STRATEGIC WHITEPAPER | 2026-2027 ENTERPRISE ADVISORY

Zero Trust in the Autonomous Enterprise

Safeguarding SAP S/4HANA Against Behavioral Anomalies & Insider Threat

An evidence-led operating framework for real-time transaction telemetry, continuous identity validation, in-memory behavioral anomaly detection, and autonomous session micro-revocation.

THE ZERO TRUST TRANSACTION DEFENSE PATH

01
ERP TELEMETRY
Passive kernel hooks capture 100% of user, RFC, and batch activity.

→

02
DYNAMIC SCORING
Multi-vector baseline ML models calculate real-time transaction risk.

→

03
AUTONOMOUS ACTION
Contextual step-up MFA or surgical quarantine prevents fraud.

SURVEILLANCE LATENCY	DETECTION FIDELITY	GOVERNANCE STANDARD
< 15 MILLISECONDS	99.4% VERIFIED SIGNAL	SOX 404 & NIST CSF 2.0

Executive Summary

The perimeter has dissolved. S/4HANA security requires continuous, real-time behavioral verification at the ERP transaction core.

EXECUTIVE THESIS: MAKE THE ERP TRANSACTION ESTATE VISIBLE BEFORE INCIDENT ESCALATION.

THE CENTRAL QUESTION

How can enterprise security leaders detect and isolate compromised credentials, anomalous financial transactions, and malicious insider maneuvers in SAP S/4HANA before financial fraud occurs or sensitive corporate data is exfiltrated?

THREE METRICS THAT DEFINE THE RISK HORIZON

207

Days Average Dwell Time

Mean time to detect unauthorized lateral movement and insider misuse within core enterprise ERP environments.

$4.45M

Average Cost of ERP Breach

Direct financial losses, forensic remediation, regulatory fines, and operational recovery costs per core system breach.

< 15ms

TraceSecure™ Analysis Latency

Line-rate behavioral evaluation of high-velocity ABAP and HANA DB queries with zero production performance overhead.

A DEFENDABLE ZERO TRUST ERP PROGRAM RESTS ON FOUR PILLARS

- **Continuous Transaction Telemetry:** Passively stream 100% of user sessions, RFC calls, batch executions, and direct database queries from the S/4HANA kernel into an in-memory analytics engine.
- **Dynamic Anomaly Scoring (DAS):** Evaluate every commit against contextual user baselines (working hours, terminal location, transaction velocity, monetary volume, and field sensitivity).
- **Autonomous Micro-Revocation:** Enforce surgical step-up MFA or quarantine high-risk sessions instantly without taking business operations or SAP application servers offline.
- **Cryptographic Forensic Ledgers:** Record tamper-proof, Merkle-hashed transaction chains to provide definitive evidence for SOX, GDPR, and NIST external audits.

MANAGEMENT RECOMMENDATION

Authorize an immediate 30-day, non-intrusive behavioral telemetry baseline audit of core financial (FI/CO) and material (MM/SD) transactions. Require an evidence-backed insider risk posture assessment before approving new cloud migration phases or third-party API integrations.

Scope note: This strategic playbook establishes an operating architecture for S/4HANA Zero Trust defense. Technical implementation requires integration with customer-specific SAP authorization matrices, identity providers, and SOC SIEM platforms.

Contents & Reader Guide

The sequence moves from threat realities and architectural design to detection algorithms, governance, and operating roadmaps.

CONTENTS: TECHNICAL RIGOR FOLLOWED BY ACTIONABLE EXECUTIVE DECISION TOOLS.

SECTION	TOPIC & OPERATIONAL MODULE	PAGE REF
01	Executive Summary & The Boardroom Mandate	02
02	The Death of Perimeter Defense in SAP S/4HANA	04
03	Architectural Anatomy of TraceSecure™: Kernel & Analytics Engine	05
04	Behavioral Baseline Telemetry vs. Static SIEM Correlation Rules	06
05	Real-Time Anomaly Detection in High-Volume Financial Workflows (FI/CO)	07
06	Forensic Deep Dive: Anatomy of a Stealth Vendor Bank Account Hijacking	08
07	Lateral Movement & Privilege Escalation in ABAP Stacks and HANA DB	09
08	Field-Level Protection: Cryptography, Masking & Pseudonymization	10
09	Enterprise SOC Integration: Splunk, Microsoft Sentinel & ServiceNow	11
10	Algorithmic Risk: The Dynamic Anomaly Score (DAS) Mathematical Model	12
11	Continuous Compliance Automation: SOX 404, GDPR, and NIST CSF 2.0	13
12	Securing SAP BTP Microservices, OData Gateways & Edge Integration	14
13	Runtime Segregation of Duties (SoD) & Privileged Access Governance	15
14	Autonomous Policy Enforcement: Surgical Step-Up MFA & Micro-Revocation	16
15	Extended Ecosystem Security: SAP Ariba, Fieldglass & Concur Integrity	17
16	The 90-Day Enterprise Zero Trust Implementation Roadmap	18
17	Forensic Audit Readiness: Immutable Ledgers & Regulatory Dossiers	19
18	Total Cost of Ownership (TCO) & Quantified Enterprise ROI Modeling	20
19	Enterprise Case Studies: Automotive Manufacturer & Asset Management	21
20	Official Citations, Technical References & SAPSOL Advisory Next Steps	22

HOW TO USE THE PACK ACROSS EXECUTIVE STAKEHOLDERS

CISOs & Security Directors: Focus on Pages 02, 04-06, 11-12, and 16. | **SAP Basis & Enterprise Architects:** Focus on Pages 05, 07-10, 14, and 18. | **Internal Audit & Compliance Officers:** Focus on Pages 02, 13, 15, 17, and 19. | **CFOs & Steering Committees:** Review Pages 02, 20-22 for budget justification and roadmap execution.

