

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.

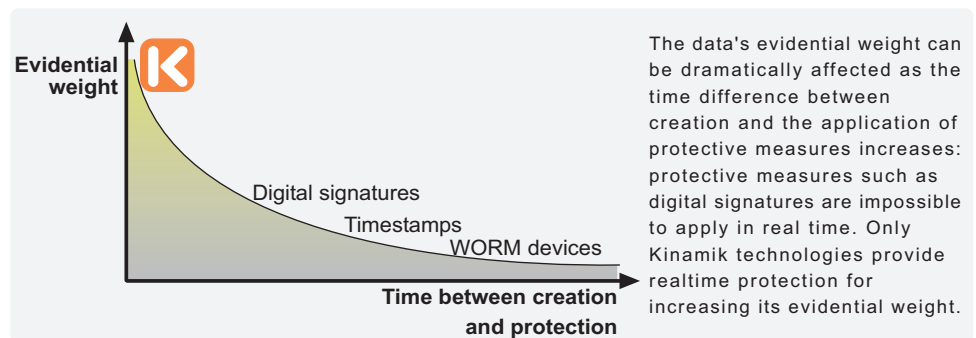
What are the benefits of Kinamik's realtime data integrity solutions?

- ▶ Support litigation in a Court of Law by increasing evidential weight of electronic 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.).

Is your sensitive data "evidence-ready"?

It is an absolute requirement for digital evidence to be verifiable and to be maintained with provable integrity protection. To satisfy these kinds of evidentiary requirements, organizations often use an arduous combination of batch-based security technologies and labor-intensive processes.

However, these compensating controls and other protection mechanisms may not be sufficient when the requirement is to use these records as digital evidence, as they create a window of opportunity for undetectable manipulation to occur and yield questionable authenticity of the data. Organizations today also rely upon expert witnesses to verify integrity, which can be costly, time-consuming and wholly dependent on a the viability of the subject matter expert. These measures can also compromise data's chain-of-custody, which can question the viability of introducing this data as evidence in a court of law.



Insufficient or non-existent data integrity can have considerable impact, including:

- ▶ **Weak evidential weight:** a primary failing when using digital data as evidence is that they may not be proved to be authentic. Access controls, segregation of duties, encryption and the application of digital signatures or time stamps applied after a period of time are inappropriate or incomplete methods for protecting the authenticity and integrity data destined as digital evidence. Without realtime integrity protection, opportunities for undetected manipulation may occur -for example with a privileged user that may have imperceptibly modified data prior to the file being digitally signed-creating a false sense of security. The need for protection is reflected in various standards, rules and regulations, including UK's BS10008 and the Spanish National Security Framework (*Esquema Nacional de Seguridad*).
- ▶ **Higher costs:** where the evidential weight of digital data is weak, its value for being used in court is significantly reduced. If the data is critical to the case, organizations may be forced to incur in additional forensics and analysis costs for building complementary information that will support the litigation at hand.
- ▶ **Compromised chain-of-custody:** a sound chain-of-custody is necessary to show that the integrity of the evidence has not been affected during its production, as it details the precise manner in which data was collected, evaluated and preserved. Any weaknesses can bring immediate risks such as a lack of Privilege Waiver or spoliation, leading to sanctions that can include monetary penalties, exclusion of evidence, and dismissal or default judgment.

How do Kinamik technologies help?

Kinamik technologies enable organizations to achieve “digital evidence readiness” by increasing the evidential weight of their sensitive data. By acting as an “always-on” flight data recording device that captures and vaults sensitive information at the moment of its creation, they close the security time gap vulnerability that would otherwise exist before data is secured. Kinamik’s technologies also provide a scientifically-proven tamper-evident approach to detect the manipulation of data and maintain chain of custody.

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. 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

Kinamik is a trademark of Kinamik Data Integrity, Inc. All other trademarks contained herein are the property of their respective owners.

© 2011, Kinamik Data Integrity, Inc.

Selected features

Legal admissibility

▶ Chain of custody preservation: from the realtime 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 as a snapshot using Kinamik’s data integrity verification process.

Cost reduction

▶ Compression capabilities: provides network and storage cost-reduction using data compression (in transit and at rest).

▶ Data Retention Policy tool: allows the definition of specific retention policies for each data source, enabling compliance with laws, regulations and standards (e.g. CALEA, EU-DRD, etc.).

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 protection of private keys.

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
Fax: (+34) 933 041 681
www.kinamik.com
info@kinamik.com