

Identity-First Security for SAP Landscapes with NTT DATA and OKTA

How the Okta Identity Control Plane
Secures SAP Against Modern Attacks – and
Replaces SAP IdM for Good



Executive Summary

Identity has become the dominant attack vector across the enterprise. Three independent threat intelligence sources reach the same conclusion: the 2025 Verizon Data Breach Investigations Report identifies stolen credentials as the most common initial access vector, present in 22% of breaches; the IBM X-Force Threat Intelligence Index 2025 reports that 30% of all intrusions begin with valid, compromised accounts; and CrowdStrike's 2026 Global Threat Report finds that 82% of detections involve no malware at all – adversaries log in rather than break in. SAP landscapes concentrate this risk: they ship with well-known default accounts, and the attack techniques most relevant to SAP – valid accounts, privilege abuse, hidden users – are identity techniques. The most effective place to detect, contain and eradicate these attacks is therefore not the network perimeter and not the endpoint: it is the identity layer itself.

This white paper makes the case for identity-first SAP security. It shows how Okta as the unified identity control plane across SAP and the entire application landscape turns identity from the primary attack surface into the primary line of defense. A single Okta API call can suspend a compromised user, cascade SCIM deprovisioning into SAP and terminate active sessions in every connected application that supports Universal Logout. We demonstrate this in a largely automated response workflow that, in tests in our environments, neutralizes a compromised privileged user account within minutes, with SAP-native detection by SIEM and orchestration by SOAR solutions feeding the Okta control plane. The timing is decisive. SAP Identity Management ends mainstream maintenance in 2027 (extended maintenance until 2030), and every SAP customer must choose a successor solution. That choice determines whether identity remains a fragmented legacy burden or becomes the strategic control plane described in this paper. Our recommendation is unambiguous: Okta Identity Governance, adopted through a phased coexistence strategy and delivered by NTT DATA, is the platform on which to build.

Introduction: Identity is the SAP Attack Surface

SAP systems sit at the core of the enterprise. They drive financial transactions, manage supply chains, process HR data and execute mission-critical operations which is precisely why they attract sophisticated adversaries. A single successful intrusion can yield access to financial records, trade secrets and operational controls.

Look closely at how these intrusions actually happen, and a pattern emerges, one that is now documented across the industry's most-cited threat research. The 2025 Verizon DBIR, built from more than 22,000 analyzed incidents, names stolen credentials the single most common initial access vector at 22% of breaches, with 88% of basic web application attacks involving stolen credentials. IBM X-Force finds that 30% of all intrusions in 2024 began with valid, compromised accounts, and describes the shift in one phrase: attackers are logging in, not hacking in. CrowdStrike's 2026 Global Threat Report completes the picture – 82% of detections in 2025 involved no malware whatsoever, because adversaries increasingly rely on stolen credentials, native tools and existing administrative functions. Notably, these three research teams do not coordinate: Verizon draws on partner-submitted incident data, IBM on its own incident response caseload and CrowdStrike on endpoint telemetry. Three independent datasets, one conclusion.

SAP landscapes concentrate this identity risk structurally. SAP systems ship with well-known default accounts such as the built-in superuser SAP*, DDIC and EARLYWATCH, whose standard passwords frequently survive into production due to missed hardening steps. Adversaries abuse valid accounts and unsecured RFC connections, create hidden users for persistence and escalate privileges to disable audit logging. Cloud-connected deployment models, like S/4HANA, BTP, RISE or GROW, have widened the attack surface, but the entry point remains constant: identity. In the MITRE ATT&CK mapping presented later in this paper, the single most consequential technique for SAP is "T1078 – Valid Accounts". The attacker's favorite tool is a working login.

This has a strategic consequence. If identity is the attack surface, then identity must be the control plane. An SAP security architecture that treats identity as an afterthought, e.g. by using a provisioning utility running quietly in the background, will always respond too slowly, because containment and eradication ultimately mean one thing: taking the attacker's identity away, everywhere, at once. Only a unified identity platform that spans SAP and every other connected application can do that in minutes rather than hours.

