



# Internal Fraud Prevention

Fight Internal fraud proactively

# The rising cost of occupational fraud

In 2024, the banking and financial services industry accounted for 19% of all occupational fraud cases - the highest among all sectors. These incidents resulted in an average loss of over \$1.5 million, with a median undetected duration of 8 months.

Traditional approaches - based on static rules, manual controls, and fragmented oversight - not only fail to detect fraud early, but also generate overwhelming volumes of false positives. Even when initial red flags are raised, the time it takes to move from suspicion to grounded, actionable evidence is often too long. This delay allows harmful activity to continue, increasing financial loss and reputational risk.

## Next-Gen Internal Fraud Protection

Vyntra's Internal Fraud solution offers a proactive and continuous approach to internal fraud detection, going beyond traditional rule-based systems. By employing our advanced 3D AI combined with business logic, it can detect suspicious situations without relying on predefined scenarios. The solution leverages behavioral signs from employees and customers profiling to enhance detection accuracy. This adaptability ensures that even previously unknown fraud techniques are identified.

### Fraud we stop

- Misappropriation of assets
- Unauthorized Funds Transfer
- Internal-external collusion
- Client Statement Manipulation / Performance
- Misrepresentation Window Dressing / Temporary Fund Movement
- Account Takeover
- Check and Payment Tampering
- And others

## Key Benefits



Delivers effective results quickly, with minimal setup or overhead.



Discourage opportunistic fraud by introducing continuous and proactive monitoring.



Detects fraud without relying on predefined scenarios, thanks to AI anomaly detection.



Drastically improves operational efficiency, by streamlining investigations.

**85%** Reduction in false positives

10x faster investigations

## Core capabilities

### 1. Drive Operational Efficiencies

Our AI does all the heavy lifting, offering deeper insights, reducing false positives, and improving operational efficiency. Alerts are aggregated by risk actors, e.g. employees, filtered according to business logic, and presented by degree of significance, enabling experts to focus on what matters most. Customizable workflows ensure full transparency, with proper documentation and segregation of duties.

### 2. Unrivaled Investigative Tools

Standardized, intuitive, widget-based dashboards support fast, effective case assessments by presenting at a glance all business-relevant information about employees and customers. Filtering, drill-down, and correlation capabilities enable more sophisticated and proactive investigations, helping analysts manually detect intricate cases across transactional, employee, and customer data.



### 3. Powerful Analytics and Adaptive Monitoring

Advanced AI models work alongside business logic to detect anomalies and suspicious patterns. The system combines pre-packaged use cases with agnostic analytics to uncover unknown fraud schemes, while an adaptive monitoring framework ensures new patterns and behaviors are easily integrated. Full customization guarantees flexibility across any business environment.



# Key Features

## Smart case aggregation mechanism

AI models detect suspicious scenarios using pattern recognition and anomaly detection powered by 3D AI. From the many generated events, only a select few are escalated to investigators. Events are automatically filtered and grouped by risk actor -such as employees or roles - based on business- defined logic, and continuously fed into existing cases.

This ensures that each case evolves with new evidence, while minimizing noise and preserving critical signals. By structuring cases around individuals or roles, the system makes it easy for investigators to follow up, monitor, and build a complete picture of suspicious employee behavior over time. Business logic is enforced at case creation to ensure alignment with your organization’s structure and risk appetite, enabling efficient

Created	04/03/2025 12:01 PM	Status	New
Source User	JACK	Assignee	
Priority	-not set-	Subject	Employee alert

## AI Model alerts

RISKY TRANSACTION:71916269144309771						
CONSOLIDATED AI ALERT						
Transaction Timestamp	Account ID	Transaction ID	Transaction Amount	Transaction Counterparty	Transaction Inputter	Transaction Validator
2025-03-19T11:16:27+01:00	66621314179365	71916269144309770	28130.45	1111	JACK	JACK

## Automated case prioritization

Once high-risk events are filtered and cases are created through smart aggregation, this feature ensures investigators start with what matters most.

Cases are automatically scored and ranked based on business-defined severity criteria, such as the number of related events and the associated financial amounts. Prioritization takes into account the context of the risk actor and known fraud typologies, helping fraud teams focus first on the most suspicious and impactful cases. This reduces time to action and improves investigative efficiency.

## Case assessment dashboard

A centralized, widget-based interface provides investigators with all relevant contextual and investigative data for each case - at a glance. Information related to the risk actor, behavioral anomalies, transaction history, and linked entities is presented in a clear, structured format. Powerful filtering, drill-down, and correlation tools support efficient, repeatable assessments, helping investigators understand the full scope of a case quickly and take informed action. By consolidating all critical insights in one place, the dashboard accelerates workflows and improves the consistency and quality of internal fraud investigations.

## Monitoring dashboard

A dedicated interface enables ongoing monitoring of flagged events that were not escalated to full cases. Analysts use their business expertise and external intelligence - such as HR signals, whistleblower reports, or contextual knowledge to identify patterns and assess risk beyond what automated logic may detect. The dashboard allows manual filtering, review, and investigation of lower-severity signals, helping to surface emerging threats or subtle behaviors. By bridging automated detection with expert-driven insight, this feature enhances adaptability and supports proactive internal fraud prevention.

The dashboard interface includes a timeline at the top with a search bar and a 'Last 1M' filter. Below the timeline, there are several data widgets:

- Internal Fraud Case Assessment** (Section Header)
- user004** (Employee id)
- Thomas Wattson** (User name)
- COCR - Credit Control** (Department)
- 2** Customer impacted
- 1** Counterparty account id
- 70,000.00** Sum of amounts
- 40,000.00** Max Amount
- 30,000.00** Min amount

At the bottom, there is a 'VALIDATOR' section with a table:

order_id	validator_id	valid_date	validator_user_name	validator_department