be flagged as suspicious before there is activity. Trust will be scored through dynamic score engines to replace analytics, and this dynamic scoring will change as the behavior of devices and users alters. Streaming analytics and feature stores will become the bedrock for development of scalable low-latency real-time risk modelling. This will increase automation and reduce dependence upon manual tuning of rulesets.

Zero Trust 2.0 develops quantum-resistant cryptography (3-5 year transitions) and data-centric models with AI/ML for predictive detection (91.7% accuracy, 72 hours early) [11]. Federated protocols minimize third-party risks by 57%, while Secure Access Service Edge (SASE) convergence reduces incidents by 43%.With research emphasis in hybrid models, 6G/IoT standards, and AI-driven reactions, Zero Trust 3.0 aims to integrate resilience and make autonomous policy adjustments [4, 11]. As CARTA develops for adaptive planning, the FIDO Alliance and OpenSSF will improve supply chain security and authentication [12-14]. By tackling post-quantum risks and cognitive systems, frameworks such as CMMI-ZT minimize lawful access denials by 34% and speed up implementations by 37% addressing post quantum risks, cognitive system to decrease denials which are legitimate by 34%.

Phishing-Resistant Identities and Management of Credentials

Identities still form the bedrock of Zero Trust so enhancements in this area will be made to eliminate password-based authentication. Increased organizations will adopt phishing-resistant credentials such as FIDO2, passkeys and hardware tokens. Management of identities through the life cycle by automated governance would ensure frequent provisioning, de-provisioning, and elevation of privileges. Management of secrets will be done through vaults as well as rotation of credentials made attestable thereby rendering unmanaged service accounts and long-lived API keys outmoded. These will vastly decrease the attack surface for threats suffered from exploits of credential misuse [15]. By removing weak passwords with FIDO2 passkeys and biometrics, Phishing-resistant identities in Zero Trust Architecture (ZTA) can reduce credential theft by up to 85%. SSO and just-in-time permission from centralized identity

providers improve security while reducing user annoyance.

Legacy Integration via Lightweight Proxies and Attestation

Extending Zero Trust to legacy is a vital area that will be pursued and as expansion this will be a significant challenge that future plans and suggestions for action will take cognizance of. Non-invasive ideas will be taken into consideration to spread Zero Trust to legacy systems. There will be use of lightweight proxy patterns and attestation trees that will wrap around older applications avoiding the need for re-writing legacy as is during re-integration of legacy programs. These proxies will be used to insert hooks for telemetry and reinforce patterns of authentication that would be compatible with current and new constructs for identities. Centralized analytics will correlate legacy work with other trust types being developed in conjunction to ensure unilateral policy application. This will ensure Zero Trust coverage across hybrid types without disruption of current heavy duty legacy work.

Enforcement of Secure Software Supply Chain Processes

Zero Trust will increasingly find its way into CI/CD pipeline where it would enhance its status to keep the software supply chain intact from development through to production. Generation of SBOM's as well as signing of artefacts and reproducible build will all become necessary gateways for release to production systems. Activation of attestation during all the remaining steps will solidify the provenance of artefacts as well as the integrity and provenance of artefacts. Activation of exploits to check both vulnerabilities and check origin will all be automated and enforced across every stage intermediacy. These will mitigate against threats from dependency injections, products of code compromised and code with abnormalities that reveals illicit changes in the code.

Metrics for Board and KPIs for Business Risk

Zero Trust maturity will translate into measurable KPIs to underpin executive decision-making. The security posture will be delivered via dashboards aligning technical controls and frameworks for enterprise risk. Metrics such as trust score distribution, policy enforcement coverage, and response time to incidents will become standard. This information will help boards assess ROI on Zero Trust initiatives and prioritize investments. Ultimately, Zero Trust will evolve from technical framework into a strategic governance tool. Board metrics for ZTA monitor risk reduction (e.g., 42% lower breach costs) and maturity (e.g., >95% MFA coverage) in stated in [16] and also reflects business alignment, KPIs focus on ROI, aiming for 83% fewer incidents and <5% MFA denial rates.

