

## 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.

## The security gap in Identity and Access Management

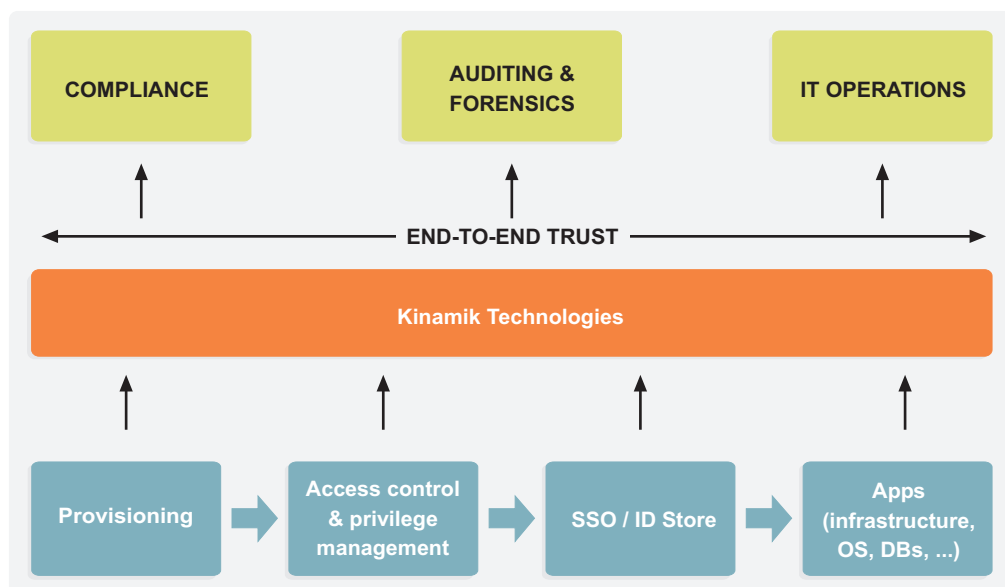
Having an assured association to an electronic identity is a foundational security element that most security controls depend upon. However, Identity and Access Management (IdAM) implementations can often overlook the risk of rogue users modifying electronic identity files, thus effectively committing unnoticeable identity theft.

To mitigate these risks, and to provide assurances of non-manipulation of the association between events and users, organizations often attempt to implement a variety of batch-based security technologies and compensatory controls. Typically, these steps fail to solve these issues since the associations, which are recorded in each system's audit trails, are easily modifiable by any privileged user, bringing catastrophic consequences for an organization (litigation, forensics investigation, internal or external audit procedures, etc.).

## Potential impacts felt across the organization

This trust gap can impact many key areas and processes of an organization:

- ▶ **Compliance:** for enforcing controls such as segregation of duties and privileged access controls, laws and regulations require a unique electronic identity. However, lack of assurances of the event-user association are being increasingly identified by auditors as an issue that causes significant break within in the end-to-end trust required for compliance (e.g. SOX, PCI-DSS, GCSX-Code of connection, etc.).
- ▶ **Legal:** if organizations fail to provide sufficient assurances of authenticity and integrity protection of audit trail data, the association between a user and an event could be forged and/or not trusted, severely affecting its evidential weight.
- ▶ **Security:** where organizations cannot demonstrate end-to-end trust of the association of a user to an audit record, the inability to monitor and enforce information security policies put the foundations of an organizational security posture at high risk.
- ▶ **IT:** enabling trust in audit records reflecting the user-electronic ID association is a foundational attribute to IT security postures, and to support the compliance and legal requirements of end-to-end trust.
- ▶ **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 consequences including phantom losses for the line of business.



Kinamik technologies provide end-to-end trust, supporting compliance, IT operations and audit & forensic processes.

## How do Kinamik technologies help?

Kinamik's technologies can be seamlessly deployed within IdAM implementations for securing all sensitive data generated. Kinamik's products collect, seal and protect IdAM data in realtime and at the highest level of granularity, providing irrefutable proof that it hasn't been tampered with—even by privileged users- from the moment of creation. Innovative data integrity technologies from Kinamik help build secure IdAM implementations and deliver end-to-end trust.

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

▶ 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

▶ 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](http://www.kinamik.com)  
info@kinamik.com