KASEWARE

# Security Convergence

## A Unified Approach to Modern Security Challenges

2025

# Table of Contents

# Security Convergence in an Increasingly Interconnected World

The ever-increasing number of networked devices across public and private organizational real estate poses significant challenges for security professionals. This interconnected web of hybrid cyber/physical systems both increases overall vulnerability and exposes gaps in coordination between the traditionally distinct functions of physical security and cybersecurity.

As most security professionals know, a successful cyber or physical attack on an organization's networks or industrial control systems can disrupt operations, deny critical services to the public, or even cause more severe consequences. **When physical security and cybersecurity teams operate in silos—along with the tools they use—threat visibility is obscured, making successful attacks more likely and increasing the severity of their impact**.

This paper focuses on the benefits of a security strategy that aligns cybersecurity and physical security functions with organizational priorities, and business objectives, together with the proper software tools to support this strategy.

# Security Convergence: A Vital Strategy

Security convergence is the integration of all security domains to identify, prioritize, and manage business security risks effectively. It focuses on protecting people, assets, and information from harm. In today's world, **cybersecurity and physical security are inseparable**, meaning a cyber-attack can cause real-world consequences such as financial loss, identity theft, and operational disruption.

> "Security convergence is the integration, in a formal, collaborative, and strategic manner, of the cumulative security resources of an organization in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings".
>
> – Dave Tyson, past ASIS International President (2015)

Tyson, D (2007) Security Convergence: Managing Enterprise Security Risk, Elsevier.

To further define it, security convergence contains the following elements:

- **Formal cooperation** between previously separate security functions
- **Strategic alignment** that involves **processes and accountability**
- More than just an organizational reshuffling—it must involve both an **organizational** and **technology-driven approach**

As organizations strive to implement a unified security strategy, it becomes clear that security convergence is not just about integrating processes—it is about addressing the growing interconnectivity between cyber and physical systems. **One of the most significant drivers of this convergence is the rise of the Internet of Things (IoT)**. The proliferation of IoT devices has introduced new complexities, expanding the attack surface and reinforcing the need for seamless collaboration between cybersecurity and physical security teams. Understanding the implications of IoT security is crucial for developing a holistic, risk-based approach to modern security threats.

# The Scope of IoT and Its Security Implications

While IoT (Internet of Things) is not a new concept, it continues to be relevant to the convergence discussion, as technologies and methodologies continue to evolve. As cyber-physical systems become more prevalent, their connection to the broader Internet of Things ecosystem becomes increasingly evident. The rapid expansion of networked devices amplifies security concerns and underscores the need for a unified security strategy.

As of 2024, the number of IoT devices connected globally is estimated at 18.8 billion, reflecting a 13% increase from 16.6 billion in 2023.

- **Every second, 127 new IoT devices connect to the internet**, increasing the attack surface available to threat actors.
- Projections indicate that **40 billion IoT devices** will be connected **by 2030**, significantly increasing the attack surface for cyber threats. This rapid growth necessitates a more integrated security approach to mitigate risks associated with the expanding interconnectivity of both personal and industrial IoT systems. (IOT Business Review).
- This includes not only personal devices such as **smartphones and tablets**, but also **security sensors**, **cameras**, and **IoT-enabled security devices**.

**IoT security is a key driver of Security Convergence**, as highlighted by CISA. The increasing adoption of IoT and Industrial IoT (IIoT) devices has created a complex, interconnected cyber-physical system (CPS). This growing network expands the attack surface and blurs the traditional boundaries between cybersecurity and physical security.

David Clark, a converged CSO and former ASIS UK Chapter Chair, managed a smart building enterprise in London, with thousands of IoT sensors and systems stated that, "without a converged security approach, protecting the building would be nearly impossible. The complexity of these interconnected devices requires integrated monitoring and risk management to prevent vulnerabilities being exploited."

