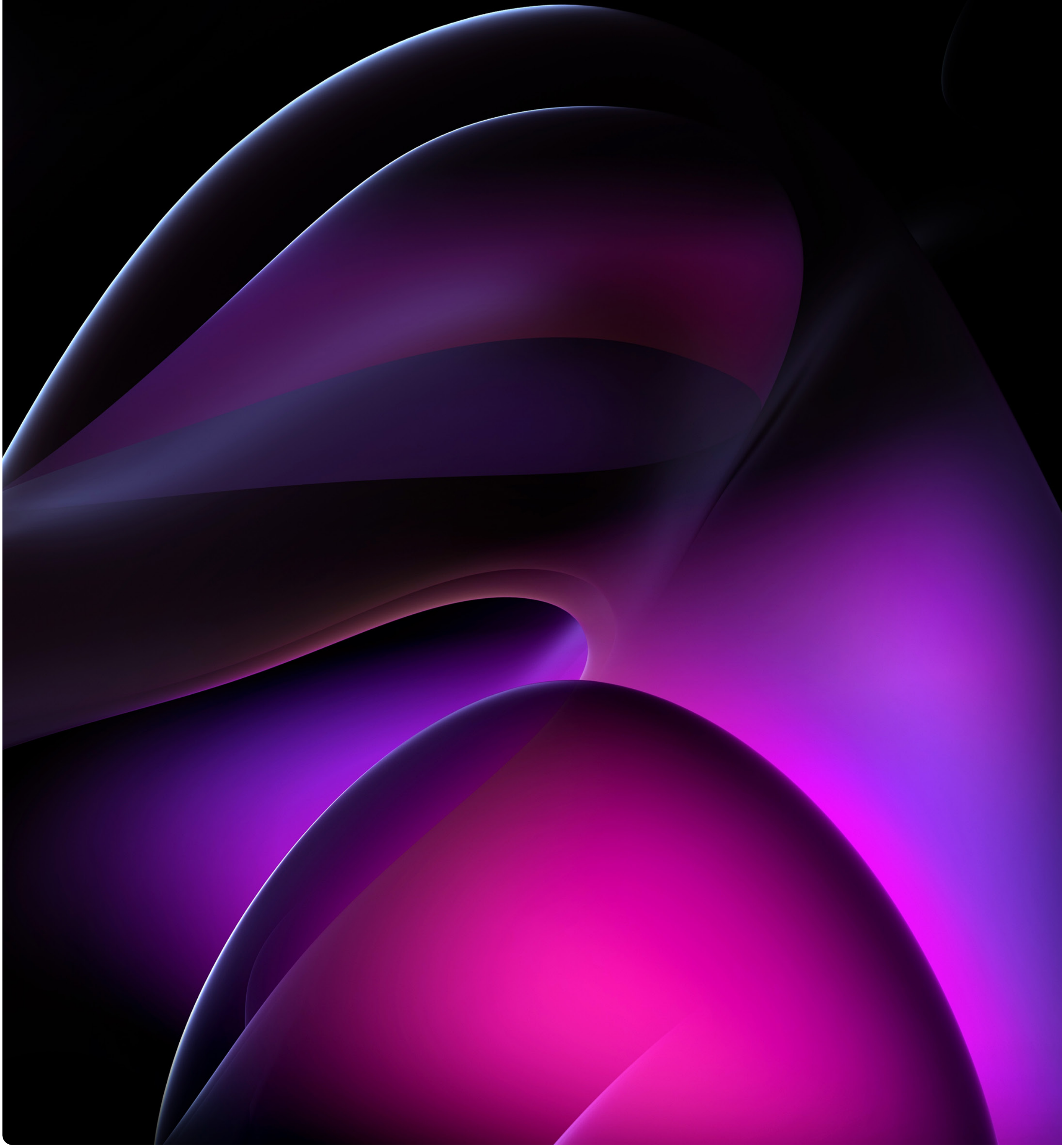
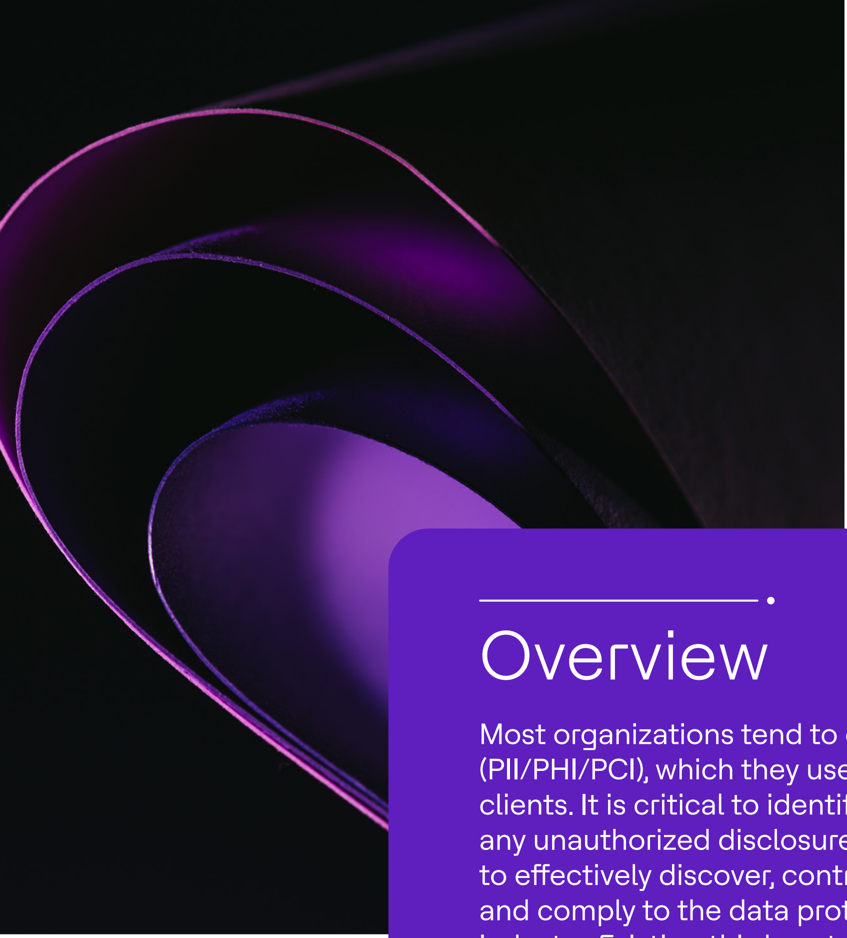
HCLTech | Supercharging Progress™

