

## What is Kinamik Secure Audit Vault?

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.

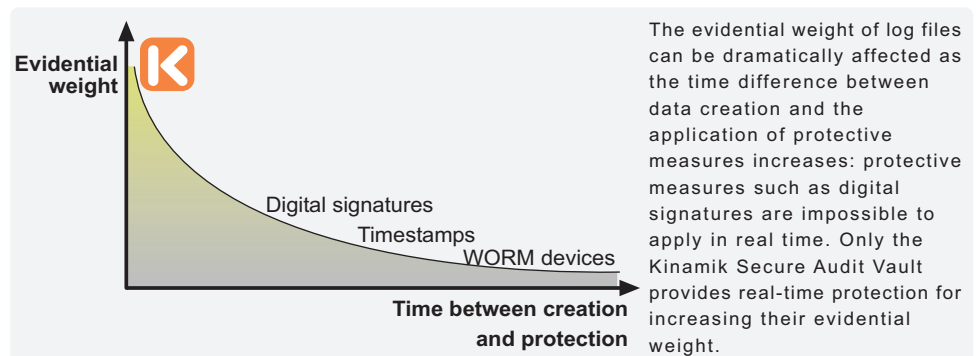
## What are the business benefits of Kinamik Secure Audit Vault?

- ▶ Supports litigation in a Court of Law by increasing evidential weight of electronic records
- ▶ Facilitates discovery processes by proactively building a centralized data vault, making them tamper-evident
- ▶ Reduces risk of unwanted or malicious manipulation by providing end-to-end trust
- ▶ Meets the most stringent anti-tampering regulatory and best practice measures (e.g. SOX, PCI-DSS, NIST, etc.) especially when dealing with identity assurances
- ▶ Protects the evidence's Chain of Custody by digitally signing exported data.

## Are your audit trails (logs) evidence-ready?

It is an absolute requirement for digital evidence to be authentic and to be maintained with provable integrity protection. The wealth of information residing in audit trails (including the "what", "who", "when" and "where" of events) explains why they are being used to support incident response, forensic investigations and law proceedings. When these audit log files are a crucial part of a body of evidence, for satisfying these e-discovery requirements organizations frequently use solutions for collecting and analyzing log files. However, these protection mechanisms implemented may not be sufficient for using these records as electronic evidence since they create a window of opportunity for undetectable manipulation to occur. These insufficient approaches ignore the imposed requirements of digital evidence and yield questionable authenticity of the audit trail data.

Considering that the chances of success in a court of law depend heavily on the availability of strong evidence, organizations that do not properly protect their audit trails risk serious negative impact on the record's evidential weight, particularly when these audit trail records play an important part in the case being presented.



Insufficient or non-existent audit trail protection can have considerable impact, including:

- ▶ **Weak evidential weight:** a primary failing when using audit trails as evidence is that they may not be proved to be authentic. Without real time integrity protection opportunities for undetected manipulation appear, for example with a privileged user that may have imperceptibly modified data prior to the file being digitally signed. Several standards, rules and regulations reflect this concern, including the United Kingdom's BS10008 (Evidential Weight and Legal Admissibility of Electronic Information), or the Spanish National Security Framework (*Esquema Nacional de Seguridad*).
- ▶ **False sense of security:** access controls, segregation of duties, encryption or the application of digital signatures or time stamps after a period of time are inappropriate or incomplete methods for protecting the authenticity and integrity of audit trail data. Due to their nature, they could either be subverted by a privileged user or create a window of opportunity for manipulation to occur from the moment data is created until the moment it is secured, creating a dangerous false sense of security.
- ▶ **Higher costs:** where the evidential weight of audit trail data is weak its value for being used in court is significantly reduced. If these audit trail data is key in building 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.

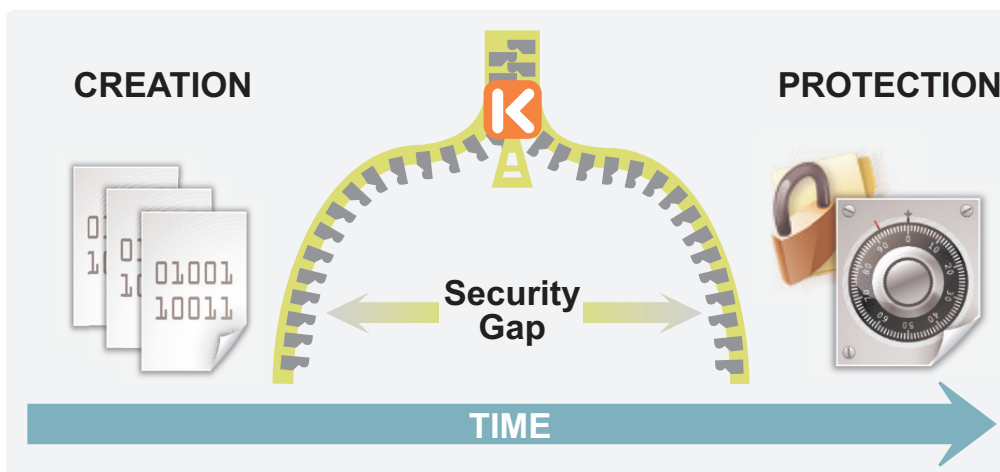
## How does Kinamik Secure Audit Vault help?

