The Identity Singularity 2035

Zero Trust as a strategic operating system and architectural convergence

Capgemini

Table of *contents*

Executive *abstract*

By 2035, leading enterprises can operationalize Zero Trust as a policy-driven operating model – not a toolset – built on an **Identity Fabric** that converges policy, context, signals, and enforcement *[1]*. The differentiator is not product choice; it is an industrialized control-plane design with measurable outcomes: privilege exposure time (PET), time-to-access, time-to-revoke, and blast-radius containment. This target state is achievable in stages across cloud, hybrid, and on-premises estates, with distinct transformation paths for cloud-native and legacy/OT-heavy organizations. The scope is global and standards-based.

On February 11, 2026, Palo Alto Networks completed its acquisition of CyberArk [12], one of the largest cybersecurity transactions on record and the most significant identity security deal to date. This landmark transaction validates the central thesis of this paper: that identity is no longer a component of security – it is becoming the control plane of security.

This paper is informed by practical delivery experience across enterprise IAM programs in Germany and internationally. Where it projects forward to 2035, it does so with awareness that most organizations in 2026 are still struggling with basic access recertification, orphan account hygiene, and the gap between policy intent and enforcement reality. The target state described here is directionally correct – but reaching it will require hard choices about sequencing, budget, and organizational change that no architecture diagram can resolve on its own.

01

Introduction:

The *strategic* paradigm shift

By 2035, Zero Trust should be understood not as a loose collection of technologies, but as a strategic operating system for enterprise security and digital trust. The shift from “trust but verify” to “never trust, always verify” represents a cultural and organizational transformation[1]. Zero Trust is not cloud-only; it is an architectural approach to protect resources regardless of where they run – on-premises, cloud, or hybrid.

Dissolution of silos: The rigid separation between network, identity, and application teams erodes. Security becomes a shared business responsibility.

Asset-centric protection: Enterprises stop defending abstract perimeters and define granular protect surfaces for business-critical data and processes.

Cultural transformation: Privilege is treated as transient and must be re-earned continuously based on context.

02

The Identity Fabric:

The *architectural* connective tissue

The Identity Fabric becomes the technical nervous system of this vision: a universal abstraction layer that weaves identity sources, directories, and security services into one policy-driven control plane.

Orchestrator across domains: The Fabric connects specialized solutions – such as Saviynt, Palo Alto Networks/CyberArk[12], and Illumio – into a coherent system, preventing identity silos and enabling consistent policy enforcement.

Resilience through abstraction: It decouples applications from underlying identity providers, increasing migration flexibility and improving systemic resilience.

To make the Fabric precise and implementation-grade, it is described through explicit policy planes[1]:

PAP (Policy Administration Plane): Governance, authorship, versioning, and lifecycle of policies.

PDP (Policy Decision Plane): Evaluates policies and attributes; returns permit/deny/obligations.

PEP (Policy Enforcement Plane): Enforces decisions at proxies, agents, gateways, services, and resources.

PIP (Policy Information Plane): Supplies attributes (user/device/workload/data/risk) to the PDP.

Signal Plane: Standardized signals and events (SSF [5] / CAEP [6]) plus equivalent event feeds, including latency and confidence handling.

This defines the “singularity” as the convergence of policy, context, signals, and enforcement – not as a marketing label.

AI-Assisted Operations Plane

Modern IAM platforms are introducing AI agents and copilots to improve policy hygiene, access reviews, and operational workflows. This capability changes how the Fabric is operated, but must be governed like any other control plane component [10] [11].

Policy hygiene automation: Detect policy gaps, recommend improvements, and generate policy review evidence.

Governance workload acceleration: Support access reviews and documentation tasks with controlled, auditable automation.

Non-negotiable guardrails: AI actions must be policy-bound, versioned, and evidence-backed (inputs » decision » enforcement), with deterministic rollback and clear human accountability where required.

03

The *convergence* of IGA and PAM

The first major step toward convergence is the fusion of identity governance and administration (IGA) and privileged access management (PAM). The completion of the Palo Alto Networks/CyberArk transaction *[12]* – one of the largest cybersecurity acquisitions on record – is a definitive market signal that this convergence is no longer theoretical.

Role hierarchy erosion: In cloud-native and DevOps environments, almost every identity can become privileged. A unified system manages the full lifecycle – from standard users to highly privileged admin-bots – in one coherent data model.

