International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 11 | Nov - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Zero Trust Identity Consolidation: A Governance Framework for Transitional Identity Risk in Hybrid Microsoft Environments

Saviona Pereira
Independent Researcher, London, UK
savu24@gmail.com

Abstract*—Enterprise identity consolidation, in which multiple Active Directory forests and Microsoft 365 tenants are merged into a single hybrid Microsoft Entra ID estate, creates a transitional period during which the identity attack surface commonly grows rather than shrinks. Mechanisms intended to be temporary, including sIDHistory attributes, dual-directory legacy authentication and migration-era standing privilege, frequently persist long after technical cutover because no governance mechanism forces their removal. AI agents acting with delegated access amplify this exposure, since they inherit whatever transitional over-privilege remains. This paper proposes Zero Trust Identity Consolidation (ZTIC), a five-phase practitioner framework (Discover, Decouple, Deploy Guardrails, De-risk Standing Access and Sustain) that treats the migration window as the highest-risk phase of the identity lifecycle. Each phase carries an explicit exit criterion and is supported by deterministic controls, namely Privileged Identity Management, Conditional Access, Defender for Identity and recurring access reviews, together with an AI-assisted intelligence layer positioned as decision support rather than autonomous access control. A five-level maturity model is provided for self-assessment. The framework is applied to an illustrative composite enterprise consolidating four forests, in which a register-driven, owner-accountable approach closed transitional sIDHistory exposure substantially faster than a reactive approach. These results are illustrative rather than statistically validated. The central contribution is a sequencing and governance discipline: transitional identity states require the same rigor, ownership and time-boxing as target states.

***Keywords*—Zero Trust, identity governance, Active Directory consolidation, privileged access management, sIDHistory, AI agent identity**

I. INTRODUCTION

Identity has replaced the network perimeter as the primary control plane for enterprise security [1], [2]. Within the Microsoft ecosystem this shift is visible in the platform itself: Conditional Access, once an add-on, is now positioned as a baseline control [3]; legacy authentication protocols are being deprecated at the platform level [4]; and Microsoft Entra Privileged Identity Management (PIM) has matured into a control that regulators and auditors increasingly expect to see evidenced rather than merely described in policy.

The enterprises adopting these controls, however, are rarely greenfield. Most have been through at least one merger, divestiture or subsidiary consolidation, and the mechanism commonly used to preserve business continuity during that consolidation, sIDHistory injection, allows a migrated security principal to retain the resource access of its pre-migration security identifier (SID) [5]. Left in place, the same mechanism undermines the Zero Trust assumptions the organization is trying to adopt: a sIDHistory attribute is, functionally, a standing trust exception that bypasses the single-identity model Zero Trust architecture assumes.

A second development makes the timing more pressing. The identity population itself is changing. Copilot Studio has automatically created a Microsoft Entra Agent ID for each new agent since May 2026 [6], [7], so agent creation is no longer a rare, centrally controlled event; it happens wherever business users build agents. A consolidation program that governs only human and service accounts will finish with a directory that already contains a growing, largely ungoverned third category of identity. At the same time, AI-assisted identity tooling has matured to the point where it can support the continuous visibility a transitional state requires. This paper treats both developments, AI as a new source of identity risk and AI as a governance aid, as part of the same consolidation problem.

The central problem is sequencing. Consolidation projects are typically scoped and funded as directory-migration exercises, with security modernization deferred until "the migration settles." In practice, sIDHistory attributes, dual-forest trusts and legacy protocol support that are meant to be temporary scaffolding routinely become permanent, because removing them requires application remediation work that has no owner once the migration project closes. Consolidation can therefore increase the attack surface for months or years relative to the pre-migration state, even though the end-state architecture is more secure on paper. Public guidance largely addresses "how to migrate with sIDHistory" and "how to configure Zero Trust controls" as separate topics; this paper treats them as one problem.

The objectives of this paper are fourfold: (i) to characterize the mechanisms by which the transitional state of an identity consolidation increases exposure; (ii) to propose Zero Trust Identity Consolidation (ZTIC), a five-phase sequencing framework with explicit exit criteria for each phase; (iii) to define a bounded role for AI as decision support within that framework; and (iv) to illustrate the framework's application through an anonymized composite case.

The scope covers consolidation of multiple on-premises Active Directory (AD) forests and/or Microsoft 365 tenants using sIDHistory as a transitional mechanism, elimination of legacy authentication (NTLM, basic authentication, unsecured LDAP binds and legacy POP/IMAP/SMTP authentication), Entra PIM for just-in-time privileged access, Conditional Access design for a consolidating identity landscape, Microsoft Defender for Identity as a detective control, and the governance needed to sustain least privilege afterwards. Non-Microsoft identity

providers, multi-cloud federation, detailed licensing cost modeling, application-level remediation techniques and non-identity Zero Trust pillars are out of scope except where they interact directly with identity controls. The intended audience is practitioners: security architects, identity and access management engineers and technical leads.

