

The Human Factor

How Agentic AI and Graph Analytics Mitigate Insider Threats

Executive summary

Insider threats—malicious, negligent, or compromised users—remain a top cause of breaches and loss. Visium TruContext combines persistent multi-layer graph modeling with agentic Artificial Intelligence (“AI”) to turn noisy user telemetry into precise, prioritized actions. Rather than just alerting, TruContext’s agents investigate, enrich, prioritize by business impact, and where authorized, orchestrate containment and remediation so teams stop insider incidents before they escalate.

The insider threat challenge

- **Varied origins:** threats arise from malicious insiders, careless employees, and externally compromised credentials.
- **Subtle signals:** risky behavior often looks like legitimate activity and hides in high-volume telemetry.
- **Operational overload:** security teams drown in alerts; manual enrichment and investigation slow response and increase drift.

These realities demand contextual reasoning that links identity, data access, asset relationships, and business impact—at scale and in real time.

TruContext approach: graph context plus agentic AI

- **Persistent multi-layer graph** Continuously models users, identities, devices, applications, data stores, flows, and third-party relationships to reveal true context for every action.
- **Behavioral baselining and predictive analytics** Models normal user behavior across identity, device, location, and data access to surface early anomalies that precede insider incidents.
- **Agentic AI orchestration** Autonomous agents traverse the graph and telemetry to perform rapid investigation, produce concise evidence packages, recommend prioritized mitigations, and—when governance permits—execute containment steps such as credential revocation, endpoint isolation, or blocking exfiltration channels.

Concrete agent workflows against insider threats

- **Anomalous access triage** Agents aggregate suspicious file reads, unusual data exports, and abnormal access times; they enrich events with asset criticality and recent configuration changes and present a single, prioritized alert for analysts.
- **Compromise vs. intent analysis** Agents correlate email behavior, login patterns, device health, and third-party access to distinguish between compromised accounts, negligent misuse, and intentional exfiltration, reducing false positives.

- **Attack-path exploration** Agents simulate lateral movement from a suspect account through the graph to high-value data stores and external sinks, ranking likely escalation paths and recommending focused containment points.
- **Controlled remediation orchestration** Agents create prioritized tickets with exact artifact lists, trigger SOAR playbooks, or perform approved containment actions with full audit trails, shortening the attacker's window and preserving forensic evidence.
- **Post-incident hardening** Agents produce clear remediation roadmaps—segmentation changes, policy updates, privileged access reviews—and simulate how each change reduces future attack-path availability.

Business outcomes and metrics

- **Faster, higher-confidence detection** — early indicators flagged and enriched so analysts focus on real risks.
- **Reduced mean time to remediate** — agentic orchestration shortens handoff cycles and automates routine containment.
- **Lower analyst fatigue** — agents handle enrichment and routine actions, freeing humans for complex decisions.
- **Better executive visibility** — business-aligned risk scoring converts technical events into decision-ready summaries.

Implementation and governance

- **Integrates with existing stacks** — SIEM, SOAR, IAM, EDR, cloud providers, and ticketing systems.
- **Policy-first automation** — agent actions adhere to governance rules; high-impact operations require authorization and produce immutable audit logs.
- **Phased adoption** — start with discovery and alert enrichment, then enable prioritized recommendations, and finally move to controlled orchestration once playbooks and approvals are in place.

Conclusion

Insider risk is a people-centric problem that needs context-aware, action-oriented defenses. Visium TruContext combines deep graph context with agentic AI to detect the nuanced signals of insider threats, prioritize them by business impact, and turn investigation into decisive, auditable actions. The result is a proactive posture that defends sensitive data, reduces disruption, and gives security teams the clarity and agency they need to manage the human factor effectively.