Kinamik Secure Audit Vault (kSAV) helps organizations in increasing the evidential weight of audit trail data such as DB logs, IdAM audit trails, physical entry records and other electronic records such as IM logs and video and audio surveillance data. It seamlessly integrates with the organization's systems and applications, acting as a passive black box that records and preserves data in real time, producing a searchable, forensic and digital evidence-ready vault of data.

Kinamik Secure Audit Vault's connectors collect audit trails as they are being generated, processing data up to the most granular level (i.e. transaction or event level). These electronic records are made tamper-evident and optionally timestamped, and from that point forward processed data cannot be modified without detection - not even by administrators or other privileged users; effectively, this means that the Kinamik Secure Audit Vault acts as an "auditor of the auditors". Moreover, the original audit trail data is digitally signed when exported, providing a simple mechanism for proving that its Chain of Custody is fully maintained.

With the Kinamik Secure Audit Vault, organizations are able to reduce forensic and litigation costs by centralizing sensitive information and easing e-discovery processes, providing demonstrable proof of the authenticity and integrity of the secured records. In addition, they are able to maximize the evidential weight of the processed electronic records, boosting confidence in the reliability and authenticity of the data. This confidence and ease in management can be further increased by the use of kSAV's optional encryption.

In summary, the Kinamik Secure Audit Vault is a cost-effective, scalable software for increasing the evidential weight of electronic records, allowing organizations to proactively prepare for any litigation need. It is an easy-to-deploy solution that can be transparently installed over and about the existing systems in the organization and requires no modification to the IT system infrastructure.



By securing data in real time, Kinamik Secure Audit Vault closes the security gap existing between data creation and the application of protective controls.

### About Kinamik

Kinamik software protects digital records from being altered. We build a Centralised Audit Vault for sensitive data with integrity and authenticity at a fine granular level, creating in the digital world a similar level of evidence than to traditional paper-based records. Kinamik deters, detects and demonstrates data manipulation to guarantee the correctness of digital information.

Our mission is to bring a higher level of trust, accountability and privacy protection to industries that deal with large volumes of sensitive information. We address data integrity mainly in financial, health, government, and IT hosting sectors.

Kinamik is a Sun Startup Essential Partner and an Oracle Partner



## Selected features

- ▶ Messages in transit compression: reduce bandwidth usage by compressing up to 70% messages sent to the integrity processing component.
- ▶ LDAP user management: Kinamik Secure Audit Vault integrates into existing Enterprise user management and is compliant with LDAP and Active Directory.
- ▶ Data Retention Policy tool: Kinamik Secure Audit Vault allows the definition of specific retention policies for each data source, enabling compliance with laws, regulations and standards (e.g. PCI-DSS, HIPAA, Basel II, SOX, MiFID, etc).
- ▶ Regular expressions text search within centralized repository: use web-based search capabilities for an exact localization of specific text strings and expressions within the secured data.
- ▶ Easy-to-interpret comprehensive integrity report: evaluate trust level of data with one simple snapshot. Pinpoint any integrity infringement down to the event level.
- ▶ Archival and storage compression capabilities: reduce storage and archiving costs with the Kinamik Secure Audit Vault's archiving compression capabilities, with up to 5:1 compressing ratio.
- ▶ Easy integration with reporting tools: easily export integrity data to Jasper Reports for customized reporting.

**Kinamik**  
Data you trust

**Kinamik Data Integrity**  
Diputació 238, àtic 5  
08007 Barcelona Spain  
Tel: (+34) 931 835 814  
Fax: (+34) 933 041 681  
[www.kinamik.com](http://www.kinamik.com)  
[info@kinamik.com](mailto:info@kinamik.com)

Every effort has been made to ensure that the information included in this datasheet is accurate and up-to-date at the time of going to press. Nevertheless, the products described herein are subject to continuous development and improvement and Kinamik reserves the right to change their specifications at any time. We disclaim any liability with respect to this document, and no contractual obligations are formed directly or indirectly with its contents. Kinamik is a trademark of Kinamik Data Integrity, S.L. All other trademarks contained herein are the property of their respective owners.

© 2010, Kinamik Data Integrity S.L.