

Cos'è Kinamik Secure Audit Vault?

Kinamik Secure Audit Vault è una soluzione software innovativa che raccoglie, protegge e centralizza le informazioni di audit provenienti da diverse fonti e fornisce una inconfutabile prova di integrità. Aiuta le aziende a ridurre i costi di audit e di compliance, diminuisce le minacce interne, fornisce l'ammissibilità legale e offre la migliore prova in caso di controversia

Quali sono i benefici di Kinamik Secure Audit Vault?

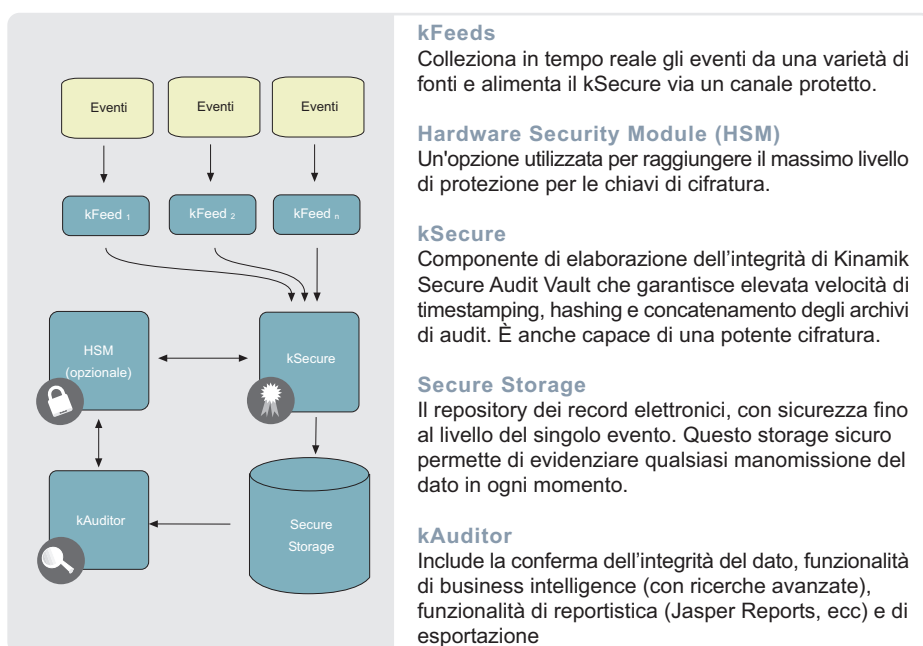
- ▶ Riduce i costi del supporto per Governance Risk Compliance, audit, e-discovery e dei processi legali
- ▶ Impedisce la frode e riduce il rischio e l'impatto del pericolo rappresentato dalle minacce interne mediante un'accountability che va oltre il controllo degli accessi
- ▶ Fornisce un supporto nelle cause legali aumentando il peso probatorio dei documenti elettronici
- ▶ Soddisfa le più severe normative sulla manomissione dei dati e le misure di best practice

Puoi fidarti dei dati sottoposti alla conformità normativa, alla minaccia interna e all'e-discovery?

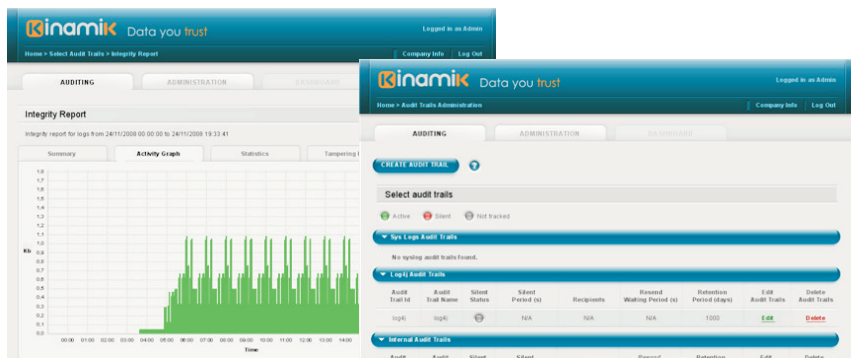
La tempestività nel controllo dei dati, nella gestione del rischio, nella conformità alle normative e nell'e-discovery sono per le aziende una necessità primaria. Gli sforzi per queste attività costituiscono una sfida costante e sempre più impegnativa: è sempre più costoso e difficile rispettare le normative, le minacce interne sono in aumento, la capacità di giustificare le prove nelle procedure di e-discovery è costosa e complessa. Non riuscireci espone le aziende ad un grande rischio.

Kinamik affronta queste sfide con la creazione del Secure Audit Vault, un sistema centralizzato per tutti i dati di audit. Kinamik Secure Audit Vault rende semplice archiviare, recuperare e ricercare le informazioni, conservando il dato in sicurezza con il più alto livello di integrità. Kinamik Secure Audit Vault può gestire senza problemi un gran numero di dati in ingresso provenienti da fonti diverse, tra cui applicazioni, database, server e dispositivi di rete. I record contenuti nel Secure Audit Vault sono conservati nel loro formato nativo, resi sicuri fino a livello del singolo evento e resa tracciabile ogni eventuale modifica. Utilizzando un'interfaccia web-based, Kinamik Secure Audit Vault consente di recuperare e analizzare gli eventi raccolti fornendo la garanzia della loro integrità ogni qualvolta sia necessario.