Zero standing privileges (ZSP): Permanent admin rights are eliminated. Privileges exist only just-in-time (JIT) for a task-specific duration.

Operational hardening

Privilege exposure time (PET): A core metric measuring the total time privileged entitlements are effective; ZSP/JIT makes PET measurable and reducible.

Exception lifecycle: Every exception is time-bound, justified, risk-rated, technically enforceable (PDP/PEP), and audit-ready.

PET operational definition: PET is computed over a defined measurement window (T) as the sum of durations where privileged entitlements are effective (human and non-human), counted from grant/elevation to revoke/expiry (including break-glass and exceptions). PET can be reported per identity, per asset tier (e.g., Tier-0/Tier-1), and as an aggregate; optional weighting by entitlement criticality can be applied.

04

The ecosystem of giants: The *Strategic* Matrix 2035

Capability domain	Fabric plane(s)	Leading vendors (2026+)	Strategic direction 2035
Identity governance and administration (IGA)	PAP, PDP, PIP	SailPoint, Saviynt, Palo Alto Networks/CyberArk, Okta (OIG), One Identity	Converges with PAM into unified identity lifecycle; AI-driven access reviews and policy recommendations
Privileged access management (PAM)	PDP, PEP, PIP	Palo Alto Networks/CyberArk, BeyondTrust, Delinea, Saviynt	ZSP/JIT becomes default; PET as core metric; full NHI lifecycle coverage
Identity provider / access management (IdP/AM)	PDP, PEP, PIP, Signal Plane	Microsoft Entra ID, Okta, Ping Identity	SSF/CAEP interoperability *[5] [6]*; continuous authentication; identity threat detection (ITDR)
Non-human identity (NHI) / workload identity	PEP, PIP, Signal Plane	SPIFFE/SPIRE *[13]*, HashiCorp Vault, Palo Alto Networks/ CyberArk (Conjur), Venafi (now CyberArk)	Secretless architecture; cryptographic attestation replaces static credentials
Microsegmentation / Zero Trust segmentation	PEP	Illumio, Zscaler, Palo Alto Networks, Akamai (Guardicore)	Label-driven containment; automated blast-radius reduction on signal triggers
Security service edge (SSE) / ZTNA	PEP, Signal Plane	Zscaler, Palo Alto Networks (Prisma), Netskope	Cloud-delivered enforcement; replaces VPN; identity-aware transport
Policy engine / authorization	PAP, PDP	OPA/Rego (CNCF)*[14]*, Styra, PlainID, Axiomatics	Policy-as-code becomes standard; ABAC*[4]* replaces static RBAC; testable, versioned, audit-ready
Signal / ITDR / XDR	Signal Plane, PIP	CrowdStrike, Microsoft Sentinel, Palo Alto Networks (Cortex), SentinelOne	Real-time risk signals feed policy decisions; SSF/CAEP *[5] [6]* standardized event delivery

Note: Vendor placement reflects capability focus as of early 2026. The PANW/CyberArk acquisition *[12]* closed on February 11, 2026; operational integration of these platforms is in its earliest stages and will take years to reach full interoperability. Claimed end-to-end integration outcomes should be validated against actual deployment evidence, not marketing roadmaps. Market consolidation will continue to reshape boundaries. Enterprises should evaluate vendors against their specific Fabric plane requirements, not against marketing categories.

05

Non-human identities (NHI): **The new** *majority*

A key complexity driver is the explosion of machine identities. Reported enterprise telemetry shows NHIs can materially outnumber human identities: Entro Labs reports a ratio of 144:1 in H1 2025 *[2]*; Veza reports 17:1, depending on definitions and scope *[3]*. The direction is consistent – NHIs dominate the identity landscape.

Method note: Ratios depend on telemetry scope, identity definitions, and customer population bias (often cloud-forward); enterprises should measure their own NHI baselines and lifecycle hygiene.

Secretless architecture: Static secrets (API keys, passwords) are systematically eliminated. Workload identity is verified via cryptographic attestation using frameworks such as SPIFFE/SPIRE *[13]*.

Infrastructure binding: Bots are tied to workload identity and enforcement domains (including segmentation). Anomalies trigger automated privilege revocation and containment via defined enforcement actions.

NHI governance discipline

Inventory and ownership: Every workload identity has a clear owner and lifecycle (create/rotate/revoke) with bounded policy scope.

Attestation and issuance: Workload/node attestation, issuance of short-lived identities (SVIDs), rotation/TTL, and federation patterns *[13]*.