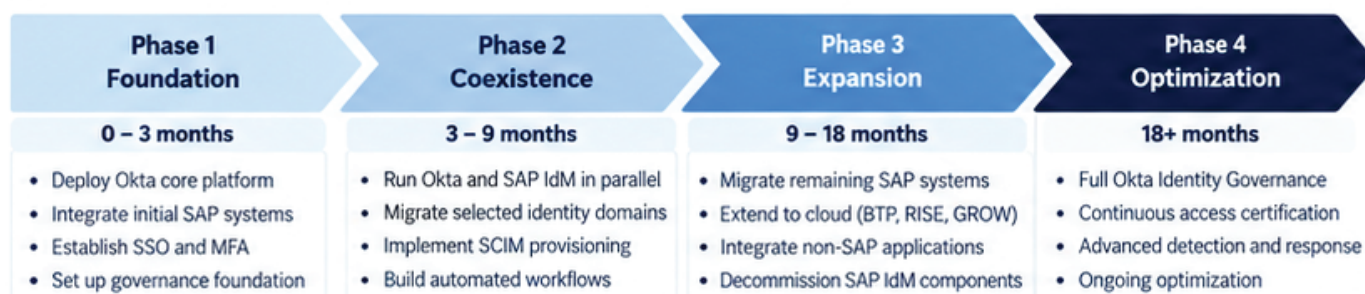
The timing for this architectural shift could not be better. SAP Identity Management, the platform that has quietly run SAP identity for two decades, ends mainstream maintenance in 2027 (extended maintenance until 2030). Every SAP customer must choose a successor solution. This paper shows why that successor should be Okta and what becomes possible once it is.

The Coexistence Strategy: Migrating at Your Own Pace

The SAP IdM sunset should not be treated as a disruptive rip-and-replace event. It is a strategic opportunity to modernize on your own schedule. A coexistence strategy lets organizations maintain full operational continuity while migrating governance functions incrementally from SAP IdM to the Okta Identity Governance (OIG) platform. Phased integration keeps critical business processes stable while identity controls are progressively unified. Through the Okta SAP On-Prem Connector, centralized governance begins on day one by replacing migration anxiety with immediate, measurable visibility across the hybrid environment well before the legacy system retires. Every SAP customer must choose a successor. This paper shows why that successor should be Okta, and what becomes possible once it is.

Replacing SAP IdM with Okta: Phased Coexistence Strategy

A pragmatic path to a modern, unified identity control plane.



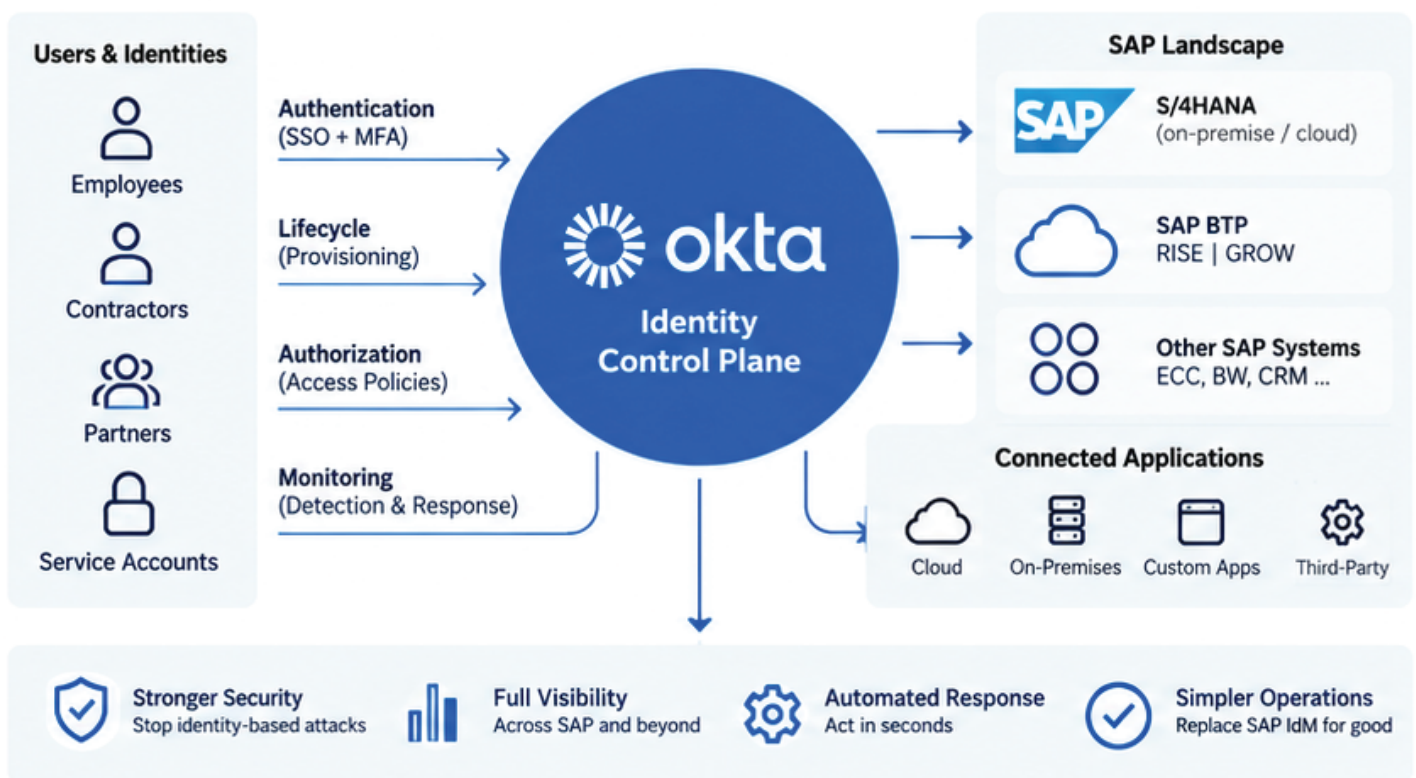
Result: A unified, modern identity control plane with Okta – replacing SAP IdM for good.

