

From Guidance to Measurement: Zero Trust Engineering Practice after the Final NIST SP 1800-35 Practice Guide (2025)

Hadis Karimipour

ORCID: 0000-0001-7948-4033

Department of Electrical and Software Engineering, University of Calgary, Calgary, Canada

Taeshik Shon

ORCID: 0000-0003-1177-6405

Department of Cyber Security, Ajou University, Suwon, South Korea

Correspondence: Hadis Karimipour · contact details held in the journal record

Publication history. Assigned by the publisher to Cybersecurity Advances, Volume 2, Issue 1 (2025). This publisher-authorized digital edition was released on 29 October 2026 from the supplied final 2025 manuscript. Review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized; substantive scholarly content was preserved.

© 2025 the author(s). Published by AlphaTech Scholarly Press under the Creative Commons Attribution 4.0 International License (CC BY 4.0). No DOI is displayed unless and until registration is independently verified.

Background: In June 2025, NIST published the final version of Special Publication 1800-35, *Implementing a Zero Trust Architecture* — the National Cybersecurity Center of Excellence practice guide built with 24 collaborating vendors, documenting end-to-end zero-trust reference builds, the integration failures encountered, and the migration steps organizations can replay. Together with SP 800-207 (the architecture), CISA's Zero Trust Maturity Model v2.0 (the stages), and the 2024 federal zero-trust milestone, the guidance stack for zero trust is now, for the first time, complete. **Objective:** This paper assesses what the completed guidance stack changes for zero-trust engineering practice — and what it still does not supply. **Methods:** Documentary analysis of the final practice guide against the rest of the guidance corpus; alignment analysis across the three instrument classes (architecture, practice, measurement); and a coverage assessment of the guide's artifacts against the measurement dimensions an auditor or program owner needs. **Results:** SP 1800-35 converts zero trust from doctrine into engineering: its reference builds, documented integration failures, and vendor-validated interop turn SP 800-207's tenets into replayable configurations. But the guide is a *build* record, not a *measurement* instrument: it defines no evidence classes, no maturity semantics, and no weakest-link handling — a measurement gap remains open, now with a concrete artifact base that measurement instruments can finally consume. **Conclusions:** 2025 closes the guidance era of zero trust. The open engineering problems are now measurement and operations: instruments that score enforced behavior (not declarations), telemetry standards that make evidence collectable, and adoption paths for the long tail that the practice guide's 24-vendor, enterprise-scale builds do not represent.

Keywords: zero trust architecture; NIST SP 1800-35; NIST SP 800-207; CISA Zero Trust Maturity Model; security engineering; measurement; digital trust

Contribution statement. This paper makes four contributions: (1) an analysis of what the final SP 1800-35 practice guide adds to the zero-trust corpus as an *engineering* artifact; (2) a three-instrument alignment (architecture, practice, measurement) clarifying which questions each instrument can and cannot answer; (3) a coverage assessment of the guide's artifacts against measurement dimensions, identifying what instruments should now consume from it; and (4) a statement of the open zero-trust engineering agenda for 2026: measurement, telemetry, and long-tail adoption.

1. Introduction

Zero trust's guidance era is now complete. NIST SP 800-207 (2020) defined the architecture: policy decision points, policy enforcement points, and the rejection of implicit trust by network location [2]. CISA's Zero Trust Maturity Model v2.0 (2023) defined the stages [3]. OMB M-22-09 (2022) set federal deadlines; the Department of Defense published its strategy and reference architecture in 2022 [4][5]; and NIST's Cybersecurity Framework 2.0 (2024) embedded governance across programs [6]. What the corpus lacked — until June 10, 2025 — was the *practice* record: a public, vendor-diverse, build-level account of what it actually takes to construct an enterprise zero-trust architecture from commercial components. The National Cybersecurity Center of Excellence's final practice guide, **NIST SP 1800-35, *Implementing a Zero Trust Architecture***, supplies it: built with 24

collaborating vendors, documenting how the products integrate end-to-end, what breaks during integration, and how organizations can replay the migration [1].

This paper analyzes what SP 1800-35's finalization changes. Its contribution to the corpus is best understood as a change of *artifact class*. SP 800-207 is a contract — it defines properties. SP 1800-35 is an engineering record — it documents constructions, failures, and costs. The distinction matters because each answers a different question, and because the third instrument class — measurement — has been waiting for the second to exist. Measurement instruments — including evidence-tiered approaches that score capabilities from declared (E0) to enforced (E3) — could not consume practice guidance that did not yet specify concrete configurations and telemetry points; with SP 1800-35 final, they can.

