SISA

CUSTOMER SUCCESS STORY

SISA deploys RADAR across 85,000 endpoints to help a major bank meet compliance standards and boost data security

ABOUT THE CUSTOMER

The client is a leading bank in India and has emerged as one of the foremost public sector banks in the country. Renowned for its advanced banking solutions and technology-driven services, it aims to simplify business operations and foster inclusive growth. Digital transformation sits at the heart of their vision. Recognizing the shift in customer preferences and the evolving landscape of finance, the bank has embarked on a bold journey to digitize its core operations and enhance the customer experience. As of 2023, this bank boasts an extensive network of approximately 10,000 branches nationwide. Financially, the bank has experienced significant growth, and holds a position among the top 1000 world banks.

THE CHALLENGE

This bank's journey towards digital transformation has led to the creation of a highly complex and extensive digital infrastructure. Their ecosystem spans over 100,000 endpoints and supports more than 90,000 email users, reflecting the scale and sophistication of the bank's digital infrastructure. The bank's digital network further extends into Linux Endpoints, Databases, One Drive, SharePoint, and various cloud-based data sources.

As part of their ambitious digital expansion, the bank was confronted with significant challenges related to data protection and the risk of sensitive information exposure. It required a comprehensive solution adept at discovering and classifying sensitive data across various data sources. This capability was not just an operational need but a critical element in building a proactive defense against potential data breaches and ensuring the confidentiality of critical information.

A particular area of concern was the monitoring and protection of sensitive email communications and attachments, involving both Gmail and Zimbra platforms. The bank placed a high emphasis on this requirement, recognizing its importance in preventing the accidental sharing of sensitive data outside the organization and mitigating internal security threats. This dual-layered security approach was deemed essential for their overall cybersecurity strategy.

In addition to these concerns, the bank faced the challenge of scalability and agility in their data management system. With an anticipated 25% increase in data volume, it became imperative that the chosen solution could adapt and scale effectively. The bank needed a system that could not only accommodate this expected growth but also maintain robust security and efficiency throughout the process. This aspect was crucial in ensuring that the bank’s cybersecurity measures remained effective and responsive in an ever-evolving digital environment.

SOLUTION OFFERED BY SISA

Following an intensive technical evaluation aimed at identifying the right solution, the bank decisively selected SISA's RADAR, for its precise capabilities in data discovery and classification, crucial for protecting their digital infrastructure. RADAR's effectiveness in securing sensitive data and countering emerging cyber threats was a key determinant in its selection, reflecting the bank's commitment to a targeted and effective cybersecurity strategy.

In addressing the unique data security challenges of the Bank, SISA RADAR was not just selected for its inherent capabilities but also for its adaptability to the bank's specific needs. The tool’s integration with O365 and Zimbra was a critical enhancement, tailoring email security features to precisely identify and protect sensitive information, a necessity under the bank's stringent cybersecurity protocols.

The application of SISA RADAR's advanced AI/ML technologies was customized to the bank's context. It proficiently scanned OCR and image files, with a focus on detecting and classifying documents marked with the bank's logos or authoritative signatures, aligning seamlessly with the bank's Information Security Management System (ISMS) policies. The compatibility with DRM systems was another tailored aspect, ensuring the protection of copyrighted content critical to the bank's operations.

Moreover, offering both agent and agentless configurations, the solution meticulously adapted to fit the bank’s diverse IT environment. The implementation, overseen by SISA's expert data governance team, was methodically planned and executed. This targeted approach not only maximized efficiency but also significantly enhanced the security framework across the bank's expansive network of 85,000 endpoints, illustrating how SISA RADAR was intricately customized to meet the specific and unique data security needs of the bank.

BUSINESS IMPACT

Following the successful implementation of SISA RADAR, the bank saw significant streamlining of its data protection and governance strategies. The key benefits included:

01

Automated Data Classification

This feature significantly reduced time and effort in managing data, streamlining processes and improving efficiency.

02

Enhanced Scalability

SISA RADAR enabled the bank to effectively manage a 25% increase in data and user growth, demonstrating its capability to adapt to expanding data volumes.

03

Data Mapping and Tagging

Provided a comprehensive understanding of the spread of sensitive data within the organization, aiding in better data management and security.

04

Protection Against Data Exfiltration

Offered robust defenses against threats targeting data-in-motion, ensuring the security of sensitive information.

Integration Abilities of SISA RADAR

With Client DLP (Data Loss Prevention)

Led to the formulation of stronger DLP policies and enhanced Data Loss Prevention capabilities, ensuring tighter data security.

With Client SIEM (Security Incident and Event Management) Solutions

Improved threat monitoring and incident management, contributing to a more secure IT environment.

With Client DRM (Digital Rights Management)

Enabled tight access and content management, and supported data localization efforts, securing copyrighted and sensitive content effectively.

With O365 and Zimbra Emails

Prevented data leakage to both internal and external users in the organization, enhancing email security and data confidentiality.

The client expressed high regard for SISA RADAR's comprehensive approach in elevating their data security posture. Key benefits such as automated classification, scalable solutions for data growth, and robust integration capabilities were particularly noted for their effectiveness. The client also commended the SISA team for their consultative approach, technical proficiency, and collaborative spirit, which played a crucial role in the seamless implementation and success of the project.

SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. Industry recognition by CREST, CERT-In and PCI SSC serves as a testament to our skill, knowledge, and competence. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance

Payment Data Security

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security

Security Testing

Application Security

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

Network Security

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

Hardware and IoT Security Testing

- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing

Cyber Resilience

Managed Detection and Response Solution – SISA ProACT

- Monitoring
- Attack Simulation
- Use-case Factory
- Advanced Threat Hunting

Digital Forensics and Incident Response

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

Data Protection and Governance

Data Discovery and Classification - SISA Radar

- Card Data Discovery
- PII (Privacy) Discovery
- Data Classification
- Data Masking/Encryption

Data Security as a Service

SISA Training

Payment Data Security Implementation Programs

- CPISI
- CPISI Advanced
- CPISI-D (Developers)

Security Incident Detection and Response Programs

- CIDR

Cybersecurity Awareness

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