The remainder of the paper is organized as follows. Section II reviews related work and existing guidance and identifies the research gap. Section III describes the research design, formulates the problem and presents the ZTIC framework, its AI-assisted layer, its maturity model and its operational procedures. Section IV applies the framework to an illustrative composite case. Section V discusses implications, implementation considerations and limitations, and Section VI concludes.

II. LITERATURE REVIEW

A. From Perimeter to Identity

Zero Trust as an architectural principle, "never trust, always verify," with access decisions made per request on the basis of identity, device and context rather than network location, originated as an industry concept [8] and has since been codified as a reference architecture in NIST SP 800-207 [1]. Academic reviews observe that much of the knowledge base on Zero Trust remains practitioner-driven and that significant research gaps persist, particularly regarding how organizations move from existing architectures toward Zero Trust [9]. Microsoft's guidance places identity first among six foundational pillars (identity, endpoints, applications, data, infrastructure and network) [2], and positions Conditional Access, PIM and Defender for Identity as the baseline identity control set for any Entra ID tenant handling sensitive data.

B. Legacy Authentication as an Ongoing Liability

Legacy authentication protocols predate multi-factor authentication (MFA) and cannot carry the additional signals (device state, location, risk score) on which Conditional Access relies. Because they authenticate with a static credential alone, they are disproportionately exploited by credential-stuffing and password-spray campaigns. Microsoft's 2025 Digital Defense Report, covering July 2024 to June 2025, found that more than 97% of identity attacks observed across its ecosystem were password-based, and that MFA blocks over 99% of identity-based attacks when actually enforced at the point of authentication [10]; legacy protocols, by construction, cannot receive that protection. Microsoft disabled Basic Authentication by default for most Exchange Online protocols from October 2022, with SMTP AUTH for client submission on a repeatedly extended retirement timeline, currently set to be disabled by default for existing tenants at the end of December 2026 [4]. Long-lived hybrid environments nonetheless retain legacy protocol support for specific dependencies such as multifunction printers, scanners, fax integrations and line-of-business service accounts, creating a durable minority of legacy traffic that persists well past platform-level "default off" milestones.

C. Standing Privilege and the Just-in-Time Shift

Standing membership in Domain Admins, Enterprise Admins or equivalent Entra ID roles (Global Administrator, Security Administrator, Privileged Role Administrator) creates a permanently elevated blast radius: any compromise of the account's credentials or session grants the attacker its full privilege. Entra PIM's just-in-time (JIT) model, in which roles are "eligible" rather than "active" and activation requires justification, approval and/or MFA and expires automatically, is now the reference pattern for reducing this exposure. It does not eliminate the risk of a compromised session during an activation window, but it materially reduces the duration of exposure and creates an audit trail that standing membership does not.

D. sIDHistory and Multi-Forest Consolidation

sIDHistory is an AD attribute that allows a migrated principal to carry forward the SIDs of its pre-migration accounts, so that access control lists (ACLs) referencing the old SID continue to resolve without an exhaustive ACL rewrite before cutover [5]. It is the standard mechanism used by the now-retired Active Directory Migration Tool (ADMT) and its commercial successors, and remains near-universal in large consolidations because rewriting every ACL in advance is rarely feasible. The trade-off is architectural. An auditor inspecting a migrated account's current group memberships will not see the access it retains through sIDHistory, because that access resolves through SIDs of an identity that no longer exists as a distinct principal. This is an accepted practice only if the grant is time-boxed, tracked and actively decommissioned; in practice it frequently is not. No public benchmark records how many enterprises are mid-consolidation at any given time, but the pattern of multiple forests inherited through mergers and acquisitions, a cloud-first tenant strategy layered over unconsolidated on-premises identity, and Zero Trust adoption advancing faster on the cloud side than on-premises is consistently described in vendor case studies and in Microsoft's hybrid identity guidance.

E. AI Agents as a New Identity Population

Traditional application identities, usually service principals, were designed for long-term stability, known ownership and a managed lifecycle. AI agents break those assumptions: they can be created in bulk, change purpose quickly and be retired as easily as they were built. Microsoft's response is a dedicated construct, the agent identity, a special type of service principal with no credentials of its own that can carry a sponsor recording the human user or group accountable for it [6]. Conditional Access and ID Protection now extend to agent identities, including a template that blocks sign-ins from high-risk agents [7], and Entra ID Governance provides lifecycle and access-review capabilities for them [11]. For consolidation the significance is direct. The sponsor field is the agent-era equivalent of the named-owner discipline this paper argues for with sIDHistory, and an agent acting with delegated user access carries whatever that user can reach, including standing privilege that was meant to be temporary.

F. Limitations of Current Approaches

Migration tooling. ADMT and commercial migration tools are effective at moving objects and preserving access via sIDHistory, but none of the major tools reviewed in practice enforce or default to a decommissioning timeline for the sIDHistory they create; the control is opt-in and manual.

Report-only Conditional Access as a safety net. A common practice is to deploy new policies in report-only mode during migration and "tighten later." Without an owner assigned to review report-only telemetry and promote policies to enforcement, the safety net becomes a permanent gap.