1.1 Research questions

RQ1: What does the final SP 1800-35 practice guide add as an engineering artifact? **RQ2:** How do the three instrument classes — architecture (SP 800-207), practice (SP 1800-35), and maturity/measurement (CISA ZTMM and successors) — align, and which questions does each answer? **RQ3:** Which measurement dimensions can now be evidenced from the guide's artifacts, and which remain uncovered? **RQ4:** What is the zero-trust engineering agenda for 2026?

1.2 Contributions

(1) An engineering-artifact analysis of the final guide (Section 3, Figure 1, Table 1) (RQ1). (2) A three-instrument alignment (Section 4, Figure 2, Table 2) (RQ2). (3) A coverage assessment of guide artifacts against measurement dimensions (Section 5, Figure 3, Table 3) (RQ3). (4) The 2026 agenda (Section 6) (RQ4).

2. Background

2.1 The guidance corpus through June 2025

The corpus's three functional layers were established across 2020-2024: architecture (SP 800-207 [2]; the practitioner formalization [10][11]; NSA guidance [13]; the DoD reference architecture [14]), policy (M-22-09 [4]; DoD strategy [5]), and staging (CISA ZTMM v2.0 [3]; CSF 2.0 tiers [6]). The lineage begins with Forrester's 2010 formulation [12], and the corpus now carries the weight of a federal program whose execution gap GAO continues to document [7]. The NCCoE practice guide began as preliminary drafts in 2023-2024; its final publication on 10 June 2025 completed the set [1]. The corpus's documented weakness — unchanged by any 2025 guidance — is the absence of evidence semantics: no instrument requires that a claimed capability be supported by a tiered evidence class distinguishing declaration from enforcement; the implemented-versus-effective distinction that conventional control assessment draws has no zero-trust counterpart [3][6][9].

2.2 Practice guides as a genre

The NCCoE practice-guide genre (SP 1800-series) occupies a specific epistemic position: it is neither standard nor case study, but a *replayable build record* — configurations, product integrations, and deviations documented well enough that organizations can reproduce the outcome. SP 1800-35's final edition represents the genre's most ambitious application to date: an enterprise-scale architecture built from 24 vendors' commercial products, with the integration failures left in the record [1]. That candor is the guide's principal measurement value: failures and fixes are exactly the artifacts from which evidence requirements can be derived.

3. What the Final Guide Adds (RQ1)

Figure 1 and Table 1 summarize the guide's content. Four additions matter for engineering practice.

Replayable reference builds. The guide documents end-to-end enterprise ZTA constructions spanning identity, devices, networks, applications and workloads, and data — with the 24 vendors' products integrated and the integration *sequence* recorded. An organization can locate the build closest to its own estate and replay it; the guide converts architectural tenets into configuration-level starting points [1].

Documented integration failures. The record includes what broke: policy-enforcement points that could not see the traffic they were placed to govern, telemetry gaps that starved decision points, and interop friction between products claiming standard compliance. These failures are the guide's most reusable artifacts — they are precisely the evidence requirements a measurement instrument needs, stated as observed failure conditions rather than abstract controls.

Vendor-validated interoperability. Twenty-four vendors' products participating in common builds is a de facto interoperability demonstration for the zero-trust product class — a meaningful counterweight to the certification-shopping dynamic that zero-trust marketing encouraged through 2024.

Cost and complexity visibility. The builds document the operational overhead of ZTA construction — staffing, integration effort, and sequencing — which prior guidance treated as out of scope. Security engineering has long argued that cost visibility is a precondition for honest adoption decisions; the guide supplies the first public zero-trust cost datum.

