

What is the Kinamik Secure Audit Vault™?

The Kinamik Secure Audit Vault is an innovative software solution that collects, secures and centralizes audit information from different sources, while providing irrefutable proof that data hasn't been manipulated without being noticed and pinpointed. It helps organizations in increasing the evidential weight of their electronic data, providing best-evidence in case of litigation.

What is the Kinamik Data SafeSealer™?

The Kinamik Data SafeSealer is innovative electronic data signature technology that secures the integrity of any digital binary data. It enables high-performance, realtime protection of streaming audio, video and network traffic data with minimal computational overhead, providing irrefutable proof of the data's authenticity and integrity, increasing its evidential weight and facilitating data protection and security compliance requirements.

What are the benefits of Kinamik's realtime data integrity solutions?

- ▶ Provide support for litigation in a Court of Law by increasing evidential weight of streaming records and extend the data's chain of custody from capture until exporting.
- ▶ Ease compliance processes by creating a tamper-evident vaulted environment.
- ▶ Reduce the risk of unwanted or malicious manipulation by providing end-to-end trust.
- ▶ Meet or exceed the most stringent anti-tampering regulatory and best practices measures (e.g. BSI10008, PCI-DSS, FISMA, etc.).

Does your CCTV video data carry sufficient evidential weight?

The evidential weight of CCTV digital data is dependent upon proof of the data's authenticity and integrity. This is of higher concern when dealing with digital data due to the increase in opportunities to undetectably modify video and audio data.

The advanced analytics and storage cost reductions derived from digital CCTV also establish complex compensating controls that attempt to address digital evidential weight and privacy requirements.

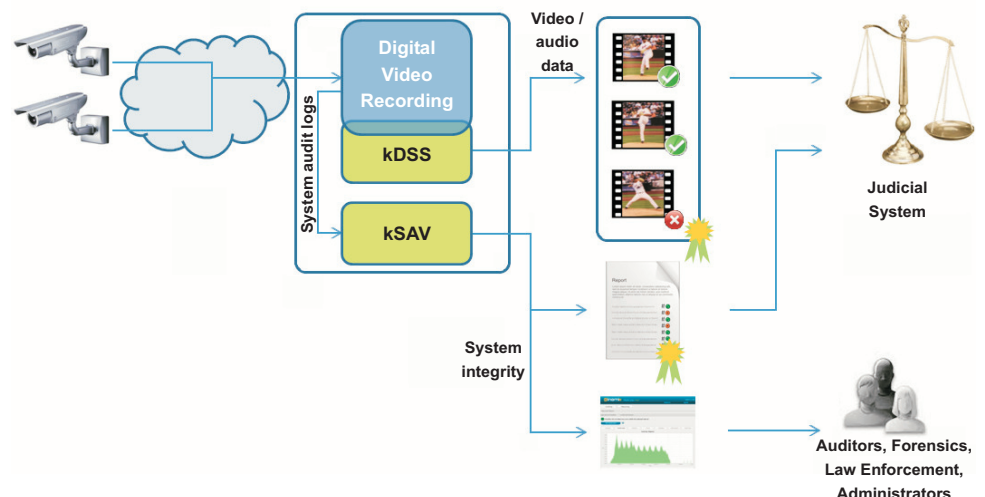
Is the CCTV data trustworthy?

A solid, defensible end-to-end approach towards maintaining the authenticity and chain of custody is required to support the evidential weight of the digital video data and the CCTV systems audit logs. A weakness in this process can have dramatic negative effects on the data's suitability as digital evidence.

As with other types of sensitive digital data, CCTV data is also subjected to both internal and external threats that can access and change or spoil the data.

It is common practice for audit logs to be employed to support insights on systems integrity and to prove that the collection, processing, use and storage of the data has good integrity and has not been manipulated. The use of audit logs also support the prevention of privacy abuse that can occur with such intrusive capabilities, for example being able to use the CCTV to view physical spaces considered private.

Various techniques such as access controls, encryption and digital watermarks have been employed to protect the confidentiality and integrity of the video data and system audit trails. However, access controls do not provide sufficient protection against privileged users; encryption is only effective if the data does not need to be read as the decryption process provides a window of opportunity for undetectable manipulation. Digital watermarks modify the original data and are deemed not effective to identify undetectable manipulation (e.g. deletion). Evidential weight and admissibility as evidence for video images can be impacted by whether the image's audit trail from the digital recording to the court is robust and whether the integrity of the image can be proven (BS 8495).



