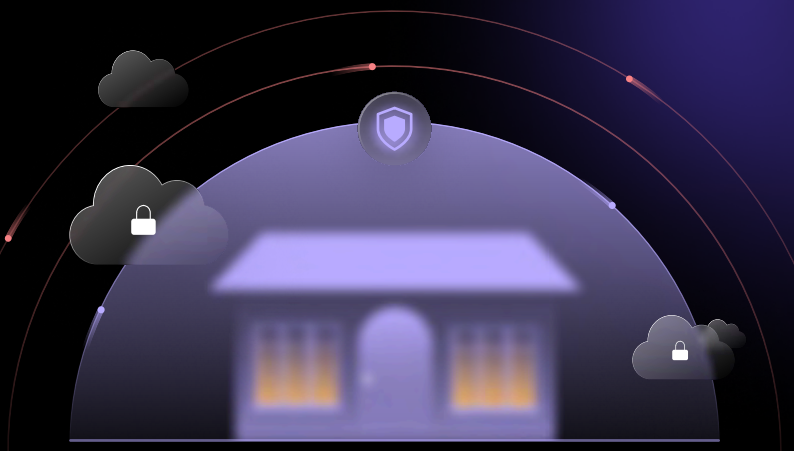
sentra

How a Mortgage Lender Ensures Sensitive Data Gets Masked and Stays Masked



One of the largest U.S. mortgage lenders manages over $350 billion in loans across a complex ecosystem of production and non-production cloud environments. They rely on data-intensive applications to support underwriting, processing, and customer management. Given the nature of their business, mortgage lenders and financial institutions are subject to stringent and multi-layered data protection and privacy regulations, such as; FTC Safeguards Rule, Gramm-Leach-Bliley Act (GLBA), Consumer Financial Protection Bureau (CFPB), SOX, FFIEC guidelines, and increasingly state-level privacy laws like the California Consumer Privacy Act (CCPA). Compliance requires rigorous control over non-production data environments where customer data often gets replicated for development and testing. Most relevant regulations either require or recommend data masking for sensitive customer data.

The mortgage lender had a legacy DSPM solution that generated large volumes of false positives, and lacked the precision to support automated masking workflows needed to ensure compliance. This created significant manual overhead for the data security team.

The financial institution's data security and compliance teams turned to Sentra and within weeks, they gained column-level visibility into regulated data, automated classification and masking of workflows, and uncovered hundreds of orphaned data stores that could be deleted to both significantly **improve regulatory compliance, reduce storage costs** and **reduce manual workload** for the security team.

The Challenge:
Manual Masking and Limited Data Visibility

The mortgage lender uses a data masking tool to mask regulated data in non-production environments. Their previous DSPM solution lacked depth and breadth of classification and created too many false positives, leading to over-masking and a labor intensive manual verification process. This made it very difficult to spot what data needed to be masked.

Like all financial institutions, the lender also has many sensitive data classifications unique to its business operations that had to be manually tagged. Together, all these classification limitations made it difficult to create data reports to feed to their data masking tool. For known and correctly classified sensitive data, their data masking tool was able to transform it into realistic synthetic records. Once the original required data masking was performed, there was no reliable way to confirm whether data remained masked after refreshes, especially since the masked data resembled real data so closely. The mortgage lender needed visibility into where PII/PCI and toxic data combinations lived across non-production environments and accurately classified sensitive data before and after being masked.

The challenge wasn't just masking data; it was the persistent uncertainty of whether that data stayed masked after system refreshes. We needed a reliable way to verify ongoing compliance at a granular level.

— Chief Compliance Officer, Leading US Mortgage Lender

Why Sentra:

Column-Level Precision, Workflow Automation, and Immediate ROI

After a thorough evaluation of leading DSPM vendors, the mortgage lender chose Sentra due to several key capabilities. Its flexible classifier system, which supports both regex and contextual logic using AI-powered classifiers, made it easier to identify masked and unmasked data accurately. The platform's policy engine offered automated scanning for missing or reverted markers, helping teams detect issues early. Sentra also seamlessly integrated into existing workflows without requiring invasive changes to systems or processes.

Key Outcomes:

- **Fast AI-Driven Column-Level Classification:** Sentra's precise tagging engine classified sensitive data across their entire environment in just six weeks, outperforming other vendor tools by automatically identifying PII/PCI, financial data, and compliance-relevant data types.

- **Improved Accuracy:** With Sentra the compliance and data security teams are able to create a clear view of all the data that needs to be masked and feed this information into their data masking tool for future masking. Sentra can detect whether a dataset contains markers like "@example.com" emails or specially formatted SSNs.

- **Automated Data Masking via Jira:** Sentra integrated with their existing data masking tool to mask data and pushed alerts to Jira, enabling end-to-end remediation workflows with executive visibility.

- **Granular Visibility:** By using data classifications and logical negation (e.g., “does not contain marker”), the compliance team can isolate and track both compliant and non-compliant datasets.

- **Policy-based Automation:** Sentra’s automatic policies engine is set to run on a regular schedule, identifying data assets without expected markers, allowing the compliance and data security teams to take action before audits or incidents occur.

- **Compliance Confidence:** Able to ensure compliance with multi-layered data protection and privacy regulations and internal security mandates for precise access and masking.