Incident response cascade: Signal » policy decision » enforcement (session termination, token attenuation, segmentation quarantine) as a formal, auditable process.

AI agents as NHI: Delegation, provenance, and control planes

Delegation as the primary control problem: Agent authority must be expressible as a bounded delegation chain (who delegated what, for which scope, for which duration), not as an unconstrained service account with broad rights.

Token mediation and on-behalf-of patterns: Delegated execution patterns map to OAuth token exchange semantics (subject/actor separation) *[7]*, preventing ambiguous “agent acts as user” privilege escalation.

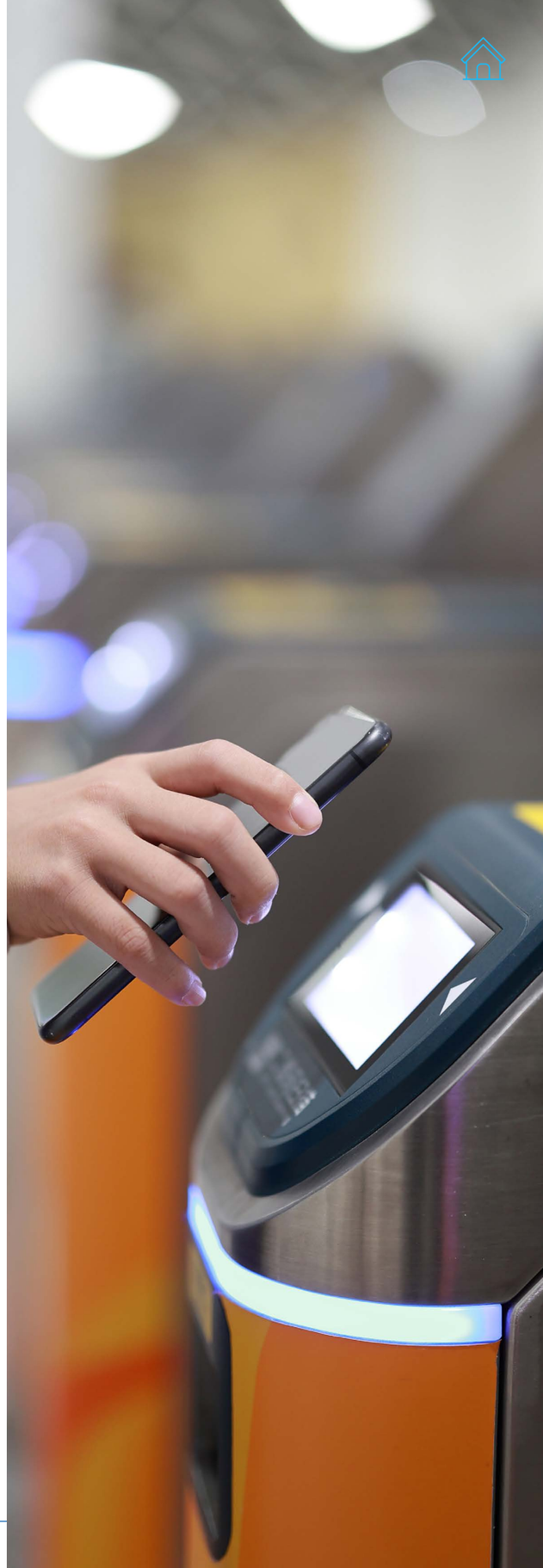
Fine-grained authorization beyond coarse scopes: Structured authorization requests *[8]* enable intent- and resource-bounded permissions that are testable, versioned, and auditable within the PAP/PDP/PEP model.

Provenance and runtime attestation: Agent identity requires verifiable lineage (creator, environment, attestation state, policy version, signal inputs, enforcement outcome) to make decisions and audits defensible at scale.

Enforceable tool and data boundaries: Policy must explicitly constrain tool access, data access, and output handling; violations trigger deterministic attenuation and containment actions.

Agent runtime risk as a signal source: Prompt injection, insecure output handling, and tool misuse patterns *[9]* are treated as operational security risks that feed the Signal Plane and drive near-real-time policy attenuation.

AI governance integration: AI risk management practices *[10] [11]* must be integrated into the same lifecycle discipline (authoring, testing, deployment, monitoring, exception handling) that governs identity and privilege.



06

Authorization evolution:

From RBAC to ABAC and policy-centric *control*

The singularity requires moving beyond static roles.