Data patrol

Discover and protect sensitive data with built-in isolation and ticketing mechanism





Overview

Most organizations tend to collect large volumes of sensitive data (PII/PHI/PCI), which they use to provide relevant customized services to its clients. It is critical to identify and protect the collected sensitive data from any unauthorized disclosure and it is the responsibility of every organization to effectively discover, control and manage their sensitive data footprints and comply to the data protection laws relevant to the country and its industry. Existing third-party solutions for sensitive data discovery lack ML prowess and cloud integration capabilities to tackle sensitive data leaks and are often too expensive to adopt in real-time use-cases.

Hence, having robust automation and bringing new scalable ML supported technologies to detect sensitive data at point of ingestion/integration and take necessary actions to avoid any leakage becomes critically important.

HCLTechvs DataPatrol Framework leverages native AWS services to provide end-to-end automation right from scanning the sensitive data at the point of ingestion to dashboarding key insights for business consumption. This ML-powered framework can seamlessly detect several identified and custom sensitive data types catering to any industry, supporting PII protection and strictly adhering to data privacy, compliance and regulatory needs such as GDPR, PCI-DSS and HIPAA.

Framework

To improve the sensitive data discovery and governance in AWS environment, HCLTech has provisioned a framework, referred as DataPatrol Framework which is built using rich set of AWS services like Amazon Macie, AWS Lambda, AWS Security Hub, Amazon EventBridge, Amazon SNS and Amazon QuickSight among other services to accomplish critical tasks during the life cycle of sensitive documents being patrolled.

Key Features

This solution comprises of the following key features, each having several interesting capabilities that are crucial for building a robust and complete data patrolling solution.

