KASEWARE

Connected Security for Critical Data Infrastructure

Unifying teams, tools, and intelligence across your most complex security environment

Complexity Is the New Attack Surface

Data centers are now the operational backbone of the global economy. As their criticality grows, so does the sophistication of the threats targeting them. Physical intrusions, insider threats, third-party access risks, and cyber incidents are no longer separate concerns managed by separate teams. They are converging, and most security programs were not built to handle that convergence.

Security operations leaders are managing sprawling environments with lean teams, disconnected tools, and workflows that were designed for a simpler threat landscape. When a contractor badge event, a network anomaly, and an open investigation live in three different systems, the connections that matter most go unseen.

Built for the Operational Demands of Data Center Security

Unified Case & Incident Management

Manage physical security events, access anomalies, contractor issues, cyber-adjacent incidents, and active investigations in one configurable platform, so SOC, site security, IT, and operations teams work from the same picture.

Link Analysis & Intelligence Tools

Surface connections across people, badges, vehicles, facilities, incidents, vendors, and locations using link analysis and geospatial tools, helping teams identify patterns that may affect uptime, safety, or asset protection.

Insider Threat & Access Risk Investigations

Bring security, IT, HR, and compliance stakeholders into connected investigative workflows with layered access controls and relationship mapping that ensures proper documentation and chain of custody without sacrificing efficiency.

Workflow Automation & Configurable Operations

Reduce manual coordination with customizable workflows, dynamic forms, automated alerts, and task management built for high-volume data center security operations.

Integrated Data, Reporting, & Executive Visibility

Centralize SIEM, OSINT, access logs, field reports, and incident data into unified dashboards and automated reports for board-level visibility and continuous improvement.

Closing the Gaps That Put Data Centers at Risk

- **Cross-Team Coordination:** Break down silos between security, IT, and compliance teams with shared workflows and a unified operational picture.
- **Threat Pattern Recognition:** Connect incidents, access events, and anomalies across sites and facilities using link analysis and geospatial intelligence.
- **Investigation Speed:** Reduce time from alert or incident to resolution with automated workflows, centralized case data, and dynamic reporting.
- **Vendor & Third-Party Accountability:** Track and manage contractor, vendor, and visitor risk within a centralized, auditable environment.
- **Scalable Operations:** Help lean security teams manage complex, high-availability environments through automation and configurable workflows.
- **Audit-Ready Documentation:** Maintain structured records of investigations, incidents, and decisions for audits, reporting, and accountability.

Partner with Kaseware

Kaseware helps data center security teams strengthen resilience through connected intelligence, coordinated investigations, and shared security operations workflows. By reducing fragmented processes and improving visibility across incidents, access events, vendor activity, and site-level risks, Kaseware helps security, IT, facilities, and compliance teams respond faster, coordinate more effectively, and protect the high-availability environments their customers and operations depend on.

Contact Us

844-kaseware

www.kaseware.com