

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?

- ▶ Reduces costs in supporting GRC, audit, e-discovery and forensics processes
- ▶ 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
- ▶ Meets the most stringent anti-tampering regulatory and best practice measures (e.g. SOX, PCI-DSS, NIST, etc.) specially when dealing with identity assurances

The security gap in Identity and Access Management

Identity and Access Management (IdAM) solutions provide a wide range of benefits to organizations, including IT and help desk cost reduction, improvements in security management, boost in user productivity and ease in compliance processes. However, implementing an IdAM is not exempt of risks and there is a key point usually forgotten: regulations and legislations require organizations to maintain insights on activities performed by a user for the implementation of their directives (e.g. privileged access, separation of duties, etc). There is a significant and growing security trust gap created by the lack of proper guarantees of the association between the application, operating system or database that generated an event and the user associated to that event.

To enable this required end-to-end trust, organizations must be able to provide assurances of non-manipulation of the association between events and users. The need of assurance goes from the provisioning of an electronic identity and its association to a person or resource, up to the correlation made by a single-sign-on (SSO) device to an application or any another endpoint. These associations and correlations, recorded in each system's audit trails, are easily modifiable by any user with proper access. As a result, any weak point within the IdAM applications or the components through to the endpoint may result in a user disputing its association to an event. This can bring catastrophic consequences for an organization if the need arises (litigation, forensics investigation, internal or external audit procedures, etc.)

Kinamik's Secure Audit Vault provides support for this end-to-end trust requirement by capturing audit trails produced by the whole chain of IdAM systems and the endpoint.

Deep impact across the organization

This trust gap has severe impacts in many key areas and processes of an organization:

- ▶ **Compliance:** laws and regulations require a unique electronic identity to enforce controls such as segregation of duties, privileged access controls, etc. Weaknesses created from unsecure implementations of IdAM systems create lack of assurance of the users' association to an auditable event. This lack of assurance is being increasingly identified by auditors as an issue that causes significant break within in the end-to-end trust requirements of many laws and regulations (e.g. SOX, PCI-DSS, GCSX-Code of connection, etc)
- ▶ **Legal:** one of the duties any organization has is to properly authenticate users of computer systems. Audit records, often used as evidence, are facing greater scrutiny and their authenticity is increasingly challenged. Where assurances of a user's association to an audit record is of weak evidential weight, legal council faces an increasingly difficult task when managing liability impacts.
- ▶ **Security:** strong association of an event to a user enables monitoring and enforcement of information security polices. Where it is not possible to provide end-to-end trust of the association of a user to an audit record, the foundations of an organizational security posture are at high risk.
- ▶ **IT:** enabling trust in audit records generated by a user (and its association to identity stores) is a foundational attribute to achieve a reasonable IT security posture, and to support the compliance and legal requirements of end-to-end trust. The importance of this matter is dramatically increased by the growing complexity of IT services and the security perimeter shift created by Cloud Computing.

► **Line of Business:** each business unit is ultimately responsible and the owner of their data. Lack of electronic identity assurance and end-to-end trust can have severe impact on the line of business.

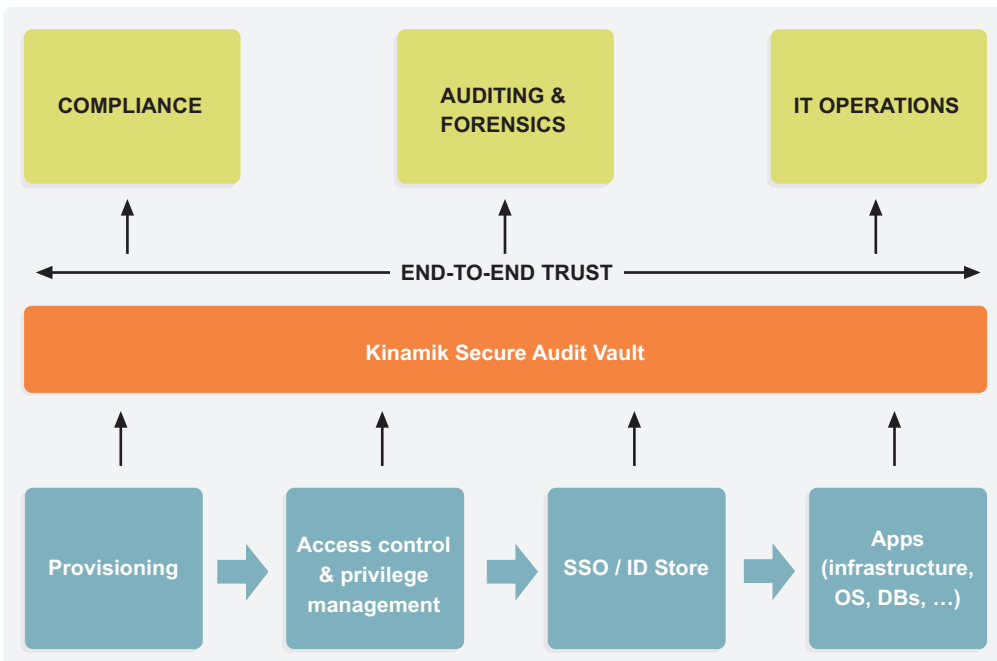
How does Kinamik Secure Audit Vault help?

Kinamik Secure Audit Vault's (kSAV) agents collect and transmit audit trail events in real-time, as they are generated. Events are transmitted through a secure encrypted channel to the kSAV integrity processing module, where they are made tamper-evident upon arrival. An implementation of the Kinamik Secure Audit Vault supporting the Identity and Access management components and the application or endpoints provides end-to-end trust in the authenticity of the audit event and, most important, trustworthy assurance of their association to a user.

The highest levels of security are achievable through the use of:

- an optional Hardware Security Module (HSM) to protect the cryptographic keys;
- a third-party trusted Time Stamping Authority (TSA);
- optional data encryption using strong industry standard protocols, effectively providing data with strong confidentiality.

Kinamik's pricing model, based on the maximum amount of data processed daily, enables deployment of as many feeds and servers (load balancing, high availability, fault tolerance) as required. Each server is capable of securing up to 40,000 events per second. Kinamik Secure Audit Vault's privileged access control functionality allow users to access only the audit trail data relevant to them.



Kinamik Secure Audit Vault provides end-to-end trust, supporting compliance, IT operations and audit & forensic processes.

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

► **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 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 5:1 compressing ratio.

► **Easy integration with reporting tools:** easily export integrity data to Jasper Reports for customized reporting.



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