The Okta Identity Control Plane for SAP

Okta Workforce Identity Cloud is the architectural center-piece of identity-first SAP security. It is not one tool among several, it is the layer through which every user, every session and every entitlement in the landscape is governed.

Identity-First Security for SAP Landscapes

Turn identity from the primary attack surface into the primary line of defense.



Five capabilities make it the control plane that SAP defense requires.

① Universal Directory: one identity, everywhere.

Okta Universal Directory consolidates identities from HR systems, Active Directory, SAP and cloud applications into a single authoritative source. Every user has exactly one identity with one lifecycle state – which means every security decision, from login policy to incident response, operates on complete, current information. During an investigation, an analyst pulls a user's 30-day activity history and group memberships from one place instead of five.

② Lifecycle Management: automation as prevention.

Okta Lifecycle Management automates the joiner-mover-leaver process end to end. HR events in SuccessFactors or Workday trigger provisioning workflows; access changes propagate instantly to SAP and every other connected application via SCIM. The security value is preventive: orphaned accounts, over-provisioned users and dormant privileged access – the raw material of T1078 attacks – are eliminated systematically rather than hunted down manually. This is the core function Okta performs today, delivered with an accuracy, speed and audit trail that legacy tooling cannot match.

③ Adaptive MFA and ThreatInsight: risk-based access decisions.

Okta's adaptive Multi-Factor Authentication evaluates every authentication in context (device, location, network, behavior) and escalates friction only when risk demands it. Okta ThreatInsight adds network-level threat intelligence drawn from across Okta's global customer base, blocking authentication attempts from known-malicious infrastructure before a password is ever tested. For SAP, this means the default-credential attack described later in this paper can be stopped at the front door.

④ Universal Logout: containment across the entire landscape.

When an account is compromised, revoking future logins is not enough. The attacker's existing sessions and cached tokens must die too. Okta Universal Logout turns containment from an application-by-application scramble into a centralized action by sending a server-to-server termination signal to supported SAML and OIDC applications and session termination endpoints. While instantaneous revocation of all access tokens isn't always technically possible, this capability ensures that any application configured with a Universal Logout endpoint immediately receives the command to kill active sessions and refresh tokens, drastically reducing the attacker's window of opportunity.

⑤ Okta Identity Governance: continuous least privilege.

Okta Identity Governance (OIG) extends the control plane with access certifications, access requests and separation-of-duties guardrails. Entitlements are reviewed continuously rather than annually; access is requested and approved through governed workflows rather than tickets and emails. Combined with Xiting XAMS for SAP-native SoD analysis at the authorization-object level, OIG closes the governance loop that regulators like NIS2, CRA and/or SOX increasingly demand.

Knowing the Adversary: MITRE ATT&CK® for SAP

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques built from real-world observations. Mapping SAP-specific threats to ATT&CK's common taxonomy gives security teams a shared language for threat hunting, sharpens detection rules and makes attack progressions recognizable early.

The following table illustrates common SAP attack scenarios and their MITRE ATT&CK mappings, giving security teams a quick-reference guide for incident analysis and classification. Note how many of these techniques are related to identity techniques – valid accounts, privilege abuse, hidden users – and therefore fall squarely within the reach of the identity control plane:

