KASEWARE

Facilitating Operational Resilience for Financial Security Operations

Connecting intelligence, investigations, and response workflows to reduce risk and support faster decisions

Modern Threats Expose Operational Gaps

Security teams at financial institutions protect systems that support economic stability, customer trust, and business continuity and are managing increasingly complex and connected threats across cyber, fraud, insider risk, physical disruption, and supply chain risk, all while maintaining operational resilience. Yet many investigative, intelligence, and response functions remain fragmented across disconnected systems and siloed teams, slowing response, limiting visibility, and increasing operational and financial risk.

As threat timelines compress and regulatory expectations evolve, resilience increasingly depends on connected intelligence, coordinated response, and the ability to transform risk into action. Kaseware helps organizations unify investigations, intelligence, and response workflows to support faster, more informed decision-making.

Why Financial Institutions Choose Kaseware

Unified Operational and Financial Intelligence

Bring security incidents, fraud investigations, threat intelligence, OSINT findings, field reports, and response activity into one connected environment so teams can improve visibility across branches, corporate offices, ATMs, data centers, executives, vendors, and other high-value operations.

Coordinated Investigations and Response

Help physical security, fraud, cyber, intelligence, compliance, legal, HR, and enterprise risk teams work from shared case information, assign ownership, manage handoffs, and reduce delays when threats cross departments or business units.

Risk-Driven Investigation Workflows

Turn alerts, referrals, suspicious activity, insider concerns, and external threat signals into structured investigative workflows with clear priorities, approvals, evidence management, tasking, and escalation paths.

Force Multiplication for Lean Security Teams

Reduce manual reporting, duplicate data entry, email-based coordination, and tool switching so lean teams can manage more cases, incidents, and operational requests without losing context or consistency.

Regulatory Compliance Support

Support regulatory and audit requirements through structured workflows, role-based access, traceable actions, and reporting that help teams demonstrate how investigations and response activities were managed.

Enabling Risk-Driven Operations

- **Get a shared risk picture:** Connect fraud, cyber, insider, physical, and reputational signals so teams can see related risks faster.
- **Get coordinated investigations:** Bring security, fraud, compliance, legal, and risk teams into one workflow for ownership, escalation, and response.
- **Get defensible records:** Track actions, approvals, evidence, and outcomes so teams can support audits, reviews, and regulatory responses.
- **Get more capacity from existing teams:** Reduce manual handoffs, duplicate entry, and tool switching so analysts can focus on higher-priority cases.
- **Get clearer operational visibility:** Give corporate and regional teams better visibility into active investigations, response status, repeat issues, and emerging risks across locations and business lines.

Connecting Intelligence to Action

Kaseware helps financial services organizations improve operational resilience through connected intelligence, coordinated investigations, and shared operational workflows.

By reducing fragmented processes and improving decision-making, Kaseware helps security, fraud, and resilience teams respond faster, coordinate more effectively, and improve operational visibility across today's evolving financial threat landscape.

LEARN MORE

Contact Us

844-kaseware

www.kaseware.com