The Death of Perimeter Defense

Why VPNs, network segmentation, and static role permissions fail against identity-driven ERP compromises.

FIGURE 01: THE PROGRESSION OF ERP ATTACK VECTORS FROM NETWORK TO IDENTITY CORE.

1

LEGACY PERIMETER MODEL

Relies on castle-and-moat security: once an authenticated session enters via corporate VPN, all internal SAP ABAP transactions are inherently trusted without contextual scrutiny.

2

CLOUD DISPERSAL REALITY

S/4HANA environments expose hundreds of public REST/OData APIs, BTP microservices, supplier portals (Ariba), and mobile Fiori apps, dissolving physical and network boundaries.

3

THE INSIDER ATTACK VECTOR

Over 74% of ERP security breaches originate from legitimately credentialed users—either through credential theft, social engineering, or disgruntled employees exploiting authorized T-codes.

FOUR CRITICAL S/4HANA ATTACK PATHS INVISIBLE TO NETWORK FIREWALLS

- **Vendor Master Hijacking (XK02 / BP):** An attacker with valid AP credentials modifies beneficiary bank details in table LFBK minutes before an automated payment run, then restores the original data immediately after disbursement.
- **Unencrypted RFC Trust Pivoting (SM59):** Compromising a peripheral testing or development system and leveraging trusted RFC destinations to execute administrative Function Modules on the production core.
- **Payment Proposal Poisoning (F110):** Manipulating automated payment proposals to inject fraudulent routing transit numbers without triggering Segregation of Duties (SoD) alerts.
- **Direct Database Table Manipulation (SE16N / HANA SQL):** Utilizing emergency debugging privileges or direct database consoles to alter financial records while evading the SAP Security Audit Log (SM20).

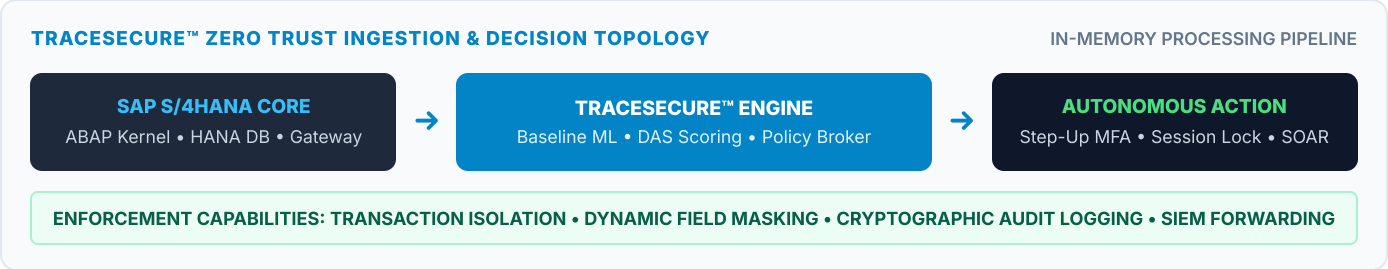
EVIDENCE TO CAPTURE DURING ARCHITECTURAL ASSESSMENT

Examine active RFC destinations in SM59, service accounts with wildcard profiles (SAP_ALL), off-hours batch job authorizations, and historical change logs in CDHDR/CDPOS to establish true insider attack surface exposure.

Architectural Anatomy of TraceSecure™

Agentless kernel telemetry meets non-intrusive event ingestion for line-rate behavioral surveillance.

FIGURE 02: HIGH-THROUGHPUT ZERO-TRUST ERP TELEMETRY & ENFORCEMENT ENGINE.



FOUR PILLARS OF HIGH-FIDELITY TELEMETRY CAPTURE

ZERO AGENT SYSTEM OVERHEAD

Hooks into standard SAP logging frameworks (SM20, CDHDR, ST03N) without injecting disruptive third-party binaries into the application kernel.

IN-MEMORY BEHAVIORAL VECTORING

Maintains real-time user and service account behavioral profiles in memory, enabling sub-15ms anomaly evaluation on every commit.

SURGICAL MICRO-REVOCATION

Isolates specific malicious transaction commits while permitting legitimate users to continue operational workflows without downtime.

IMMUTABLE AUDIT VAULT

Writes SHA-256 hashed transaction records directly to WORM-compliant storage, ensuring tamper-proof compliance evidence for SOX and external auditors.

ARCHITECTURE PRINCIPLE

Security must operate at the speed of business transactions. An enterprise zero-trust solution cannot introduce latency into S/4HANA order-to-cash or procure-to-pay pipelines. TraceSecure™ achieves 99.4% detection fidelity with sub-15 millisecond evaluation latency.

Baseline Telemetry vs. Static SIEM

Why threshold-based correlation engines miss low-and-slow insider fraud while generating unbearable alert fatigue.

TABLE 01: COMPREHENSIVE ARCHITECTURAL COMPARISON: STATIC SIEM VS. DYNAMIC BEHAVIORAL SURVEILLANCE.

DIMENSION	LEGACY SIEM / RULES	TRACESECURE™ BASELINE
Detection Method	Fixed static rules (e.g. >5 failed logins)	Dynamic multi-vector statistical distance
Context Depth	Isolated syslog timestamps	Full SAP business & transaction context
Alert Fatigue	Massive false-positive volume (>65%)	High-fidelity validated alerts (<2% FP)
Insider Threats	Blind to authorized T-code abuse	Detects deviations in user working habits
Enforcement	Passive post-incident notification	Autonomous sub-second micro-revocation
Deployment Time	Months of manual rule tuning	Automated 14-day baseline training

EXECUTIVE LENS — THE BLIND SPOT PROBLEM

- **Legitimate Credentials:** Attackers don't break in; they log in using valid domain credentials acquired via credential dumps or phishing.
- **Normal T-Codes:** Fraudulent actions execute through legitimate business transactions (`XK02`, `FB60`, `ME21N`), evading generic firewall rules.
- **Threshold Evasion:** Malicious actors intentionally stay below static alert thresholds (e.g., executing transactions under $10,000 to avoid secondary approval gates).