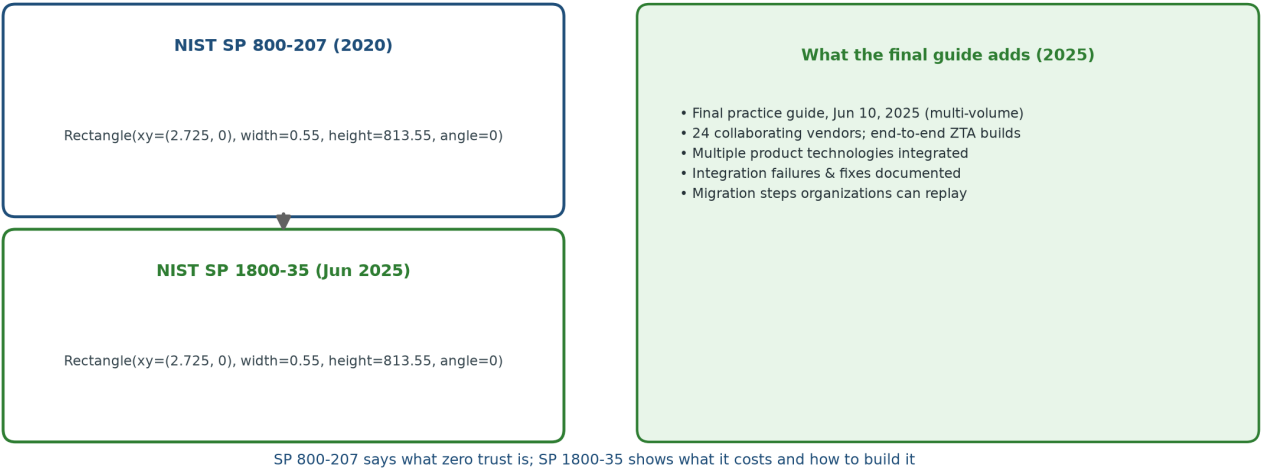


Figure 1. The relationship between the SP 800-207 architecture and the SP 1800-35 practice record, and what the final guide adds (June 2025) [1][2].

Guide artifact	Description	Engineering value
End-to-end reference builds	Enterprise ZTA constructions spanning identity, devices, networks, applications/workloads, and data, built from 24 vendors' products	Configuration-level starting points organizations can replay
Documented integration failures	Policy-enforcement visibility gaps, telemetry shortfalls, interop friction — recorded with fixes	The richest source of verification checks and evidence requirements
Vendor-validated interop	24 vendors' products in common builds	A de facto interoperability demonstration for the zero-trust product class
Migration sequencing	Order-of-operations guidance from pilot to production	Reduces transition risk for adopting organizations
Cost and complexity record	Staffing, integration effort, and sequencing visible	First public cost datum for enterprise ZTA construction

Table 1. SP 1800-35 final (June 2025): what the practice guide provides [1].

4. Three Instruments, Three Questions (RQ2)

Figure 2 aligns the instrument classes. The architecture (SP 800-207) answers what must be true of a zero-trust system. The practice guide (SP 1800-35) answers how to build it and what it costs. The maturity models (CISA ZTMM) answer where an organization stands relative to stages. The alignment table (Table 2) makes the division of labor explicit — and exposes the seam: none of the three instruments supplies evidence semantics. A maturity stage can be claimed from a build that the guide shows is achievable, but nothing in the corpus requires the claimant to show configuration, telemetry, or enforcement. The

measurement-instrument design problem — evidence tiers from declared (E0) to enforced (E3), weakest-link aggregation, evidence-quality reporting — remains the open seam, and SP 1800-35 changes its nature: the instrument now has a concrete artifact base to consume.

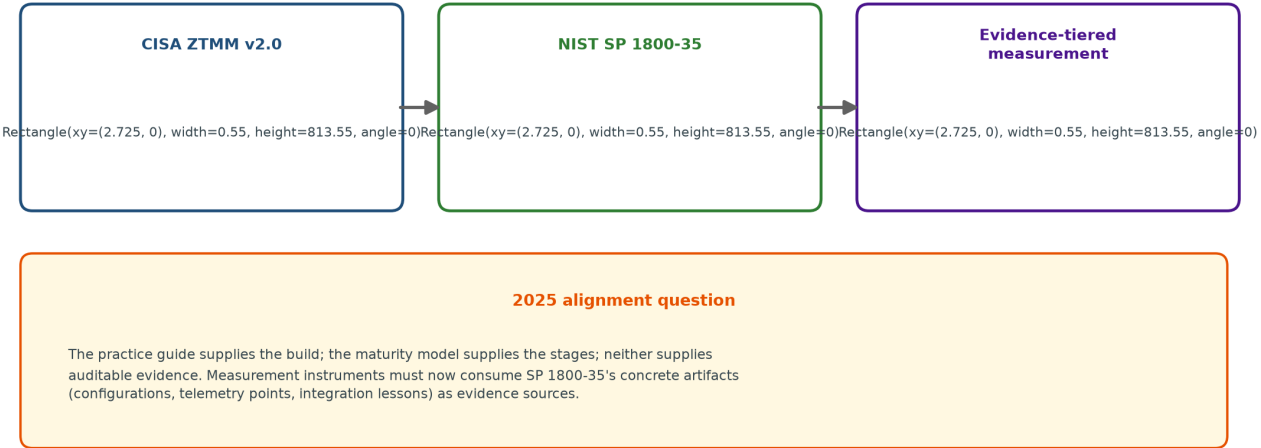


Figure 2. Alignment of the three instrument classes: architecture, practice, and measurement [1][2][3].