PIM adoption without role-assignment cleanup. Organizations frequently enable PIM without removing pre-existing standing assignments to the same roles, so a user can hold both a time-boxed eligible assignment and a never-expiring active one. PIM's protection is then bypassed entirely, and the coexistence is not prominently flagged by default.

Defender for Identity not tuned to migration topology. Defender for Identity depends on sensors on domain controllers and per-forest configuration [12]. During multi-forest consolidation, sensor coverage commonly lags the migration schedule, newly merged forests become blind spots, and lateral-movement path analysis degrades when only part of a two-forest topology is visible.

AI-assisted policy tooling that inherits the report-only failure mode. Microsoft's Conditional Access Optimization Agent, built on Security Copilot, scans the tenant daily for new users, applications and agent identities and checks whether policies apply to them [13]. By default it creates new policies in report-only mode, a safe design that keeps administrators in control but that reproduces the failure mode above if no owner promotes its suggestions. The tooling improves detection of the problem; it does not supply the ownership needed to fix it.

G. Research Gap

Existing reference architectures and consulting methodologies give strong guidance on the target state (what a well-configured Zero Trust tenant looks like) and on migration mechanics (how to move objects between forests). What is consistently under-specified is transition-state governance: the controls, tracking and decommissioning discipline that should apply while both states coexist. The gap appears in four ways. First, there is no standard sIDHistory decommissioning service level: vendor documentation describes how to add and remove sIDHistory but rarely prescribes a time-boxed, owned and inventoried process with an exception path. Second, Conditional Access and PIM guidance assumes a single, stable identity source, not authentication that may occur against either of two directories depending on migration wave. Third, Defender for Identity deployment guidance treats on-premises AD as a stable topology, although multi-forest scenarios are acknowledged as advanced [12]. Fourth, agent identity guidance [11] implicitly assumes that the human identities agents act for are already consolidated and least-privileged, and does not address agents introduced into a directory that is still mid-consolidation. This paper addresses that gap.

III. METHODOLOGY

A. Research Design

The study follows a design-oriented, conceptual research approach. The artifact developed is a governance framework (ZTIC) together with a maturity model and an AI-assisted intelligence layer. The framework was derived from practitioner synthesis of recurring patterns observed over the author's more than 12 years of delivery experience in hybrid Microsoft 365, Entra ID and Active Directory migration and security modernization engagements, cross-referenced against vendor documentation for the product mechanics on which it relies [2]-[7], [11]-[13]. The artifact is evaluated through an illustrative application to an anonymized composite case (Sections III-G and IV). The composite does not describe any single organization and contains no audited figures; its purpose is to demonstrate how the framework's mechanisms operate, not to provide empirical validation. Prospective validation across multiple independently tracked organizations is identified as future work.

B. Problem Formulation

The specific problem addressed is that, during an active AD consolidation using sIDHistory, an organization's overall identity attack surface commonly increases relative to its pre-migration state, and this increase is frequently allowed to persist well past technical completion because no governance mechanism forces its removal. Four compounding mechanisms produce this effect.

1) Dual-protocol exposure

Both legacy and target directories must remain operational during migration and, in many designs, both accept legacy authentication to avoid breaking applications mid-cutover. The attack surface is the union of both environments' weaknesses, not the target environment's improved state.

2) Untracked sIDHistory accumulation

Each migrated identity typically carries sIDHistory entries from its origin domain. Without explicit tracking, the inventory of identities with legacy SID-based access grows throughout the project and is rarely reconciled against a decommissioning target.

3) Privilege duplication

Administrators frequently need standing access in both directories to manage the migration itself, and this dual standing privilege is rarely time-boxed or placed under the PIM controls the target environment is meant to enforce.

4) AI amplification

Agents introduced during or shortly after coexistence operate on the transitional access state rather than the intended target state. An agent acting with delegated rights cannot distinguish deliberate access from migration leftovers; it uses whatever the identity can reach, at machine speed and scale. Over-privilege that might previously have gone unexploited for months becomes available to automated workflows as soon as they are switched on.

Four root causes sustain these mechanisms. *Technically*, sIDHistory and coexistence are meant to be temporary, but tooling does not enforce temporariness and no default telemetry flags attributes that have outlived their plan. *Organizationally*, migration projects are time-boxed; once cutover is declared, the team disbands and residual cleanup falls between a closed project and business-as-usual operations that never scoped it. *Economically*, remediating applications that depend on legacy authentication or sIDHistory-resolved ACLs is often the most expensive and schedule-risky part of a consolidation, so deferral is the path of least resistance and is rarely made visible as a quantified risk. *From a regulatory standpoint*, audit cadences (for example under ISO 27001 or SOC 2) are typically annual and directed at the steady-state environment, so transitional artifacts such as sIDHistory are rarely examined unless explicitly scoped.

C. The ZTIC Framework

The gap identified in Section II-G is not a tooling gap: PIM, Conditional Access and Defender for Identity can all enforce the target state. It is a sequencing and governance gap. Nothing in the standard toolset ensures that transitional artifacts are tracked, time-boxed and closed, or that Zero Trust guardrails are applied to the legacy and target environments concurrently rather than to the target alone once it is "ready." ZTIC addresses this with five phases, each with an explicit exit criterion, so that the transition state carries the same governance discipline as the target state (Fig. 1, Table I).

