NEXTLABS

How to Safeguard Financial and Customer Data with Dynamic Data Anonymization & Segregation

Case Study of NextLabs Zero Trust Data Security Suite

fiserv.

Since its establishment in 1984, Fiserv has become a leading global fintech company with its headquarters in Wisconsin, U.S. Fiserv has been recognized by Aite Group as one of the "best in class" core banking providers, offering superior API-enabled integration, responsive design, and a unified user experience to clients in various sectors. Its innovative solutions in payment, processing, risk and compliance, customer and channel management have helped thousands of financial institutions, including banks, credit unions, and leasing companies, as well as millions of businesses in over 100 countries, to efficiently move money and enhance their financial management practices for ongoing success.

With the rise of virtual global workforces and increasingly strict cybersecurity requirements, Fiserv faces the challenge of securely collaborating and sharing confidential information, such as customer and financial data, while also retaining agility and cost control. To safeguard the confidentiality and integrity of its data assets, Fiserv implemented NextLabs's Zero-trust Data Security Suite, which provides dynamic data-level security controls and fine-grained data access governance in real time. This dynamic approach enables Fiserv to automate security and compliance management, segregate sensitive data in single global instance, maintaining its business agility amidst evolving requirements.

Within a 4-month timeline, Fiserv's Global Fintech, Analytics & Digital Transformation team closely collaborated with NextLabs team to successfully implement Nextlabs' Data Access Enforcer (DAE). The solution enables dynamic data-level security controls such as encryption, decryption, masking, and segregation to enhance Fiserv's cybersecurity for its digital transformation objective. With this zero-trust data-centric approach using DAE, Fiserv's sensitive customer and financial data is encrypted in non-human readable format at the database level, preventing the data assets and backups from being compromised or accessed by authorized users. This provides an additional protection shield across heterogenous applications and systems to keep data safe and secure at-rest and in use at all times.

"We were able to implement NextLabs Data Security Suite for SAP S4/HANA in our organization within a 4-month aggressive timeline." stated Roopa Prakash, Sr. Director of Fin Tech Digital Transformation at Fiserv. "NextLabs did an amazing job working together with our SAP S4/HANA Fintech team, their team members were responsive, knowledgeable, went beyond the call of duty to get things done, while achieving all of our project goals," said Rajan RayChaudhury, Sr. Director of Fin Tech Digital Transformation at Fiserv.

How to Safeguard Financial and Customer Data with Dynamic Data-Level Security Controls

fiserv.

Brookfield, Wisconsin

Industry
IT services and IT consulting

Products and Services
Solutions for Account Processing, Biller, card, ATM, Credit & Debit, Deposit, Lending, Output, Remittance, and Credit Union Platforms

Employees
41,000

Revenues
$22.5 billion (USD)

Solution
NextLabs Data Access Enforcer (DAE)

Before: Challenges and Opportunities
- Prevent unauthorized access and data breach to confidential information causing compliance failure and reputational damage.
- Need to efficiently protect critical customer data from a client base of financial institutions, banks, and mortgage providers, etc.
- Personally identifiable information (PII) and Payment Card Industry (PCI) compliance necessitated enhanced protection from the unauthorized access and usage.
- Fiserv's S/4 HANA system required additional security control to meet cyber security requirements in terms of data protection.
- These needs spark an opportunity to consider dynamic data masking and encryption as holistic powerful approach for SAP eco-system applications.

Why NextLabs
- Best in class Zero Trust Data Centric Security solution.
- Offers out-of-the-box support for numerous leading enterprise and cloud applications including SAP ERP, SAP BW, SAP HANA, Microsoft Power BI, and Azure Data Lake.
- Expertise in ERP, big data application, and experience implementing large scale data governance, risk, and compliance solutions.
- Provides data masking, data encryption, and dynamic authorization of business transactions to ensure regulatory compliance.
- Can be seamlessly integrated and implemented within a matter of weeks, enabling Fiserv to meet all project objectives successfully while maintaining optimal security coverage.

After: Value Driven Results
- Implemented NextLabs DAE encryption in S/4 HANA system to ensure and streamline compliance requirements set by Cyber Security Group within Fiserv.
- Protected customers' sensitive information at rest using encryption, securing data access by segregating and obfuscating, and enforcing least privilege access control to applications.
- Automated and simplified security management to safeguard confidential information.
- Centrally logged and tracked all data access activity for audit and compliance reporting
- Modernize IT and accelerate business process unification to achieve ERP transformation without compromising security coverage and ownership cost.

NEXTLABS®

Compliance
Improve security & streamline compliance to meet cybersecurity requirements

Preventive Security
Protect against data breach & reduce attack surface

Quick Time-to-Value
100% completion of scope within aggressive timeline

Automation
Quickly adapt to new business requirements, simplify change, & escalation management

NEXTLABS

fiserv.

Takeaways

The Fiserv Cyber Security Team and NextLabs productively collaborated to implement NextLabs dynamic data protection solution seamlessly, meeting Fiserv' ERP transformation objectives. With the NextLabs' solution in place, Fiserv can prevent data breaches and wrongful disclosure of customers' sensitive financial data, unifying Fiserv's global ERP application under a single global S/4 HANA instance. NextLabs' Data Access Enforcer introduces an additional layer of data protection to applications with real-time enforcement, eliminating many manual tasks and reaching compliance set by the Fiserv's team and evolving regulations.

NextLabs DAE for SAP

User Role	Activity	Flow Steps
Policy Administration/ NextLabs Admin	**Pre-requisite:** Policy Authoring for Sensitive fields and configure the field mapping at SAP	**Step 0**
NextLabs Admin	**Bulk Encrypt:** Bulk encrypt data for policy configured sensitive fields / Pre-process **Bulk Re-encrypt:** Key Rotation (ad-hoc)	1a, 1b
SAP User / End User (Authorized)	**Decrypt:** if authorized via Policy evaluation	2a, 2b, 2c
SAP User / End User (Un-authorized)	**No Action:** Display encrypted data for un-authorized via Policy evaluation	2a, 2b
SAP User / End User (All users)	**Encrypt:** Add, modify the sensitive field data	3a, 3b, 3c