SAP FRAUD · BEHAVIORAL DETECTION · MANAGED EXTENDED DETECTION & RESPONSE (M/XDR)

From Transaction Noise to Board-Level Evidence:

Governing Fraud Exposure Across SAP Environments

How Banyax turns fragmented SAP transaction monitoring into a board-ready fraud prevention governance program with measurable KRI reduction, automated audit trails, and structural client retention.

INDUSTRY Cross-Industry · Mid-to-Large Enterprise · SAP ECC / S/4HANA Environments

01 · WHAT CLIENTS ACHIEVE

Four measurable outcomes before reviewing any technical architecture.

Detection Speed	False Positives Drop	SAP Coverage	Audit Trail
5 Hours	**90% to 10%**	**100%**	**Auto**
vs. 2 weeks with manual review/audit	*via behavioral correlation*	*modules monitored 24×7×365*	*audit evidence with minimal manual effort*

Before Banyax, the mid-to-large enterprise running SAP operated with three disconnected supervision layers: ERP transaction logs, manual audit sampling, and periodic vendor master reviews. No correlation. No behavioral baseline. No board-level visibility into procurement fraud exposure.

After Banyax, those three layers collapse into a single fraud governance program with Key Risk Indicator (KRI) trending available to the CFO and Audit Committee quarterly, and forensic evidence auto-generated for any investigation. The organization doesn't just detect faster. It governs.

02 · THE PROBLEM NO ONE WAS SOLVING

Three disconnected supervision layers, zero correlation — and a fraud exposure window that grows every quarter without active governance.

Three silos, zero correlation

Vendor master changes, purchase order patterns, and payment approvals live in separate SAP modules and audit processes. No control correlates them. A coordinated fraud scheme spanning all three stays invisible inside each one.

The authorized user gap

The highest-risk vector in SAP fraud is not an external attacker — it's the authorized user with legitimate credentials acting outside their normal pattern. Static rule-based controls cannot distinguish a routine update from premeditated internal collusion.

No evidence when it matters most

When a fraud incident surfaces weeks or months later, organizations lack a consolidated, tamper-proof record of what changed, who approved it, and what the context was. Forensic reconstruction is manual, slow, and incomplete when auditors or regulators request it.

03 · THREE CORRELATED USE CASES — ONE GOVERNANCE PROGRAM

Detection with real business context, not static rules. Banyax's Security Operations Center (SOC) operates all three use cases in a correlated fashion through Banyax Quest, our proprietary platform. AI-led: AI processes the volume, human analysts validate every escalation.

UC1 New Vendor Monitoring and First-Payment Threshold Detection

Banyax establishes a behavioral baseline for vendor onboarding and initial payment activity. Any first payment to a recently created vendor that exceeds a configurable threshold or bypasses standard approval chains generates an anomaly score. Banyax Quest's engine cross-references vendor creation date, the approving user's historical pattern, and whether a corresponding purchase order exists within the expected lead time.

AI-led role: *Continuous scoring across the full transaction universe, at speed and scale no audit team can sustain manually. Banyax analysts validate every prioritized case.*

UC2 Vendor Master Data Change Correlation

Every modification to a vendor's bank details, tax ID, or contact information is correlated against the role of the user making the change, its timing relative to upcoming payment runs, and whether a formal change request exists in the ticketing system. Detects account takeover attempts — internal or external — where a legitimate vendor's payment destination is silently redirected before a major disbursement.

AI-led role: *Banyax Quest detects the combination of signals — change + user + timing + missing ticket — that individually appear normal but together form a fraud signature. Impossible to sustain in real time with manual review.*

UC3 Duplicate or Near-Duplicate Purchase Order Detection

The engine analyzes consecutive purchase orders from the same vendor, amount proximity within a configurable tolerance, and approval sequence. Detects both exact duplicates — with direct financial impact — and deliberate near-duplicate patterns: the known signature of splitting schemes designed to stay below approval thresholds. Each cluster of suspicious orders is presented as a single consolidated case, not individual alerts.

AI-led role: *Automatic clustering of splitting patterns across hundreds of transactions is the key differentiator. Banyax Quest builds the case; the analyst decides the escalation.*

04 · HOW THE SERVICE OPERATES

From capture to forensic evidence package in five steps — all orchestrated through Banyax Quest.

1	2	3	4	5
CAPTURE	**INGEST**	**CORRELATE**	**ALERT**	**RESPOND**
SAP RFC/API connector or log extraction layer	*Normalized feed: transactions, master data, approval events*	*Behavioral baseline + role context + approval flow + payment calendar*	*Prioritized case queue with risk scoring & evidence*	*Audit-ready evidence package delivered to client/auditors*

05 · WHY BANYAX — THE STRUCTURAL MOAT

Four differentiators that create governance dependency, not contract dependency.

- **Behavioral baseline advantage.**
  The value is not in the ruleset — it's in months of accumulated normal behavior per user, per vendor relationship, and per business unit. A competitor entering today would need 60–90 days of transactional history to detect what Banyax detects from the first anomaly.

- **Managed governance service, not a compliance checklist.**
  The client buys outcomes: qualified alerts, contained fraud exposure, quarterly KRI reports for the Audit Committee, and forensic packages ready for any investigation. No internal team required to operate the detection layer.

- **Business-context detection, not another rules engine.**
  Most SAP fraud controls are threshold-based and role-agnostic. Banyax correlates identity, approval history, procurement calendar, and transaction sequence through Banyax Quest. The result is a signal that reflects the real business context — not a static rule match.

- **Structural retention through governance dependency.**
  Quarterly reporting to the CFO and Audit Committee embeds Banyax inside the organization's governance structure. The relationship shifts from vendor-to-IT to program-to-board. That completely transforms the renewal conversation.

06 · IDEAL CLIENT PROFILE

Mid-to-large enterprises and financial institutions running SAP ECC or S/4HANA with active procurement and accounts payable operations — particularly those that have experienced vendor fraud incidents, are under internal audit pressure to strengthen preventive controls, or operate in regulated industries where transactional traceability is a compliance requirement.

07 · LEARN MORE & CONTACT

Learn more about Banyax M/XDR (Managed Extended Detection & Response) for SAP

Discover how Banyax's Managed Extended Detection & Response (M/XDR) service continuously governs fraud exposure across SAP environments — with AI-led behavioral detection, expert human validation, and board-ready KRI reporting.

Visit: banyax.com

Want to learn more?

If this document was forwarded to you and you'd like to explore how Banyax can help your organization govern SAP fraud exposure — reach out directly.

Email: marketing@banyax.com

Website: banyax.com