RBAC collapse: Role-based models trigger role explosion and become unmanageable in dynamic environments.

ABAC and policy-centric authorization: Access decisions rely on attributes (risk score, location, device health, data sensitivity) evaluated against explicit policies *[4]*.

Policy-as-code: Declarative policy engines such as OPA/Rego[14] enable consistent enforcement, testing, versioning, and auditability across the Fabric.

A word of caution: Policy-as-code introduces its own operational risks. A misdeployed policy update to the PDP can silently deny legitimate access at scale or – worse – silently permit access that should be blocked. Production environments need canary deployment patterns, automated policy diffing against the approved PAP baseline, and deterministic rollback mechanisms before policy-as-code can be trusted as the primary enforcement path. We have seen environments where a well-intentioned policy refactor broke emergency break-glass access for 48 hours because the rollback procedure had never been tested under load.

Terminology clarification

ABAC is defined in NIST SP 800-162 *[4]*, including PDP/PEP/PIP/PAP architectural concepts. **Policy-centric authorization** describes the operational model: policy is externalized, versioned, testable, and audit-ready; ABAC provides attribute logic within that model.

07

Technological synergy:

Shared signals and real-time *security*

The operational backbone is the OpenID Shared Signals Framework (SSF) *[5]* and the Continuous Access Evaluation Profile (CAEP) *[6]*, enabling standardized event delivery and near-real-time access attenuation across cooperating systems.

A continuous risk score (continuous authentication) becomes operationally meaningful only when enforcement is consistent. The Signal Plane must also carry AI-agent runtime risk events as first-class signals that can trigger policy attenuation during execution *[9]*.

If risk drops below a threshold (e.g., an EDR malware signal), the Fabric executes coordinated enforcement across identity control, SSE transport, and segmentation domains – terminating sessions, attenuating tokens, and containing workloads.

Interoperability and migration realism

If SSF/CAEP *[5][6]* is not end-to-end available, the Signal Plane runs on equivalent event/risk feeds with explicit latency, confidence, and revocation SLAs. The target state remains SSF/CAEP interoperability; implementation is staged.

A persistent blind spot in practice: Revoking a session at the IdP does not guarantee that the session is terminated at the resource layer. SaaS applications with long-lived tokens, cached OAuth grants, or independent session stores will continue to honor the old credential until their own token lifetime expires. This is the gap SSF/CAEP is designed to close – but until adoption is universal, enterprises must audit token lifetimes at every resource boundary and implement forced re-authentication triggers as a compensating control. In our experience, this is the single most common revocation failure pattern in enterprise environments, and is routinely missed during tabletop exercises.

08

Technological synergy:

Shared signals and real-time *security*

Unified Zero Trust becomes an enterprise efficiency driver when outcomes are engineered and measured:

OPEX reduction: Consolidation of point solutions and removal of manual ticket workflows can materially reduce operational burden; realized impact depends on baseline, scope, and maturity and must be decomposed into measurable cost blocks.

Reduced blast radius: Segmentation-driven containment localizes impact, reducing recovery scope and downtime.

Business enablement: Automated, policy-driven access improves time-to-market and reduces friction in secure delivery.

Board-grade measurement framework

Cost blocks: VPN/remote access operations, JML ticketing, recertification/audit overhead, incident containment/recovery, tool duplication.

KPI/SLO reference table

The following table defines recommended program-level controls. Target values represent mature-state benchmarks for cloud-native environments; legacy/OT paths should define intermediate SLOs aligned with their transformation stage.

KPI / Metric	Target: Cloud-native (Path A)	Target: Legacy/ OT (Path B)	Measurement	Business impact
Time-to-access (P50)	< 15 min (automated)	< 4 hours	Request to provisioned entitlement; decision enforcement latency	Developer velocity; workforce productivity
Time-to-access (P95)	< 2 hours	< 24 hours	95th percentile incl. approval workflows and exception paths	Exception handling; SLA compliance
Mean time to revoke	< 1 hour	< 8 hours	Trigger (leaver/signal) to entitlement removal at PEP; includes IdP propagation AND resource-layer session termination	Blast-radius reduction; compliance
Privilege exposure time (PET)	Trending↓ QoQ; Tier-0 near-zero	Baselined;↓YoY	Sum of active privileged entitlements per tier (grant/elevation to revoke/ expiry)	Core Zero Trust maturity indicator
Policy drift rate	< 3% deviation	< 10% deviation	Deployed policy vs. approved PAP baseline (automated diff)	Governance integrity; audit readiness
Audit findings rate	Zero critical; ≤ 3 moderate	Trending to zero critical	Identity-related findings per audit cycle	Regulatory compliance; board confidence
Blast-radius scope	Contained to single segment	Contained to zone/ VLAN	Lateral spread in incident/ simulation (red team, tabletop)	Recovery cost; downtime
NHI lifecycle coverage	> 95% with owner + rotation	> 70% inventoried; rotation staged	Ratio of discovered NHIs with assigned owner and active rotation policy	Supply chain security; credential hygiene