For a deeper understanding of IoT security and best practices, refer to the **IoT Security Foundation Guide.**

READ NOW

# Key Benefits of Security Convergence

According to **ASIS International's report, "The State of Security Convergence,"** organizations implementing security convergence experience the following benefits:

- Better alignment of security strategy with corporate goals
- Enhanced communication and cooperation
- More versatile and well-rounded security staff
- More efficient security operations
- Greater visibility and influence with the C-suite and board
- Cost savings through reduced duplication of effort and technology convergence
- Establishing shared security practices across cybersecurity, physical security, and business continuity teams

One of the most substantial benefits of security convergence is the cost savings on shared IT and office space, energy consumption, rental of equipment, and fewer meetings as there is one team to work with instead of two. Of course, fraud is easier to detect given an attack could occur by compromising physical access but if this is linked seamlessly to the network access, an unauthorized sign in will not match the physical location of the staff member. Hence a log-in from home when the authorized person is in the office will be denied. Since many attacks are remote this will obviously cut the risk associated with online fraud. Given that some fraud schemes take years to uncover, implementing integrated security monitoring significantly enhances an organization's ability to detect and respond to threats in real-time.

**As technology continues to blur the line between physical and cyber security**, the benefits of convergence far outweigh the challenges of organizational restructuring. A fully converged security strategy ensures a proactive, efficient, and effective response to today's security challenges.

# Converged Security Centers: Real-Time Risk Management

The next step in security convergence is the development of Converged Security Centers, which integrate cyber and physical monitoring into a unified platform. These centers offer real-time threat detection and response capabilities. For example, a security officer can suspend a VPN connection if the authorized employee is physically present in the office, preventing unauthorized remote access.

The array of cyber physical security capabilities enabled by these technologies is rapidly developing but is only deployed in a few leading global companies.

## CYBER-PHYSICAL SYSTEMS (CPS)

The United States **National Institute of Standards and Technology (NIST**) defines a Cyber-Physical System (CPS) as:

> “Smart systems that include engineered interacting networks of physical and computational components.”

A **cyber-physical system device** includes **video cameras**, **robots**, and **thermostats**, which are crucial to security convergence because they serve as both input and output devices in an interconnected security network. These devices collect, transmit, and process data that bridge the gap between physical and cyber security domains, making them essential for an integrated security strategy., among others. Any analysis of such devices must emphasize the robustness of their design to ensure they remain a **valued component of an overall security strategy**.[1]

## KEY FEATURES OF CONVERGED SECURITY CENTERS:

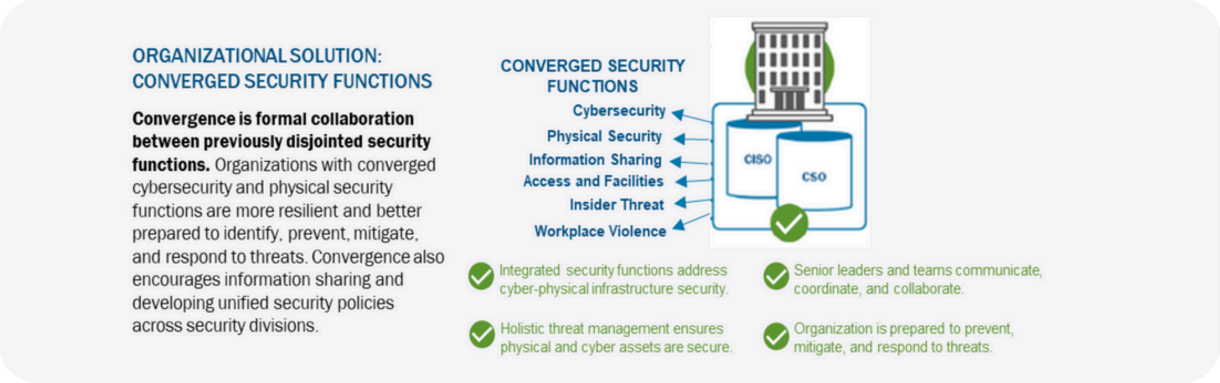
- Integrated security platforms for cyber and physical threats
- Real-time alerts and automated incident response
- Enhanced fraud prevention by linking logical (network) and physical access data
- Centralized visibility into security operations

[1] National Institute of Standards and Technology (NIST). (2016). Framework for cyber-physical systems (NIST Special Publication 1500-201). U.S. Department of Commerce.

# Challenges in Adoption and the Role of Leadership

Most **CISOs** will plan to develop existing **network operations centers** or build new ones but **these will not normally include technologies or software to monitor physical security, building management systems, or IoT devices and systems**. Despite increasing threats highlighted by CISA, many CISOs hesitate to take responsibility for these areas. It is essential for system owners to secure these systems and track access, as poorly configured networks are prime targets for cybercriminals.

