

## 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 of integrity. It helps organizations reduce audit and compliance costs, mitigates insider threat and gives legal admissibility and best-evidence in case of litigation.

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

- ▶ Increases SaaS customer confidence, by providing enhanced secure audit capabilities.
- ▶ Supports cost-effective compliance with anti-tampering legislative and regulatory best practice measures (e.g. SOX, PCI-DSS, NIST, etc.).
- ▶ Assists end user's compliance needs by providing assurances of the application of security controls and policies.
- ▶ Supports litigation in a Court of Law by increasing evidential weight of electronic records.
- ▶ Reduces risk of unwanted or malicious manipulation by providing end-to-end trust.

## Security in Cloud Computing: the elephant in the room

Software as a Service (SaaS) providers are struggling to get wide scale adoption of their services in part due to the lack of trust end users have in cloud computing. With audit ability being a primary concern of internal and external auditors, security, compliance and legal staff, SaaS providers need to directly address these concerns within their solutions. Audit trails are increasingly being relied upon to assess the adoption of controls and evidence of compliance, monitoring of user and service activity, incident response and evidence within law courts.

Retaining and assuring the integrity of audit trails is not just a prerequisite in many legislative, regulatory and best practice requirements; proof of audit trail data's integrity also provides deterrent effect and offers significant legal evidential weight in case of litigation.

## Why is it important for SaaS providers?

The inability to produce trustworthy audit trails, and the security concerns created by this lack of audit assurance have important consequences for SaaS providers.

### ▶ A potential deterrent for new customer adoption

Cloud Computing shows steady and clear growth figures, with benefits being recognized by the majority of executives globally. However, recent studies expose a substantial gap between the number of organizations that acknowledge the potential value in cloud computing and those that are actually embracing it. Despite more than 60% of decision-makers agree on cost-reduction possibilities, 61% of organizations are not using cloud computing today and 84% are not planning to do so over the next 12 months. When explaining this resistance, two issues are constantly being brought to the table: fears of security threats and loss of control of the information. By a five-to-one margin, organizations feel that their own IT systems are more secure than the cloud.

### ▶ Need to support you existing customer's compliance needs

Your clients may be bound to comply with laws, regulations and internal policies. For this purpose, SaaS providers need to offer reliable assurances of security controls and activity within the technology stack supporting their service. This issue is of particular concern to:

- *Auditors*, who can no longer rely on the multiple levels of controls that existed in their organizations, and are looking beyond access control to gain assurances of the integrity of data used to support the implementation of expected controls.
- *Security officers*, who often use ISO 27002 as guide for controls, and look for proper protection of system logs since "if the data can be modified or data in them deleted, their existence may create a false sense of security". Additionally, incident response teams will require insights on events that may have disrupted the service.
- *Compliance officers*, who understand that even though the SaaS provider may be the custodian of data, the ownership -and the liability for non-compliance- resides with the end client. Examples include EU Data Protection Act (fines up to £500,000), PCI-DSS (multiple levels of fines) and of course FISMA (whose non-compliance means criminal offence).
- *Legal teams*, who recognize that the use of digital evidence in courts of law demands proof of the data's authenticity and integrity. Where this is not possible, the data will not be usable or its evidential weight can be dramatically affected, having significant impact on the case.

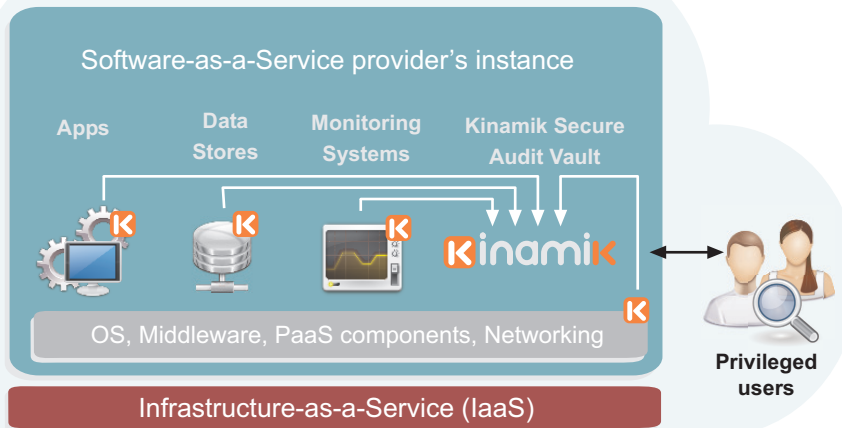
## ► Complex and expensive compliance processes

For providing compliance assurances you will need to comply yourself as a provider. Complying with different laws and regulations has always been a complex and expensive task, which requires high investments in terms of money and resources. Given the inherent complexities in architecture and data management for SaaS providers, cloud computing makes compliance processes even harder. Furthermore, when trying to deal with different laws and regulation's requirements of the governance of audit trails, this task may seem simply impossible, thus increasing costs dramatically.

## How does Kinamik Secure Audit Vault help?

The Kinamik Secure Audit Vault (kSAV) is designed to seamlessly integrate into your SaaS solution, acting as a passive black box. Its connectors or feeds can reside on operating systems, applications, databases, virtual machines, monitoring components or any other infrastructure element. These feeds capture data in real time as it is generated, and is transmitted to kSAV via a secure channel. Upon arrival, a centralized tamper-evident chain of events is built, and the preserved audit trail data cannot be manipulated without detection, not even by the most privileged user. The audit trail data is preserved for the any established retention period, and can be available to trusted third parties through the use of PKI access controls. Optionally, data can also be encrypted to enhance confidentiality.

Having the Kinamik Secure Audit Vault implemented in your SaaS infrastructure will effectively create a repository of immutable audit logs, which will allow you to provide trust in all the auditable activities of your users, operational staff and trusted third parties. Preserving these business records enables proof of compliance to a multitude of regulations -both for you and your customers- and offers the foundations for reducing the ever increasing trust gap that causes resistance for cloud computing adoption. Furthermore, it increases the evidential weight of the preserved audit trail data, should it be required for forensics investigations or during any litigation or dispute resolution.



Kinamik Secure Audit Vault - Example of a deployment within a SaaS provider infrastructure

### About Kinamik

Kinamik software protects digital records from being altered. We build a Centralized 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

- Data collection agents: Kinamik Secure Audit Vault's agents collect and transmit data in real-time through a secure encrypted channel.
- TSA compatible: for achieving a higher level of security and integrity protection, the Kinamik Secure Audit Vault is fully compatible with external time stamping authorities (TSA).
- Optional data encryption: using strong industry standard protocols for encryption, all the data existing in the secured audit vault can be rendered confidential.
- Data Retention Policy tool: Kinamik Secure Audit Vault allows users to define different retention policies for each independent data source, enabling compliance with laws, regulations and standards (e.g. PCI-DSS, HIPAA, Basel II, SOX, MiFID, etc.) that mandate specific data retention periods.
- 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.



**Kinamik Data Integrity**  
Diputació 238, àtic 5  
08007 Barcelona Spain  
Tel: (+34) 931 835 814  
Fax: (+ 34) 934 517 628  
[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.