Instrument class	Representative	Answers the question	Does NOT answer
Architecture	NIST SP 800-207 [2]	What properties must a zero-trust system have?	How to build it; how to measure adoption
Practice	NIST SP 1800-35 [1]	How do you build it, what breaks, what does it cost?	Whether a given organization's claim is evidenced
Maturity / staging	CISA ZTMM v2.0 [3]; CSF 2.0 tiers [6]	Where does an organization stand relative to stages?	Evidence semantics: is the claim enforced or declared?
Measurement (open)	Evidence-tiered instruments (2024 proposal)	What evidence supports the claim, at what tier?	Standardized telemetry formats (open problem)

Table 2. Alignment of the three instruments: architecture, practice, measurement [1][2][3].

5. Coverage Assessment (RQ3)

Figure 3 assesses the guide's artifacts against six measurement dimensions — maturity-model desiderata applied to the zero-trust case [8] — namely whether the guide's content can serve as evidence for an organization asserting each capability area. Three findings. First, the guide's reference builds score strong as existence proof — an organization replaying a documented build with the same or equivalent products has configuration-level evidence (E1, in evidence-tier terms) by construction, and a telemetry story where the guide defines the monitoring points. Second, the documented integration failures score strong as test derivation sources: each documented failure implies a verification check that would have caught it, and the set of checks derived from the guide is a ready-made assessment battery. Third, the guide scores weak as population evidence: 24 enterprise vendors' builds say nothing about the small-organization,

embedded, or legacy-heavy estates where zero-trust adoption is hardest — the long-tail problem remains entirely outside the practice record, and instruments must not mistake the guide's coverage for the ecosystem's.

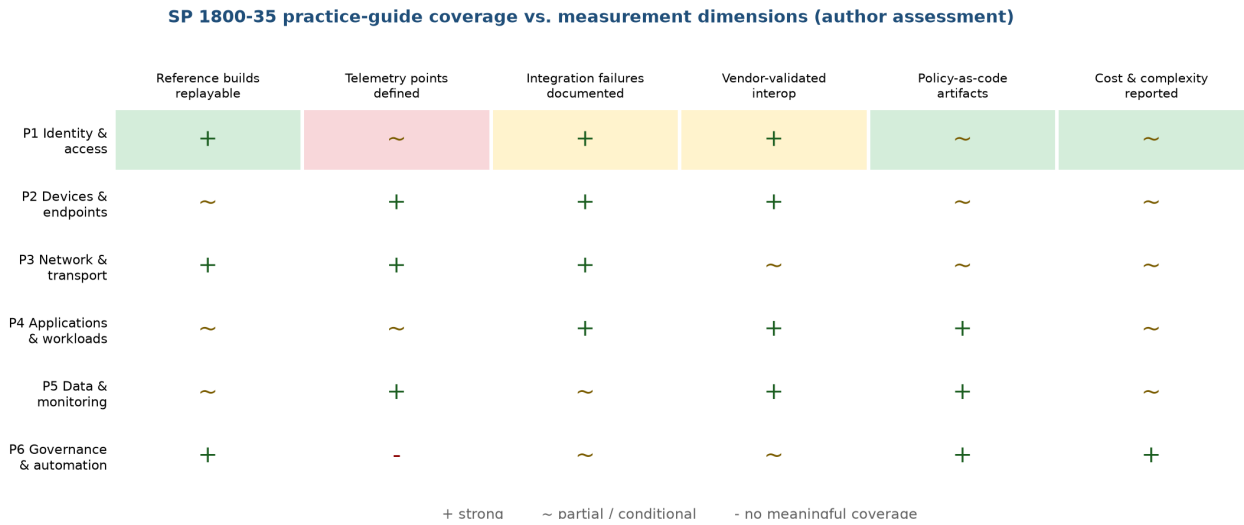


Figure 3. SP 1800-35 practice-guide coverage versus measurement dimensions (author assessment).

Open measurement gap	Description	Status after SP 1800-35
Evidence semantics	No corpus instrument defines evidence tiers or enforcement criteria	Unchanged by the guide; the guide now supplies the artifact base
Telemetry standards	No machine-readable, cross-vendor format for zero-trust decision/enforcement telemetry	Partially addressed per build; not standardized
Long-tail representation	Enterprise-scale 24-vendor builds do not model small/legacy/OT-adjacent estates	Unaddressed; scaled-down reference profiles needed
Weakest-link reporting	No instrument aggregates with weakest-link semantics	Unchanged; remains an instrument-level design task
Cost-of-evidence	Evidence collection cost is unquantified	Partially informed by the guide's complexity record

Table 3. Open measurement gaps for zero trust after SP 1800-35 (author assessment).