SAP Attack Scenario	MITRE ATT & CK Tactic	Technique ID & Name	SAP Context Example
Exploiting default or weak SAP credentials	Initial Access/Credential Access	T1078 – Valid Accounts	Use default SAP* password to log in
Abusing unsecured RFC connections	Execution/Lateral Movement	T1021 – Remote Services (RFC)	Remote call to execute sensitive transactions
Uploading and running malicious ABAP programs	Execution/Persistence	T1059 – Command & Scripting Interpreter (ABAP)	Malicious report in production
Exploiting SAP Gateway or Message Server	Initial Access	T1190 – Exploit Public-Facing Application	Gateway misconfigurations exploited
Reading sensitive tables without authorization	Collection	T1005 – Data from Local System	Unauthorized SE16H queries
Modifying ABAP code to conceal fraud	Defense Evasion	T1565.001 – Stored Data Manipulation	Altered payment routines
Scheduling malicious background jobs	Persistence/Execution	T1053.003 – Scheduled Task/Job: Cron (SAP Jobs)	Nightly data exfiltration job
Pivoting via SAPRouter misconfiguration	Lateral Movement	T1021 – Remote Services	SAPRouter tunnel into restricted network
Exporting large datasets via SAP transactions	Exfiltration	T1030 – Data Transfer Size Limits	Mass download from SE16
Disabling SAP audit logs	Defense Evasion	T1070 – Indicator Removal	Audit logs cleared to cover tr

Embedding this mapping into incident response ensures that SAP investigations follow the same structured discipline as the rest of the enterprise. An analyst who spots an unusual batch job in SM37 can immediately cross-reference T1053.003, recognize a likely persistence tactic and recommend targeted remediation including the identity-layer question that matters most: which account created this job, and should that account still exist?

Structuring the Defense: NIST Incident Response for SAP

The NIST Incident Response framework (Special Publication 800-61) provides the process backbone: Prepare, Detect and Analyze, Contain, Eradicate, Recover and learn from every incident. Applying it to SAP requires translation into SAP-specific terms and, in an identity-first architecture, each phase gains an identity dimension.

Preparation means hardening configurations and baselining normal operations, but it equally means preparing the identity layer: SCIM provisioning between Okta and SAP configured and tested, Universal Logout enabled, lifecycle policies defined and approval gates for account reactivation in place before they are ever needed.

Detection must be tailored to SAP's architecture including Security Audit Logs, transports, change documents, correlated with OS and database events and enriched with SAP-specific threat intelligence. SAP-native monitoring flags the anomaly; the identity platform supplies the context that makes it actionable: is this access pattern normal for this user, this role, this time?

Containment and eradication in SAP must be rapid yet surgical as indiscriminate shutdowns can cause as much damage as the attack. Here the identity control plane is the difference between hours and minutes: disabling the compromised account, revoking entitlements and killing sessions are identity operations, executed once in Okta and enforced everywhere. Recovery then restores verified access through governed re-provisioning, and post-incident lessons flow back into detection rules, lifecycle policies and access baselines.

Amplifying the Loop: Agentic AI and SOAR

Agentic AI and SOAR platforms give the NIST lifecycle speed and scale. AI correlates SAP logs, RFC activity, network telemetry and business context to detect multi-stage attacks and infer attacker objectives; SOAR automates triage, evidence collection and response execution. In the architecture presented here, SOAR plays the orchestrator role, and the most consequential action in every playbook it runs is an identity action: a call to the Okta API. Detection can come from many sensors; response converges on the identity control plane.



Identity-First Response in Practice: T1078 – Valid Accounts

What follows demonstrates the operational agility an organization gains once Okta is established as the identity control plane. The scenario: an attacker exploits default or weak SAP credentials as addressed by MITRE ATT&CK technique “T1078 – Valid Accounts”. SAP systems ship with the built-in super-user SAP*, whose default password frequently survives into production. The attacker authenticates from an unusual IP address, typically off-hours, then executes privileged transactions such as SU01 or SE16 to create backdoor accounts, extract data or disable audit logging.

The defense chain: SecurityBridge provides SAP-native detection inside the ABAP stack, SOAR orchestrates the playbook – and Okta executes the response. Upon detecting the anomaly, SecurityBridge forwards alerts via webhook into the SOAR solution. Here the alert becomes enriched and, once the risk score exceeds threshold, the Okta Lifecycle Management API is called for action. That single call suspends the user, cascades SCIM deprovisioning into SAP and triggers Universal Logout in every connected application that supports it. In tests in our environments, detection to full identity lockout took minutes, with no SAP restart required.



Phase ① Preparation: Wiring the Control Plane

The decisive work happens before any incident. On the Okta side, the SAP application integration is configured with SCIM provisioning, so that any lifecycle state change in Okta cascades automatically to SAP role and session management. Universal Logout is enabled on the SAP SAML integration for instant, cross-application session termination. Role-based human approval gates are defined for the one action that must never run unattended: account reactivation during recovery.

On the detection side, SecurityBridge deploys natively inside the SAP ABAP stack with over 100 preconfigured signatures – SAP* logins, off-hours access, geo-anomalies – and enables HyperLogging, its tamper-proof forensic logging capability, on the Security Audit Log (SM20), system log (SM21) and user change documents (SCU3). The SOAR solution connects the two worlds: webhook intake from SecurityBridge, bi-directional API connectors to Okta (Lifecycle Management and SCIM), SAP (RFC/BAPI), ServiceNow and the SIEM.