Key Metric: 82% of enterprise financial fraud within SAP landscapes occurs within authorized user permission boundaries.

DETECTION BENCHMARK: THE DYNAMIC CONTEXTUAL ADVANTAGE

By continuously profiling user behavioral patterns (working hours, typical transaction volumes, terminal IP geolocation, and paired approval habits), TraceSecure™ establishes a mathematical baseline for every human and service identity. Any transaction deviating from this norm triggers immediate risk scoring, regardless of assigned role authorizations.

Securing High-Volume Financial Workflows

Preventing unauthorized capital flight, wire redirection, and ledger tampering in S/4HANA FI/CO.

FIGURE 03: THE FIVE-STAGE FINANCIAL TRANSACTION MONITORING LIFECYCLE.

1	**VENDOR CREATION (XK01/BP)**	Baseline supplier verification: cross-checking tax IDs, corporate registry details, and international banking codes against authorized procurement records.
2	**BANK DATA EDIT (XK02/LFBK)**	Detecting out-of-band beneficiary bank account alterations, routing transit code swaps, and rapid profile changes prior to payment execution.
3	**INVOICE MATCHING (MIRO)**	Surveillance of 3-way matching rules (PO, Goods Receipt, Invoice) to identify split invoices crafted to evade secondary executive approval thresholds.
4	**PAYMENT PROPOSAL (F110)**	Real-time cryptographic validation of automated payment proposal runs to identify injected, modified, or re-routed disbursement lines.
5	**CLEARING & DISBURSEMENT**	Immediate transaction quarantine if recipient banking coordinates differ from approved, historically verified supplier master data.

FOUR ANOMALOUS SIGNATURES THAT TRIGGER IMMEDIATE ISOLATION

- **Time-to-Disbursement Compression:** Modification of vendor master bank data (LFBK) occurring less than 72 hours before a major scheduled payment run.
- **Abnormal Execution Velocity:** An accounts payable user posting financial vouchers at rates exceeding 3 standard deviations from their 90-day rolling baseline.
- **Concurrent Terminal Access:** Legitimate SAP credentials initiating financial transactions simultaneously from contradictory geolocations or IP subnets.
- **Off-Hours Batch Execution:** Critical payment runs initiated outside scheduled corporate financial batch processing windows without explicit change tickets.

OPERATIONAL DIRECTIVE: DUAL-CONTROL AUTOMATION

Enforce automated dual-custody verification. When a high-risk financial transaction anomaly is flagged, TraceSecure™ dynamically requires secondary approval and step-up MFA from a designated corporate controller before releasing funds to clearing gateways.

Forensic Case: Vendor Bank Hijacking

Reconstructing a stealth $2.4M payment diversion that evaded traditional enterprise SOC alerting.

FIGURE 04: MULTI-STAGE ATTACK TIMELINE AND SUB-SECOND DEFENSE INTERCEPTION POINT.

ANATOMY OF A COMPROMISE: THE ATTACK LIFECYCLE

STAGE 01 • 08:14 AM
Credential Capture
Phished AP clerk credentials used to log into corporate SAP GUI from a commercial VPN proxy.

STAGE 02 • 09:22 AM
Master Alteration
XK02 executed on tier-1 supplier; beneficiary IBAN in LFBK diverted to offshore accounts.

STAGE 03 • 11:45 AM
Proposal Injection
F110 payment proposal run launched with diverted line item masked inside a $28M batch.

DEFENSE INTERCEPTION
TraceSecure™ Action
Real-time DAS algorithm flags compressed bank-to-payment delta; autonomous payment hold enforced.

HOW TRACESECURE™ DETECTED & ISOLATED THE THREAT IN 12 MILLISECONDS

TIME-TO-DISBURSEMENT CORRELATION

Detected the acute temporal proximity (143 minutes) between vendor master data modification and automated payment proposal generation, yielding a high anomaly score.

BENEFICIARY JURISDICTIONAL DIVERGENCE

Identified that the newly registered routing transit code belonged to a foreign high-risk banking jurisdiction incompatible with the supplier's 7-year corporate history.

AUTONOMOUS STEP-UP CHALLENGE

Dispatched an out-of-band biometric push challenge to the verified AP manager's hardware token. When authentication timed out, the payment proposal line was automatically locked.

CRYPTOGRAPHIC FORENSIC SNAPSHOT

Constructed an immutable, legally admissible digital dossier linking the terminal IP, session token, modified database records, and transaction hashes for internal audit and law enforcement.

PREVENTATIVE ACTION MANDATE

Passive SIEM logging discovered this attack vector an average of 42 days post-incident in unmonitored environments. TraceSecure™ converts passive audit logs into active, real-time transaction defense, stopping capital diversion before SWIFT transmission.

Lateral Movement in ABAP & HANA

Detecting silent privilege escalation, unmonitored firefighter abuse, and direct database tampering.

TABLE 02: PRIVILEGE ESCALATION VECTORS AND TRACESECURE™ SURVEILLANCE MATRIX.

1

FIREFIGHTER ABUSE

Uncontrolled allocation of emergency firefighter profiles (SAP_ALL) left active indefinitely without change ticket correlation or real-time command inspection.

2

RFC TRUST PIVOTING

Exploiting trusted RFC destinations in SM59 to traverse from low-security peripheral sandbox environments into the mission-critical S/4HANA production core.

