

Seceon aiFraudGuard360

Claims, Premium and Payout Fraud Defence for Insurance

Real-time payout interception, account-takeover and push-payment scam defence, AML and sanctions screening, and graph analytics that exposes the whole fraud ring decided before funds move, on Seceon OTM.



Product Overview

Insurance fraud now runs at machine speed. Deepfake identities, forged telematics and stolen KYC packs pass through automated claims portals. Authorised push payment scams divert premium and settlement flows into multi-hop mule networks. Collusive rings rotate claims across carriers so that each one stays under every insurer's investigation threshold.

Single-transaction rules see five separate, normal claims and pay all five. Retrospective SIU review then recovers cents on the dollar. aiFraudGuard360 moves the decision forward: it evaluates the payout request in-line and places fraudulent claims and account takeovers on hold before the wire leaves the bank.

Because aiFraudGuard360 runs on the same Seceon OTM stream-processing core as aiSIEM and aiXDR, the fraud decision is informed by cyber telemetry identity, email, network and endpoint rather than built as a siloed fraud-only tool. The practical outcome is fewer fraudulent disbursements, ring-level evidence for prosecution, and a deployment that stays inside the customer's borders.



Highlights



Real-time payout interception, account-takeover and push-payment scam defence, AML and sanctions screening, and graph analytics that exposes the whole fraud ring decided before funds move, on Seceon OTM.



Real-time payout interception scoring behaviour, bank-account change recency and payee risk



Account-takeover and SIM-swap defence via direct carrier signalling (HLR/HSS)



Authorised push payment (APP) scam shield that detects remote-access screen sharing during claims sessions



Fuzzy AML and sanctions screening against UN, OFAC and regional watchlists before binding or claim release



In-memory graph analytics that exposes multi-hop syndicates and freezes the whole cluster, not one case



Identity, email, network and endpoint signals feed one decision; asset-based pricing, not per transaction



What aiFraudGuard360 Intercepts

What aiFraudGuard360 Intercepts

Area	What it does
Real-time payout interception	Scores behavioural velocity, bank-account change recency and payee risk inside the authorisation path, before high-value settlement wires or mobile wallet transfers clear
Account takeover and SIM swap	Verifies recent SIM-swap events on the claimant's number through carrier signalling (HLR/HSS); a recent swap or impossible-travel velocity places a high-value disbursement on protective hold
Push-payment scam shield	Uses endpoint and session telemetry to detect active remote-access screen sharing during claims and servicing sessions the pattern where the victim authorises the payment themselves
AML and sanctions screening	Fuzzy screening against UN, OFAC and regional watchlists prior to policy binding or claim release; produces the audit trail and regulatory report drafts
Fraud ring detection	Graph traversal links shared phone numbers, device identifiers, IBANs, repair shops and loss adjusters into one connected structure, beyond the second degree
Cluster freeze	Holds claims across the entire ring at the same time instead of one case at a time
Evidence pack	Complete visual evidence pack suitable for SIU escalation and legal prosecution
Cross-carrier sharing	Anonymised hashes of flagged claims, rogue repair shops and mule wallets exchanged between insurers, with no PII exposure



The Fraud Patterns It Addresses

Threat	How it works	aiFraudGuard360 response
Claims portal exploitation	Deepfake identity, forged telematics and stolen KYC packs submitted through automated claims portals	Identity, device and session signals scored with the claim before payout
Payment diversion (APP)	Social engineering leads the victim to authorise premium or settlement flows into mule networks	Remote-access screen-sharing detection and payee-risk scoring in the authorisation path
Account takeover	SIM swap or credential theft used to change payout details and redirect a disbursement	Carrier SIM-swap check, impossible-travel velocity and bank-account change recency trigger a protective hold

Threat	How it works	aiFraudGuard360 response
Collusive syndicates	Corrupt garages, staged claimants, dishonest adjusters and rogue clinics rotate claims across carriers	Multi-hop graph analytics exposes the ring and freezes the whole cluster
Cross-insurer smurfing	Each claim kept below every insurer's SIU trigger	Anonymised cross-carrier hash sharing through a fraud defence exchange
Synthetic identities	Ghost policies sharing phone numbers, devices and bank accounts	Shared-attribute linkage surfaces identities that should not overlap
Sanctions and AML exposure	Listed parties bound to policies or paid on claims	Fuzzy watchlist screening before binding or release, with an audit trail



Decision Signals and Fraud Value

Signal domain	Example signal	Fraud value
Payment and payee	Bank-account change recency, payee risk, behavioural velocity	Stops diverted or fraudulent payouts before funds clear
Telecom carrier	Recent SIM-swap events via HLR/HSS	Flags account takeover on the claimant's number
Endpoint and session	Active remote-access screen sharing during a claims session	Catches APP scams the victim authorises
Identity	Logon behaviour, impossible travel, credential misuse	Distinguishes the real policyholder from an impostor
Email and network	Phishing delivery, suspicious infrastructure	Links cyber intrusion to the fraud attempt
Graph entities	Shared phones, devices, IBANs, repair shops, adjusters	Exposes collusive rings and synthetic identities
Watchlists	UN, OFAC and regional sanctions lists	AML and sanctions control before binding or release

Key Capabilities

Payout and transaction defence (core product surface)

- In-memory transaction and payout scoring in the authorisation path
- Protective hold on high-value disbursements on SIM-swap or impossible-travel signals
- Remote-access scam detection from live endpoint and session telemetry
- Fuzzy AML and sanctions screening with audit trail and regulatory report drafts