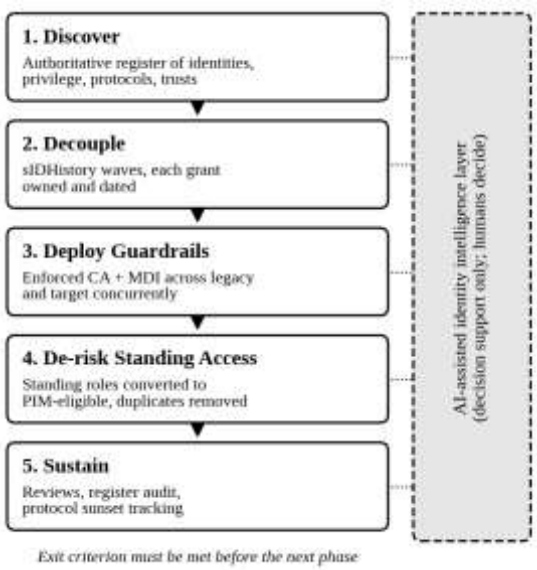


Fig. 1. The five ZTIC phases with the cross-cutting AI-assisted intelligence layer.

TABLE I. ZTIC PHASES, CONTROLS AND EXIT CRITERIA

Phase	Objective	Primary controls	Exit criterion
1. Discover	Build an authoritative inventory of identities, standing privilege, legacy protocol usage and inter-forest trust dependencies	AD/Entra ID access reviews, sign-in log analysis, protocol usage audit	Signed-off inventory covering 100% of in-scope forests/tenants; every legacy-protocol consumer and standing privileged account named and owned
2. Decouple	Migrate identities in controlled, tracked sIDHistory waves; give every grant an explicit decommission date	ADMT/migration tooling, sIDHistory tracking register	Every migrated identity has a logged register entry with an owner and a target removal date
3. Deploy Guardrails	Apply Conditional Access and Defender for Identity across both legacy and target environments concurrently	Conditional Access enforced (not report-only) for privileged roles from day one; sensors on all in-scope domain controllers	No authentication path, legacy or target, is unmonitored or outside baseline Conditional Access
4. De-risk Standing Access	Convert standing privileged assignments to PIM-eligible, time-bound activation; remove duplicates	Entra PIM, access reviews, role mining	Zero standing (non-PIM) assignments to Tier-0-equivalent roles in either environment
5. Sustain	Institutionalize the cadence that prevents transitional exceptions from becoming permanent	Recurring access reviews, register audit, protocol sunset tracking, PIM activation review	Register reaches zero outstanding entries within the committed timeline; legacy protocols disabled with only documented, time-boxed exceptions

The ordering is deliberate. Discovery comes first because every later phase depends on knowing what exists; truncated discovery is, in the composite evidence, the most common root cause of scope creep and rework. Guardrails (Phase 3) precede de-risking (Phase 4) because Conditional Access and Defender for Identity coverage must be in place while dual-directory coexistence is at its peak. This is the period of maximum exposure identified in Section III-B, and also the period when migration-related administrative accounts are most likely to be created as an expedient standing-access shortcut.

D. The AI-Assisted Identity Intelligence Layer

ZTIC treats AI as a cross-cutting intelligence layer rather than a sixth phase. In each phase, AI reduces the time needed to find, correlate and prioritize risk, while the accountable decision remains with a named human owner (Table II). AI is positioned as decision support, never as autonomous access control. The layer's value lies in compressing the interval between drift and detection: in the reactive pattern described in Section II-F, transitional risk persisted mainly because nobody was looking. An AI-assisted layer makes "nobody was looking" much harder to sustain, but it cannot make "nobody was accountable" any less damaging, which is why ownership remains the framework's central control.

TABLE II. AI-ASSISTED CONTRIBUTION AND HUMAN-RETAINED DECISIONS BY PHASE

Phase	AI-assisted contribution	Decision retained by humans
1. Discover	Correlating sign-in logs, privileged group exports and application dependencies to surface relationships requiring investigation; drafting KQL queries for the register	Sign-off of the inventory and ownership attribution
2. Decouple	Flagging sIDHistory grants approaching or exceeding their removal date; grouping grants by the dependency they preserve	Approval of any exception beyond the 90-day default

Phase	AI-assisted contribution	Decision retained by humans
3. Deploy Guardrails	Continuously checking Conditional Access coverage for new users, applications and agent identities; identifying gaps across environments	Promotion of policies from report-only to enforcement
4. De-risk	Detecting accounts holding both standing and PIM-eligible assignments to the same role; flagging unusual activation patterns	Conversion, revocation and approval-workflow design
5. Sustain	Surfacing drift between review cycles, including reappearing legacy authentication, new standing assignments and agent identities without a sponsor	Quarterly access review decisions and escalation

E. Maturity Model

To allow organizations to self-assess independently of their current ZTIC phase, a five-level maturity model provides a companion lens focused on outcomes rather than activity (Table III). Organizations in the composite evidence typically entered consolidation at Level 0–1 and exited the technical migration at Level 1–2, having achieved the target architecture without the target governance discipline.