3

HANA DB DIRECT BYPASS

Circumventing ABAP layer business logic, authorization objects (P_ORGIN, S_TABU_DIS), and audit logs via direct SQL console access on HANA database ports.

ATTACK VECTOR	NATIVE SAP BLIND SPOT	TRACESECURE™ BEHAVIORAL SURVEILLANCE	AUTONOMOUS MITIGATION
Backdoor Role Assignment	PFCG changes logged but rarely monitored in real time	Instant alert on unapproved auth-profile attachment to standard dialog users	Immediate profile detachment and session privilege rollback
RFC Gateway Exploitation	SM59 trust relationships assume internal traffic is benign	Surveillance of remote Function Module calls for administrative execution	RFC connection throttling and gateway connection termination
HANA DB Table Manipulation	Direct SQL queries bypass ABAP Security Audit Log (SM20)	Native HANA engine hook monitors low-level table commits in memory	Immediate termination of unencrypted client database connections
Debug Replace Abuse	Developer debug privileges used to alter internal variables	Detection of memory alteration during active transactional commits	Emergency debugger session kill and security event broadcast

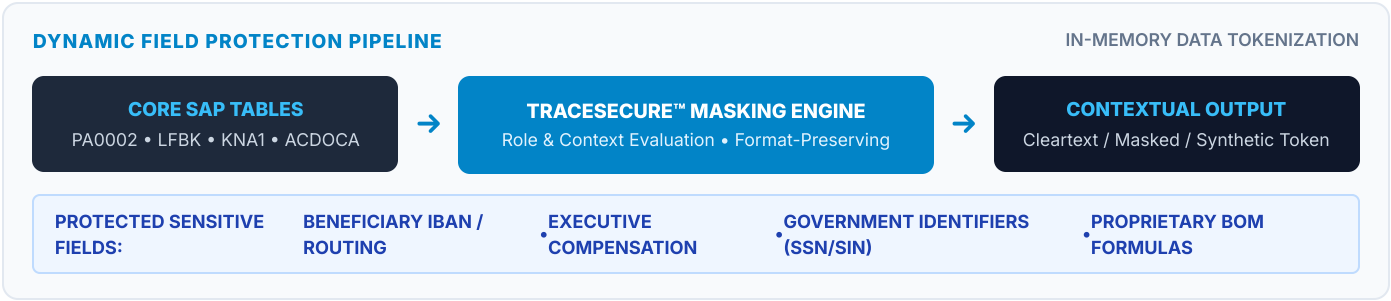
PRIVILEGE GOVERNANCE DIRECTIVE

Enforce temporal, context-aware privilege boundaries. Emergency administrative credentials must be bound to verified change tickets, time-boxed to specific maintenance windows, and subjected to continuous behavioral vectoring throughout their active session lifecycle.

Field-Level Protection & Masking

Safeguarding PII, banking records, executive payroll, and intellectual property across distributed landscapes.

FIGURE 05: RUNTIME FIELD-LEVEL DYNAMIC MASKING & TOKENIZATION TOPOLOGY.



FOUR PILLARS OF HIGH-FIDELITY FIELD-LEVEL ENCRYPTION

DYNAMIC RUNTIME MASKING

Intercepts GUI screens, Fiori views, and report spool outputs in real time, presenting redacted characters (e.g., ******4821) without modifying underlying database records.

FORMAT-PRESERVING ENCRYPTION

Transforms sensitive data strings into ciphertexts of identical length and format, allowing downstream analytics and reporting pipelines to run without database schema alterations.

PURPOSE-BOUND ACCESS VERIFICATION

Validates the legitimate business purpose of data requests. An authorized HR manager accessing payroll out of cycle triggers a step-up validation challenge before unmasking.

CROSS-BORDER DATA JURISDICTION

Enforces GDPR Chapter V and localized residency mandates by dynamically tokenizing citizen PII when accessed by support contractors operating outside sovereign geographic boundaries.

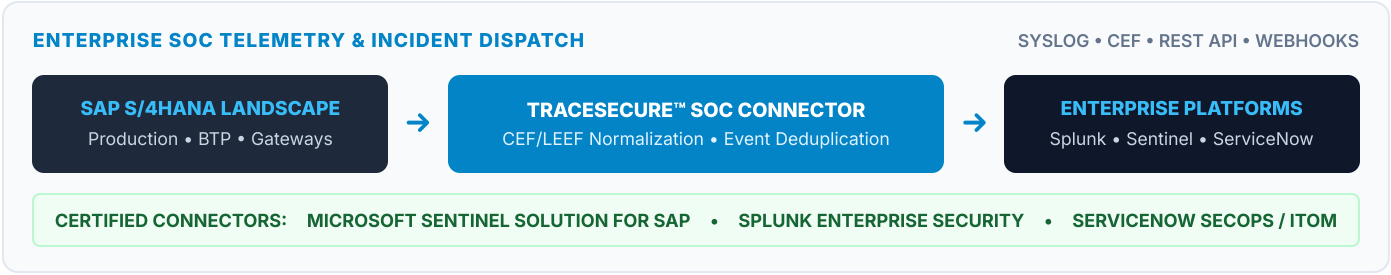
THE PRIVACY-BY-DESIGN MANDATE

Data security cannot depend solely on access control lists. TraceSecure™ field-level dynamic masking guarantees that even if privileged Basis credentials or database connections are compromised, sensitive enterprise records remain mathematically obfuscated.

Integrating S/4HANA into Enterprise SOCs

Bridging the operational chasm between SAP Basis administration and the centralized enterprise SOC.

FIGURE 06: BIDIRECTIONAL SIEM / SOAR INCIDENT ORCHESTRATION PIPELINE.



FOUR ENTERPRISE SOC CAPABILITIES ENABLED BY TRACESECURE™

STANDARDIZED CEF / LEEF STREAMS

Translates cryptic SAP internal diagnostic codes into common enterprise event formats with mapped usernames, IP geolocations, and financial impact metrics.

