

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?

- ▶ Increase enterprise confidence by providing an independent and trustworthy auditing platform with enhanced revision capabilities.
- ▶ Support cost-effective compliance with anti-tampering legislative and regulatory best practice measures (e.g. ISO 27001, SOX, PCI-DSS, FISMA, etc.)
- ▶ Ease compliance processes by creating a tamper-evident vaulted environment.
- ▶ Support litigation in a Court of Law by increasing evidential weight of electronic records.
- ▶ Reduce risk of unwanted or malicious manipulation by providing end-to-end trust.

When a reputation is on the line, SaaS-associated cost savings have little value

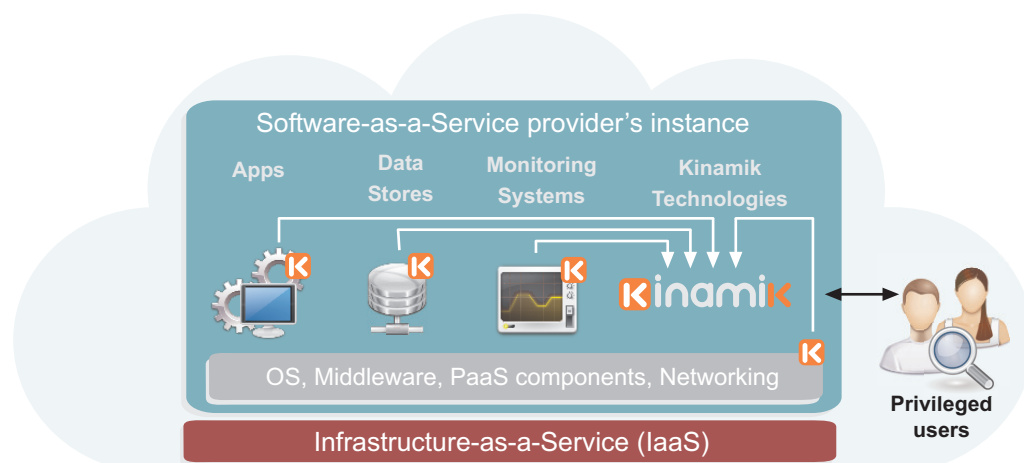
A lack of transparency in data handling is one of the major factors that discourage enterprises from adopting Software-as-a-Service (SaaS) offerings, especially in highly regulated industries such as banking, healthcare or government.

Having the ability ability to audit and verify the implementation of required security measures -and providing proof of the execution of these measures- is often an essential requirement for internal and external auditors, security, compliance and legal staff. However, SaaS providers today face serious challenges when attempting to deliver these assurances, and must rely instead on compensatory controls (encryption, access control, etc.) that merely mitigate security issues.

Providing trust in untrusted environments

The inability to produce trustworthy digital data has important consequences for SaaS providers.

- ▶ **A potential deterrent for new customer adoption:** Even though Software-as-a-Service adoption shows a steady growth and its benefits are clearly recognized, studies expose a substantial gap between the number of organizations that acknowledge the value in SaaS and those that are actually embracing it. Further, SaaS providers are considered high-value targets for possible attacks due to their multi-tenancy nature: SaaS provider's data stores can often contain enormous sensitive data from various organizations, thus convenient targets for an adversary.
- ▶ **Need to support existing customer's compliance needs:** when SaaS users need to comply with laws, regulations and internal policies, SaaS providers need to offer reliable assurances of security controls and trustworthy activity data within the technology stack supporting their service. This issue is of particular concern to auditors (who look beyond encryption and access control to gain assurances of the integrity of audit and activity); security officers (who demand proper protection of audit logs of systems containing the organization's data); compliance officers (who understand that although the provider may be the custodian of data, the ownership -and liability for non-compliance- resides with the end client); and legal teams (who recognize that the evidential weight of digital evidence demands proof of the data's authenticity and integrity).
- ▶ **Complex and expensive compliance processes:** SaaS providers need to comply with a broad range of laws and regulations, and the complexities normally associated to compliance processes are significantly increased in Cloud environments. An inability to produce unquestionable authentic data can make these compliance processes even harder, dramatically increasing the resulting costs.



Example of a deployment within a SaaS provider infrastructure

How do Kinamik technologies help?

Kinamik technologies bring trust to untrusted cloud infrastructures. Kinamik enables realtime cryptographic data integrity protection to sensitive data, including -but not limited to- customer data and system audit logs. The data is secured and preserved in real-time, at a granular level, increasing the data's evidential weight and providing unquestionable assurances of authenticity and integrity.

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 in a snapshot using Kinamik's data integrity verification process.

Cost reduction

- ▶ High performance: Kinamik's technology can process up to 40.000 events per second.
- ▶ Compression capabilities: provides network and storage cost-reduction possibilities using its compression functionalities (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. EU-DRD, CALEA, etc.).

Data protection

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