Phase ② Detection and Analysis: Context from the Identity Layer

SecurityBridge fires a critical alert when three signals converge: SAP* authenticates successfully, the source IP is outside all known corporate ranges and privileged transaction SU01 executes within 90 seconds of login. The SOAR platform ingests the alert and enriches it with context that comes from the identity platform: the user's 30-day activity history and group memberships from Okta Universal Directory confirm whether this pattern is genuinely anomalous. SIEM correlation, threat-intelligence reputation checks and ServiceNow change-ticket cross-referencing complete the picture. Shortly afterwards, a case record carries a composite risk score and the ATT&CK T1078 tag

Phase ③ Containment: Surgical, Not Disruptive

Because SAP is business-critical, containment is surgical: SOAR triggers Okta to lock the SAP* account via BAPI_USER_LOCK, blocks the source IP at the SAP network ACL layer and terminates the active session – targeted actions that stop the attacker without touching legitimate users. The SAP Basis team is notified via Slack with a one-click escalation option; a ServiceNow P1 ticket opens with the full timeline. SecurityBridge re-verifies the landscape – SAP* locked on all SIDs, no additional suspicious sessions, no unauthorized transports – while HyperLogging preserves the forensic trail.

Phase ④ Eradication: One API Call, Total Lockout

Eradiation is where the identity control plane shows its full value. SOAR calls the Okta Lifecycle Management suspend endpoint. That single call executes a three-step sequence. First, the user can no longer authenticate to any Okta-protected application, SAP included. Second, the Okta SAP integration propagates an “active=false” SCIM PATCH to SAP, stripping the user's entitlement and session access with no manual administrator action. Third, Universal Logout invalidates every active SAML and OIDC session across the landscape so cached tokens in the attacker's hands become worthless, and lateral pivot is cut off. The attacker is locked out of everything, everywhere, within minutes.

In parallel, SOAR revokes SAP roles from backdoor accounts created during the attack window, removes unauthorized SAP* entries from USR02 and clears the attacker IP from allowlists. SecurityBridge runs a post-incident hardening scan validating “login/no_automatic_user_sapstar = 1” on all SIDs and checking other default accounts for unchanged passwords.

Phase ⑤ Recovery: Governed Re-Provisioning

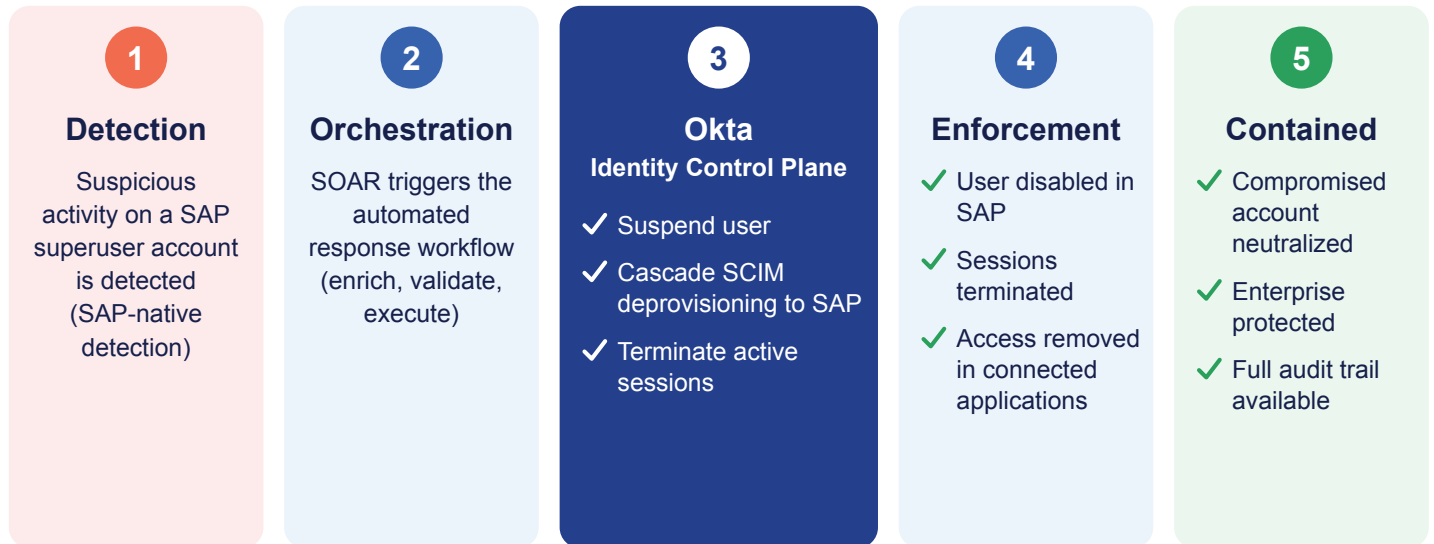
Recovery runs through a human-approved workflow – the approval gate defined in Phase 1. Once a senior analyst confirms eradication, SOAR calls the Okta unsuspend endpoint. Okta's SCIM integration re-provisions SAP access, but restores only the roles confirmed legitimate by the change-document review; anything created or modified during the attack window is excluded. Recovery through the identity control plane is not merely fast; it is governed, so attacker-created access can never slip back in. Business owners are notified, the P1 closes with MTTR metrics and an auto-generated compliance package, and monitoring for default accounts stays elevated for 30 days.