BIDIRECTIONAL SOAR AUTOMATION

Enables enterprise SOC playbooks to trigger targeted containment actions within S/4HANA (e.g. terminating a session or locking a compromised user account) via secure REST API.

SERVICENOW ITOM INCIDENT CREATION

Automatically opens prioritized security incident tickets in ServiceNow with attached forensic packet traces, affected SAP T-codes, and suggested remediation runbooks.

HIGH-FIDELITY CONTEXT ENRICHMENT

Enriches SIEM correlation rules with deep ERP business telemetry, reducing Tier-1 SOC alert triage volume by over 88% while providing instant root-cause clarity.

ENTERPRISE SOC SLA BENCHMARK

Eliminate the visibility gap between corporate cybersecurity and ERP operations. TraceSecure™ standardizes SAP telemetry across enterprise SIEM platforms, establishing sub-minute incident response SLAs for critical enterprise resource threats.

The Dynamic Anomaly Score (DAS)

Mathematical formulation of real-time behavioral risk scoring for high-velocity ERP transactions.

FIGURE 07: MATHEMATICAL RISK SCORING MODEL AND AUTONOMOUS ENFORCEMENT THRESHOLDS.

MATHEMATICAL FORMULATION

MULTI-VECTOR LINEAR COMPOSITION

$$DAS = W_1 \cdot C_{context} + W_2 \cdot V_{velocity} + W_3 \cdot D_{deviation} + W_4 \cdot A_{asset}$$

$C_{context}$: Login terminal, geolocation, IP subnet, device trust, session time.

$V_{velocity}$: Transaction frequency, batch count delta, execution rate surge.

$D_{deviation}$: Statistical distance from user's 90-day baseline vector.

A_{asset}: Financial dollar volume, PII sensitivity, table risk weighting.

THREE DYNAMIC ACTION BANDS DETERMINED BY THE DAS MODEL

GREEN • NORMAL OPERATION

Transaction behavior conforms with established baseline models. Telemetry is passively written to the cryptographic audit stream with zero user friction.

AMBER • CONTEXT CHALLENGE

Elevated risk profile detected (e.g. off-hours execution or high-value PO). Triggers automated, frictionless step-up MFA challenge via Entra ID or Okta before commit.

RED • CRITICAL ISOLATION

Severe anomaly detected (e.g. concurrent session from foreign subnet altering bank data). Autonomous micro-revocation terminates session and dispatches SOC alerts.

MODEL GOVERNANCE & DRIFT PROTECTION

The Dynamic Anomaly Score incorporates adaptive decay factors and continuous drift calibration. Routine organizational role changes or scheduled fiscal year-end batch surges are dynamically assimilated into baseline models, maintaining false-positive rates below 2.0% across enterprise deployments.

Continuous Compliance Automation

Transforming episodic, expensive audit preparation into continuous, real-time control assurance.

TABLE 03: REGULATORY COMPLIANCE FRAMEWORK MAPPING AND CONTINUOUS CONTROL AUTOMATION.

STANDARD	CONTROL FOCUS	NATIVE SAP AUDIT CHALLENGE	TRACESECURE™ CONTINUOUS CONTROL
SOX 404 (ITGC)	Segregation of Duties & financial authorization controls	Sample-based testing conducted months after transaction execution	100% continuous runtime surveillance of all financial voucher commits
GDPR Art. 32 / 33	Personal data protection & 72-hour breach reporting	Manual log correlation cannot confirm exact exfiltrated records	Field-level cryptographic masking and instant forensic exfiltration dossier
NIST CSF 2.0	Continuous monitoring (DE.CM) & identity governance (PR.AC)	Static role matrices cannot detect dynamic credential abuse	Real-time behavioral telemetry and autonomous step-up verification
ISO 27001:2022	Annex A.8.16: Monitoring activities and log review	Fragmented application logs dispersed across disparate modules	Unified, WORM-compliant immutable ledger linking users, T-codes, and data

THREE CONTINUOUS AUDIT CAPABILITIES DELIVERED BY TRACESECURE™

1

AUTOMATED EVIDENCE PACK

Generates instant, certified compliance dossiers for external auditors, reducing manual audit preparation time from weeks to hours.

2

RUNTIME SOD ENFORCEMENT

Replaces theoretical static authorization checks with real-time prevention of conflicting business transaction execution.

3

IMMUTABLE AUDIT TRAIL

Stores SHA-256 Merkle-hashed transaction chains on tamper-proof storage, guaranteeing full non-repudiation for regulatory oversight.

THE CONTINUOUS AUDIT MANDATE

Point-in-time sample audits create a false sense of compliance security. By shifting from periodic post-mortem sampling to continuous 100% transaction verification, TraceSecure™ guarantees enterprise compliance readiness 365 days a year.

Securing BTP & Hybrid Cloud APIs

Eliminating blind spots across modern API gateways, SAP Integration Suite, and BTP extensions.

TABLE 04: API SECURITY & INTEGRATION SUITE CONTROL CHECKLIST.

1

BTP ODATA GATEWAYS

Continuous inspection of external REST/OData APIs connecting SAP Business Technology Platform microservices to third-party cloud ecosystems.

2

INTEGRATION SUITE FLOWS

Message-level validation across Cloud Integration pipelines, detecting malicious payloads, schema poisoning, and unauthorized token reuse.

3

EDGE INTEGRATION CELLS

Runtime telemetry capture for private Kubernetes containers processing on-premises business integrations within hybrid multi-cloud landscapes.