Implementation:
From Manual Compliance Burden to Automated Remediation

The mortgage lender deployed Sentra in under six weeks, scanning thousands of data stores across AWS, Snowflake and other cloud and SaaS environments and applied accurate sensitivity labels. Sentra’s classification output determined user roles based on data sensitivity. The integration with Jira and their data masking tool enabled an automated masking workflow, flagging issues to executives and eliminating manual triage.

Following the initial deployment, the financial institution decided to build on this momentum and extend Sentra’s coverage to Google Workspace.

Real Business Impact:
Data Visibility, Accurate Masking, and Compliance Confidence

With Sentra, the data security and compliance teams gained deep visibility into sensitive and regulated data across cloud environments and SaaS applications, transforming how they enforce compliance and scale a proactive, automated data protection strategy.

Mortgage Lender and Sentra:
Turning Compliance into a Competitive Advantage

What started as a goal to streamline masking and compliance has become a long-term foundation for cloud data governance. The data security team replaced an underperforming legacy DSPM and gained deep visibility into sensitive and regulated data across cloud environments and SaaS applications, transforming how they enforce compliance and scale a proactive, automated data protection strategy. They also implemented a strategic, automated framework for protecting customer data across every environment and ensuring compliance.

Together, the mortgage lender and Sentra have transformed how the financial institution security team supports excellence in development speed, data protection, and regulatory compliance.

Gartner Peer Insights Customers' Choice 2025

Gartner Peer Insights™

4.9 ★★★★★

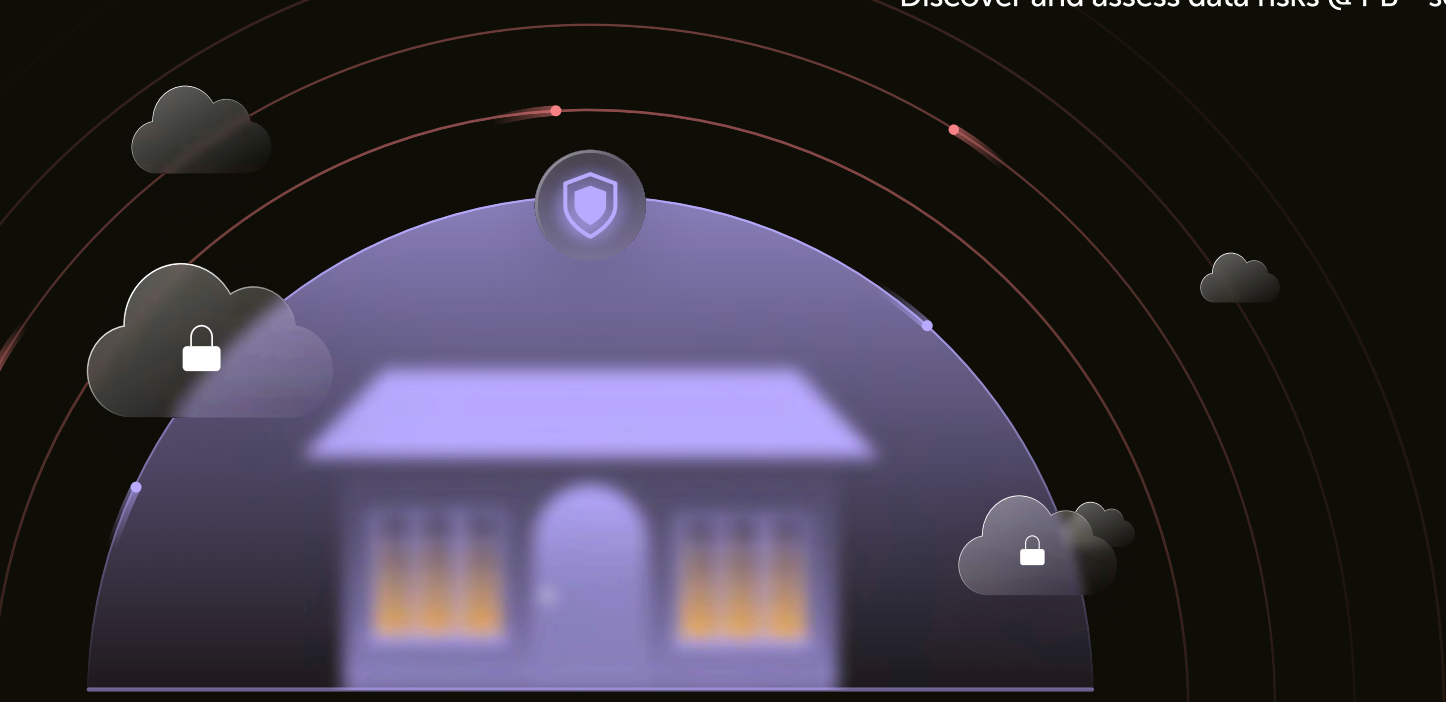
By Sentra in Data Security Posture Management (DSPM)

Setting a New Standard in Data Security

>95% Accuracy
AI-powered classification

10x more efficient
In scanning compared to industry

In less than 1 week
Discover and assess data risks @ PB - scale



sentra

Visit www.sentra.io | Watch a demo

For more information, please contact us at info@sentra.io