Recommendations What We Should Start Doing Tomorrow

a. ***Map critical assets and identities***: know what we are trying to protect and what identities can access them.
b. ***Pilot phishing-resistant auth*** for privileged users, to be expanded as lessons learned.
c. ***Instrument telemetry*** for high value flows and centralize streaming analytics.
d. ***Adopt policy as code*** and put policies under version control, with CI/CD testing.
e. ***Mandate SBOMs and artifact signing*** for production releases.
f. ***Define measurable KPIs*** (MTTD, MTTR, percent phishing resistant identities, telemetry coverage) and tie these in with leadership reporting.
g. ***Invest in worker enablement***: reduce friction and simplify secure choices, as compared to insecure ones.

Conclusion

Zero Trust is no longer a theoretical posture. It is practical architecture that mitigates many modern risks in the environment we have both learned to work in. Its promise will only happen when organizations raise the maturity of identity practices, telemetry, automation and supply chain controls in conjunction. The next phase of Zero Trust will be defined by continuous adaptive models (CARTA), ubiquitous telemetry, AI-enhanced decisioning (with strong model governance) and standardized provenance of software artifacts. Organizations that consider it a measurable, iterative program (integrated with developer workflows, compliance challenges and business risk metrics), will have gained durable security advantages and gotten stronger on operational resiliency. For immediate

next things: focus on identity (phishing resistant authentication), telemetry completeness and automated policy orchestration. Because those three areas open the largest possible returns and lay the foundation for more advanced capabilities such as adaptive trust and attested supply chains.

References

1. National Institute of Standards and Technology. Zero Trust Architecture (NIST SP 800-207) (2020). https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
2. Gartner. Gartner Predicts 2025: Cybersecurity — Scaling Zero Trust and Resilience to Meet Growing Threats (2024). https://www.gartner.com/en/documents/5534669
3. Gartner. Top 8 Cybersecurity Predictions for 2023-2025 (2023). https://www.gartner.com/en/articles/gartnertop-security-trends-and-predictions
4. Gartner. Zero Trust Strategy Toolkit for Public Sector (2024). https://www.gartner.com/en/documents/5534669
5. Gartner. Survey Analysis: Zero Trust Adoption Trends (2023). https://www.gartner.com/en/documents/5524669
6. Gambo ML and Almulhem A. "Zero Trust Architecture: A Systematic Literature Review". arXiv (2025).
7. Osman MA., et al. "Zero Trust Cybersecurity: Critical Success Factors and a Maturity Assessment Framework". Computers & Security (2023).
8. Security Brief. Zero Trust Delivers Security Gains, but AI Adoption Lags Behind (2025). https://securitybrief.co.uk/story/zero-trust-delivers-security-gains-but-ai-adoption-lags-behind
9. Yahoo Finance. Security Leaders Embrace Zero Trust to Combat Rising Threats (2025). https://finance.yahoo.com/news/security-leaders-embrace-zero-trust-040100651.html
10. Stafford V. "Zero Trust Architecture". Forbes (2020). https://www.forbes.com/sites/forbestechcouncil/2020/10/15/zero-trust-architecture/
11. Syed Z., et al. "Zero Trust 2.0: Advances, Challenges, and Future Directions in ZTA". ResearchGate (2025).
12. FIDO Alliance. Passkeys: Phishing-Resistant Authentication (2025). https://fidoalliance.org/passkeys/
13. OpenSSF. Secure Software Supply Chain for Zero Trust (2025). https://openssf.org/
14. SSH Communications. Continuous Adaptive Risk and Trust Assessment (CARTA) (2025). https://www.ssh.com/academy/iam/carta
15. Microsoft Learn. Identity, the first pillar of a Zero Trust security architecture (2025). https://learn.microsoft.com/en-us/security/zero-trust/deploy/identity
16. Security Brief. Zero Trust Delivers Security Gains, but AI Adoption Lags Behind (2025). https://securitybrief.co.uk/story/zero-trust-delivers-security-gains-but-ai-adoption-lags-behind