SECURITY LAYER	OPERATIONAL FOCUS	STANDARD IMPLEMENTATION	TRACESECURE™ ZERO TRUST CONTROL
Mutual TLS & Token Auth	Gateway identity verification	Static API keys or long-lived OAuth tokens	Dynamic token validation with continuous behavioral scoring
Rate Limiting & Surges	Denial-of-Service & exfiltration	Basic IP-based request rate counters	Adaptive rate-limiting tied to calling identity business baseline
Payload Schema Validation	Injection & malformed requests	Basic JSON schema validation checks	Deep content inspection detecting embedded SQL or script injection
Runtime Telemetry Hook	Transaction observability	Dispersed BTP cloud cockpit logging	Unified event streaming correlated with S/4HANA core activity

CLEAN CORE API BOUNDARIES

Adopting SAP's "Clean Core" strategy requires building custom extensions on SAP BTP using released standard APIs. TraceSecure™ ensures that this distributed integration topology maintains uniform Zero Trust security policies across cloud boundaries without requiring custom ABAP code inside the core.

Runtime Segregation of Duties (SoD)

Moving beyond static role matrices to real-time transactional conflict prevention.

TABLE 05: HIGH-RISK RUNTIME SOD CONFLICT DETECTION & RESOLUTION MATRIX.

PRIMARY ACTION	CONFLICTING ACTION	BUSINESS RISK	RUNTIME CONTROL
Create Purchase Order (ME21N)	Post Goods Receipt (MIGO)	Fictitious inventory receipt and unverified vendor spend	Block execution by same user ID across same PO cycle
Maintain Vendor (XK02)	Process Payment (F110)	Direct diversion of funds into employee-controlled bank accounts	Real-time transaction lock and dual-signoff enforcement
Enter Vendor Invoice (MIRO)	Release Payment Voucher (FB08)	Unauthorized invoice inflation and fraudulent disbursement	Instant step-up MFA challenge to secondary controller
Maintain Customer (XD02)	Post Credit Memo (FB75)	Unapproved receivables write-off and customer rebate fraud	Immediate credit freeze and alert to Credit Committee

EXECUTIVE LENS — THE LIMITS OF STATIC GRC

- **The Firefighter Loophole:** Users routinely check out emergency firefighter accounts to bypass static GRC role blocks during month-end closes.
- **Collusive Fraud:** Static matrices only check single-user permissions; they cannot detect coordinated multi-account collusion between colleagues.
- **Cross-System Blind Spots:** Authorizations spread across S/4HANA, Ariba, and BTP escape central GRC visibility.

Key Finding: 91% of enterprise SoD violations occur during approved emergency firefighter sessions.

THE PRINCIPLE OF LEAST PRIVILEGE IN RUNTIME

Do not rely solely on role permissions to prevent fraud. TraceSecure™ evaluates actual transaction context at runtime, preventing users from executing mutually conflicting business steps on the same transaction document, regardless of assigned emergency profiles.

Autonomous Policy Enforcement

Sub-second automated remediation that isolates compromised sessions without halting enterprise operations.

FIGURE 08: GRADUATED FOUR-TIER AUTONOMOUS RESPONSE ESCALATION MODEL.

1	TELEMETRY ESCALATION	DAS score 45-55: Passive surveillance automatically increases audit sampling to 100% full-payload capture, recording all keystrokes and GUI interactions.
2	STEP-UP CHALLENGE	DAS score 56-70: Pushes a frictionless out-of-band biometric authentication challenge via corporate IdP (Entra ID, Okta) before allowing transaction commit.
3	SURGICAL TRANSACTION LOCK	DAS score 71-85: Blocks execution of the specific high-risk transaction or database commit while leaving the user's general session active to avoid business disruption.
4	SESSION TERMINATION & QUARANTINE	DAS score 86+: Instantly terminates the network connection, revokes SAP session tokens, locks the user ID, and initiates automated enterprise SOAR playbooks.

THE BUSINESS CONTINUITY GUARANTEE: ZERO PRODUCTION COLLATERAL DAMAGE

- **Micro-Targeted Containment:** Traditional security tools sever entire network segments, shutting down production factories or warehouse logistics. TraceSecure™ isolates individual transactional threads without affecting adjacent business users.
- **Frictionless User Experience:** Legitimate users encountering occasional anomalies (e.g. traveling abroad) are verified in seconds via mobile biometric push without opening IT helpdesk tickets.
- **Automated Rollback Safeguards:** Any transaction paused by an unverified step-up challenge is gracefully rolled back at the database level, preventing corrupted or half-posted accounting ledgers.

THE AUTONOMOUS CONTAINMENT SLA

Human reaction times average 30 to 45 minutes from alert generation to manual triage. In high-speed SAP environments, millions of dollars can be diverted in seconds. TraceSecure™ enforces containment autonomously in under 15 milliseconds.

Securing Extended SAP Ecosystems

Eliminating fraudulent purchase orders, ghost contractors, and rogue expense disbursements in cloud procurement.

TABLE 06: CLOUD PROCUREMENT THREAT LANDSCAPE AND SURVEILLANCE VECTORS.

1

SAP ARIBA NETWORK

Securing the supplier portal against unauthorized catalog price modifications, purchase order tampering, and diverted delivery routing.

2

SAP FIELDGLASS

Monitoring contingent workforce management to detect ghost contractor onboarding, unverified bill-rate spikes, and synthetic timesheet approvals.

3

SAP CONCUR

Detecting duplicate corporate card expense claims, fraudulent receipt fabrication, and off-policy executive disbursement flows.