Phase ⑥ Post-Incident: The Loop Closes

The SOAR platform now reconstructs the timeline, maps each step to T1078 sub-techniques and proposes MTTR improvements – for example, querying Okta for the user's authentication state before executing BAPI_USER_LOCK so the two lockout mechanisms sequence optimally. SecurityBridge adds a zero-tolerance rule: any default system account authenticating from any IP triggers an immediate critical alert. And the identity layer learns too: lifecycle policies, access baselines and MFA policies are tuned based on what the incident revealed.

Automated Response to a Compromised SAP Superuser

From detection to full containment, in minutes.



Result: Attack neutralized in minutes, not hours

Compromised user suspended everywhere

Active sessions terminated

Access removed across SAP and beyond

Full audit trail for compliance

Key Outcomes

- Alert raised, enriched and risk-scored automatically before any analyst is involved
- In tests in our environments, user suspended, SAP access removed and all SSO sessions terminated via Okta within minutes of the initial signal
- Lateral pivot cut off – Universal Logout ends sessions and tokens in every application connected to it
- Response actions largely executed without analyst intervention; human approval only for account reactivation
- Zero SAP system restarts thanks to surgical, identity-layer containment
- Recovery restores only verified, legitimate roles through governed Okta re-provisioning

Beyond Security: The Strategic Path from SAP IdM to Okta

The Identity Fabric Opportunity

Moving from SAP IdM to Okta Identity Governance lets enterprises leave isolated identity management behind and adopt an Identity Fabric model. SAP IdM has historically struggled to manage identity consistently across hybrid-cloud ecosystems, leaving on-premise and cloud identities in silos. Consolidating those stores on Okta's unified platform unlocks centralized visibility, consistent policy enforcement and a lower total cost of ownership by transforming identity management from an administrative

burden into the strategic capability this paper has described: a control plane for security, compliance and digital transformation alike.

The cost argument deserves emphasis. Every custom integration in a fragmented legacy IDM estate, every manual provisioning workflow, every ungoverned account represents cost, risk and latency. A unified platform provides central visibility across all identity stores (SAP, cloud SaaS, on-premise) reducing manual workload and identity-centric risk at the same time.