TABLE III. ZTIC MATURITY MODEL

Level	Characteristics	Organizational posture
0 - Ad Hoc	No inventory of sIDHistory grants or legacy protocol usage; standing privilege is the default access model	Migration decisions made application by application with no central register
1 - Reactive	Inventory exists but is not maintained; Conditional Access report-only for some roles; PIM enabled for a subset of roles without cleanup of standing duplicates	Security modernization separate from, and lagging, the migration program
2 - Managed	Register maintained with removal dates; Conditional Access enforced for privileged roles; sensors cover most in-scope forests	Ownership assigned for transitional cleanup; residual risk visible and tracked
3 - Proactive	sIDHistory grants time-boxed by policy at creation; legacy protocols disabled by default with time-limited exceptions; PIM is the only path to privileged activation	Access reviews scheduled and evidenced on a fixed cadence tied to sustainment
4 - Adaptive	Transitional artifacts automatically flagged when they exceed policy age thresholds; risk-based Conditional Access adapts to real-time signals across both environments	Continuous verification; sIDHistory actively minimized across the estate, not only within projects

F. Operational Procedures

1) Discover: instrumentation before migration

Discovery combines three data sources, cross-referenced rather than used independently. The first is Entra ID and on-premises authentication logs filtered for legacy protocol usage: Entra ID sign-in logs expose a client-application field distinguishing modern from legacy authentication, while on-premises coverage requires domain controller auditing of NTLM events through Advanced Audit Policy Configuration. The second is a full export of privileged group memberships (Domain Admins, Enterprise Admins, Schema Admins and their Entra ID equivalents), attributed to named owners and business justifications. The third is a trust and dependency map covering inter-forest trusts, planned sIDHistory usage per wave and applications that perform SID-based rather than group-based access checks, since these are most likely to break if sIDHistory is removed prematurely.

The output is a single register, practically a tracked spreadsheet or, at higher maturity, a lightweight database, with one row per sIDHistory grant, per standing privileged assignment and per legacy-protocol-dependent application, each with an owner and a target closure date. This register is the backbone of Phases 2 to 5. As a starting point for the legacy-authentication inventory, the Kusto Query Language (KQL) pattern in Fig. 2, run against the SigninLogs table in Log Analytics or Microsoft Sentinel, surfaces successful sign-ins that do not use modern authentication.

```
SigninLogs
| where TimeGenerated > ago(30d)
| where ClientAppUsed in ("Other clients",
    "Exchange ActiveSync", "IMAP4", "POP3",
    "Authenticated SMTP")
| where ResultType == 0
| summarize SignInCount = count(),
    LastSeen = max(TimeGenerated)
    by UserPrincipalName, ClientAppUsed,
    AppDisplayName
| order by SignInCount desc
```

Fig. 2. Illustrative KQL query for the legacy-authentication inventory.

This is a skeleton rather than a finished detection rule. It should be tuned to the tenant's actual ClientAppUsed values and cross-referenced with on-premises NTLM audit data (Event ID 8004 on domain controllers with NTLM auditing enabled) to cover authentication that never reaches Entra ID.

2) Decouple: migration with tracked sIDHistory

The mechanics of sIDHistory migration are well documented [5] and are not repeated here. ZTIC adds a procedural requirement: no migration wave completes without a dated register entry that specifies which ACLs or applications each grant is intended to preserve, so that a later removal attempt has a concrete test list rather than an undifferentiated "see if anything breaks" exercise. A useful discipline is a default removal target of 90 days from migration, with any extension requiring a named exception approved by the identity governance owner rather than the migration project manager, whose incentives favor declaring the project complete.

3) Deploy guardrails: Conditional Access and Defender for Identity during coexistence

Rather than deploying Conditional Access in report-only mode until migration settles, ZTIC recommends three steps. First,

enforce MFA for all privileged role activations from the start of Phase 3, through PIM's MFA-on-activation requirement reinforced by a Conditional Access policy targeting the relevant roles. Second, block legacy authentication tenant-wide, with narrowly scoped, named and time-boxed exclusions rather than a blanket exclusion for "the migration period." At the policy level this is expressed as: assignment to all users and all cloud apps; client-app conditions covering Exchange ActiveSync clients and other clients (the two categories representing legacy authentication); exclusion of a single named security group (for example, sg-legacy-auth-exception) populated only with accounts identified in the register, each with a removal date; and a grant control of block. The exclusion group, not the policy, is what the monthly review examines. Third, apply sign-in risk and user risk policies through Entra ID Protection as early as licensing allows, since risk-based signals protect against credential compromise regardless of which directory the credential resolves against.

Defender for Identity sensors should be deployed to every domain controller in every in-scope forest before migration waves begin, running concurrently with Phase 2. Where licensing or infrastructure delays full coverage, the gap itself is logged as a register item with a target closure date.