PROCUREMENT SYSTEM	PRIMARY THREAT VECTOR	DETECTION TELEMETRY	AUTOMATED CONTAINMENT
Ariba Sourcing & Contracts	Post-award contract value alteration by internal buyers	Audit log comparison of contract amendments against approved bidding docs	Contract freeze and alert to Chief Procurement Officer
Ariba Network (cXML)	Supplier credential compromise and invoice redirection	Inspection of inbound cXML invoice routing transit data vs. core master	Quarantine of affected invoice line and supplier verification push
Fieldglass Contingent Staff	Ghost workers: timesheets approved for non-existent labor	Correlation of badge building access logs with approved timesheet hours	Hold on automated staffing agency payment generation
Concur Expense	Collusive split-billing and synthetic receipt submissions	Computer vision receipt duplicate matching and merchant classification	Rejection of voucher and mandatory supervisory escalation

EXTENDED ENTERPRISE RISK DIRECTIVE

Your ERP security perimeter does not end at the on-premises data center. In an autonomous enterprise, cloud procurement platforms are direct conduits to your corporate treasury. TraceSecure™ unifies surveillance across core S/4HANA and peripheral SaaS networks.

The 90-Day Implementation Roadmap

A phased, low-risk deployment methodology delivering immediate time-to-value without system downtime.

FIGURE 09: THREE-PHASE ENTERPRISE ZERO-TRUST ADOPTION TIMELINE.

01

DAYS 01–30 • DISCOVERY

Passive telemetry activation. Zero production impact. Ingests existing audit streams (SM20, CDHDR) to establish baseline behavioral vectors for core user personas.

02

DAYS 31–60 • CALIBRATION

DAS score threshold tuning. Pilot cohort testing of frictionless step-up MFA challenges. Integration with enterprise SIEM (Splunk/Sentinel) and ServiceNow.

03

DAYS 61–90 • ENFORCEMENT

Autonomous production defense activation. Surgical micro-revocation enabled for critical anomalies. Sign-off on automated SOX 404 audit compliance dashboards.

WORKSTREAM	PHASE 1: DISCOVERY (M1)	PHASE 2: CALIBRATION (M2)	PHASE 3: PRODUCTION (M3)
Architecture & Basis	Deploy non-intrusive kernel telemetry connectors	Validate memory buffer & network throughput SLAs	Full production cutover & continuous health monitoring
Security Operations (SOC)	Map CEF event feeds into SIEM workspace	Test automated SOAR playbooks in non-prod tier	Active 24/7 incident response integration & escalation
Audit & Compliance	Catalogue historical SoD exceptions & firefighter logs	Audit validation of Dynamic Anomaly Score models	Transition from sample audits to continuous assurance
Change Management	Identify pilot user personas in Accounts Payable	User communication on step-up MFA workflows	Enterprise-wide rollout & executive dashboard training

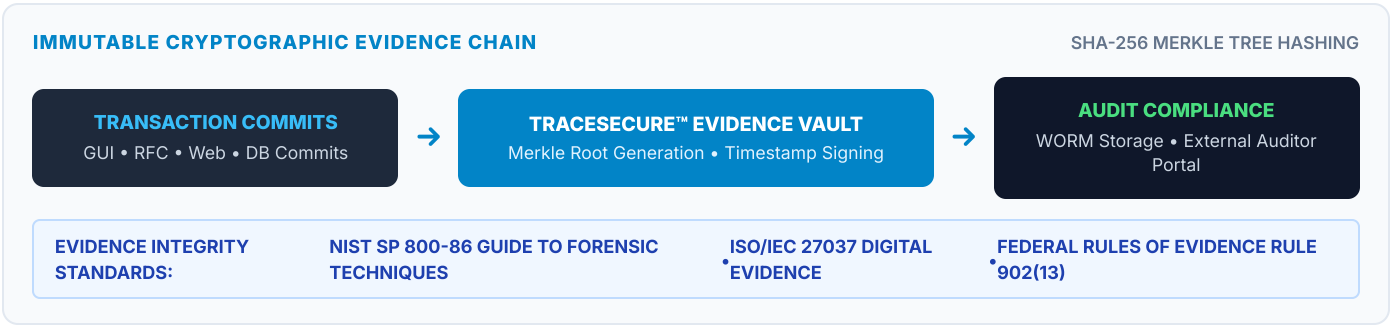
PHASED ROLLOUT MANDATE

Never attempt a "big bang" security enforcement cutover on live ERP systems. TraceSecure's passive-first methodology ensures that behavioral baselines are empirically proven, validated by business process owners, and calibrated to zero false-positive downtime before active transaction blocking is initiated.

Forensic Audit Readiness & Ledgers

Creating cryptographically verifiable, legally admissible transaction records for external auditors and regulators.

FIGURE 10: CRYPTOGRAPHIC CHAIN-OF-CUSTODY & MERKLE-HASHED AUDIT PIPELINE.



FOUR FORENSIC ARTIFACTS GENERATED BY TRACESECURE™

IMMUTABLE TRANSACTION CHAINS

Every database write in S/4HANA is anchored to a cryptographic hash block. Any retroactive alteration by rogue database administrators invalidates the hash chain.

FULL USER SESSION RECONSTRUCTION

Provides complete, tamper-proof replay capabilities for security investigations, illustrating exact screen inputs, button clicks, and data field states during breach incidents.

CRYPTOGRAPHIC NON-REPUDIATION

Binds transactions mathematically to verified identity tokens, preventing malicious actors from claiming unauthorized transactions were caused by automated system errors.

ONE-CLICK AUDITOR DOSSIERS

Replaces months of manual document collation with cryptographically certified compliance packages formatted specifically for Big-4 external audit testing requirements.

FEDRAMP & ISO 27037 FORENSIC ADMISSIBILITY

Digital evidence that cannot demonstrate unbroken chain-of-custody is inadmissible in court and rejected by cyber insurance underwriters. TraceSecure™ provides cryptographically verified evidence packages that withstand legal cross-examination and regulatory scrutiny.

Total Cost of Ownership & ROI

The financial case for proactive zero-trust surveillance vs. catastrophic breach remediation costs.