IT, Physical Security, and Facilities Management leaders must collaborate with cybersecurity specialists to ensure real-time monitoring of IP video surveillance, access controls, and building management systems. Integrating security policies within a centralized platform allows for automated detection of anomalous device behavior. Even well-protected IP cameras can be hijacked, potentially enabling unauthorized access. For instance, attackers could redirect a camera's focus, allowing an accomplice to enter undetected. Given that some fraud schemes take years to uncover, implementing integrated security monitoring significantly enhances an organization's ability to detect and respond to threats in real time.



ORGANIZATIONAL SOLUTION:
CONVERGED SECURITY FUNCTIONS

**Convergence is formal collaboration between previously disjointed security functions.** Organizations with converged cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats. Convergence also encourages information sharing and developing unified security policies across security divisions.

CONVERGED SECURITY FUNCTIONS

✓ Integrated security functions address cyber-physical infrastructure security.

✓ Holistic threat management ensures physical and cyber assets are secure.

✓ Senior leaders and teams communicate, coordinate, and collaborate.

✓ Organization is prepared to prevent, mitigate, and respond to threats.

Figure Source: DHS, CISA, ISA. Security Convergence: Achieving Integrated Security

## KEY CHALLENGES INCLUDE:

- Escalating and emerging threats
- Risk of oversight and managing false alarms
- Overwhelming amounts of security data
- The need for real-time response to mitigate threats

CSOs are increasingly investing in new security technologies for their Security Operations Centers, yet many overlook cyber solutions for managing risks to physical security systems. Integrating these capabilities would enable faster threat response, real-time risk visibility, and the ability to prevent both on-site and remote attacks.

To address these issues, **senior leadership must drive convergence efforts**. In the U.S., security leaders are now expected to **manage all security risks holistically** rather than treating cybersecurity and physical security as separate domains.

> "Senior leaders set the vision and tone for organizations and are key to instituting cultural change. Because the current siloed security model cannot efficiently mitigate today's complex threats and attack vectors, organizations must begin to evolve their senior-most security leadership to assume responsibility for all aspects of enterprise security."
>
> Integrated security depends upon cooperative partnerships between multiple professionals including IT specialists, facility engineers, resource managers, physical security specialists, and cybersecurity specialists. Proper organizational alignment is key, and departments or agencies should ensure organizational alignment recognizes, supports, and sustains a converged approach to security that addresses the threats stemming from attacks targeting both physical and cyber assets. Approaches to accomplish this include one or more of the following: Governance, Organizational, and Procedural".

DHS, CISA, ISA. Security Convergence: Achieving Integrated Security[1]

## ORGANIZATIONAL SIZE AND CONVERGENCE

A survey of over 1,000 CSOs, CISOs, and business continuity heads found that **smaller organizations tend to have higher levels of convergence**, whereas larger companies struggle due to organizational complexity and resistance to change.

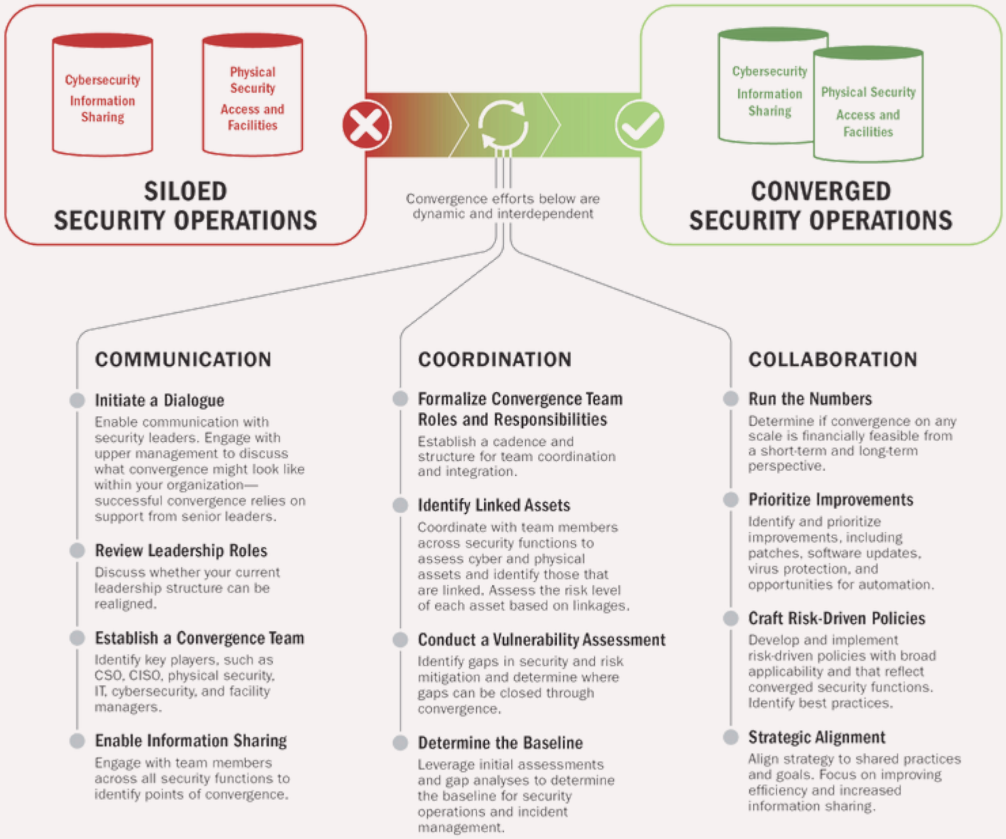
## KEY FINDINGS FROM THE SURVEY:

- Utilities and energy sectors have the highest convergence levels
- Financial services and hospitality follow closely behind
- Retail, healthcare, and manufacturing show the lowest convergence levels

# Achieving Convergence: A Strategic Framework

A successful convergence strategy must align security functions with **organizational priorities and business objectives**, together with the proper tools to support this effort. Any organization, regardless of size, can pursue convergence by focusing on **Communication, Coordination, and Collaboration (The 3 C's)**.

## SECURITY FUNCTIONS FRAMEWORK



### COMMUNICATION

- **Initiate a Dialogue**
  Enable communication with security leaders. Engage with upper management to discuss what convergence might look like within your organization—successful convergence relies on support from senior leaders.
- **Review Leadership Roles**
  Discuss whether your current leadership structure can be realigned.
- **Establish a Convergence Team**
  Identify key players, such as CSO, CISO, physical security, IT, cybersecurity, and facility managers.
- **Enable Information Sharing**
  Engage with team members across all security functions to identify points of convergence.

### COORDINATION

- **Formalize Convergence Team Roles and Responsibilities**
  Establish a cadence and structure for team coordination and integration.
- **Identify Linked Assets**
  Coordinate with team members across security functions to assess cyber and physical assets and identify those that are linked. Assess the risk level of each asset based on linkages.
- **Conduct a Vulnerability Assessment**
  Identify gaps in security and risk mitigation and determine where gaps can be closed through convergence.
- **Determine the Baseline**
  Leverage initial assessments and gap analyses to determine the baseline for security operations and incident management.

### COLLABORATION

- **Run the Numbers**
  Determine if convergence on any scale is financially feasible from a short-term and long-term perspective.
- **Prioritize Improvements**
  Identify and prioritize improvements, including patches, software updates, virus protection, and opportunities for automation.
- **Craft Risk-Driven Policies**
  Develop and implement risk-driven policies with broad applicability and that reflect converged security functions. Identify best practices.
- **Strategic Alignment**
  Align strategy to shared practices and goals. Focus on improving efficiency and increased information sharing.

Figure Source: Cybersecurity and Infrastructure Security Agency (CISA). (2021). Cybersecurity and physical security convergence. U.S. Department of Homeland Security.

# Creating a Cross-Functional Convergence Team Led by One Chief Security Officer

In today's rapidly evolving threat landscape, **security convergence is no longer optional—it's essential**. A single Chief Security Officer (CSO) leading a cross-functional security team ensures better coordination, risk prioritization, and a unified response to emerging threats. Of course, depending on the organization, number, and skill sets of the staff it may be that the CSO and CISO share responsibility. But central is a collaborative approach to enable a single view of risk.