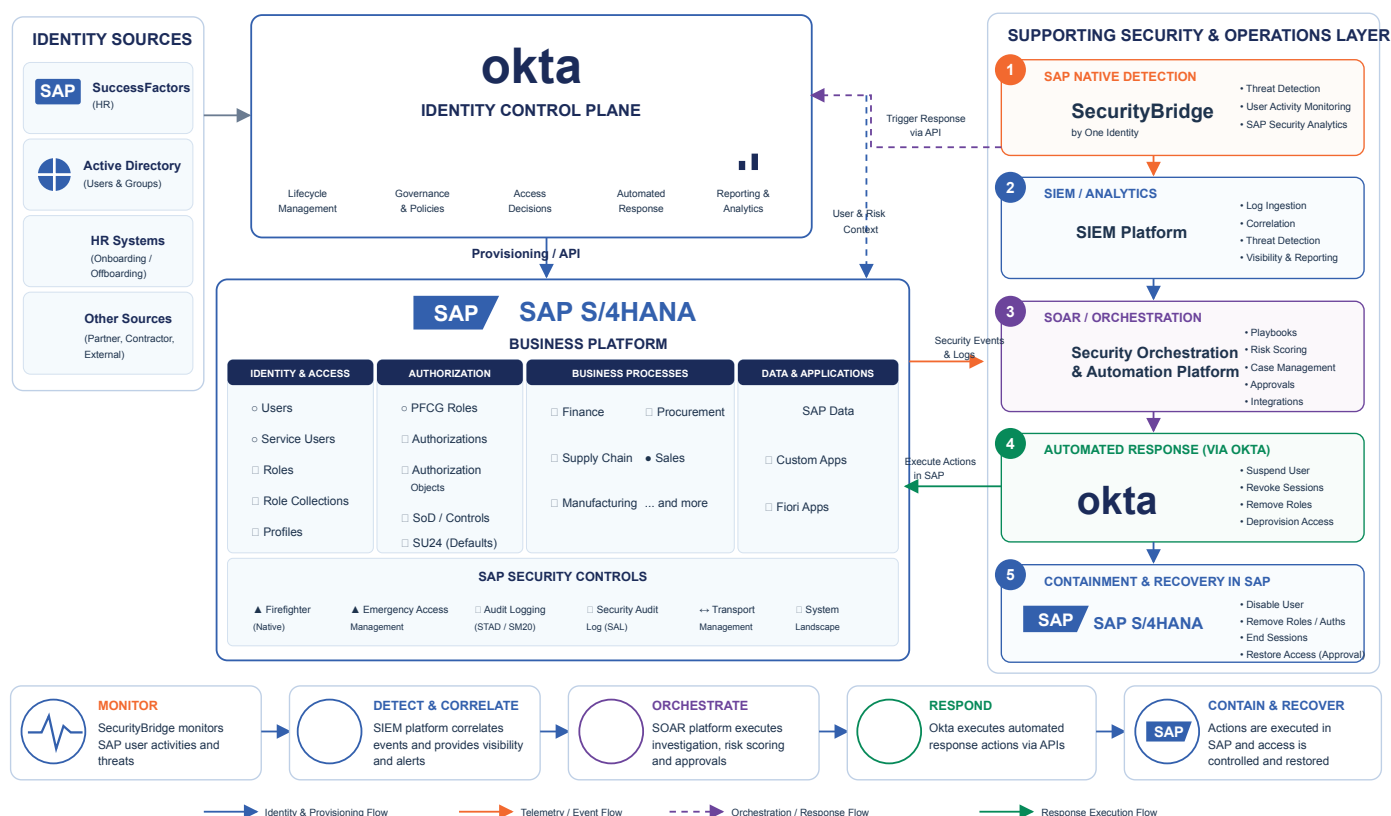
The Okta SAP On-Prem Connector: The On-Ramp

The Okta SAP On-Prem Connector is the on-ramp for the transition. It connects existing SAP ABAP systems (ECC and S/4HANA included) to the Okta Workforce Identity Cloud without waiting for a full migration, so visibility, automation and governance benefits begin accruing from day one. Transparency about complexity builds trust, so it should be stated plainly: for standard scenarios, out-of-the-box connectivity covers the large majority of use cases. Organizations with highly customized authorization models or complex multi-system landscapes will need partner-led customization – which is precisely where NTT DATA bridges the gap.

From a design perspective an OKTA-centric SAP security architecture is created as shown in the next figure.

Okta-Centric SAP Security Architecture

Identity Governance, Threat Detection and Automated Response for SAP S/4HANA



Why Okta Over Microsoft Entra ID

SAP has recommended Microsoft Entra ID as the strategic successor to SAP IdM (DSAG Technologietage, February 2024). The recommendation carries weight – particularly for organizations already deep in the Microsoft ecosystem – but it deserves scrutiny. For most SAP customers, Okta Workforce Identity Cloud is the stronger choice.

Entra ID fits best where Microsoft 365, Azure and Intune already form the identity backbone. But the typical SAP landscape is heterogeneous: on-premise ECC and S/4HANA, BTP, SuccessFactors, Ariba, non-Microsoft SaaS and frequently multi-cloud infrastructure spanning AWS, Google Cloud and Azure. In that reality, Entra ID's Microsoft-centric architecture becomes a constraint.

The differences are concrete. According to Turnkey Consulting, a specialist SAP consultancy, Entra ID cannot perform SoD checks on its own and cannot manage the depth of SAP's hierarchical entitlements; a full replacement of SAP IdM with Entra ID is, according to rz10.de, not yet possible and not expected in the near future. Okta closes this gap with connectors for SAP ECC, S/4HANA, SuccessFactors and BTP and full SCIM provisioning, extended by Xiting XAMS for SAP-native SoD analysis at the authorization-object level. And where Entra ID deepens Microsoft dependency, as access policies, workflows and group structures become Microsoft-proprietary artifacts, Okta's foundation of open standards (SAML, OIDC, SCIM, OAuth 2.0) keeps integrations portable and preserves negotiating independence.

For organizations with heterogeneous SAP landscapes, multi-cloud ambitions or a strategic priority to avoid deepening vendor lock-in, the joint recommendation of NTT DATA and Okta is clear: Okta Workforce Identity Cloud is the superior successor to SAP IdM.