09

The CISO transformation:

From tool manager to risk *architect*

The future CISO designs digital trust rather than operating isolated tools. The mission shifts toward orchestrating a unified trust operating model:

Policy ownership: Business risk owners together with technical platforms and control owners.

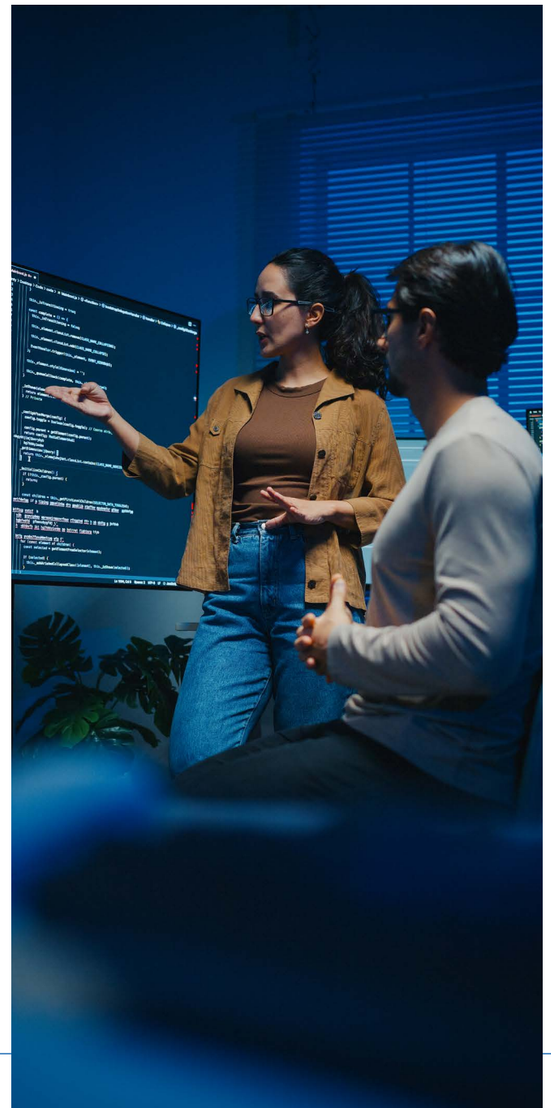
Policy lifecycle: Author » test (policy-as-code) » deploy » monitor (signals) » audit/controls testing» exception handling with enforced sunset.

Assurance: Proof of the enforcement chain (PDP decision + PEP enforcement + signal inputs) as an auditable artifact.

Realism 2035:

Two-speed *security*

10



The reality remains bifurcated - 2035 is a target state planning horizon, not a promise of uniform adoption.

Modern cloud-native enterprises: Approach the target state with tight integration across Entra, SSE transport, and segmentation.

Legacy-heavy organizations (OT/public sector): Constrained by long hardware lifecycles and dependency chains. The viable strategy is staged modernization via proxy/gateway patterns, segmentation-first containment, and governance overlays, with incremental expansion of the Signal Plane.

Transformation paths

Path A (cloud-native): Fabric-first, policy-as-code, NHI-first, SSF/CAEP *[5][6]* interoperability prioritized.

Path B (legacy/OT): Proxy/gateway patterns, segmentation-first containment, governance overlay, staged Signal Plane.

Common dependencies: Asset discovery, data classification, identity quality, and telemetry coverage (required for ABAC *[4]* and signals).

How Capgemini enables the *Identity Singularity*

The Identity Singularity 2035 is not a vendor deliverable – it is a transformation that requires strategic clarity, implementation discipline, and deep platform expertise. As a global leader in cybersecurity consulting and system integration, Capgemini is uniquely positioned to guide enterprises through this convergence.

