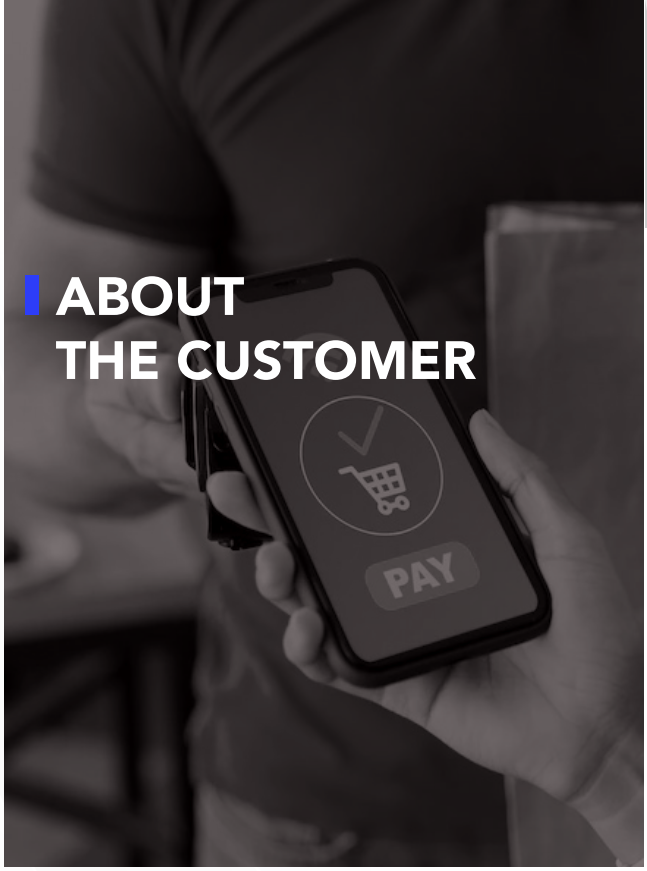
SISA

CUSTOMER SUCCESS STORY

SISA Radar's customized solutions helped an Indian fintech company streamline sensitive data discovery and classification to achieve compliance.



ABOUT THE CUSTOMER

The client is an India-based fintech company that offers a wide-ranging suite of payment solutions to vendors, merchants, and e-commerce platforms. It is an online payment gateway that is designed to handle end-to-end payments for businesses. The client also provides access to all major payment modes including credit card, debit card, net banking, Unified Payments Interface (UPI), and e-wallets. It offers a single platform that facilitates bank transfers, recurring payments, tax payments as well as capital loans.

THE CHALLENGE

Being a one-of-a-kind payment solutions company in the region with a vast and dynamic data environment, scanning its multiple platforms, endpoints, servers, and storage locations was not an easy task. The size of the data environment varied from 10 GB to 500 GB in Google Drive (GDrive), up to 1 TB on the Windows server, and up to 1 TB used data in Azure Blob Storage. With data scattered across the network environment, identifying sensitive information (Cardholder data and PII data), and complying with Payment Card Industry Data Security Standards (PCI DSS) was a complex task.

It was challenging for the client to scan GDrives and emails of 4,000+ users with different user IDs and passwords. A majority of previously tested data discovery and classification tools were unable to provide a solution to successfully scan the cloud platforms. Scanning of shared drives in G Suite and Containers, File Shares, and Queues in Azure storage for 500+ accounts was also an uphill battle. The client also confronted challenges while scanning work-from-home (WFH) servers that were operating on Windows, Linux, and Mac OS. Moreover, the fintech company received a higher percentage of false positives as the existing tool was unable to differentiate between real card numbers and transaction numbers.

SOLUTION OFFERED BY SISA

As a first step, SISA created a customized cloud scanner for G Suite and deployed it in the Google Cloud Platform (GCP) to scan the emails, GDrives, and common folders. SISA also created one admin ID to simplify the scanning process for all 4,000+ G Suite users. With both onsite and web deployment of SISA Radar, the payment solutions company was able to successfully initiate the scans for both the on-premises and WFH users (Windows, Linux, and Mac OS) with the help of agents and scanners. SISA Radar agent was also deployed and tested on Mac systems with low, medium, and high scan options to optimize the impact on the CPU. By creating one single account key to scan all Containers, File Shares, and Queues, SISA Radar was able to streamline the scans for 500+ Azure storage accounts and identify the PCI and PII data present in Azure Blob Storage.

Integration with AI and ML solutions enabled SISA Radar to minimize the percentage of false positives and improve the accuracy of the scans. After the completion of the data discovery process, SISA Radar also assisted the client with the classification of sensitive data into multiple criticality types such as public, private, internal, confidential, or restricted data. The client also leveraged SISA Radar to take remediation actions for the identified sensitive data by masking, truncating, deleting, or quarantining it to secure locations. SISA Radar also provided customized and portable reports of the complete process as per the client's requirements.

SISA also shared best practices and recommendations from forensics learnings derived from previous investigations to help the client address the security gaps in sensitive data exposure. The forensics learnings which encompass a set of 'Preventive and Detective' controls above and beyond the PCI controls, helped the client implement stronger controls, and achieve compliance with PCI standards.

BUSINESS IMPACT

With the customized solutions provided by SISA Radar, the client was able to achieve compliance with Payment Card Industry Data Security Standards (PCI DSS) and identify the Personally Identifiable Information (PII). The learnings from SISA's forensics-driven cybersecurity approach helped build in the requisite custom features in SISA Radar to be used in this specific case. By choosing SISA Radar, the client automated the process of discovering, classifying, and remediating sensitive data, avoiding the risk of exposure to card data in multiple locations. SISA Radar also enabled the fintech company to facilitate quarterly scans across the network with reduced time and cost.

SISA

A forensics driven cybersecurity company, trusted by organizations across the globe for securing their businesses with robust preventive, detective, and corrective security services and solutions.

Compliance

PCI Compliance

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ

PCI Compliance

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Swift
- Cloud Security
- Risk Assessment
- Quarterly Security Audits

Security Testing

Application Security

- Application
- Penetration Testing
- CREST/CERT-in Approved
- Security Testing
- API Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- ASV Scan

IoT Security Testing

Managed Security Services

Phishing Simulation

Cyber Resilience

Managed Detection and Response Solution

SISA ProACT

Incident Response and Forensics

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation

Advanced Threat Hunting

Data Protection

Data Discovery and Classification Tool - SISA Radar

- Card Data Discovery
- PII (Privacy) Data Discovery
- Data Classification

Data Discovery as a Service

Training

Payment Data Security Implementation Programs

- CPISI
- CPISI Advanced
- CPISI-D

Security Incident Detection and Response Programs

- CIDR

Forensic Learning Sessions for Senior Management

For more Information visit us at www.sisainfosec.com
OR
write to us at *contact@sisainfosec.com*

Follow us