CUSTOMER CASE STUDY

Insurance Company reduces IBM Guardium administration effort by 90% with Imperva Data Security Fabric

Expands data protection while improving efficiency and lowering costs

Overview

This 150-year-old company based in North America specializes in property and casualty insurance. The trust of their customers is critical to the business and protecting customer data is key to protecting their brand and reputation.

The company's security strategy is managed by its information security group. Responsibility for complying with security policies falls to each of the 35 individual business units, which the information security group supports. This group historically has used IBM Guardium™ Database Activity Monitoring (DAM) for data compliance and governance.

Challenge

As the company continued to grow, and the pressures of regulations and expectations of customers grew along with them, there was a notable internal priority shift from compliance to security use cases. The company's Senior Governance Specialist shared how "customers were increasingly considering their own potential risks when determining what insurance services to use. Combined with the added complexity of regulations such as GDPR, CCPA, and NYFDS, and the very visible data breaches in the news, it was critical for us to stay ahead of it." The new security emphasis created a significant focus on proactively managing the detection and prevention of unauthorized activities around sensitive data. This meant the IBM Guardium™ tool they originally implemented to satisfy compliance requirements was re-evaluated for its data security potential.

The critical business requirements evaluated included coverage for additional data repositories that Guardium™ did not support, elimination of the manual labor that traditionally comes with security incident response, and easy access to long-term audit information for reporting and forensic investigation. The company chose to implement Imperva Data Security Fabric as the best option to meet these requirements, optimize their current investment in Guardium™, and accelerate their approach to data security.

90% reduction in administrative workload.

Automation of production data edit process.

Ability to focus on **higher value** security events.

Agentless support for MarkLogic with no change to infrastructure.

Deployment

The Imperva Imperva Data Security Fabric (DSF) platform reduces the costs of Guardium™ while expanding capabilities. Imperva DSF leverages agentless collection methods to deliver greater coverage of all data repositories, reduce manual operations, and provide richer, actionable security intelligence. For companies with mature data security programs, Imperva DSF can integrate seamlessly with existing investments in IBM Guardium™, saving money on hardware and operations costs, while gaining threat intelligence and comprehensive support for cloud databases.

The company's Senior Governance Specialist shared that "once he learned about Imperva Data Security Fabric he thought we'd be crazy not to go this route." Before Imperva DSF, the team used to collect raw data from Guardium™ and perform all data classification, search, analysis, and change reconciliation manually. They would then individually distribute .csv logs out to 150 different people across data, security, and compliance teams. The insurance company has since migrated a majority of its manual reporting operations into automated workflows driven by Imperva DSF. This change alone has reduced their administrative workload by 90% and lets them focus on introducing more advanced security practices.

> **"We spent a significant amount of investment in building our DAM program and were ready to get more value out of it. We know Guardium's™ reporting and retention capabilities were going to be a problem when we started talking security strategies."**
>
> Senior Governance Specialist

Results

By leveraging Imperva Data Security Fabric, the team can orchestrate their end-to-end processes around sensitive data. Specifically, they automate their production data edit process and have fully integrated their ticketing system, ServiceNow™, so all alerts and requests are assigned to the relevant owners without the information security team needing to be the middleman. In addition, they utilize Imperva Data Security Fabric machine learning algorithms to automatically perform behavioral analysis and easily identify any data access events that are outside of the normal activity.

Looking forward, the company is in the process of beginning a fairly large deployment of MarkLogic®. This database is not supported by their Guardium™ DAM solution, but with Imperva DSF they can easily support MarkLogic®, plus other new data sources, and deploy their data security strategy across the new workloads with no change to their underlying infrastructure.

	BEFORE	AFTER
Data Retention	Collectors – 14 Days Aggregator – 31 Days	Multi-year audit data retention Sessions & Exception Data – 1 Year Instance Data – 2+ Years
Reporting & Workflows	Aggregator Issues Performance Issues System Monitoring	Actions taken in seconds Greater reporting timeframes Ticketing style justify workflow
Security	Compliance Focus	Automated Threat detection with User and Entity Behavior Analytics (UEBAs)
Coverage	Unsupported Data Sources	MarkLogic supported via gateway Quick support for any new environment