DATAGUISE

DATA PROTECTION OPTIMIZED FOR INSURANCE BIG DATA

DATAGUISE DETECTS AND PROTECTS SENSITIVE DATA IN HORTONWORKS' BEST-IN-CLASS INSURANCE HDP PLATFORM

Today, insurers are more data-driven than ever, leveraging Hadoop to create new risk products, reduce fraud, and accelerate customer insights. Increasingly, insurers use Hadoop technologies to incorporate all of their data sources, including mobile telematics, clickstreams, claims notes and diary, transcriptions, and underwriter notes — data sources previously unavailable to risk-based pricing, fraud, settlement prediction, and more. These newer data sources invariably contain private, sensitive, or personal data that poses compliance and breach risks if stored or used in the open.

To give insurers total visibility and control over all of their sensitive data, Dataguise has developed **the first data-centric security solution optimized for Hortonworks' insurance solution blueprint.** With Dataguise, insurers can precisely detect, protect, and audit all sensitive data, using the central dashboard of the Hortonworks data governance framework that tracks and controls data with Apache Atlas and Apache Ranger platforms.

Core Benefits of the Dataguise Approach:

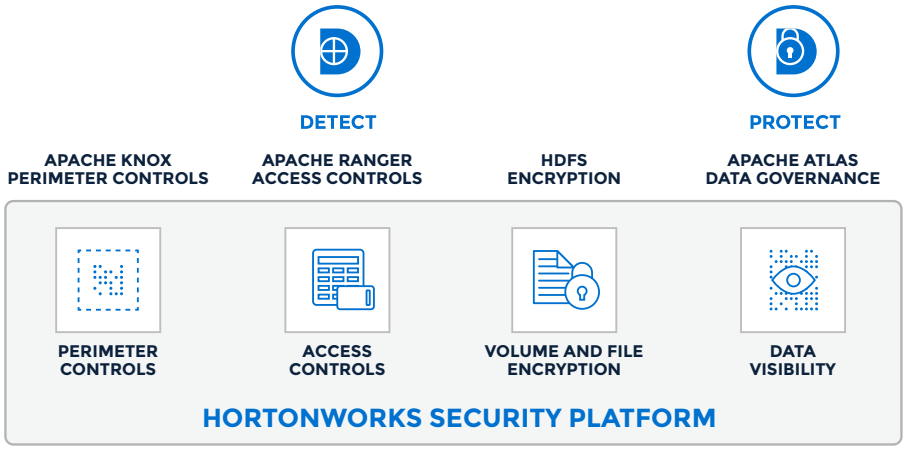
- Detects and manages security risks: Insurers need to pinpoint sensitive data in hard-to-profile semi-structured or unstructured data sets. Dataguise data detection can be deployed for claims adjuster notes, sales portals, customer voice-to-text transmissions, insurance application submissions and attachments and other unstructured data sources.
- Fits closely inside Hortonworks' HDP security platform: New sensitive data discovery can drive data governance through API integration with Apache Atlas.
- Delivers data-centric protection: Precise protection at the data level. Data-centric masking and encryption of sensitive data at the cell or field level enable insurers to enforce security policies, audit what sensitive data is entering HDP, and dynamically protect sensitive data elements (e.g., names, URLs, credit cards, purchase amounts, date-of-birth information, VINs, etc.).
- Fits directly inside Datastax Enterprise security: Dataguise's detection and dynamic protection complement and interoperate directly with Datastax Enterprise's native security features, including user audit, transparent data encryption, and the entire user authentication/permission management framework.
- Supplies 360-degree views with 100% confidence: Keep highly personal customer information secure to build trust with the customers insurers rely on to grow.

CASE STUDY: DATA-CENTRIC SECURITY FOR A TOP-THREE US INSURER

Dataguise empowers a leading US-based insurer with:

- Complete data visibility: Runs Dataguise detection to accurately examine, detect, and track sensitive data across underwriter apps, telematics, clickstream and web logs, transcriptions, and sales portals.
- Hadoop data consolidation: Brings all data into Hadoop, including sentiment data, telematics and sensors, and agency field notes — to reinforce risk pricing and subrogation applications.
- Breach risk management: Selectively uses masking to de-identify or redact data for third-party applications that don't require direct access to original sensitive elements.

HOW DATAGUISE DETECTS AND PROTECTS SENSITIVE INSURANCE DATA



Insurance data entering Hadoop

- Inspect and detect all data sources for sensitive PII, PHI, and PCI data.
- Optionally mask, redact, or encrypt data that needs enhanced protection.

Analytics — dynamic data protection

- Authorized access to sensitive data in HIVE, Revolution, SAS, and other analytic frameworks.
- Close and native integration with Apache Atlas to track and control sensitive data at scale with automated Apache Ranger ACLs based on sensitive data "traits."
- High performance — pay protection price only when needed.

HADOOP PLATFORMS CAN ACCELERATE	DATA SOURCES	NEW SECURITY CHALLENGES
Single view of customer.	Application documents, clickstream and web logs, marketing research, CRM records, and social media.	• Coverage for multiple file types and sources. • Critical detection to find and measure sensitivity risk.
Claims optimization and fraud detection.	Policy records, claims databases, receipts, accident reports, emails, and transcriptions.	• Reduce or eliminate PCI scope for Hadoop. • Detect new sensitivity risks in hard-to-reach unstructured data.
Price risk with new, untapped data sources.	Mobile telematics, sensor data, social media, and voice-to-text files.	• High scale. • Large sets of small files. • Detection and protection of unstructured data.
Application processing.	Claims data, insured prior loss data, and claims adjuster notes.	• Masking of sensitive data for data sharing. • Sensitive data auditing.
Secure data that is shared with third parties.	Reporting bureaus, third-party claims administrators (TPAs), telematics service providers (TSPs).	• Tiered access — highly granular roles with differing needs/views for sensitive data.

To learn more about Dataguise's one-stop data security solution that detects and protects sensitive data across all repositories, visit: www.dataguise.com

DATAGUISE