Fraud ring and collusion detection

- Graph traversal across claimants, adjusters, devices, accounts and repair shops, beyond the second degree
- Cluster-wide claim freeze and visual evidence pack for SIU and prosecution
- Anonymised, PII-free sharing of flagged claims, rogue repair shops and mule wallets between carriers

Platform (OTM)

- Unified with cyber telemetry: identity, email, network and endpoint feed the same fraud decision
- Native Kafka and Spark stream pipeline with no proprietary relational database in the hot decision path
- Horizontal scale-out on hardened Linux and Kubernetes
- Federated, multi-tenant, multi-tier administration for groups, reinsurers and federations



Primary Use Cases

Use case	How aiFraudGuard360 helps
Digital claims settlement	Evaluates each payout in-line so fast settlement does not mean paying fraud faster
Motor claims rings	Links garages, adjusters, claimants and shared IBANs; freezes the cluster; produces the evidence pack
Policyholder account takeover	SIM-swap and impossible-travel checks hold the payout when contact or bank details were just changed
Settlement and premium diversion	Detects remote-access sessions and risky payees before an authorised push payment clears
Sanctions control at binding	Screens parties against UN, OFAC and regional lists before policy binding or claim release
Compulsory motor growth markets	Claims and premium fraud interception on fast-growing lines, with an evidence pack for reinsurance compliance
Federation fraud exchange	Cross-carrier hash consortium that blocks rings rotating claims between member insurers



Why aiFraudGuard360

Use case	How aiFraudGuard360 helps
Digital claims settlement	Evaluates each payout in-line so fast settlement does not mean paying fraud faster
Motor claims rings	Links garages, adjusters, claimants and shared IBANs; freezes the cluster; produces the evidence pack
Policyholder account takeover	SIM-swap and impossible-travel checks hold the payout when contact or bank details were just changed
Settlement and premium diversion	Detects remote-access sessions and risky payees before an authorised push payment clears
Sanctions control at binding	Screens parties against UN, OFAC and regional lists before policy binding or claim release
Compulsory motor growth markets	Claims and premium fraud interception on fast-growing lines, with an evidence pack for reinsurance compliance
Federation fraud exchange	Cross-carrier hash consortium that blocks rings rotating claims between member insurers
Cross-carrier sharing	Anonymised hashes of flagged claims, rogue repair shops and mule wallets exchanged between insurers, with no PII exposure



Deployment, Compliance and Data Sovereignty

- Deployment options: on-premises, air-gapped, sovereign local cloud or hybrid the customer chooses the boundary
 - No overseas AI in the decision path, a prerequisite for sovereign deployment
 - Aligned to SAMA, UAE NESAC/CBUAE, the Central Bank of Jordan and Levant data protection regimes
 - In-country sovereign hosting supports Jordan's PDPL (Law No. 24 of 2023) cross-border transfer limits
 - Hierarchical administration: central HQ keeps aggregated risk visibility while operating companies manage local policy under segregation of duties
 - AML and sanctions output provides the audit trail and report drafts; regulatory filing remains with the institution
- Detection, latency and containment service levels are engineering design targets, established in a scoped proof of concept against your own traffic



Regional Market Fit

Market	Where aiFraudGuard360 applies
Jordan	Reference deployment; supervised by the Central Bank of Jordan. Proposed with JIF as the host market for an Insurance Cyber and Fraud Defence Exchange
Lebanon	Sector restructuring under way; Beirut remains the region's reinsurance brokerage hub. Build claims and payment rails secure from the start
Iraq	Claims and premium fraud interception on fast-growing compulsory motor lines, with an evidence pack for reinsurance compliance
Palestine	Identity assurance and claims-fraud defence across a small, concentrated carrier base where one ring moves the loss ratio
GCC and North Africa	Replicate the Jordan blueprint under GAIF across member markets



Platform Evidence

Measure	Platform-wide figure
Customers protected	10,000+ across all verticals, globally
Financial organisations	2,500+, including 600+ credit unions
Events processed daily	3.2 trillion on the native stream pipeline
Active partners	850+ in multi-tier MSSP distribution



Ideal Buyers

- Primary insurers running digital claims settlement and mobile wallet or wire payouts
- Reinsurers that need evidence of cedant fraud controls and claims integrity
- Regional brokers packaging claims-payout defence with commercial placements
- Insurance federations and associations building a cross-carrier fraud defence exchange
- Groups and holding companies needing central visibility with local segregation of duties



Next Steps

Step	Detail
Proof of concept	A scoped proof of concept against your own traffic and claims data
Federation exchange	A working committee or MoU with JIF to evaluate an industry-wide consortium pilot in Jordan
Executive briefing	Book a 20-minute briefing through the GAIF 2026 meeting hub
Contact	Chandra S. Pandey, Founder & CEO · cp@seceon.com · enterprise@seceon.com · +1-978-923-0040
Seceon datasheets hub	https://seceon.com/datasheets/

One-Line Pitch

aiFraudGuard360 lets insurers stop claims and premium fraud before the payout scoring every disbursement in the authorisation path, exposing whole fraud rings with graph analytics, and running inside their own sovereign borders on the Seceon OTM platform.

About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 850 partners, Seceon supports more than 9,800 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon



Schedule a Demo

www.seceon.com/contact-us/