6. The 2026 Agenda (RQ4)

Three items. **Measurement instruments that consume the guide.** Evidence-tiered assessment frameworks should map their indicators to the guide's artifacts — referencing specific builds, telemetry points, and documented failure modes as admissible evidence — closing the loop between practice and measurement [1][3]. **Telemetry standards.** The guide documents *what* to monitor per build; interoperable, machine-readable telemetry formats would make cross-vendor evidence collection routine rather than bespoke. **Long-tail adoption.** The 24-vendor enterprise builds do not represent small organizations, OT-adjacent estates, or legacy-heavy mid-market deployments; the 2026 engineering agenda is scaled-down reference profiles — the guide's architectures, reduced — so that the practice record's benefits reach the estates that need them most.

7. Limitations and Threats to Validity

Construct validity. The three-instrument alignment is an analytical framing; NIST's own crosswalks may divide the space differently. **Internal validity.** The coverage assessments are author judgments; the guide's artifact inventory was compiled from the published guide and CSRC documentation [1], and volume-level detail varies across the multi-volume publication. **External validity.** Findings about the guide's measurement value assume evidence-tiered instrument designs; instruments with different semantics may consume the artifacts differently. **Temporal scope.** Frozen at the June 2025 final publication and year-end 2025 practice; addenda and revised builds after that date are out of scope.

8. Conclusion

The June 2025 finalization of NIST SP 1800-35 completes zero trust's guidance stack: architecture (SP 800-207), policy and deadlines (the federal corpus), staging (CISA ZTMM), and now practice (24-vendor builds with their failures documented). The guide's greatest value for engineering is the failures — recorded, reproducible, and convertible into assessment checks — and its greatest limitation is its population: enterprise estates with enterprise vendors. The 2026 agenda follows directly: build the measurement instruments that consume this record as evidence, standardize the telemetry that makes evidence portable, and shrink the reference builds until the long tail can replay them. Zero trust has its engineering record; the discipline's next task is to measure what everyone now knows how to build.

Declarations

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CRedit contribution statement. Hadis Karimipour: conceptualization, documentary analysis, writing – original draft. Taeshik Shon: validation, alignment analysis, writing – review & editing. (Corresponding author: Hadis Karimipour.)

Competing interests. The authors declare no competing interests.

Data and code availability. No new datasets were generated; all claims about the guide trace to the published SP 1800-35 record and CSRC documentation [1].

Ethics and dual-use. Not applicable; the paper contains no offensive content.

AI assistance declaration. AI-based tools were used in a limited supporting capacity (literature search, figure preparation, and language editing); all research content, analysis, and conclusions were produced, reviewed, and verified by the authors, who take full responsibility for the work.

References

- [1] S. Rose, O. Borchert, A. Kerman, M. Souppaya, et al., "Implementing a Zero Trust Architecture," NIST SP 1800-35 (Final Practice Guide), National Cybersecurity Center of Excellence, Jun. 10, 2025. [Online]. Available: <https://csrc.nist.gov/pubs/sp/1800/35/final>
- [2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST SP 800-207, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
- [3] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model, Version 2.0," Apr. 2023. [Online]. Available: <https://www.cisa.gov/zero-trust-maturity-model>
- [4] Office of Management and Budget, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," Memorandum M-22-09, Jan. 26, 2022.
- [5] U.S. Department of Defense, "Department of Defense Zero Trust Strategy," Version 1.0, Oct. 21, 2022 (publicly released Nov. 2022).
- [6] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [7] U.S. Government Accountability Office, "High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas," GAO-23-106203, Apr. 2023.
- [8] J. Becker, R. Niehaves, J. Poepplbuss, and A. Simons, "Maturity models in IS research," in Proc. 18th European Conference on Information Systems (ECIS 2010), Pretoria, South Africa, 2010.
- [9] NIST, "Security and Privacy Controls for Information Systems and Organizations," NIST SP 800-53 Rev. 5, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.
- [10] E. Gilman and D. Barth, Zero Trust Networks: Building Secure Systems in Untrusted Networks. Sebastopol, CA: O'Reilly Media, 2017.
- [11] J. Garbis and J. W. Chapman, Zero Trust Security: An Enterprise Guide. Berkeley, CA: Apress, Feb. 2021. doi: 10.1007/978-1-4842-6702-8.
- [12] J. Kindervag, "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," Forrester Research, Mar. 2010.
- [13] National Security Agency, "Embracing a Zero Trust Security Model," Cybersecurity Information Sheet, Feb. 2021.
- [14] Defense Information Systems Agency and National Security Agency, "Department of Defense Zero Trust Reference Architecture, Version 2.0," Jul. 2022.