4) De-risk: converting standing access to PIM-eligible

Phase 4 follows five steps designed to avoid the coexistence failure mode in Section II-F. Step one freezes new standing assignments to Tier-0-equivalent roles as an administrative policy gate. Step two inventories existing standing assignments against the register and confirms named ownership. Step three converts each to a PIM-eligible assignment with activation requirements (MFA, justification and, where role sensitivity warrants, approval) and a maximum activation duration of a small number of hours for Tier-0 roles. Step four removes the original standing assignment once the eligible assignment is confirmed functional; the interval between steps three and four should be measured in hours or days, not left open. Step five re-runs the inventory query on a recurring basis to catch new standing assignments that bypass the gate.

5) Sustain: the governance cadence

Sustainment is a recurring cadence rather than a one-time phase. It comprises quarterly access reviews of PIM-eligible assignments (Entra ID Governance can automate the request-and-attest workflow, but decisions require a human owner with context); a monthly sIDHistory register review that tracks outstanding grants against target dates and escalates overdue grants without approved exceptions; and continuous legacy authentication monitoring through sign-in analytics or a SIEM such as Microsoft Sentinel, to detect resurgence from newly onboarded applications or misconfigured service accounts.

6) Applying the AI-assisted layer in practice

Four practices operationalize the AI layer. *Natural-language investigation*: Security Copilot in Entra lets administrators investigate risky users and applications and review Conditional Access policies conversationally, which speeds triage during Discovery; the authoritative register, however, must still be built from reproducible queries so that every entry can be re-verified. *Continuous coverage checks*: the Conditional Access Optimization Agent [13] serves as an early-warning control in Phases 3 and 5, particularly for agent identities created after the initial inventory; its suggestions are assigned to the identity governance owner and reviewed on the same monthly cadence as the register, and its activity is auditable in Entra and Purview audit logs. *Agent identities as a register category*: agent identities become a fourth row type, each with a sponsor, a scoped purpose and a review date; where licensed, lifecycle workflows can automate sponsor reassignment [11]. *Validation discipline*: every AI-generated query, correlation or recommendation is treated as a hypothesis and tested against source logs before it changes a register entry or an access decision, so that every decision remains explainable without reliance on the AI's reasoning.

G. Evaluation Approach

The framework is applied to an anonymized composite enterprise constructed from patterns typical of multi-forest AD consolidation and hybrid Microsoft 365 security modernization engagements. Two trajectories are contrasted: a reactive trajectory, in which consolidation proceeds as a directory-migration project without a Zero Trust workstream, and a ZTIC trajectory, in which the five phases are applied to the residual state after month 9. The indicators examined are outstanding sIDHistory grants, standing privileged assignments, accounts using legacy authentication, Conditional Access enforcement state for privileged roles, Defender for Identity coverage and maturity level. All figures are illustrative and internally consistent; they are not drawn from a controlled study and should not be cited as benchmarks.

IV. RESULTS

A. Starting State

The composite enterprise is a professional services organization of roughly 8,000 identities, formed through the merger of four regional entities, each with its own AD forest. It set out to consolidate onto a single Entra ID tenant and a single target forest, driven by a Microsoft 365 licensing consolidation and a security modernization mandate following a control-framework audit finding on inconsistent MFA enforcement. At project start it had four forests with two-way trusts between several pairs, no central register of privileged membership, Basic Authentication enabled tenant-wide in the primary tenant, and no PIM deployment: all Global Administrator and Domain Admin-equivalent access was standing.

B. Reactive Trajectory (Months 0-9)

The migration was executed as a directory consolidation without an explicit Zero Trust workstream. sIDHistory was applied per standard ADMT practice in each of three waves. Conditional Access MFA policies for privileged roles were deployed in report-only mode in month 4, with an intention to "enforce once migration is complete." By month 9, three of four forests were consolidated, but report-only policies had not been reviewed or promoted, sIDHistory grants from all three waves remained in place with no register, and two migration-era service accounts with standing Domain Admin-equivalent access had not been reviewed for removal. In the reactive comparison scenario, where no register is introduced, sIDHistory attributes from the first wave remain unreviewed on 62% of migrated accounts at month 18, double the planned nine-month duration, and Basic Authentication remains enabled on a subset of Exchange Online connectors for approximately 14 months after documented policy asserted it was disabled tenant-wide.

C. ZTIC Applied (Months 9-18)

Following the audit finding, an identity governance owner independent of the migration team was appointed and the ZTIC phases were applied to the residual state. *Discover* (months 9–10): sign-in analysis identified legacy authentication from 340 distinct accounts concentrated in 12 applications, six traced to

scanning and fax hardware and six to older reporting tools using basic-auth service accounts. The privileged group audit identified 46 standing Domain Admin-equivalent or Global Administrator assignments, nine of which could not be attributed to a current employee. *Decouple* (month 10): approximately 1,900 existing sIDHistory grants were logged with default 90-day removal targets, and 14 were flagged for extended exception pending remediation of the 12 dependent applications, each with a named engineering owner. *Deploy guardrails* (months 10–12): legacy authentication was blocked tenant-wide with time-boxed exclusions for the six hardware-dependent and six reporting-tool accounts, and Defender for Identity sensors were extended to the remaining fourth forest. *De-risk* (months 12–15): the 37 attributable standing assignments were converted to PIM-eligible with a four-hour maximum activation and mandatory approval for Domain Admin-equivalent roles, and the nine unattributed assignments were revoked outright. *Sustain* (month 15 onward): quarterly access reviews and monthly register reviews were instituted. By month 18, 1,886 of 1,900 grants had been removed, with the remaining 14 tracked against remediation timelines and two of the 12 dependent applications remediated. Table IV summarizes the indicators.