Strategic advisory and roadmap design

Capgemini's IAM practice has extensive global delivery experience spanning IGA, PAM, and Zero Trust architecture across regulated industries. Our approach begins with identity maturity assessment and produces actionable transformation roadmaps aligned to business risk – not technology hype. Recent initiatives include rapid-assessment programs that exploit existing Microsoft Entra ID capabilities to accelerate governance outcomes without costly re-platforming.

Platform implementation at scale

We partner with all major IAM vendors – including Palo Alto Networks/CyberArk, SailPoint, Saviynt, Okta, Microsoft, and Ping Identity – and deliver end-to-end implementation, integration, and migration services. Our certified engineering teams bring deep technical expertise in PAM vault architecture, IGA connector development, ABAC policy design, and NHI lifecycle automation.

Hybrid and OT transformation

For legacy-heavy and OT environments – common across German manufacturing, automotive, and critical infrastructure – Capgemini delivers Path B transformation: proxy/gateway patterns, segmentation-first containment, and governance overlays that enable staged modernization without disrupting production systems. Our global OT/IoT cybersecurity practice brings specialized expertise in securing environments where the Identity Fabric must coexist with decades-old infrastructure.

Managed identity services

Beyond project-based transformation, Capgemini provides managed identity services through its global cybersecurity operations capabilities, offering continuous operational support for identity infrastructure, monitoring, and incident response. This ensures that the Identity Fabric remains operational, compliant, and adaptive to evolving threats.

Conclusion

The 2035 target state expresses a clear direction: identity is no longer a component of security – it becomes the control plane of security *[1]*. The convergence of policy, context, signals, and enforcement – implemented through an Identity Fabric – reduces privilege exposure, improves containment, and enables business velocity. The Palo Alto Networks/CyberArk acquisition *[12]* confirms this trajectory at the highest level of industry commitment.

For legacy-heavy environments, this remains an incremental transformation, not a one-step conversion. For all enterprises, the question is no longer whether to pursue this convergence, but how fast and through which path.

Terminology and definitions

Acronym	Full Term
ABAC	Attribute-based access control
AI	Artificial intelligence
CAEP	Continuous Access Evaluation Profile
CI/CD	Continuous integration / continuous delivery
EDR	Endpoint detection and response
IGA	Identity governance and administration
IdP	Identity provider
ITDR	Identity threat detection and response
JIT	Just-in-time
JML	Joiner / mover / leaver
KPI	Key performance indicator
MTTR	Mean time to repair/recover
NHI	Non-human identity
OPA	Open policy agent
OBO	On-behalf-of (delegated execution pattern)
PAM	Privileged access management

Acronym	Full Term
PAP	Policy Administration Plane
PDP	Policy Decision Plane
PEP	Policy Enforcement Plane
PIP	Policy Information Plane
PET	Privilege exposure time
RBAC	Role-based access control
RFC	Request for Comments (IETF standard)
SLO	Service level objective
SPIFFE	Secure Production Identity Framework for Everyone
SPIRE	SPIFFE Runtime Environment
SSE	Security service edge
SSF	Shared Signals Framework
SVID	SPIFFE Verifiable Identity Document
TTL	Time to live
ZTNA	Zero Trust Network Access
ZSP	Zero standing privileges

References

[1]NIST SP 800-207 (Zero Trust Architecture)

[2]Entro Labs NHI Secrets Risk Report (H1 2025; 144:1 ratio)

[3]Veza State of Identity & Access Report 2026 (machine identity ratios)

[4]NIST SP 800-162 Update 2 (ABAC)

[5]OpenID Shared Signals Framework (SSF) 1.0

[6]OpenID CAEP 1.0 (Final)

[7]OAuth 2.0 Token Exchange (RFC 8693)

[8]OAuth 2.0 Rich Authorization Requests (RFC 9396)

[9]OWASP Top 10 for LLM Applications (Version 2025)

[10]NIST AI RMF 1.0 (NIST AI 100-1)

[11]NIST GenAI Profile (NIST AI 600-1)

[12]Palo Alto Networks: Completes acquisition of CyberArk (February 11, 2026)

[13]SPIFFE: Secure Production Identity Framework for Everyone (CNCF)

[14]Open Policy Agent (OPA) - CNCF Graduated Project

Author:

Thomas Willner

Head of Identity & Access Management,
Capgemini Germany

thomas.willner@capgemini.com

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real | www.capgemini.com

For more details contact:

cybersecurity.in@capgemini.com

Capgemini