Sensitive data discovery

Fully managed, updated machine learning techniques for PII detection and ability to define and use custom datatypes using regular expressions have proven to deliver quality discovery of variety of sensitive datatypes from customer's source data

Secure data isolation and encryption

This feature will assist in effective isolation of high sensitive data files right at the ingestion layer in itself and prevent further leakage to the downstream systems

Severity based email alerts

Based on the Amazon EventBridge events, this workflow automatically triggers Amazon SNS service to send custom email notifications to its subscribed users containing critical details on the sensitive data file location along with its severity level warnings (High/Medium/Low)

Centralized management of sensitive data findings

Integration with AWS Security Hub provides a comprehensive vision and security findings management strategy to aggregate and analyze all high sensitive data findings from a single window stored as a standard AWS Security Finding Format (ASFF) for further processing

Audit and compliance reports

A consolidated DataPatrol report for each patrolling job will be auto-downloaded to a customer specified location for quick review and action on the findings

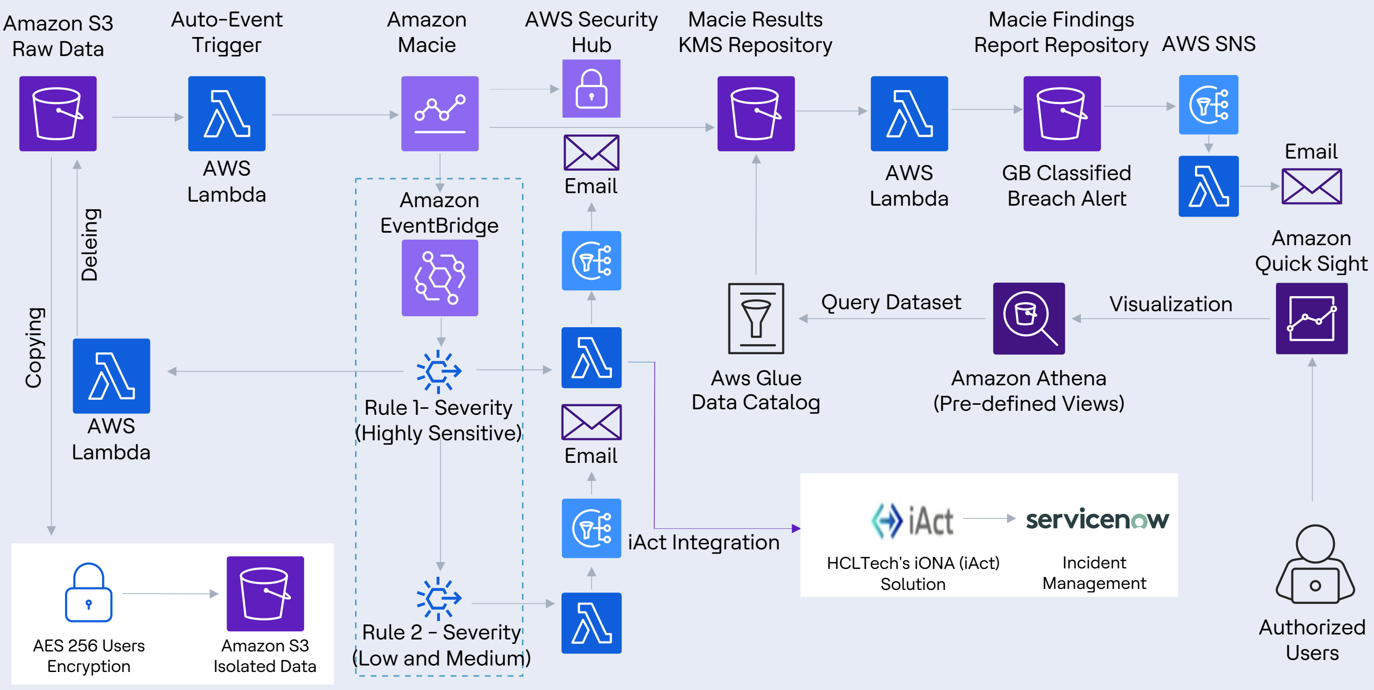
Incident reporting and management

HCLTech's DataPatrol framework is fully integrated with its iONA (iAct) solution to auto-create incident in ServiceNow tool for every high severity detection and assign to appropriate user group for further review and action