TABLE IV. COMPOSITE CASE INDICATORS BEFORE AND AFTER ZTIC (ILLUSTRATIVE)

Indicator	**Month 9 (reactive state)**	**Month 18 (ZTIC applied)**
Outstanding sIDHistory grants	~1,900, untracked, no register	14, each a named exception with an owner
Standing Tier-0-equivalent assignments	46 (9 unattributable)	0 (37 converted to PIM-eligible, 9 revoked)
Legacy authentication	340 accounts across 12 applications	Blocked tenant-wide; time-boxed exclusions only; 2 of 12 applications remediated
Conditional Access MFA for privileged roles	Report-only	Enforced
Defender for Identity coverage	Partial; fourth forest uncovered	All forests
Transitional-state owner	None	Named identity governance owner
Maturity level (Table III)	0–1	2–3

D. Comparison of Trajectories

Table V contrasts the two approaches across the dimensions identified in Section III-B. In the ZTIC trajectory the sIDHistory register reached zero outstanding non-exception entries roughly five months after the start of Phase 4, whereas in the reactive scenario exposure remained open at 18 months and beyond. At month 18 the composite organization had reached approximately maturity Level 2–3, from an entry point of Level 0–1. The nine-month recovery duration is a modeling choice for this illustration, not a measured or generalizable outcome.

TABLE V. REACTIVE APPROACH VERSUS ZTIC SEQUENCING

Dimension	**Deferred/reactive approach**	**ZTIC sequencing**
sIDHistory grants without a removal date	Common; often the majority of grants by the 12-month mark	Zero by design; every grant logged with a target date at creation
Conditional Access for privileged roles	Report-only “until migration settles,” sometimes for a year or more	Enforced from the start of Phase 3, concurrent with migration
Standing and PIM-eligible coexistence	Common; PIM protection silently bypassed	Explicitly checked and closed in Phase 4
Defender for Identity coverage	Lags the migration schedule; blind spots in merged forests	Deployed with migration waves; any delay tracked in the register
Attack surface during transition	Union of legacy and target weaknesses, often for 12–24+ months	Bounded by per-phase exit criteria with register-driven visibility
AI agent identities	Created outside governance; inherit transitional over-privilege	Registered with sponsor and review date; delegated access bounded by de-risked privilege

V. DISCUSSION

A. Interpretation and Implications

Because both approaches eventually reach the same target architecture, the value of ZTIC is best understood as a reduction in exposure duration rather than exposure elimination. The composite illustrates the mechanism, that a tracked register with named ownership closes faster than an untracked one, rather than a predictive figure for any particular organization. ZTIC does not reduce total engineering effort; remediating sIDHistory or legacy-protocol dependencies is the same work either way. Its contribution is making residual risk visible and time-boxed rather than allowing it to become an invisible, permanent feature of the environment. The clearest lesson is organizational: every control applied in the recovery phase was available and licensed from month 0. What changed was the appointment of an accountable owner for the transitional state and a register that made its residual risk visible enough to act on.

B. Implementation Considerations

Prerequisites. Executive sponsorship is needed to freeze new standing privileged assignments and to fund the application remediation identified in Discovery; without it, Phase 4 and sIDHistory removal stall. Entra ID P2 (or equivalent) licensing is required for PIM and risk-based Conditional Access, and Defender for Identity licensing must cover every in-scope domain controller, including newly acquired forests. A named identity governance owner, independent of the migration project manager, must persist beyond project closure. AI-assisted

capabilities also carry explicit costs: Security Copilot features consume security compute units (SCUs), at least one of which must be provisioned and is billed monthly even when unused, and governance features for agent identities carry their own licensing requirements that should be confirmed before Phase 5 relies on them.

Sequencing and change management. Discovery typically takes longer than scoped, because privileged-group sprawl and legacy-protocol usage exceed initial assumptions, so contingency belongs in this phase specifically. Enforcing the legacy-authentication block requires outreach to application owners beforehand, since the most affected applications are often unowned or under-documented. Freezing standing assignments is usually the most contentious step; framing it as a time-boxed gate tied to the PIM conversion, rather than an isolated permanent change, reduces resistance.

Integration points. Sign-in logs should be exported to a SIEM, since native retention windows are typically too short for the longitudinal analysis sustainment requires. The sIDHistory register and PIM access reviews should be reconciled periodically; in the composite, separate teams maintained them, so the same application dependency appeared both as an open sIDHistory exception and as a standing-access justification without anyone connecting the two.