## THE POWER OF ONE SECURITY LEADER

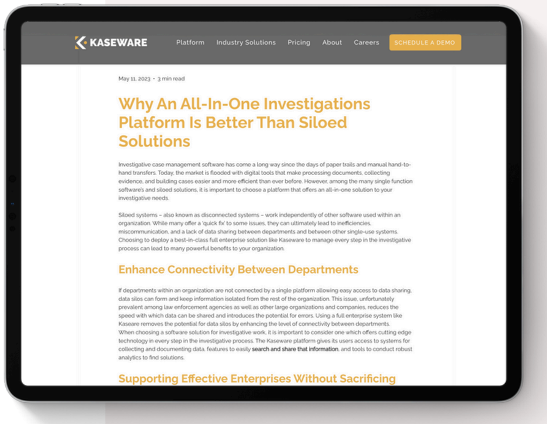
Having one point of contact for all security-related issues can significantly enhance organizational efficiency. According to the PWC/Information Security Awareness Forum (2010), this structure could reduce senior-level meetings by up to 50%, establish a common reporting line, and ensure that all security incidents receive the attention they deserve. With a single comprehensive risk report, organizations gain a holistic view of security threats—enabling them to prioritize and reduce risks more effectively.

## HISTORICAL SUCCESSES OF CONVERGED SECURITY OPERATIONS

Security convergence is not a new concept. Julius Caesar's encrypted military messages, Bletchley Park's WWII intelligence efforts, and modern intelligence-led operations all showcase the power of integrated security strategies. During World War II, coordinated land, sea, and air intelligence allowed Allied forces to defeat a formidable enemy, demonstrating that seamless cooperation across security functions can determine success or failure.

In 2003, Alessandro Lega, a leading European security professional stated, "looking at the physical and logical side of the equation together is important if the results are to truly yield meaningful protection for the company". More recently Axel Petri, Deputy Chief Security Officer of Deutsche Telekom, explained, "Security has realized that silo solutions won't be successful any longer. Security can only be reached if all stakeholders join forces. This is true for the cooperation between physical and cybersecurity in organizations as well as in national companies that are parts of global groups ... Only if we combine our forces can we be successful in tackling new emerging threats".

Security leaders must **break down traditional silos** and embrace a **unified**, **intelligence-led approach**. The time for security convergence is now – **and it starts with a collaborative, integrated security team**.



May 11, 2023 • 3 min read

Why An All-In-One Investigations Platform Is Better Than Siloed Solutions

Investigative case management software has come a long way since the days of paper trails and manual hand-to-hand transfers. Today, the market is flooded with digital tools that make processing documents, collecting evidence, and building cases easier and more efficient than ever before. However, among the many single function software's and siloed solutions, it is important to choose a platform that offers an all-in-one solution to your investigative needs.

Siloed systems – also known as disconnected systems – work independently of other software used within an organization. While many offer a 'quick fix' to some issues, they can ultimately lead to inefficiencies, miscommunication, and a lack of data sharing between departments and between other single-use systems. Choosing to deploy a best-in-class full enterprise solution like Kaseware to manage every step in the investigative process can lead to many powerful benefits to your organization.

Enhance Connectivity Between Departments

If departments within an organization are not connected by a single platform allowing easy access to data sharing, data silos can form and keep information isolated from the rest of the organization. This issue, unfortunately prevalent among law enforcement agencies as well as other large organizations and companies, reduces the speed with which data can be shared and introduces the potential for errors. Using a full enterprise system like Kaseare removes the potential for data silos by enhancing the level of connectivity between departments.
When choosing a software solution for investigative work, it is important to consider one which offers cutting edge technology in every step in the investigative process. The Kaseware platform gives its users access to systems for collecting and documenting data, features to easily search and share that information, and tools to conduct robust analytics to find solutions.

Supporting Effective Enterprises Without Sacrificing

### BREAKING DOWN SECURITY SILOS

Siloed systems create inefficiencies and data gaps. Kaseware's all-in-one platform enables seamless collaboration and secure data sharing.

**Discover how a unified solution enhances security operations.**

Read More

## LESSONS FROM THE PANDEMIC: THE CASE FOR SECURITY CONVERGENCE

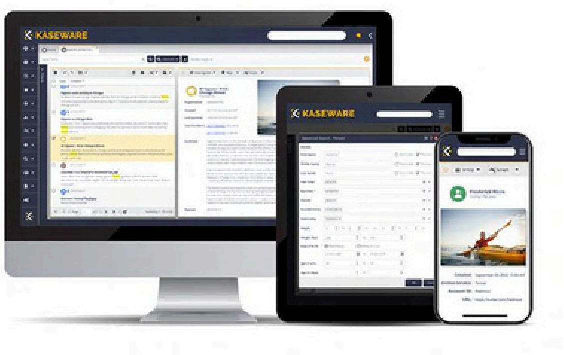
The COVID-19 pandemic provided a real-world example of how converged security strategies drive effective crisis response. In South Korea, authorities integrated technology and data across cybersecurity and physical security systems to track and isolate virus cases. The results were far fewer deaths (35,000) compared to countries like the UK (230,000). This **data-driven security approach** highlights how **convergence improves real-time decision-making** and **risk mitigation**.