How do Kinamik technologies help?

Kinamik's technologies enable compliance with BS 10008, "Evidential weight and Legal Admissibility of Electronic Information" and BS 8495, "Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence". Integrating Kinamik's solutions with CCTV systems (e.g. Network Video Recorders) provides trustworthy and digital evidence-ready system, video and audio data.

Advanced technologies from Kinamik enable organizations to protect the authenticity and integrity of their digital data in realtime, increasing its trustworthiness for business, regulatory and legal use. Kinamik's patented data integrity protection tools can be applied on any continuously appending data, including:

- ▶ IT infrastructure audit logs (operating system, databases, routers, etc.);
- ▶ Business system audit records (application transactions, instant messages, documents, e-mails);
- ▶ Physical security systems (e.g. CCTV video and audio data, etc).

Kinamik's innovative technologies collect data as it is being generated, securing it at a granular level (i.e. transaction, event, video frame or byte, depending on the data type). These electronic records are made tamper-evident, and from that point forward, processed data cannot be modified without detection -not even by administrators or other privileged users. Moreover, the original data is also digitally signed when exported, providing a simple mechanism for proving that its chain of custody has been fully maintained.

Kinamik's optional encryption and hardware-based key management plug-in capabilities (HSM) can also boost confidence in the reliability and confidentiality of data and the keys that safeguard this information.

Kinamik Secure Audit Vault (kSAV) can seamlessly integrate with an organization's systems and applications, preserving audit trail data in realtime and producing a searchable, forensic and digital evidence-ready vault of data.

Kinamik Data SafeSealer (kDSS) is capable of authenticating any streaming or continuously appending digital media securing it as it is being captured and verifying that it has not been modified or deleted.

Kinamik delivers cost-effective, scalable and easy-to-deploy technology solutions that allow organizations to proactively prepare for virtually any security, compliance, and forensics or litigation requirement whenever the trustworthiness of the data is paramount.

Kinamik solutions differentiation

	System-wide Integrity	For any binary data	Embedded technology	HSM plug-in	GUI	Role-based access
kSAV	✓			✓	✓	✓
kDSS		✓	✓	✓		



About Kinamik Data Integrity, Inc.

Kinamik technology protects digital records at rest or in flight from being altered. We provide a Centralized Audit Vault repository for sensitive data that adds integrity and authenticity at a fine grain level, creating in the digital world a level of evidence that is analogous to paper-based records. Kinamik's solutions deter, detect and demonstrate data manipulation to guarantee the authenticity and assurance of digital information.

Our mission is to bring a higher level of trust, accountability and privacy protection to data in mission-critical industries that deal with large volumes of high-value data and sensitive information. We provide advanced data integrity assurance capabilities to industries such as financial, health, life sciences, transportation, public sector agencies and IT hosting sectors.

Kinamik is a McAfee SIA Partner and a Sun Startup Essential Partner

Selected features

Legal admissibility

- ▶ Chain of custody preservation: from the real-time capture of each transaction up to its export for submission to any third party, in compliance with laws, regulations and best practices.
- ▶ Data integrity report: evaluates the data's confidence level in a snapshot using Kinamik's data integrity verification process.

Cost reduction

- ▶ Compression capabilities: provides network and storage cost-reduction possibilities using its compression functionalities (in transit and at rest)

Data protection

- ▶ Role-based access: segregation of duties integrates with Active Directory and LDAP.
- ▶ Advanced time stamping: integrates with an external Time Stamping Authority (TSA) in addition to its own time stamp.
- ▶ HSM-integrated: for private keys protection.

Kinamik technology as an embedded OEM solution

Kinamik technologies are available as application program interface (API), allowing easy and fast integration with third-party technologies. It enables the delivery of real-time data integrity assurance to virtually any product or solution, enhanced their value and final users to successfully address security, data governance and compliance requirements when dealing with sensitive data.



Kinamik Data Integrity, Inc.
303 Twin Dolphin Drive
Redwood City, CA 94065, USA
Tel: (+1) 650 632 4408
Fax: (+1) 650 551 9901

Kinamik Data Integrity, S.L.
Diputació 238, àtic 5
08007, Barcelona, Spain
Tel: (+34) 931 835 814 www.kinamik.com
Fax: (+34) 933 041 681 info@kinamik.com