C. Limitations of the Framework

ZTIC does not solve the underlying economic problem: an organization without budget for application remediation will still carry long-lived exceptions, although they will be visible and tracked rather than silently accumulating. The framework presumes a single achievable source of ownership, which may be politically infeasible in highly federated post-merger organizations, and it offers no mechanism for resolving that conflict. Discovery accuracy is bounded by pre-existing logging: where NTLM auditing was not enabled before the project, some dependencies will surface only when the blocking policy breaks something, a risk the framework mitigates through narrowly scoped exceptions but does not eliminate. Aggressive PIM activation requirements can encourage workarounds, such as unnecessarily long activation windows or approval authority concentrated in a few individuals, and ZTIC offers no mitigation beyond standard approval-workflow design. Defender for Identity's lateral-movement analysis has blind spots even at full coverage and does not replace broader detection engineering.

Further limitations concern evidence and AI. The maturity model is a structuring heuristic derived from the composite pattern and general guidance, not an externally validated standard, and the figures in Section IV are illustrative rather than statistically representative. AI output can be confidently wrong, for example by reporting a dependency that does not exist or a false "safe to remove" signal; the validation discipline mitigates this, and the framework never permits AI output alone to justify removing access. Continuous AI monitoring can also create a false sense that governance is happening automatically: if teams mistake detection for remediation, the transitional state persists as in the reactive pattern, only with better dashboards. Finally, AI tooling is itself a privileged identity, since Security Copilot agents read and propose changes to access policy, and should be included in the Phase 4 privileged-access review on the same cadence as any other high-impact identity.

D. Future Outlook

Over the next three to five years, several developments are likely to narrow, without eliminating, the gap addressed here. Platform-level deprecation will continue to shrink the legacy-protocol surface, but "disabled by default" and "removed from long-lived hybrid environments" are different milestones, and the gap between them will likely persist for scanning hardware and older line-of-business systems. Entra ID Governance capabilities will increasingly absorb the register-and-track function, although assigning ownership independent of the migration team remains a governance decision rather than a tooling one. sIDHistory may become less central as organizations consolidate directly into cloud-native identity, but for the large installed base of hybrid environments it will remain relevant for years. AI-assisted governance is likely to extend into transitional-state detection, for instance automatically flagging accounts that hold both standing and PIM-eligible assignments or ageing out sIDHistory grants against policy thresholds; this is a directional expectation, not a documented capability. More significant may be the growth of agent identities themselves, which are created faster than any migration wave and will require the same ownership and time-boxing discipline.

VI. CONCLUSION

Zero Trust identity architecture and large-scale AD and tenant consolidation are usually planned as separate initiatives, but they are the same problem viewed at different points in time. A consolidation that does not explicitly govern its transitional state (sIDHistory grants, dual-directory legacy protocol support and migration-era standing privilege) can operate for months or years with a larger attack surface than either its pre- or post-migration architecture. The ZTIC framework introduces no new technical controls; its contribution is sequencing and ownership discipline, treating the migration window as a governed state with a named owner, a register of every transitional exception and explicit exit criteria.

The principal limitations are that the framework has been illustrated on a single composite rather than validated empirically, that it does not reduce remediation cost, and that it presumes resolvable ownership. Future work should apply ZTIC prospectively across multiple independently tracked organizations and test the maturity model against a broader sample. For practitioners, the immediate step is not a tool purchase but establishing the sIDHistory and standing-privilege register, with an owner independent of the migration team, before the next migration wave begins. As AI agents join the identity estate and act with the access they are given, that discipline becomes a precondition: the transitional state is the access baseline every agent will inherit.

REFERENCES

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-207, Aug. 2020, doi: 10.6028/NIST.SP.800-207.

[2] Microsoft, "Identity, the first pillar of a Zero Trust security architecture," Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/security/zero-trust/deploy/identity

[3] Microsoft, "Microsoft Entra Conditional Access: Zero Trust policy engine," Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

[4] Microsoft, "Deprecation of Basic authentication in Exchange Online," Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online

[5] Microsoft, "Troubleshoot inter-forest sIDHistory migration with ADMT," Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/inter-forest-sidhistory-migration-with-admt

[6] Microsoft, “What is Microsoft Entra Agent ID?,” Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/entra/agent-id/what-is-microsoft-entra-agent-id

[7] Microsoft, “What’s new in Microsoft Entra Agent ID,” Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/entra/agent-id/whats-new-agent-id

[8] J. Kindervag, “No more chewy centers: Introducing the zero trust model of information security,” Forrester Research, Cambridge, MA, USA, 2010.

[9] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, “Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust,” *Computers & Security*, vol. 110, Art. no. 102436, 2021.

[10] Microsoft, “Microsoft Digital Defense Report 2025,” 2025. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

[11] Microsoft, “Governing agent identities,” Microsoft Entra ID Governance, Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/entra/id-governance/agent-id-governance-overview

[12] Microsoft, “Multi-forest considerations,” Microsoft Defender for Identity, Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/defender-for-identity/deploy/multi-forest

[13] Microsoft, “Microsoft Entra Conditional Access Optimization Agent,” Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/entra/security-copilot/conditional-access-agent-optimization