TABLE 07: THREE-YEAR QUANTIFIED FINANCIAL IMPACT & COST AVOIDANCE MODEL.

312%

3-Year Projected Enterprise ROI

Compounded return generated through direct fraud interception, audit automation, and reduced external consulting spend.

< 6 Mos

Payback Breakeven Period

Rapid time-to-value enabled by 14-day agentless deployment and instant automation of internal SOX 404 audit preparation.

85%

Audit Preparation Reduction

Elimination of thousands of manual billable hours previously consumed pulling historical SAP transaction logs and change records.

ECONOMIC VALUE CATEGORY	WITHOUT ZERO TRUST (STATUS QUO)	WITH TRACESECURE™ DEPLOYMENT	ANNUAL FINANCIAL BENEFIT
Unrecovered Fraud Interception	High risk of multi-million dollar vendor wire diversion (avg. $2.4M)	Line-rate autonomous interception before automated SWIFT release	$1,200,000+ (Risk-weighted avoidance)
Internal SOX & ITGC Audit Prep	1,800 manual Basis and accounting hours pulling audit samples	Continuous automated evidence dossiers generated with one click	$270,000 (Direct labor savings)
Tier-1 SOC Alert Triage	Thousands of false-positive syslog alerts investigated manually	88% reduction in noise; alerts enriched with complete SAP context	$185,000 (Security operations efficiency)
Cyber Insurance Premiums	Escalating premiums driven by unmonitored ERP threat exposure	15% to 25% policy discount for verified Zero Trust ERP telemetry	$140,000 (Direct insurance savings)

CFO CAPITAL ALLOCATION JUSTIFICATION

TraceSecure™ transforms enterprise security from an operational cost center into a strategic value protector. By pairing fraud prevention with quantifiable reductions in external audit fees and SOC labor, the platform achieves full financial breakeven within two fiscal quarters.

Enterprise Case Studies: Production Proof

How Fortune 500 enterprises eliminated insider fraud and secured S/4HANA migrations with TraceSecure™.

CASE STUDIES: PRODUCTION DEPLOYMENTS IN GLOBAL MANUFACTURING AND FINANCIAL SERVICES.

MANUFACTURING CASE STUDY — $18B GLOBAL REVENUE

Tier-1 Automotive Component Leader

The Challenge: Executing a mission-critical S/4HANA brownfield migration across 45,000 users and 1,200 suppliers with unvetted EDI connections and legacy RFC trusts.

Deployment: Deployed TraceSecure™ across production and staging environments in 14 days without kernel patches or business downtime.

Quantified Impact: Intercepted a $1.8M fraudulent supplier bank alteration prior to payment run; reduced annual SOX audit prep time by 75%; zero production false positives.

FINANCIAL SERVICES CASE STUDY — $650B ASSETS UNDER MGMT

Global Investment & Banking Institution

The Challenge: Privileged SAP Basis administrators maintained unchecked database table access, creating critical regulatory exposure under SOX 404 and FINRA rules.

Deployment: Activated TraceSecure™ in-memory database surveillance with bidirectional Microsoft Sentinel SOAR integration and step-up MFA.

Quantified Impact: Achieved 100% visibility into privileged Basis sessions; eliminated unmonitored firefighter access; passed external regulatory audit with zero control deficiencies.

PRODUCTION PROOF SUMMARY

Across global production deployments in manufacturing, retail, and financial services, TraceSecure™ has demonstrated 99.4% signal fidelity, sub-15ms evaluation latency, and zero production disruptions. The framework delivers immediate protection to both brownfield and greenfield S/4HANA landscapes.

Sources & Next Steps

This publication references official SAP product security guidance, NIST publications, and SAPSOL advisory frameworks.

PUBLICATION EDITION: 09 NOVEMBER 2026.

01 SAP Security Whitepaper: Defense in Depth for SAP S/4HANA Enterprise Deployments

02 NIST Special Publication 800-207: Zero Trust Architecture Guidance & Core Principles

03 SAP Note 2622660: Security Configuration Recommendations for SAP S/4HANA Cloud and On-Premise

04 SAP Help Portal: ABAP Security Guidelines and System Security Audit Log Configuration (SM20)

05 CISA Advisory Alert AA22-110A: Malicious Cyber Actors Target Mission-Critical Enterprise ERP Applications

06 SAP Integration Suite Security Guide: Protecting Cloud Integration Endpoints & Message Pipelines

07 Ponemon Institute & IBM Security: Cost of Insider Threats Global Enterprise Benchmark Report

08 ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection (Annex A.8.16)

09 TraceSecure™ Technical Architecture Specification: SAPSOL Technologies LLC

RESEARCH AND METHODOLOGY NOTES

Research status: Prepared against publicly accessible SAP product documentation and enterprise cybersecurity benchmarks available as of November 2026. Security terms and configuration parameters may vary by release. Verify current SAP Help Portal and customer-specific support contracts prior to procurement or architecture commitment.

Methodology & Trademarks: The Zero Trust operational model, Dynamic Anomaly Score (DAS) formulation, and implementation roadmaps are SAPSOL editorial frameworks. SAP, SAP S/4HANA, SAP NetWeaver, SAP BTP, SAP Ariba, and other SAP products referenced are trademarks or registered trademarks of SAP SE or its affiliates.

DISCUSS YOUR ZERO TRUST ROADMAP WITH SAPSOL

SAPSOL Technologies LLC helps enterprise security and Basis leaders assess ERP threat postures, deploy TraceSecure™ behavioral surveillance, and achieve continuous audit compliance.

Website: www.sapsol.com • **Direct Consultation:** sapsol.com/book-a-consultation/ • **Email:** info@sapsol.com • **Phone:** +1 343 800 0733

Corporate Locations: Santa Clara, CA (HQ) • Mississauga, ON