DataPatrol dashboard

It is fully capable to deliver pre-built ML driven insights with auto-narratives that are embedded contextually in the dashboard using natural language for quick interpretation

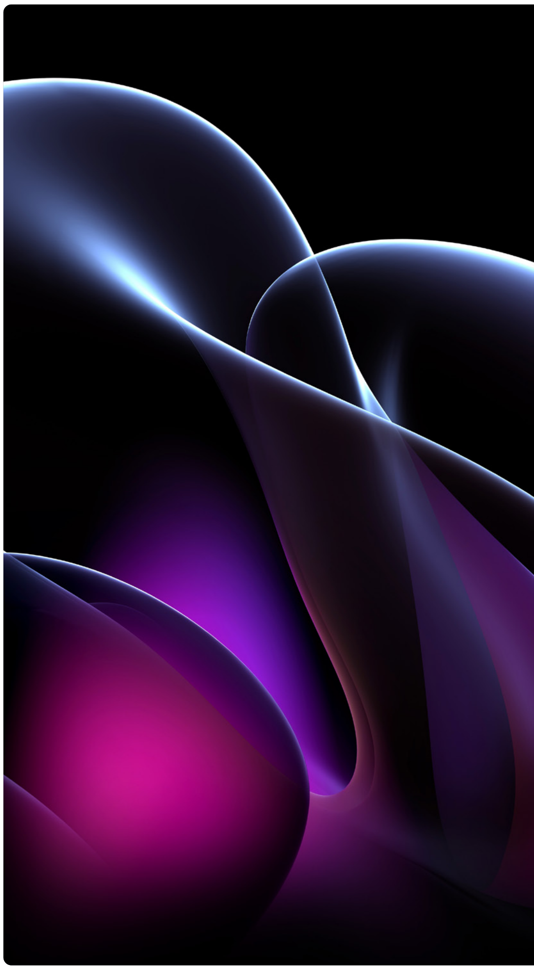
DataPatrol framework – architecture



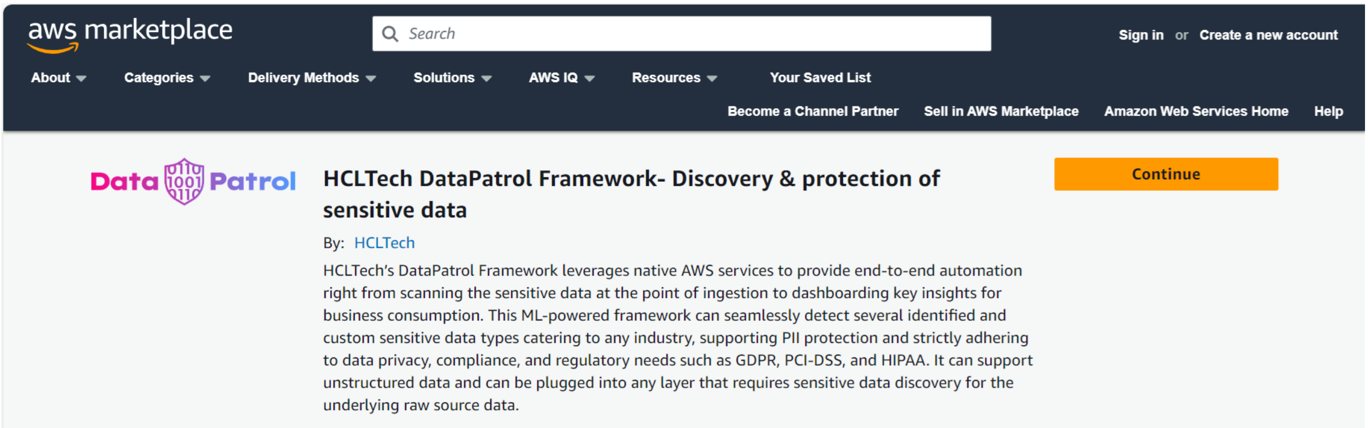
Benefits

HCLTech's DataPatrol architecture leverages native AWS Services for sensitive data discovery and analytics. Key benefits of the solution includes:

- Ability to swiftly identify and discover sensitive data including Personal Identifiable Information (PII), Personal Health Information (PHI) and Payment Card Industry (PCI)
- Provision to move high sensitive files out from source to a secure target location and prevent sensitive data leak
- Ability to notify users with custom email alerts upon sensitive data breaches
- Equip businesses with a consolidated view of DataPatrol report in an easily readable format (csv) to review the sensitive data findings for audit and compliance requirements
- Collate, monitor and process sensitive data findings coming from DataPatrol into a centralized hub, thereby providing a comprehensive view of security state and high priority security issues
- Provisioning seamless integration with ServiceNow tool to automatically raise incidents for every high severity alerts
- To empower business users with rich
- pre-configured ML driven dashboards to review the key insights on sensitive data for all of the processed DataPatrol jobs



Use case(s)	Customer issues	How does the APN partner Aaddress the issue (solution)?
Healthcare industry Protect sensitive data coming from Electronic Health Records (EHRs), Clinical Trails, Medical research, Health Insurance, Telemedicine etc.	• Healthcare data often has complex data ecosystem and securing sensitive data from these diverse systems can be a very complex task. • Clinical trial records, drug simulation data and other super sensitive data needs due protection from leakage as any failure will lead to financial penalties and loss in potential business • Complying to strict regulations such as HIPAA, GDPR, PHI to protect sensitive data can be even more challenging	DataPatrol Framework uses native AWS services and leverages machine learning (ML) and pattern-matching techniques to detect growing list of sensitive data types and helps customers swiftly identify and discover sensitive data, including personal identifiable information (PII), personal health information (PHI) etc. It entirely automates the discovery of sensitive data and prevent sensitive data leakage complying to data security standards such as HIPAA, GDPR etc.,
Finance industry Protect sensitive data which includes Customer Financial Data, Transaction data, Market data, Business Data, Regulatory data etc.	• Financial data comes in different formats and standards which makes it difficult to discover and protect sensitive data • This Industry is heavily regulated and complying these regulations can be challenging • PCI, PII, GDPR and host of country specific data privacy regulations demands that data must be secured at all times	DataPatrol Framework provides automated solution for discovery and classification of sensitive data including financial data such as credit card numbers, bank account numbers and other PII data. This solution helps financial institutions to be complaint to PCI-DSS, GDPR and hence avoid costly fines associated with data breaches. It also helps to respond to security incidents quickly with built-in ServiceNow Integration
Telecom industry Protect sensitive data including customer personal information, call records with phone numbers, customer payment details etc.	• Telecom companies intend to collect massive volumes of data which includes critical sensitive PII information which is difficult to discover, manage and secure • 3rd party involvement can introduce additional data leak risks	DataPatrol Framework can automatically identify and classify sensitive data and report the detailed findings to companies to understand the high sensitive data and prioritize its protection to comply with GDPR regulations. It can provide custom alerts for the detected severity findings and isolate the sensitive data securely to prevent leakage. It includes self service ML-Powered dashboards for quick decisioning



HCLTech DataPatrol Framework- Discovery & protection of sensitive data

By: HCLTech

HCLTech's DataPatrol Framework leverages native AWS services to provide end-to-end automation right from scanning the sensitive data at the point of ingestion to dashboarding key insights for business consumption. This ML-powered framework can seamlessly detect several identified and custom sensitive data types catering to any industry, supporting PII protection and strictly adhering to data privacy, compliance, and regulatory needs such as GDPR, PCI-DSS, and HIPAA. It can support unstructured data and can be plugged into any layer that requires sensitive data discovery for the underlying raw source data.

The solution is listed on AWS Marketplace, AWS Partner Solutions Finder and is available for customers globally. To learn more Click here

HCLTech | Supercharging Progress™

hcltech.com

HCLTech is a global technology company, home to more than 221,000 people across 60 countries, delivering industry-leading capabilities centered around digital, engineering, cloud and AI, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, Technology and Services, Telecom and Media, Retail and CPG, and Public Services. Consolidated revenues as of 12 months ending September 2023 totaled $12.9 billion. To learn how we can supercharge progress for you, visit hcltech.com.