## THE BUSINESS CASE FOR A CONVERGED SECURITY TEAM

A **2023 G4S Allied Universal World Security Report** found that 90% of security managers in large companies cited cyber threats impacting physical security as a major challenge. With attacks becoming more sophisticated, **companies can no longer afford fragmented security functions**.

# Kaseware and Security Convergence

The Kaseware software platform is designed to support security convergence by integrating **multiple security functions** into **one unified platform**, thereby enhancing collaboration and efficiency across the physical and cybersecurity domains. Here is how Kaseware aligns more specifically with the principles of security convergence:



**Unified Case Management:** Kaseware consolidates security operations - such as investigations, incident reporting, and data analysis - into a single, cohesive system. This consolidated approach facilitates seamless information sharing between physical security teams and cybersecurity units, breaking down traditional silos and promoting a holistic security approach.

**Security Communication and Collaboration:** The Kaseware platform supports secure communication tools and workflows, ensuring that sensitive information is protected while enabling real-time collaboration among security personnel. These features are crucial for coordinating responses to incidents that may span both the physical and digital realms.

**Compliance with Security and Industry Standards:** Kaseware adheres to rigorous security certifications, including SOC 2 Type 2 and CJIS compliance. Further, the Kaseware platform aligns and supports the standard of cross-functional security teams, as provided in the ASIS Security Standards Manual (2020).

**Integration Capabilities:** Recognizing the diverse needs of modern security environments, Kaseware is designed to integrate with multiple and various external systems and data sources. This flexibility allows organizations to incorporate existing security tools and technologies into the Kaseware platform, creating a comprehensive and converged security infrastructure.

By providing a centralized platform that **bridges the gap between physical and cyber security functions**, Kaseware enables organizations to implement a converged security model effectively, enhancing their overall security posture.

# About the Authors

## JAMES WILLISON

FOUNDER, UNIFIED SECURITY LTD.

James Willison is a distinguished international leader in Security Convergence and Enterprise Security Risk Management. His extensive career, marked by a blend of, advisory, academic and practical roles, showcases his contributions to the security industry. He has a practical application to convergence, and streamlining delivery within a sound business framework.

As Founder of **Unified Security Ltd** he has co-authored and published highly successful white papers on Security Convergence, Smart Cities Cyber Security, GDPR, and **Trust** for AXIS Communications.

Regular contributor to **IFSEC Global** and member of several ASIS International committees. He is an established speaker at international security conferences, including ASIS Europe (2009 – 2019) and IFSEC International (2010 – 2023).

## JOHN GILL

EXECUTIVE VICE PRESIDENT, KASEWARE

John is a seasoned security executive with 35+ years of experience in the public and private sectors. He served 25 years with the Secret Service, where he managed multi-agency security and investigative missions and held several key roles, including Attaché of the Paris Field Office and Chief Security Officer at the White House.

Since 2010, he has provided executive leadership and strategic guidance as a consultant and is currently the Executive Vice President of Kaseware, specializing in investigative case management and data analytics solutions.

KASEWARE

Our secure case management platform easily handles your operations, cases, records, evidence, and more, while providing convenient features like dashboards, link analysis, the ability to work securely from any location, and intelligent forms so you never have to fill out duplicate information again. **Our goal is to make your job easier and the world a safer place.**

## Backed by Expertise

Kaseware was founded by former Special Agents in the FBI who created Sentinel — the investigation case management software still used by the FBI today.

## Advanced Technology

Our link analysis and graphing capabilities are second to none. With Kaseware, your teams get the analytical tools needed for intelligence and insights.

## Highly Configurable

Kaseware is designed to be easily modified and configurable to the needs of your organization or agencies and even individual units and users.

Schedule a Demo

www.kaseware.com
salesteam@kaseware.com
+1 (844) 527-3927

Respond • Investigate • Resolve