Partner-Led Delivery: NTT DATA's Identity Expertise

The transition from legacy SAP IdM is often hampered by a scarcity of specialists who understand both the intricacies of SAP ABAP architecture and modern identity governance. NTT DATA bridges this gap as Okta's delivery partner for the SAP world – the strategic and technical conduit between the SAP ecosystem and the identity control plane. The engagement model rests on three pillars:

Assessment and Architecture.

A structured SAP IdM assessment inventories all connected systems, active workflows, custom provisioning logic and SoD rules. On that foundation we design the target architecture with Okta Identity Governance for lifecycle and governance, extended with Xiting XAMS for SAP-native SoD analysis and deliver a phased migration roadmap with full TCO analysis.

Deployment and Integration.

NTT DATA configures and tests the Okta SAP On-Prem Connector against the specific landscape, builds custom role mappings and SCIM pipelines and integrates SAP-native detection so that the identity control plane receives high-fidelity signals. Where standard connectors reach their limits, our SAP ABAP and Okta-certified consultants build and validate the extensions.

Managed Services and Governance.

Post go-live, NTT DATA operates identity lifecycle governance through Okta Identity Governance, SoD monitoring via Xiting XAMS and continuous SAP threat detection to close the talent gap so organizations never have to run these platforms alone.

Conclusion

The frameworks are necessary but not sufficient. NIST structures the response; MITRE ATT&CK names the adversary's moves. What turns structure and knowledge into rapid defense is architecture and the decisive architectural choice is placing identity at the center. When Okta operates as the unified control plane across SAP and the entire application landscape, containment and eradication become what they should always have been: one governed action, enforced everywhere, within minutes.

The SAP IdM sunset is the catalyst. Organizations migrating to Okta Identity Governance through a phased coexistence strategy, extending it with solutions for SAP-native SoD control and delivering it with NTT DATA's SAP and identity expertise replace a fragmented legacy stack with an identity-first architecture that is more secure, more automated and strategically independent.

Migrating off SAP IdM is not a compliance deadline to be survived. It is the opportunity to make identity the strongest layer of SAP security and with NTT DATA and Okta as partners, no organization has to build that future alone.

References

Verizon, 2025 Data Breach Investigations Report (DBIR), 18th edition – analysis of 22,000+ security incidents and 12,000+ confirmed breaches. Stolen credentials as most common initial access vector (22% of breaches); 88% of basic web application attacks involving stolen credentials. [verizon.com/dbir](https://www.verizon.com/dbir)

IBM, X-Force Threat Intelligence Index 2025 – 30% of all intrusions initiated through valid, compromised account credentials; credential harvesting present in 28% of incident response cases; 84% year-over-year increase in infostealer delivery via phishing email. [ibm.com/reports/threat-intelligence](https://www.ibm.com/reports/threat-intelligence)

CrowdStrike, 2026 Global Threat Report – 82% of detections in 2025 involved no malware; adversaries rely on stolen credentials, native tools and existing administrative functions. [crowdstrike.com](https://www.crowdstrike.com)

MITRE ATT&CK® Framework – globally accessible knowledge base of adversary tactics and techniques; T1078 (Valid Accounts) and related identity techniques referenced throughout this paper. attack.mitre.org

NIST, Special Publication 800-61 – Computer Security Incident Handling Guide; the incident response lifecycle applied to SAP in this paper. [nist.gov](https://www.nist.gov)

Turnkey Consulting, SAP IdM alternatives: considerations, strategies and solutions – SAP IdM maintenance timeline (mainstream maintenance until end of 2027, extended maintenance until 2030) and assessment of alternatives, including Microsoft Entra ID. [turnkeyconsulting.com](https://www.turnkeyconsulting.com)

rz10.de, SAP IdM abgelöst: Microsoft Entra ID als würdiger Nachfolger – SAP recommendation of Microsoft Entra ID as strategic successor (DSAG Technologietage, February 2024). [rz10.de](https://www.rz10.de)



Contact

René Bader
(he/him)

Senior Managing Consultant
Cybersecurity

info_cybersecurity@nttdata.com
[de.nttdata.com](mailto:info_cybersecurity@nttdata.com)

Start Now

Book a complimentary discovery session or a structured 3-day SAP IdM Assessment — you receive a clear migration roadmap, a coexistence plan and a defensible TCO calculation for your board.



TRUSTED ADVISOR

Trustworthy and unbiased advice up to implementation.



INNOVATIVE SOLUTIONS

Thanks to long-standing and trustworthy collaboration with our solution partners, we offer individual approaches for every customer challenge



INVESTMENT PROTECTION

The focus is on optimizing and further developing your existing systems – this way, we protect the investments you've already made.

About NTT DATA

NTT DATA is a trusted global innovator of business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have diverse experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.