Kinamik Secure Audit Vault semplifica e riduce i costi associati ai processi di conformità centralizzando le informazioni sensibili, elimina le minacce interne attribuendo un'inconfutabile responsabilità anche agli utenti con i maggiori privilegi e fornisce la migliore prova in caso di controversie, dimostrando senza alcun dubbio l'integrità degli archivi di audit.



Kinamik Secure Audit Vault · Architettura del Prodotto



Kinamik Secure Audit Vault · Grafica dell'Integrity Report e Console di Amministrazione

Caratteristiche tecniche

- ▶ Data collection agent: gli agent di Kinamik Secure Audit Vault raccolgono e trasmettono i dati in tempo reale attraverso un canale cifrato sicuro.
- ▶ Compressione dei messaggi in transito: riduce la larghezza di banda utilizzata tramite una compressione fino al 70%.
- ▶ Cifratura opzionale dei dati: utilizzando potenti protocolli standard per la cifratura, tutti i dati presenti nell'audit vault possono essere riservati.
- ▶ Gestione degli utenti con LDAP: Kinamik Secure Audit Vault si integra nella esistente gestione aziendale degli utenti ed è compatibile con LDAP e Active Directory.
- ▶ Compatibile con TSA: per raggiungere un maggiore livello di sicurezza e protezione dell'integrità, Kinamik Secure Audit Vault è completamente compatibile con le Authority esterne di Time Stamping (TSA).
- ▶ Data Retention Policy tool: Kinamik Secure Audit Vault consente di definire criteri di conservazione differenti per ogni fonte indipendente di dati, consentendo di rispettare le leggi, regolamenti e norme (ad esempio PCI-DSS, D.Lgs 196/2003, Basilea II, MiFID, ecc) che obbligano a conservare i dati per un certo periodo.
- ▶ Ricerca di testo tramite regular expression all'interno di un repository centralizzato: utilizza capacità di ricerca web-based per una localizzazione precisa di specifiche stringhe di testo e di frasi all'interno dei dati protetti.
- ▶ Report completo sull'integrità dei dati di facile comprensione: valuta il livello di attendibilità dei dati con una semplice istantanea (snapshot). Individua qualsiasi violazione dell'integrità fino al livello del singolo evento.
- ▶ Capacità di compressione dello storage e archivio: riduce i costi di storage e di archiviazione con le funzionalità di compressione con un rapporto di compressione fino a 5:1.
- ▶ Facile integrazione con gli strumenti di reportistica: esporta facilmente verso Jasper Reports per report personalizzati.
- ▶ Alte prestazioni: la tecnologia di Kinamik Secure Audit Vault è in grado di elaborare e garantire fino a 40.000 EPS (eventi per secondo)*

*Funzionalità di firma del componente KSecure. I risultati possono variare a seconda di diversi fattori come la configurazione del sistema

Architettura

- ▶ 3 livelli di architettura
- ▶ J2EE + Spring
- ▶ Completamente clusterizzabile

Algoritmi crittografici supportati

- ▶ Encryption: AES 256, RSA -1024+
- ▶ Hashing: SHA-256, SHA-512 e oltre

Piattaforme supportate

- ▶ Linux/UNIX
- ▶ Solaris
- ▶ Windows
- ▶ Ogni sistema Operativo che supporta Java

Feed Supportati

- ▶ Messaggi di Syslog
- ▶ File di testo generici
- ▶ Applicazioni JDBC
- ▶ Log4J (per applicazioni Java eseguite su JVM 1.4 o successive)
- ▶ Nativo BEA Weblogic 9
- ▶ Nativo OpenSolaris Audit
- ▶ Nuove piattaforme sono costantemente aggiunte e possono essere supportate a richiesta

Canali supportati

- ▶ HTTP/HTTPS

Protocolli di comunicazione supportati

- ▶ Burlap
- ▶ Hessian
- ▶ HTTP invoker
- ▶ JMS



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




A proposito di Kinamik

Il software Kinamik protegge i record digitali dalla manomissione. Kinamik ha costruito un Audit Vault centralizzato per i dati sensibili con un controllo sull'integrità e sull'autenticità a livello granulare, creando nel mondo digitale un livello di prova simile a quello dei record tradizionali su carta. Kinamik dissuade, individua e dimostra la manipolazione dei dati per garantire la correttezza delle informazioni digitali.

La missione di Kinamik è far crescere il livello di fiducia, responsabilità e protezione della privacy nelle aziende che trattano grandi volumi di informazioni sensibili. La soluzione di Integrity si rivolge principalmente ai settori finanziari, sanitari, governativi e di IT hosting.

Le informazioni contenute in questo documento sono aggiornate al momento della stampa. Kinamik si riserva il diritto di modificare le informazioni contenute in questo documento senza ulteriore preavviso per aggiornamenti o migliorie sul prodotto. Kinamik declina ogni responsabilità implicita o esplicita circa l'uso di questo documento. Kinamik è un marchio di Kinamik Data Integrity, S.L. Tutti gli altri marchi citati sono di proprietà delle rispettive società.